

UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA:

INGENIERÍA DE SISTEMAS

Trabajo de titulación previo a la obtención del título de:

Ingeniero de Sistemas

TEMA:

**ANÁLISIS Y PROPUESTA DE MEJORAS A LA INFRAESTRUCTURA Y
SEGURIDAD DE LA RED LAN DE LA EMPRESA SICCEC PARA
PERFECCIONAR LA DISPONIBILIDAD DE SUS SERVICIOS**

AUTOR:

DECHER WILLIAMS VALENZUELA LOZA

TUTOR:

JOSÉ LUIS AGUAYO MORALES

Quito, febrero del 2020

CESIÓN DE DERECHOS DE AUTOR

Yo DECHER WILLIAMS VALENZUELA LOZA, con documento de identificación N° 1720445806, manifiesto mi voluntad y cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del trabajo de grado intitulado: "ANÁLISIS Y PROPUESTA DE MEJORAS A LA INFRAESTRUCTURA Y SEGURIDAD DE LA RED LAN DE LA EMPRESA SICCEC PARA PERFECCIONAR LA DISPONIBILIDAD DE SUS SERVICIOS", mismo que ha sido desarrollado para optar por el título de: INGENIERO DE SISTEMAS, en la Universidad Politécnica Salesiana, que dando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hago entrega del trabajo final en digital a la Biblioteca de la Universidad Politécnica Salesiana.



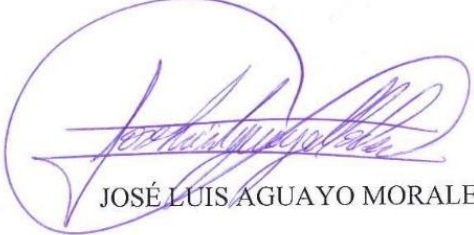
DECHER WILLIAMS VALENZUELA LOZA

1720445806

Quito, febrero del 2020

DECLARATORIA DE COAUTORIA DEL TUTOR

Yo declaro que bajo mi dirección y asesoría fue desarrollado el proyecto técnico, con el tema: "ANÁLISIS Y PROPUESTA DE MEJORAS A LA INFRAESTRUCTURA Y SEGURIDAD DE LA RED LAN DE LA EMPRESA SICCEC PARA PERFECCIONAR LA DISPONIBILIDAD DE SUS SERVICIOS" realizado por DECHER WILLIAMS VALENZUELA LOZA, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerado como trabajo final de titulación.



JOSÉ LUIS AGUAYO MORALES

Ci: 1709562597

Quito, febrero del 2020

DEDICATORIA

Dedico este trabajo principalmente a mis padres por todo el sacrificio y apoyo incondicional que he tenido durante todos estos años de estudio, a mi hermano por su apoyo anímico y el de seguir los pasos al elegir como profesión esta carrera.

A mi novia por todo su apoyo incondicional y por acompañarme en los momentos más importantes de mi vida y compartir logros como este. A mi tutor por el constante seguimiento y su ayuda a finalizar cada etapa de la tesis propuesta y de la cual se realizó un excelente trabajo.

Finalmente, a Dios por proveerme de sabiduría y paciencia para poder culminar este importante objetivo y no rendirme fácilmente.

No ha sido sencillo este camino, pero gracias a su amor y apoyo he logrado culminar esta meta de la mejor manera, muchas gracias.

ÍNDICE

CAPÍTULO 1	1
1. Introducción	1
1.1. Antecedentes	1
1.2. Descripción del problema	1
1.3. Justificación	2
1.4. Objetivo general.....	4
1.5. Objetivos específicos	4
1.6. Estado actual de la empresa	5
1.6.1. Infraestructura y procesamiento.	5
1.6.2. Seguridad.....	6
1.6.3. Telefonía IP.	7
1.6.4. Servicios críticos de la empresa.	8
1.7. Alcance	9
1.8. Marco metodológico	10
1.8.1. Metodología ágil.....	10
1.8.2. Metodología XP.	11
CAPÍTULO 2	13
2. Marco teórico	13
2.1. Virtualización de servidores	13
2.2. XenServer	14
2.3. Phishing	14

2.4.	Asterisk	14
2.5.	Issabel PBX.....	15
2.6.	IVR.....	15
2.7.	Firewall	16
CAPÍTULO 3		17
3.	Análisis y diseño de la solución.....	17
3.1.	Estado inicial de la red.....	17
3.1.1.	Topología de la red actual de la empresa.	18
3.2.	Análisis para la virtualización.....	20
3.2.1.	Comparación de las herramientas de virtualización.....	20
3.2.2.	Determinación de la herramienta de virtualización a utilizar.....	21
3.2.2.1.	Arquitectura de XenServer	22
3.3.	Diseño de la virtualización	22
3.3.1.	Implementación de Citrix XenServer.....	24
3.3.2.	Monitoreo con XenServer.	27
3.3.3.	Creación de máquina virtual para base de datos de SICCEC.....	28
3.3.3.1.	Creación de la máquina virtual, configuración de recursos y procesamiento..	29
3.3.3.2.	Requerimientos mínimos de Windows Server 2012	33
3.3.3.3.	Requerimientos mínimos de SQL Server 2017	33
3.3.3.4.	Migración de BDD	33
3.3.3.5.	Backup de la base de datos en producción	34
3.3.3.6.	Restauración del backup en el ambiente virtualizado	36

3.4.	Diseño de la solución de telefonía IP.....	38
3.4.1.	Análisis de central telefónica propuesta.....	38
3.4.2.	Diseño de la central telefónica ISSABEL PBX.....	39
3.4.2.1.	Backup de central telefónica en ELASTIX.....	40
3.4.2.2.	Implementación de la central telefónica ISSABEL PBX.....	43
3.4.2.3.	Restauración del backup de Elastix en ISSABEL PBX.....	44
3.5.	Implementación del generador de campañas de IVR	45
3.5.1.	Implementación de AudioElastixDialer.....	45
3.5.1.1.	Instalación de AudioElastixDialer.....	46
3.5.1.2.	Creación de la base de datos de AudioElastixDialer.....	49
3.5.1.3.	Modificación de los datos de conexión a la BDD.....	50
3.5.1.4.	Configuración de la troncal de salida.....	51
3.6.	Caracterización de los activos tecnológicos de la empresa	52
3.6.1.	Análisis de vulnerabilidades informáticas.....	53
3.6.2.	Vulnerabilidades en Windows server 2012.....	54
3.6.3.	Escaneo de vulnerabilidades en servidores propuestos.....	55
3.6.3.1.	Ejemplo de vulnerabilidad encontrada en servidores de prueba.....	55
3.7.	Análisis de los perfiles de usuario	58
3.7.1.	Implementación de antivirus empresarial.....	60
3.8.	Implementación de reglas en el firewall de acuerdo a las políticas de seguridad de la empresa	61
3.8.1.	Creación de la regla para el perfil de Gerencia.....	62

3.8.2.	Creación de la regla para el perfil de Sistemas.	63
3.8.3.	Creación de la regla para el perfil de Administrativos.....	63
3.8.4.	Creación de la regla para el perfil de Gestores.....	63
3.9.	Política de navegación Web.....	63
3.9.1.	Restricciones generales de sitios de navegación web.	64
CAPÍTULO 4		65
4.	Análisis de resultados	65
4.1.	Virtualización de la base de datos de SICCEC.....	65
4.1.1.	Pruebas del procedimiento almacenado de Cooperativa JEP.....	67
4.1.1.1.	Pruebas en ambiente de producción.	67
4.1.1.2.	Pruebas en ambiente propuesto.	68
4.1.2.	Pruebas del procedimiento almacenado de Novacredit.....	68
4.1.2.1.	Pruebas en ambiente de producción.	69
4.1.2.2.	Pruebas en ambiente propuesto.	70
4.1.3.	Tiempos de ejecución de procedimientos almacenados en la BDD.....	70
4.2.	Virtualización de la central telefónica de SICCEC.....	72
4.3.	Pruebas de reglas de firewall	74
4.3.1.	Perfil Gestores.	74
4.3.2.	Perfil Sistemas.....	77
4.3.3.	Perfil Administrativos.	80
4.4.	Pruebas de IVR de llamadas automáticas	83
4.4.1.	Generar campaña de llamada automática.....	85

4.5.	Análisis de la solución propuesta de manera técnica y económica	88
	CONCLUSIONES.....	91
	RECOMENDACIONES	93
	REFERENCIAS	94

ÍNDICE DE FIGURAS

Figura 1. Fases del ciclo de vida XP	12
Figura 2. Principales características	13
Figura 3. Arquitectura de un sistema de IVR	16
Figura 4 Distribución de equipos y servicios de la empresa SICCEC	18
Figura 5. Topología de la empresa.	18
Figura 6. Computadores de escritorio en Data Center de SICCEC.....	19
Figura 7. Servidor físico adquirido por SICCEC	19
Figura 8. Arquitectura Citrix XenServer	22
Figura 9. Diagrama de un Raid 0.....	23
Figura 10. Procedimiento de implementación de XenServer	24
Figura 11. Pantalla para descargar XenCenter	25
Figura 12. Citrix XenCenter	26
Figura 13. Configuración de IP de servidor en XenCenter	26
Figura 14. Información de los distintos parámetros del servidor añadido en XenCenter	27
Figura 15. Monitoreo del servidor con XenServer	28
Figura 16. Procedimiento para crear las diferentes máquinas virtuales	29
Figura 17. Nueva máquina virtual	29
Figura 18. Elección del sistema operativo.....	30
Figura 19. Medio de instalación	30
Figura 20. Asignación de Memoria RAM y vCPUs.....	31
Figura 21. Espacio en disco.....	31
Figura 22. Selección de puerto de red	32
Figura 23. Máquina virtual con Windows Server 2012 R2 creada	32

Figura 24. Proceso de Backup BDD.....	34
Figura 25. SQL Management Studio.....	34
Figura 26. Versión de SQL Server en producción	35
Figura 27. Respaldo de la BDD.....	35
Figura 28. Archivo .BAK (respaldo).....	36
Figura 29. Versión de SQL Server propuesto	36
Figura 30. Restauración del Backup respaldado	37
Figura 31. Selección del archivo .bak para la restauración	37
Figura 32. Backup mediante la interface de Elastix	40
Figura 33. Opciones seleccionadas para realizar el Backup.....	41
Figura 34. Acceso WinSCP.....	42
Figura 35. Descarga del Backup generado desde WinSCP.....	42
Figura 36. Pasos de instalación de Issabel PBX.....	43
Figura 37. Interface de administración de Issabel PBX desde navegador web.....	44
Figura 38. Backup en Issabel mediante WinSCP	44
Figura 39. Backup en interface de Issabel PBX	45
Figura 40. Pasos de instalación de AudioElastixDialer.....	46
Figura 41. Creación del directorio AudioElastixDialer.....	47
Figura 42. Descarga de AudioElastixDialer comprimido en .zip.....	47
Figura 43. Extracción de archivos .php	47
Figura 44. Crear permisos a directorios.....	48
Figura 45. Modificación de del método call-file-test	48
Figura 46. Creación de método para reproducir audio	49
Figura 47. Implementación de cambios en Asterisk (reload).....	49
Figura 48. Creación de BDD AudioElastixDialer	50

Figura 49. Modificación de del archivo Funciones.php	50
Figura 50. Configuración de trocal SIP de SICCEC	51
Figura 51. Interface Web de AudioElastixDialer mediante navegador web	52
Figura 52. Ejemplo de informe de escaneo de vulnerabilidades	56
Figura 53. Lista de parches de seguridad de acuerdo a la vulnerabilidad	57
Figura 54. Aplicación de parche de seguridad descargado	57
Figura 55. Organigrama de la empresa SICCEC.....	58
Figura 56. Perfiles de usuario propuesto	59
Figura 57. Sincronización de antivirus y firewall.....	61
Figura 58. Caso de uso de actualización de carteras	65
Figura 59. BDD de Pruebas	66
Figura 60. Tiempo de ejecución SP Producción.....	67
Figura 61. Tiempo de ejecución SP Propuesto.....	68
Figura 62. Ejecución SP Producción	69
Figura 63. Ejecución SP Propuesto	70
Figura 64. Índices creados en la BDD	71
Figura 65. Máquina virtual de Issabel PBX	72
Figura 66. Parámetros de procesamiento de Issabel PBX.....	73
Figura 67. Rendimiento de la central Issabel PBX.....	74
Figura 68. IP de prueba para validar reglas implementadas en el FW	74
Figura 69. Regla implementada para el perfil de Gestores.....	75
Figura 70. IP de origen	75
Figura 71. Prueba de acceso a juegos online	76
Figura 72. Prueba de acceso a Facebook.....	76
Figura 73. Prueba de acceso a sistema de SICCEC.....	77

Figura 74. Prueba de acceso a siccec.com.ec	77
Figura 75. Regla implementada para el perfil de Sistemas	78
Figura 76. Prueba de acceso a Facebook	79
Figura 77. Prueba de acceso a GitHub	79
Figura 78. Regla implementada para el perfil de Administrativos.....	80
Figura 79. IP de origen	80
Figura 80. Prueba de ingreso a Facebook.....	81
Figura 81. Prueba de ingreso a sistema de SICCEC.....	82
Figura 82. Prueba de ingreso a sitio de juegos	82
Figura 83. Prueba de acceso a proxy online	83
Figura 84. Interface AudioElastixDialer	84
Figura 85. Archivo CSV para generar llamadas.....	84
Figura 86. Generador de campañas automáticas	85
Figura 87. Sentencia de inserción de datos en la BDD	85
Figura 88. Campaña ingresada en la BDD	86
Figura 89. Llamadas realizadas de acuerdo a la campaña generada	86
Figura 90. CLI de Asterisk	87
Figura 91. Registro de llamadas mediante CLI.....	87

ÍNDICE DE TABLAS

Tabla 1. Características servidor SICCEC	20
Tabla 2. Comparación de herramientas de virtualización	21
Tabla 3. Requerimientos de servidores.....	23
Tabla 4. Asignación de puertos de red del servidor	24
Tabla 5. Vulnerabilidades en Windows Server 2012	54
Tabla 6. Tiempos de ejecución de procedimientos almacenados en la BDD.....	71
Tabla 7. Características de servidor para virtualizar	88
Tabla 8. Precio de servidores físicos de acuerdo al servicio	89
Tabla 9. Costo total de servidores físicos	89

RESUMEN

El proyecto desarrollado fue proponer a SICCEC algunas soluciones que ayuden a mejorar la administración y disponibilidad de sus principales servicios.

Comenzó con la implementación de entornos virtualizados que la compañía administra en la misma plataforma de hardware, para optimizar los recursos en términos de espacio, mantenimiento y costos.

La central telefónica se migró a Issabel PBX, ya que Elastix dejó de admitir a sus usuarios y se buscó un sistema telefónico actualizado y de código abierto.

Las propuestas implican la correcta administración de los servicios y la seguridad de la red, para mejorar sus servicios, costos y recursos. Para lo cual se configuraron nuevas reglas en la seguridad perimetral del firewall, con un enfoque restrictivo, donde todas las conexiones están bloqueadas excepto aquellas que están explícitamente permitidas.

El documento también contempló la implementación de un sistema para generar campañas automáticas de IVR, donde los clientes recuerdan sus deudas pagaderas en las diferentes carteras que administra SICCEC.

Como resultado, la virtualización del BDD mejoró considerablemente, ya que el proceso de carga ahora es 3.5 veces más rápido de lo que estaba en producción, la implementación del IVR automático ayuda a la gestión automática de los clientes, evitando la carga de trabajo para el gerente, que gastó aproximadamente 10 minutos para hacer 5 llamadas. Finalmente, la actualización de las reglas del firewall evitará el uso y el acceso incorrectos a los recursos de la red.

ABSTRACT

The project developed was to propose to SICCEC some solutions that help improve the administration and availability of its main services.

It began with the implementation of virtualized environments that the company manages on the same hardware platform, to optimize resources in terms of space, maintenance and costs.

The telephone exchange was migrated to Issabel PBX, since Elastix stopped supporting its users, and was sought an updated and open source telephone system.

The proposals involve the correct administration of both services and network security, to improve their services, costs and resources. For which new rules were configured in the perimeter security of the firewall, with a restrictive approach, where all connections are blocked except those that are explicitly allowed.

The document also contemplated the implementation of a system to generate automatic IVR campaigns, where customers are reminded of their debts payable in the different portfolios that SICCEC manages.

As a result, the virtualization of the BDD improved considerably, since the loading process is now 3.5 times faster than it was in production, the implementation of the automatic IVR helps the automatic management of customers, avoiding the workload to the manager, who spent approximately 10 minutes to make 5 calls. Finally, updating firewall rules will prevent improper use and access to network resources.

CAPÍTULO 1

1. Introducción

En las siguientes hojas se documentan las diferentes fases del proyecto realizado para la empresa SICCEC donde se desarrolló una propuesta para mejorar los servicios de red e infraestructura.

1.1. Antecedentes

SICCEC es una empresa con una vasta trayectoria en la recuperación de créditos en mora, tanto extrajudicial como judicialmente, es especializada en cartera de consumo, automotriz, microcrédito, tarjetas de crédito, entre otras. Adicionalmente realizan cobranza y renovación de Pólizas de Seguros y cuentan con más de 250 usuarios entre administrativos, agentes de venta y cobranza. Manejan una plataforma propia de cobranza multicanal que cuenta con una interfaz web amigable, la cual incluye aplicativos móviles para ventas, crédito y cobranzas en campo, que permiten solucionar con eficiencia el proceso completo de cobranza iniciando en la gestión preventiva, administrativa, extra judicial y cobranza judicial (SICCEC, 2009).

1.2. Descripción del problema

La empresa en los últimos años ha evidenciado en sus servicios: una disminución de la disponibilidad para realizar llamadas telefónicas; además las reglas de seguridad, de acuerdo a las políticas de la empresa, necesitan ser actualizadas, la base de datos y el servicio web presenta demoras en sus operaciones diarias, según lo manifestado por el encargado de infraestructura de la empresa en una entrevista para este proyecto.

También manifestó que en diversas ocasiones se presenta lentitud al gestionar clientes, es decir, la información del deudor se demora en ser presentada al usuario, también al guardarla, o se queda en espera. Cabe destacar que la base de datos que maneja la empresa tiene millones de registros, y su infraestructura actual posee pocos recursos para su almacenamiento.

También, se han presentado ataques de phishing en los correos institucionales de los empleados y, además, ha habido caídas en los servicios de red, que cuando no responden, deben reiniciarse los equipos sin descartar la probabilidad de que estos se encuentren infectados con algún tipo de malware.

1.3. Justificación

Este sistema informático actualmente no está apoyando eficientemente a los procesos de valor de la empresa para la gestión de los usuarios, debido a que los servicios y los equipos no se encuentran funcionando con el mejor ambiente para soportar la carga de información y procesamiento que se requiere.

Partiendo de esto la empresa cuenta con un firewall del cual no hay documentación actualizada y precisa sobre su configuración actual.

Las políticas de seguridad existen como un documento, pero no han sido implementadas en todo el sistema informático, ni en la red, ni con todos los usuarios de la misma.

Para el servicio de llamadas cuentan con Elastix, el cual es un sistema de telefonía IP basado en Asterisk. Este sistema es utilizado en la empresa, por todos los usuarios de Call Center ya sea para llamar al cliente y realizar venta o cobranza, o simplemente para comunicarse dentro de la empresa. El problema con el servidor de telefonía actual es que se encuentra implementado en una estación de trabajo, por lo que, no soporta la cantidad de usuarios y el servicio se cae.

Además, según (Smyth, 2017) otro problema con Elastix es que pronto dejará de dar soporte a la central para dar paso a nuevos sistemas de comunicación telefónica, por lo que la migración en algún momento tiene que realizarse y más aún cuando este es un servicio muy importante para la empresa.

Como respuesta a los problemas mencionados se requiere analizar la infraestructura y seguridad de la empresa SICCEC debido a que presentan inconvenientes para la gestión y desarrollo de la misma, impidiendo dar soporte a todas las actividades del negocio.

Implementar las políticas de seguridad es fundamental para evitar problemas de pérdidas de datos, caídas continuas de la red, problemas de lentitud en el procesamiento de la información, etc., ya que cada día aparecen nuevas técnicas de ataques que buscan apoderarse de información privada de la empresa, ya sea con fines de lucro o alguna otra mala intención (Moposita, 2012, pág. 6).

Además, sería conveniente optar por la virtualización de servidores como una de las facetas más importantes dentro de la tendencia de modernización e implantación de las nuevas tecnologías en el mundo empresarial (Doña, 2010, pág. 1). Para sacar provecho a los servidores que cuentan con buen procesamiento y almacenamiento, se deben implementar servicios importantes dentro de ellos, garantizando la disponibilidad hacia los usuarios finales, además de facilitar la administración de los mismos, ya que al virtualizar se pueden centralizar y monitorear los servicios.

En (Llumiquina, 2012, pág. 16) se menciona que, para las grandes, medianas y pequeñas empresas, los servicios de tráfico de voz serán una de las mayores aplicaciones para tomar ventaja completa de la red de datos. La telefonía IP contiene importantes beneficios como es la disminución de costos, estándares abiertos de interoperabilidad, redes integradas de voz y datos. Además, la propuesta para solucionar el problema de la central telefónica Elastix debe contemplar la migración al nuevo servidor de telefonía y asignar los suficientes recursos para su correcto funcionamiento mejorando la funcionalidad del sistema actual de Call Center.

Un sistema IVR es una solución tecnológica que nace de la integración de telefonía e informática para facilitar las operaciones de negocio. Cumple un rol significativo en la

provisión de un servicio eficiente al cliente y puede incrementar la satisfacción del mismo al tiempo de aminorar los costos y otorgar a la empresa múltiples ventajas competitivas (Jácome, 2013, pág. 37).

Por lo tanto, la implementación de nuevas funciones al IVR para realizar la cobranza de carteras vencidas ayudaría a la empresa a ser más productiva y más competitiva, ya que la gestión al cliente se realizaría automáticamente.

Se plantea esta propuesta ya que se espera obtener un beneficio a futuro al no perder disponibilidad de servicios hacia los clientes. Al tener un sistema informático más robusto, se espera un incremento de gestiones por parte de los empleados y esto conllevará a tener más ganancia en cuanto a cobranza.

1.4. Objetivo general

Analizar y proponer un proyecto de mejoras a los problemas de seguridad e infraestructura de red LAN de la empresa SICCEC, para mejorar la disponibilidad de los principales servicios que maneja.

1.5. Objetivos específicos

Recolectar información sobre el estado actual de la red en lo relacionado a seguridad e infraestructura.

Analizar los perfiles de usuario según el organigrama y las políticas de la empresa.

Determinar los servicios principales para la empresa correspondientes a su giro del negocio.

Desarrollar una solución centralizada y virtualizada en un nuevo servidor donde se migren los principales servicios que actualmente tienen problemas.

Implementar una solución robusta de comunicaciones telefónicas sobre IP para la empresa que interconecte a todos los usuarios de la red LAN entre ellos y hacia las redes públicas.

Diseñar las reglas del firewall que permitan la mejor operación de la red proporcionando a la vez el menor riesgo de seguridad.

Implementar un sistema que ayude a la recuperación de cartera usando un IVR que permita la gestión automática de mensajes de voz para recordar a los clientes sus deudas por pagar.

Evaluar la solución propuesta de migración e implementación de manera técnica y económica.

1.6. Estado actual de la empresa

La empresa SICCEC es una empresa líder en crédito y cobranza de carteras bancarias, la cual cuenta con más de 250 usuarios entre Quito, Guayaquil y Manta. Estos usuarios diariamente utilizan el sistema informático que maneja la empresa, entre otros servicios que son de importancia.

Recientemente se realizó la compra de un servidor con buenas características de memoria y procesamiento, con el fin de que estos servicios sean migrados. Pero hasta el momento el sistema informático no ha sido implementado en el servidor, por lo tanto, no se encuentra en producción.

En este punto se analizan los principales problemas detectados o enunciados por el gerente del departamento de sistemas, dentro del alcance definido por su importancia o su urgencia guardando el menor costo de la solución.

1.6.1. Infraestructura y procesamiento.

Actualmente la empresa trabaja a un buen nivel de operatividad, sin embargo, presenta inconvenientes ya que existe una demora en las gestiones que realiza el usuario diariamente, esto se debe a que los equipos no soportan la carga o los mismos no están preparados para un correcto funcionamiento de los servicios que operan diariamente, por lo que en ocasiones los

gestores telefónicos tienen demora en las gestiones, ocasionando que baje el nivel de operatividad de la empresa.

El área de sistemas cuenta con un servidor recientemente adquirido con excelentes características de hardware para soportar varios servicios que funcionan en diferentes equipos, por lo que se recomienda la virtualización de servidores con el fin de aprovechar los recursos que ofrece el equipo. Según (Quispe, 2014, pág. 42) en el 2010 la empresa FOCUS realizó una encuesta a diferentes empresas sobre los beneficios de la virtualización en donde encontraron al menos diecisiete, sin embargo, tomaron los cinco más importantes que se los menciona a continuación.

- Incremento en el aprovechamiento de los recursos.
- Reducción de espacio/enfriamiento/energía.
- Reducir TCO (Costo total de operación) de servidores.
- Incremento del retorno de inversión de servidores.
- Agilidad de TI mejorada.

La empresa cuenta con sistemas operativos virtualizados los cuales se encuentran funcionando sobre máquinas con buenas características, pero no para desempeñar un buen trabajo como servidores, además estos están implementados sobre plataformas de virtualización no licenciadas, lo que genera un problema ya que se necesita de parches sin autorización para que estos funcionen correctamente.

1.6.2. Seguridad.

En cuanto a seguridad la empresa cuenta con un firewall físico que por temas de confidencialidad no se menciona la marca ni versión del mismo. El firewall se encuentra ubicado en el centro de datos del área de sistemas, proporcionando muy buenas características

en seguridad ya que permite proteger la red, los usuarios y las aplicaciones directamente desde un centro de administración.

El firewall ofrece excelentes características de gestión en la seguridad de la red a continuación se consideraron las más importantes (Sophos, 2012).

- Administración sencilla.
- Implementación flexible.
- Reglas de firewall.
- Túneles cifrados.
- Restricciones web.
- Restricción de aplicaciones.
- Análisis de tráfico.

La empresa cuenta con todas estas características en el firewall adquirido, sin embargo, no se encuentran configuradas correctamente las diferentes reglas de acuerdo a las políticas de seguridad y los perfiles de los usuarios.

1.6.3. Telefonía IP.

El servicio de telefonía IP es uno de los servicios más importantes que maneja la empresa actualmente, ya que por este medio se realiza las gestiones a los clientes para el cobro de las deudas de las carteras correspondientes. Actualmente cuenta con Elastix como central telefónica, la cual está basada en Asterisk ofreciendo muy buenas características como servicio.

Una de las características de Elastix es que se pueden configurar extensiones que permitan la comunicación dentro de la empresa, ya que hace uso de la red para establecer las llamadas internas, sin embargo, para realizar llamadas externas es necesario realizar configuraciones adicionales, como la configuración de troncales y rutas salientes, para lo cual la empresa cuenta con un proveedor para este servicio. Como respaldo de llamadas externas la empresa cuenta

con equipos Gateway, los cuales ofrecen la salida de llamadas simultáneas por los diferentes chips insertados en los mismos.

La empresa cuenta con cuatro centrales telefónicas Elastix funcionando en diferentes equipos para las diferentes áreas del Call Center, pero uno de estos servicios se encuentra funcionando en un equipo de escritorio instalado en el centro de datos de la empresa, por lo que actualmente existen problemas en el equipo ya que esto ocasiona que los gestores telefónicos se queden sin servicio.

Adicionalmente la segunda central telefónica se considera la más importante, ya que cuenta con más de doscientas extensiones que hacen uso los gestores telefónicos diariamente. Esta central se la necesita migrar hacia el nuevo servidor, de manera que el equipo en el que está funcionando actualmente se lo utilice para la implementación de otro servicio. La central telefónica al ser crítica debe ser migrada a “Issabel PBX”, ya que según (Elastixtech, ISSABEL PBX, 2018) el objetivo de Issabel es el de dar continuidad a las plataformas instaladas y, de esta forma, ofrecer una alternativa a la comunidad de código abierto. De este modo nace la migración de usuarios de Elastix al momento de ser adquirida por 3CX y reemplazar todo el desarrollo de la comunidad con su software propietario.

La empresa se ve en la necesidad de migrar este servicio hacia el nuevo servidor adquirido, debido a los inconvenientes mencionados en los equipos. Al mencionar que una de estas cuatro centrales telefónicas es la más importante, la migración de Elastix a Issabel PBX se tiene que realizar a corto plazo.

1.6.4. Servicios críticos de la empresa.

Luego de realizar un análisis se pudo definir los principales servicios que son de vital importancia para tener un buen nivel de operatividad en la empresa, esto se lo hizo con el fin de proponer una solución a los inconvenientes que presentan los servicios actualmente.

Los principales problemas evidenciados fueron: demora en las gestiones que realizan los usuarios diariamente, como son los servicios: web, base de datos y comunicaciones telefónicas. Existen este tipo de problemas ya que estos se encuentran operando en equipos que no soportan el procesamiento que se necesita para tener un correcto funcionamiento de los servicios.

1.7. Alcance

Lo que se busca con este proyecto técnico es proponer una solución a los problemas mencionados anteriormente, con el fin de mejorar la productividad de empleados, garantizando la disponibilidad de servicios que se utilizan diariamente y actualizando e implementando herramientas que sobresalgan de otras empresas.

Iniciará con la recolección de información sobre el estado actual de la red en lo relacionado a seguridad e infraestructura, luego se analizarán los perfiles de usuario según el organigrama y las políticas de la empresa, y entonces, se determinarán los servicios principales para la empresa correspondientes a su giro del negocio.

En seguida, se desarrollará una solución centralizada y virtualizada en un nuevo servidor donde se migren los principales servicios que actualmente tienen problemas, la cual se implementará en la red de SICCEC, donde estará el sistema de comunicaciones telefónicas sobre IP para que interconecte a todos los usuarios de la red LAN, también se diseñarán e implantarán las reglas del firewall que permitan la mejor operación de la red proporcionando a la vez el menor riesgo de seguridad. Y entonces, se implementará el sistema de ayuda a la recuperación de cartera usando un IVR que permita la gestión automática de mensajes de voz para recordar a los clientes sus deudas por pagar.

Finalmente, se evaluará la solución propuesta de migración e implementación de manera técnica y económica.

La herramienta propuesta para la virtualización debe ser Open Source ya que es un requerimiento por parte del gerente de TI, con el fin de ahorrar recursos económicos. Por lo tanto, se analizarán herramientas libres para la virtualización que se recomienden en las buenas prácticas para garantizar la disponibilidad y seguridad de los servicios virtualizados.

Para solucionar el tema de phishing en los correos institucionales, se plantea el análisis de las políticas de seguridad y organigrama de la empresa, con el fin de implementar las correctas reglas de seguridad en el firewall, limitando el acceso a los recursos de acuerdo al perfil del usuario.

Ya que Elastix dejará de dar soporte a sus usuarios, generará un problema de obsolescencia (Smyth, 2017). La solución más factible es la migración del servicio al nuevo servidor adquirido, con la diferencia de que este será actualizado a Issabel PBX. Se propone la nueva central telefónica por la confiabilidad, modularidad y fácil uso. Estas características añadidas a la robustez para reportar hacen de él una de las mejores opciones para la migración (García, 2017, pág. 35).

Junto con la migración a Issabel PBX se propone la implementación del IVR hacia el nuevo sistema informático, utilizando un Gateway que tiene la empresa. Los IVR se basan en grabaciones de mensajes y respuestas estáticas y/o dinámicas de acuerdo a los requerimientos del usuario y alcances del propio sistema (Mena, 2009, pág. 27). Los usuarios generarán campañas de llamadas masivas automáticas para un grupo de clientes específicos.

1.8. Marco metodológico

En esta sección se detalla la metodología que se escogió para resolver el problema.

1.8.1. Metodología ágil.

La metodología que se utilizó para el desarrollo del proyecto fue de tipo ágil, la misma que se describe como un método alternativo para la gestión y desarrollo de proyectos. El método ágil

es un proceso que permite dar respuestas rápidas a cambios que sean solicitados por el cliente durante el transcurso del desarrollo del proyecto.

Se escogió una metodología ágil debido a que estas son flexibles, es decir, pueden ser modificadas para que se ajusten a la realidad de cada proyecto. El desarrollo de este proyecto se lo toma como un conjunto de proyectos pequeños, en donde cada uno es tratado de manera independiente, pero siguiendo el mismo proceso que caracteriza a este tipo de metodología (Andrés, Juan, & Jonathan, 2013, pág. 32).

1.8.2. Metodología XP.

Según (José, Patricio, & Carmen, 2012, pág. 3) XP (Programación Extrema) se basa en la retroalimentación continua entre el cliente y el equipo de desarrollo, comunicación entre todos los participantes del proyecto y simplicidad en las soluciones implementadas. Este tipo de metodología es adecuada para proyectos cuyos requisitos no están del todo claros, donde los requisitos son cambiantes y con corto tiempo de desarrollo.

Al ser un proyecto en el cual su propósito es solucionar los diferentes problemas de red encontrados en la empresa se escogió XP, ya que en comparación con las metodologías tradicionales esta permite subdividir el proyecto en proyectos más pequeños, de tal manera que se los pueda desarrollar individualmente.

XP ofrece cuatro fases sencillas para el desarrollo del proyecto como se muestra en la figura 1, llamado ciclo de vida del proyecto, el cual es muy dinámico al permitir estar en constante diálogo con el cliente, ya que utilizando esta metodología se pueden definir los requerimientos y alcances para la solución de cada uno de los problemas.

Ciclo de vida XP

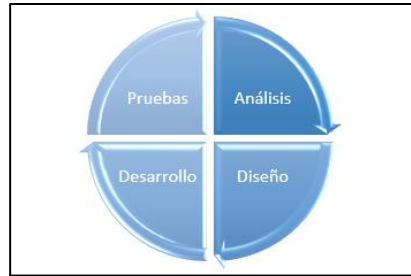


Figura 1. Fases del ciclo de vida XP
Elaborado por: Williams Valenzuela

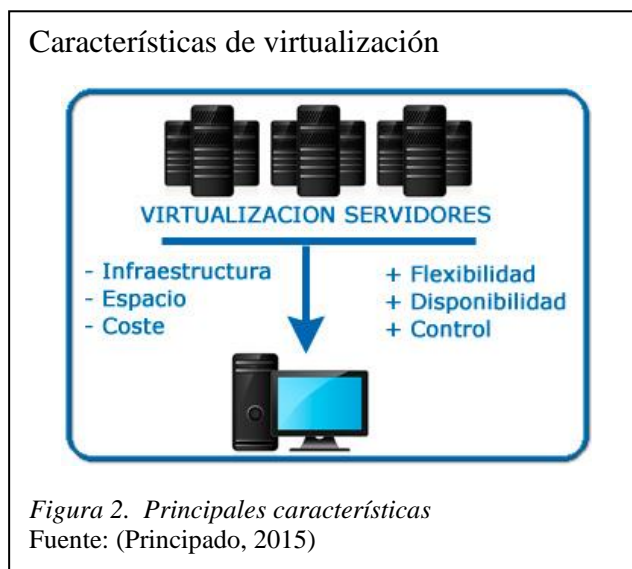
CAPÍTULO 2

2. Marco teórico

En esta sección se citan los principales conceptos que se utilizarán en la solución con el fin de ofrecer un mayor nivel de entendimiento en la lectura del documento.

2.1. Virtualización de servidores

Sin duda alguna hoy por hoy la virtualización de servidores se sitúa como una de las tendencias más importantes dentro de la modernización de tecnologías empresariales, ya que permite una mejor administración de recursos importantes a nivel de hardware y software como: almacenamiento, red y carga de trabajo (Doña, 2010, pág. 1). La virtualización posee grandes ventajas en cuanto a servidores, en la figura 2 se muestra las características más importantes.



Cuando se habla de infraestructura tiene que ver con el espacio, ya que al virtualizar optimizamos estos recursos evitando la infrautilización. La virtualización ofrece una mejor administración de servicios y una de las características más importantes la disponibilidad, ya que al ser un servicio virtualizado se pueden realizar copias de seguridad de las máquinas virtuales con el fin de recuperarlas en un caso de emergencia.

2.2. XenServer

Citrix de XenServer es una plataforma de virtualización de nube, de servidores y escritorios que presenta todas las capacidades necesarias para crear y gestionar la infraestructura virtual. De tal manera que las empresas pequeñas, grandes y medianas puedan tener esta potente solución a su alcance (Mero & Gallegos, 2015, pág. 13).

XenServer ofrece una versión Open Source gratuita con una administración centralizada, migración en vivo y herramientas de conversión para crear ambientes virtuales que maximicen el rendimiento de los sistemas operativos.

2.3. Phishing

El Phishing o más conocido como suplantación de identidad es un ataque informático que ha venido aumentando con los años, con el fin de engañar a los usuarios y robar información que sea valiosa para la empresa u organización, o simplemente sustraer información personal de credenciales de autenticación para acceder a los sistemas informáticos, ya sea con fines maliciosos o de lucro.

El ataque se puede dar por algunos medios como las redes sociales y el más importante por correo electrónico. Según los estudios realizados por el Registro de Direcciones de Internet para Latinoamérica y el Caribe (LACNIC) los ataques a Sudamérica han aumentado en un 20% más de lo que han crecido a nivel global (Paola Noreña, 2018). Por lo tanto, es importante aumentar la complejidad de las credenciales de usuario al momento de crearlas ya que el usuario por falta de conocimiento o simplemente por descuido visual puede ser vulnerable y proporcionar sus credenciales de autenticación.

2.4. Asterisk

Según (Landivar, 2009) Asterisk es un software de central telefónica de código abierto, ya que en tiempos pasados este tipo de centrales se las podía adquirir a un precio demasiado costoso.

Este software es el más utilizado actualmente, ya que ofrece una serie de características importantes para la modernización de empresas, y entre estas se tiene:

- Contestación automática de llamadas.
- Monitoreo y grabación de llamadas.
- Conferencias.
- Interactive Voice Response (IVR).

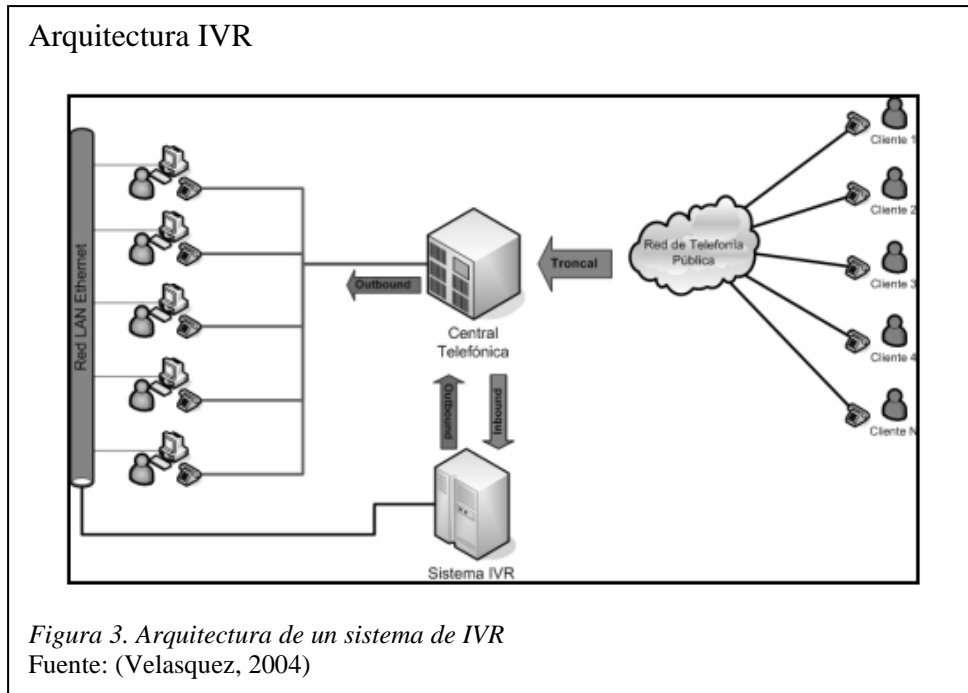
2.5. Issabel PBX

Issabel es un software Open Source de servidor de comunicaciones unificadas que junta las características PBX IP. Posee una interfaz web e incluye posibilidades de una central telefónica. Desde el momento en que Elastix fue adquirida por la empresa 3CX surgió Issabel PBX, el cual seguiría con la continuidad y soportes necesarios para seguir con el desarrollo de PBX con el apoyo de la comunidad la cual estaría compuesta por expertos, empresas, colaboradores y público en general (Yépez, 2018, pág. 34).

2.6. IVR

En los últimos años los sistemas telefónicos han ido evolucionando, de tal manera que se ha convertido uno de los servicios más importantes que manejan las empresas. Lo que buscan es mejorar la interacción con el usuario y la eficiencia en comunicar mensajes, así como ofrecer automatización a ciertos procesos.

Los IVR (Interactive Voice Response) son aplicaciones de voz interactivas que aceptan como entrada tanto tonos marcados por el usuario, como la voz del mismo, ofreciendo distintos tipos de respuesta según la programación del propio sistema; pudiendo de esta forma ofrecer servicios de información, encuestas y transacciones telefónicas (Obando, 2009, pág. 1).



La figura 3 muestra la arquitectura de un sistema IVR el cual se encuentra anclado a una central telefónica con las extensiones de los diferentes empleados de la empresa, una vez que el cliente marca al número empresarial es atendido por el IVR automáticamente y según las opciones del cliente este es dirigido al empleado con el que quiere contactarse.

2.7. Firewall

El firewall conocido también como cortafuegos es un dispositivo de hardware o una aplicación de software que sirve para proteger los dispositivos de red de los usuarios externos de la red, de acuerdo a las políticas de la empresa y perfiles de usuario. Según (Kelly, Javys, & Zúñiga, 2009, pág. 3) entre sus principales características está el bloqueo de paquetes que se originan desde determinados rangos de IP, puertos y direcciones de correo. También se utiliza para proteger de virus, malware, troyanos y spam.

CAPÍTULO 3

3. Análisis y diseño de la solución

El primer paso es el análisis y la planificación del proyecto. Siguiendo la metodología XP, indica que la comunicación es de vital importancia con el cliente, que en este caso fue el gerente de sistemas de la empresa, ya que al ser un usuario relacionado con el área fue mucho más fácil la interacción con el mismo, permitiendo entender los requerimientos de una manera más detallada para la solución de los inconvenientes.

Se realizó un análisis del estado actual de la empresa en cuanto a red e infraestructura, donde se evidenciaron los problemas mencionados por parte del cliente. En este punto se establecieron los requerimientos, las posibles soluciones y sus alcances.

3.1. Estado inicial de la red

SICCEC cuenta con un centro de datos ubicado en el departamento de sistemas, donde se han evidenciado inconvenientes con los principales servicios que facilitan su operación diaria, por tal motivo se analizó el estado actual de la red en cuanto a dichos servicios para luego mediante las soluciones propuestas mejorar la administración y disponibilidad de los mismos.

La empresa consta de múltiples servicios que se encuentran implementados en servidores y máquinas de escritorio. Cuenta con 3 Racks en su centro de datos donde se encuentran distribuidos los equipos mencionados en la figura 4.

Distribución de equipos y servicios

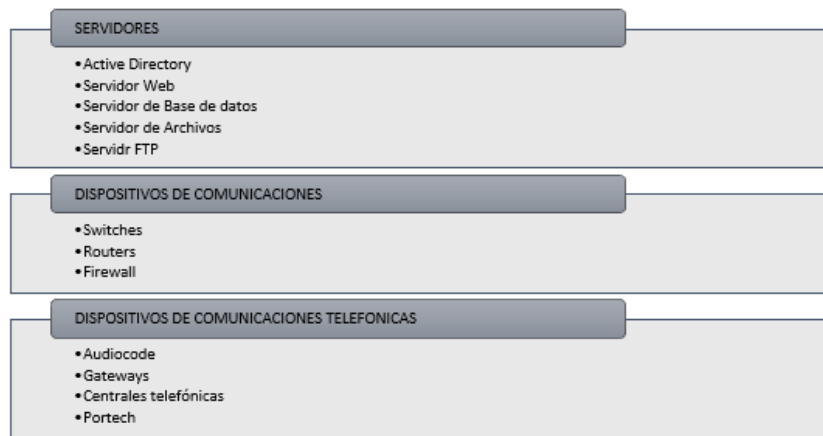


Figura 4 Distribución de equipos y servicios de la empresa SICCEC
Elaborado por: Williams Valenzuela

Al enfocarse en los servicios críticos de la empresa mencionados en el punto 1.6.4, se realizó la propuesta para solucionar los inconvenientes que presentan los mismos, con el fin de ofrecer una mejor administración y disponibilidad.

3.1.1. Topología de la red actual de la empresa.

Diagrama de red SICCEC.

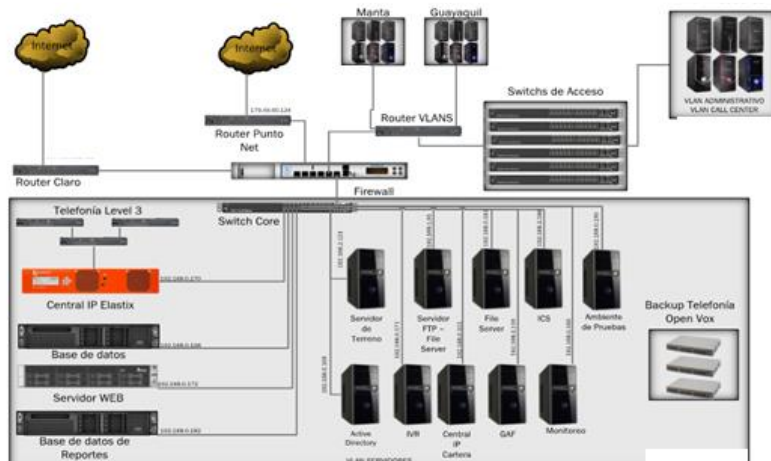
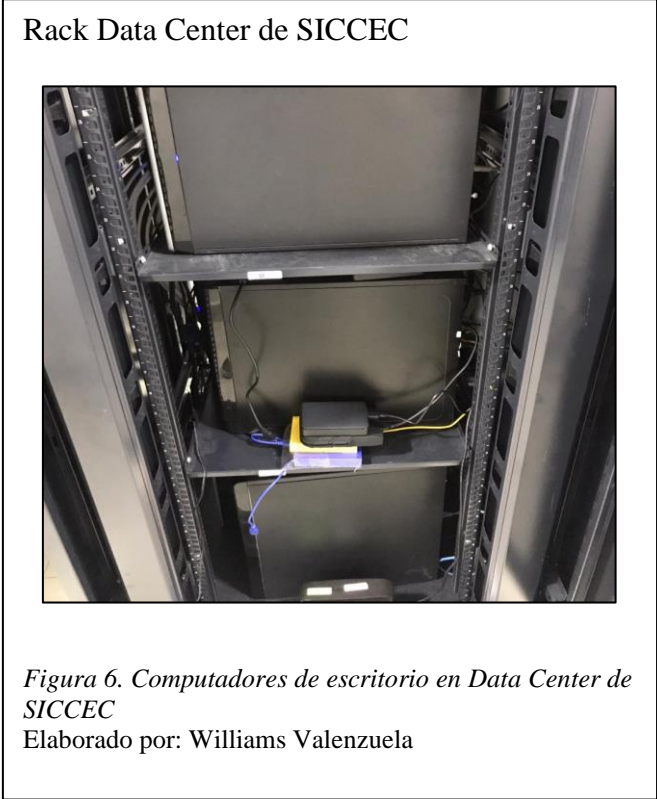


Figura 5. Topología de la empresa.
Elaborado por: Williams Valenzuela

La figura 5 muestra la topología de red actual de la empresa donde se muestra los distintos equipos que maneja, junto con su distribución en los diferentes Racks. En la figura 6 se visualiza

una parte de los servidores que actualmente maneja la empresa, donde se evidencia que los servicios se encuentran implementados en computadores de escritorio y los cuales se migraron a entornos virtualizados.



SICCEC actualmente adquirió un servidor donde se propone implementar la plataforma de virtualización para cumplir con uno de los objetivos propuestos y así mejorar la administración de los servicios, Las características y recursos del servidor se mencionan la tabla 1.



3.2. Análisis para la virtualización

Una de las propuestas fue desarrollar una solución centralizada y virtualizada en un nuevo servidor donde se migren los principales servicios que actualmente se requieren mejorar, ya que al virtualizar se sacará el máximo provecho a los recursos que posee el nuevo servidor adquirido por parte de la empresa. En la tabla 1 se muestran las principales características de hardware que posee el servidor adquirido.

Tabla 1. Características servidor SICCEC

Marca	Servidor HPE ProLiant DL360 Gen10 Intel Xeon-S 4114
Procesador	HPE Intel Xeon-S 4114 10-Core (2,20GHz 13,75MB L3 Cache)
Disco duro	4 Discos duros SAS 10K SFF SC DS HDD 1,2 TB
Memoria RAM	4 MEMORIAS RAM 16GB 1Rx4 PC4-2666
Tarjeta de red	Embedded 1Gb 4-port Ethernet Adapter

Elaborado por: Williams Valenzuela

La solución centralizada debe permitir la administración de las máquinas virtuales, con el fin de asignar los recursos correspondientes a cada servicio, de tal manera que, si existe algún inconveniente con esta, se pueda restaurar desde el sistema de administración sin necesidad de dirigirse al centro de datos. Como requerimiento por parte del gerente, la herramienta debe ser Open Source con el fin de disminuir costos.

3.2.1. Comparación de las herramientas de virtualización.

Para determinar la mejor solución del primer objetivo, se desarrolló una tabla comparativa entre las herramientas de virtualización utilizadas actualmente en la empresa frente a la herramienta que se propone, tomando en cuenta las principales características para obtener una correcta administración de las máquinas virtuales.

Tabla 2. Comparación de herramientas de virtualización

Características	Herramientas actuales			Propuesta
	Hyper-V	VMWare	Virtual Box	XenServer
Facilidad de instalación	Medio	Alto	Alto	Bajo
Conocimiento requerido para administración	Medio	Medio	Alto	Medio
Migración en vivo	SI	SI	NO	SI
Capacidad de para virtualización	SI	SI	NO	SI
Existencia de máquinas virtuales disponibles en internet	SI	SI	SI	SI
Monitoreo de rendimiento de máquinas virtuales	SI	NO	NO	SI
Open Source	NO	NO	SI	SI

Elaborado por: Williams Valenzuela

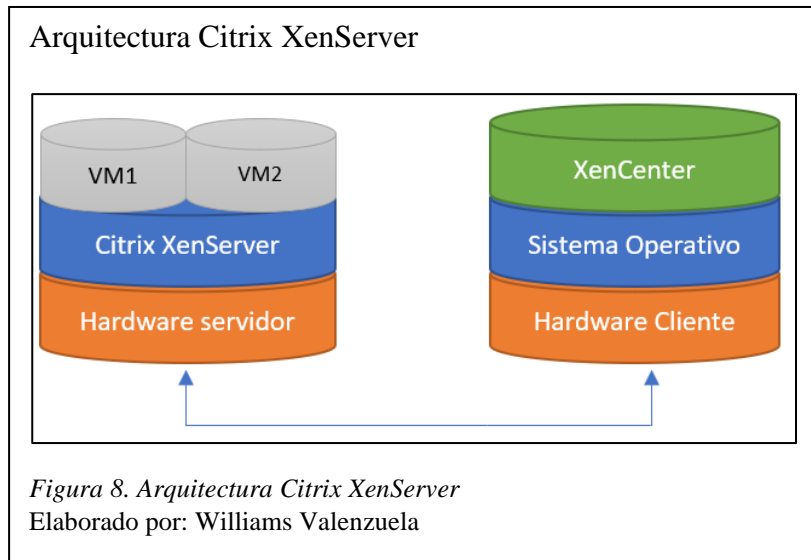
De la tabla 2, se concluye que la herramienta propuesta para la virtualización XenServer Free Edition de Citrix es la adecuada, ya que es una de las grandes compañías en virtualización la cual ofrece dos versiones. Una de pago y otra libre, en la cual la versión libre ofrece las suficientes particularidades que se necesita para la virtualización de los servidores antes mencionados. Además, existen conocimientos de virtualización en XenServer ya que anteriormente se ha desarrollado proyectos similares académicos en la Universidad Politécnica Salesiana.

3.2.2. Determinación de la herramienta de virtualización a utilizar.

La herramienta seleccionada Citrix XenServer además de ser una herramienta potente consta de un sistema operativo liviano basado en Linux donde la instalación es un poco complicada, sin embargo, esta posee de un software de administración y monitoreo llamado Citrix XenCenter. Este software de administración no necesita estar instalado en el servidor virtualizado, si no que puede estar instalado en cualquier computador remoto (Lara, 2011, pág. 32).

3.2.2.1. *Arquitectura de XenServer*

En cuanto a la arquitectura de XenServer es similar a otras herramientas de virtualización como se muestra en la figura 8.

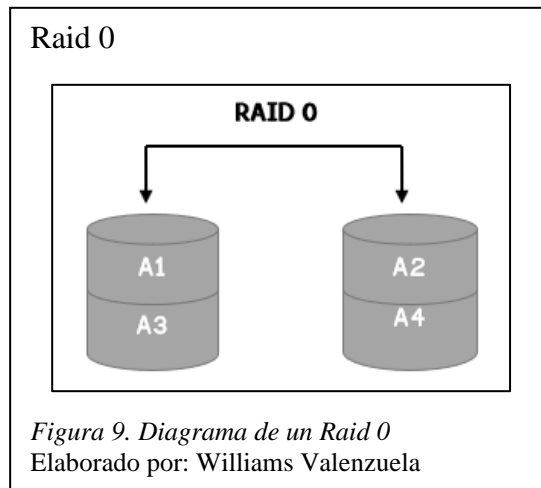


3.3. **Diseño de la virtualización**

Luego de seleccionar la herramienta de virtualización se procedió con la implementación, para lo cual se detallan los principales pasos que se utilizaron para el desarrollo de la solución.

Para la implementación de la virtualización fue necesaria realizar una configuración previa al servidor de la empresa SICCEC con el fin de preparar el mejor ambiente posible para la instalación de la herramienta seleccionada.

Se configuró un RAID 0 el cual permite la unificación de volúmenes de dos o más discos duros donde el sistema operativo solo reconocerá un disco duro con la capacidad unificada como se puede observar en la figura 9.



Al tener cuatro discos duros SAS independientes de 1 TB como se detalla en las características del servidor en la Tabla 1, se realizó la configuración mencionada obteniendo un espacio unificado de 4 TB para la instalación de XenServer y de las máquinas virtuales necesarias.

Para poder realizar el dimensionamiento de los servidores se realizó un análisis donde se establecieron los requerimientos que estos deben tener para mejorar su rendimiento, para lo cual se creó una tabla con las principales características de hardware de los servicios que se deben migrar.

Tabla 3. Requerimientos de servidores

BASE DE DATOS	
Nombre:	SRVSICUIOS02
SO	Windows Server 2012 R2 Standard
Disco:	1TB
RAM:	32 GB
CPU:	8 núcleos
SERVIDOR WEB	
Nombre:	SRVSICUIOS03
SO	Windows Server 2012 R2 Standard
Disco:	1TB
RAM:	16 GB
CPU:	4 núcleos
ISSABEL PBX	
Nombre:	SRVSICUIOS02
Disco:	1TB
RAM:	8GB
CPU:	4 núcleos

Elaborado por: Williams Valenzuela

Adicionalmente como se muestra en la tabla 1, el servidor posee una tarjeta embebida de red con cuatro puertos Ethernet, por lo que a cada máquina virtual se le asignó un determinado puerto. La Asignación del puerto a las diferentes máquinas virtuales se observa en la tabla 4.

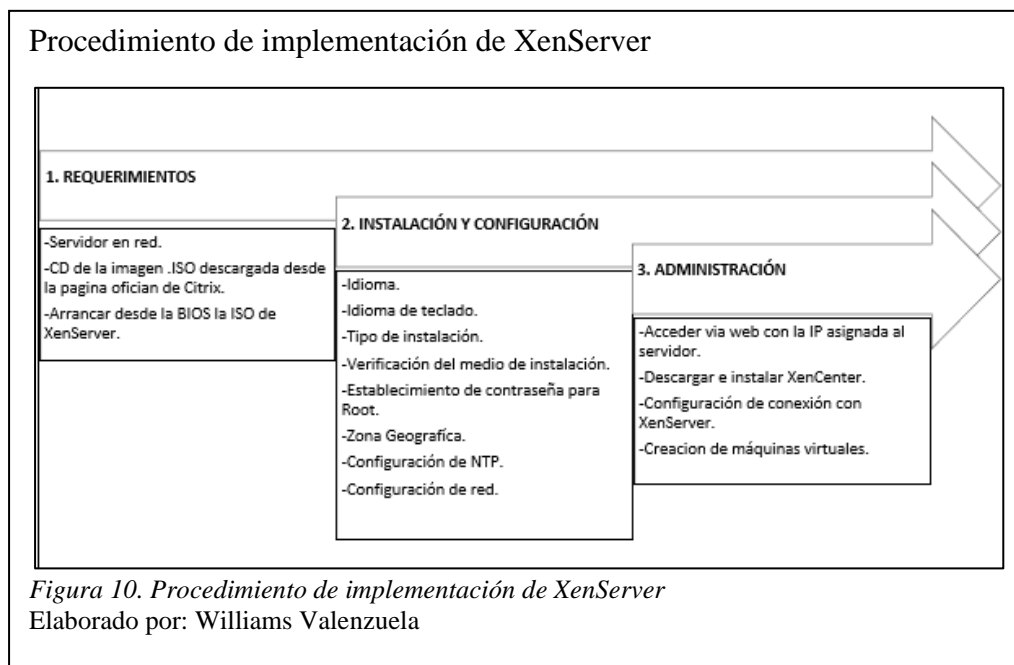
Tabla 4. Asignación de puertos de red del servidor

Network	Máquina virtual
PORT 0	Issabel PBX
PORT 1	Windows Server 2012 (Base de datos)
PORT 2	Windows Server 2012 (Servidor Web)
PORT 3	Libre

Elaborado por: Williams Valenzuela

3.3.1. Implementación de Citrix XenServer.

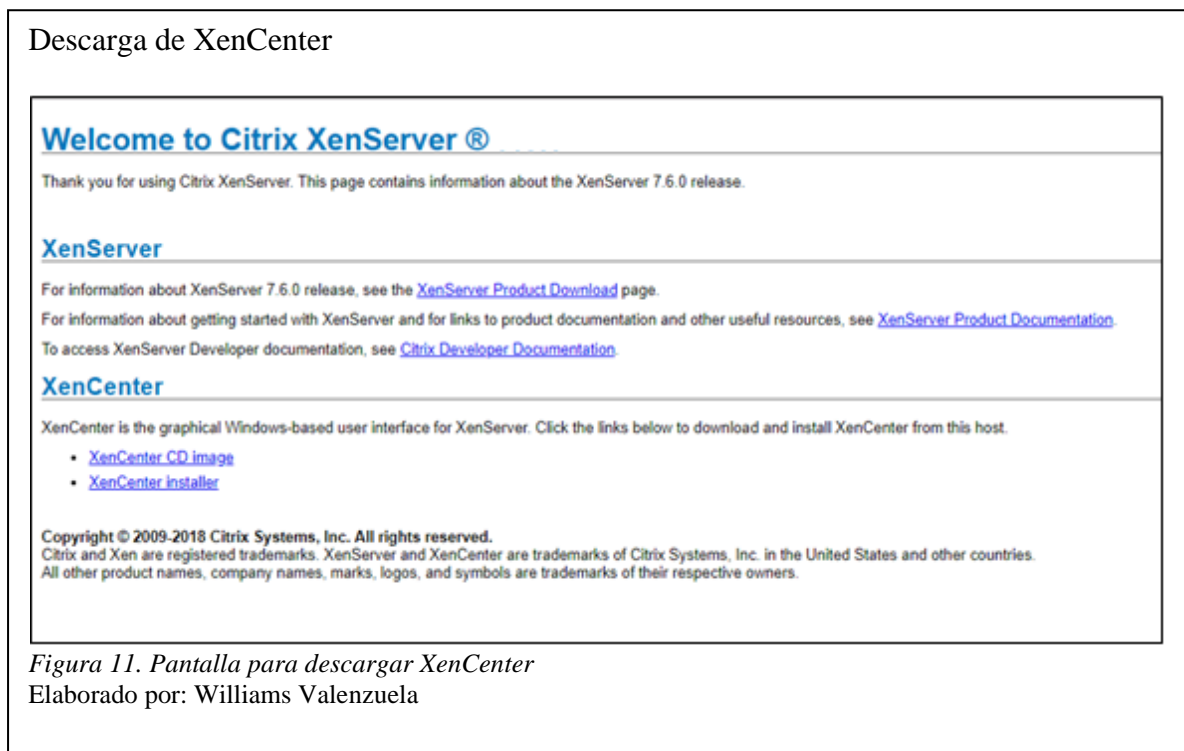
En la figura 10 se muestra el proceso de implementación de la herramienta de virtualización, la cual consta de tres actividades donde cada una tiene los respectivos pasos que se siguió para una correcta implementación de la herramienta.



Se mencionan las principales configuraciones de la actividad 3, ya que la solución se basa en una correcta administración de las máquinas virtuales.

Luego de realizar los pasos para la instalación de XenServer y configurar correctamente la red en el servidor, se accedió al mismo mediante el navegador web de cualquier estación de trabajo con la dirección IP, mostrando la pantalla que se visualiza en la figura 11.

La pantalla muestra información sobre la versión de la herramienta instalada, junto con documentación de la misma, permitiendo realizar la descarga directa de la herramienta de administración XenCenter.



Una vez descargada y realizada la instalación de XenCenter, se muestra la pantalla de administración, como se visualiza en la figura 12.

Citrix XenCenter

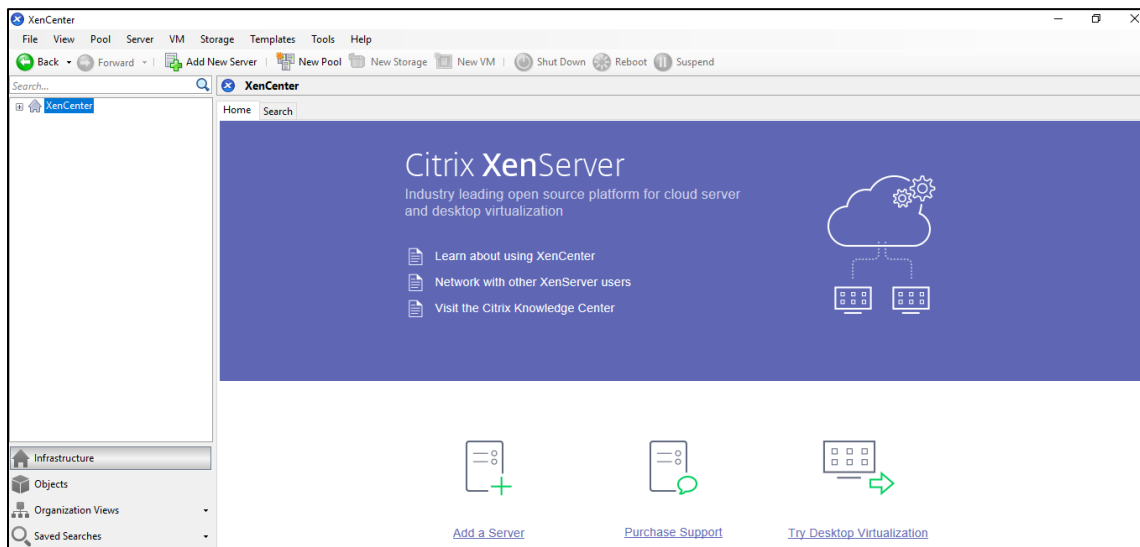


Figura 12. Citrix XenCenter
Elaborado por: Williams Valenzuela

Se estableció la conexión entre el software y el servidor de SICCEC colocando la IP del servidor junto con las credenciales asignadas al momento de la instalación.

Configuración de nuevo servidor en XenCenter

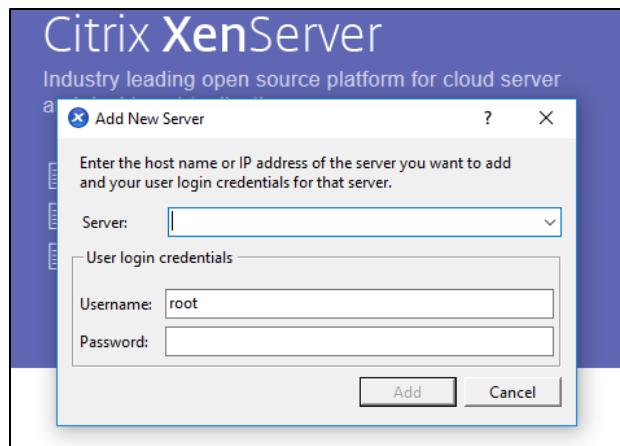


Figura 13. Configuración de IP de servidor en XenCenter
Elaborado por: Williams Valenzuela

Una vez que se registra en el servidor el usuario, se muestra información referente al mismo en la figura 14:

- Nombre del servidor.
- Memoria RAM.
- CPU.
- Redes.
- Consola del servidor.

Información del servidor añadido en XenCenter

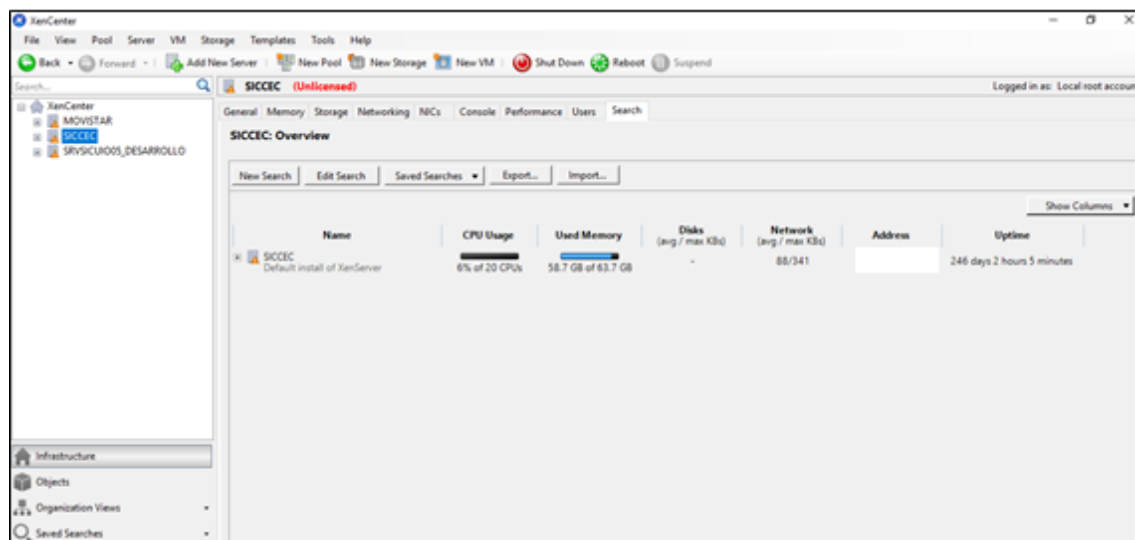
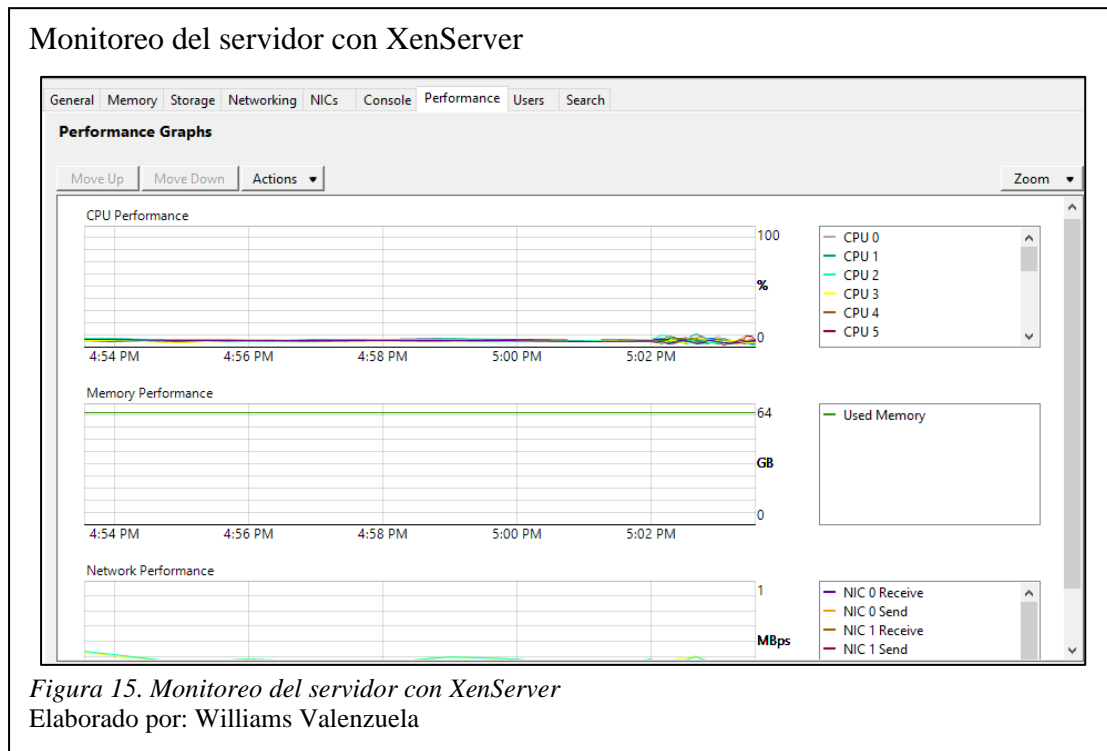


Figura 14. Información de los distintos parámetros del servidor añadido en XenCenter
Elaborado por: Williams Valenzuela

3.3.2. Monitoreo con XenServer.

Se implementó XenServer como herramienta de virtualización ya que uno de los requerimientos por parte de la empresa fue que los servidores propuestos se puedan monitorear, permitiendo tener un control de los servicios evitando la caída de los mismos.

La figura 15 muestra un apartado que la herramienta posee para monitorear los distintos parámetros del estado del servidor y de las máquinas virtuales una vez que se encuentren operativas, permitiendo tener una correcta administración con el fin de evitar fallos.

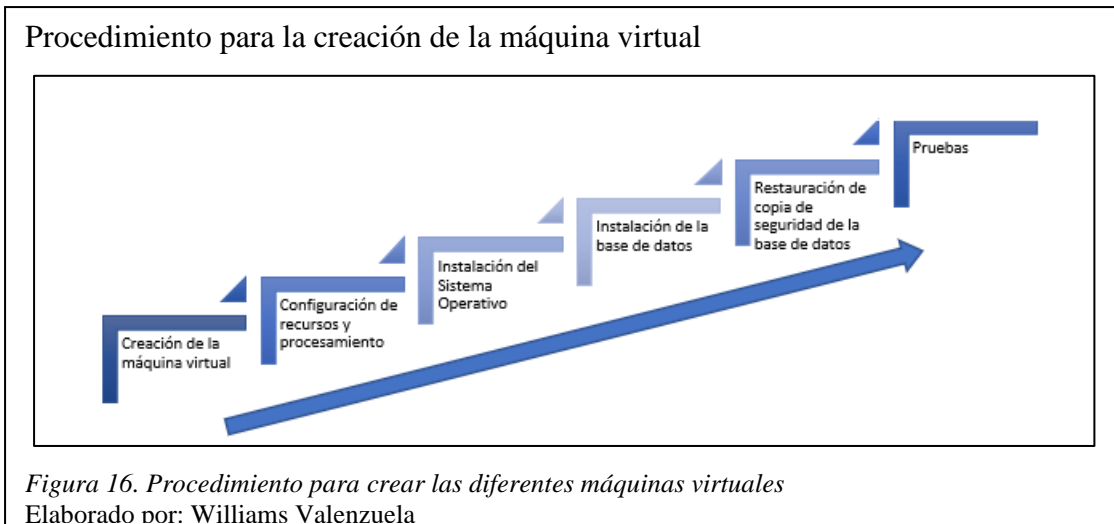


Adicionalmente se añadieron los gráficos, que ofrece la herramienta, como son: throughput, latencia, average, etc. De manera que permite obtener más datos sobre el rendimiento del servidor y de las máquinas virtuales implementadas.

3.3.3. Creación de máquina virtual para base de datos de SICCEC.

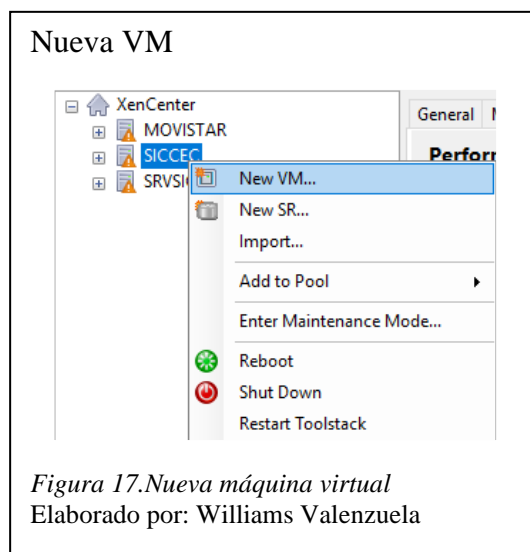
Luego de implementar XenServer en su totalidad se procedió con la creación de la máquina virtual donde se migró la base de datos que actualmente se encuentra en producción en SICCEC, para lo cual se establecieron los requerimientos de procesamiento y almacenamiento que debe tener este nuevo servidor como se muestra en la tabla 3.

Para la creación de la máquina virtual y migración de la base de datos de SICCEC se siguieron los pasos más importantes mencionados en la figura 16.

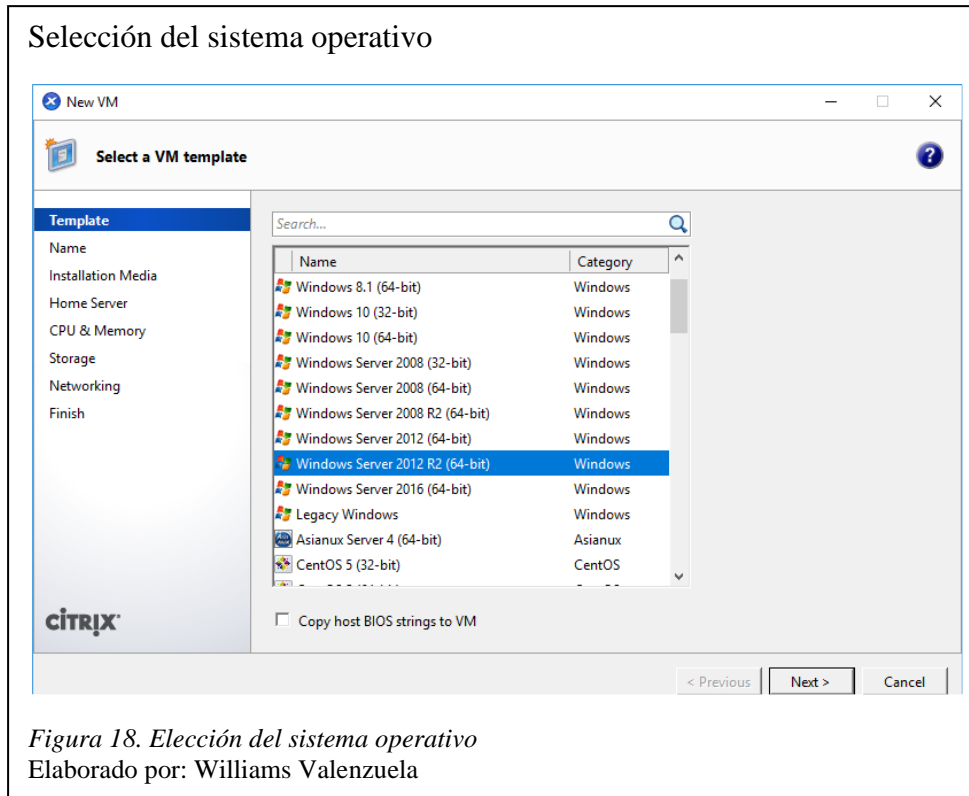


3.3.3.1. Creación de la máquina virtual, configuración de recursos y procesamiento

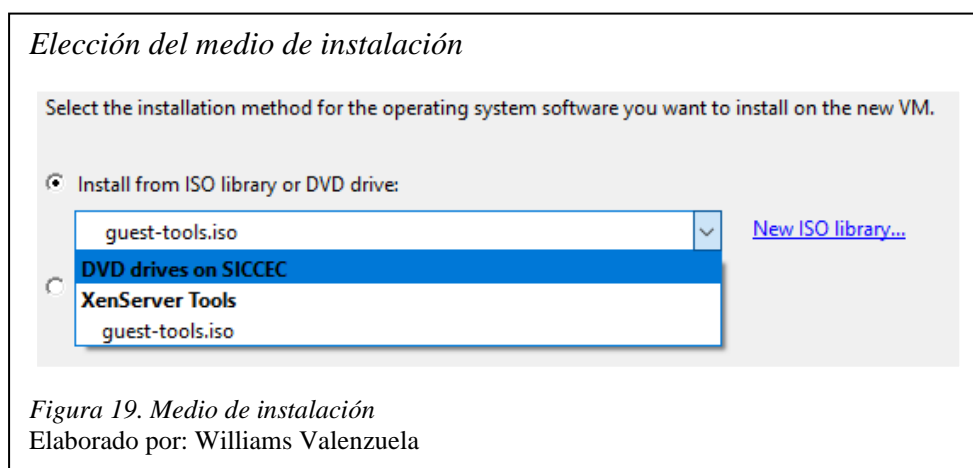
Se procedió a crear la máquina virtual en XenCenter, para lo cual se eligió la máquina principal llamada SICCEC y se seleccionó New VM.



Se abre el asistente para la configuración de la máquina virtual, se elige la plantilla pre configurada para el sistema operativo. En este caso Windows Server 2012 (64 bits).



Un paso importante para la instalación del sistema operativo es el medio de instalación, donde se configura el arranque de la imagen .ISO de Windows Server 2012, por lo que previamente se cargó la imagen en un CD para luego insertarlo en el servidor y poder arrancar el sistema operativo.



Luego se procedió con la configuración del CPU y la memoria, donde se asigna los recursos de procesamiento de la máquina virtual como se muestra en la figura 20.

Asignación de recursos de procesamiento

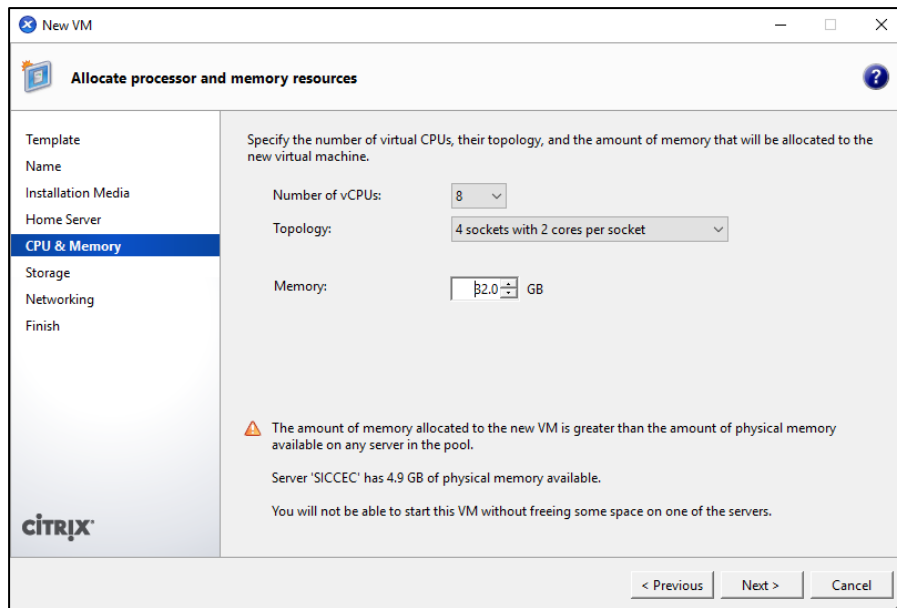


Figura 20. Asignación de Memoria RAM y vCPUs
Elaborado por: Williams Valenzuela

Una vez asignada la memoria y los núcleos se configuró el espacio en el disco que tiene la máquina virtual según los requerimientos solicitados.

Espacio en disco

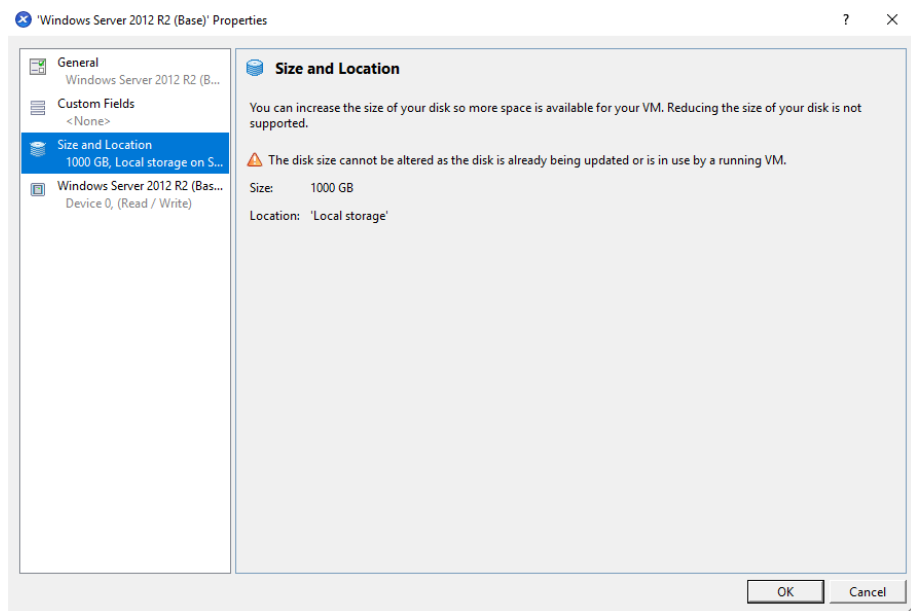
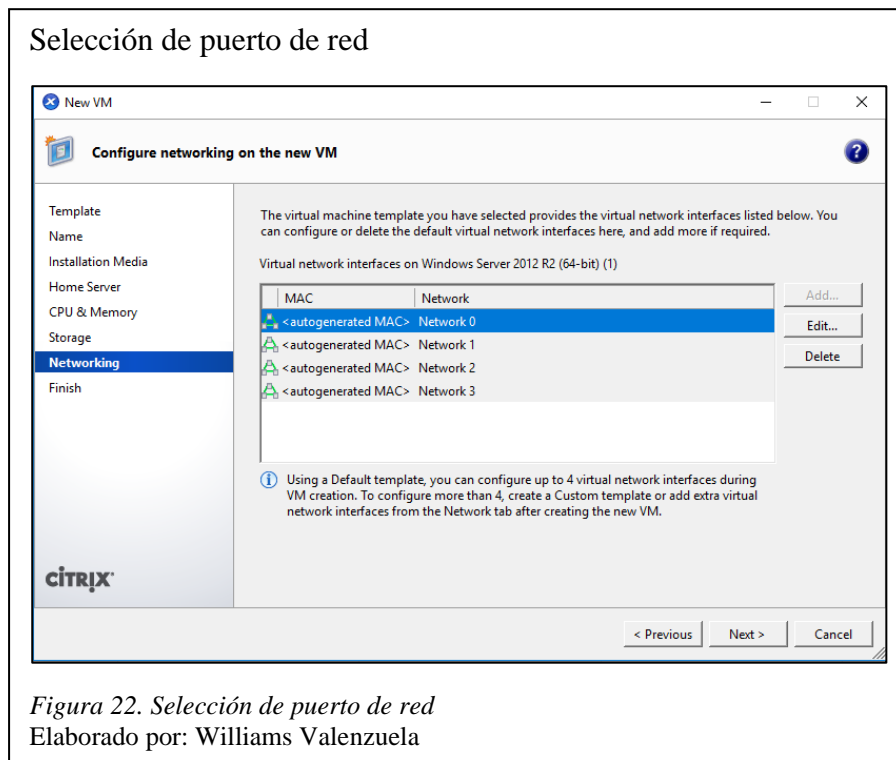


Figura 21. Espacio en disco
Elaborado por: Williams Valenzuela

El servidor donde se implementó XenServer posee cuatro puertos Ethernet, para lo cual cada servidor utilizará uno distinto como se mostró en la tabla 4. Al momento de crear la máquina virtual la herramienta ofrece la configuración de los puertos de red que se asigna a cada una cómo se puede observar en la figura 22.



Configurados los distintos parámetros, se creó la máquina virtual automáticamente. XenCenter en la figura 23 muestra un apartado de consola donde nos permite manipular la máquina creada.



Es importante mencionar que el mismo proceso se llevó a cabo para la instalación de Windows Server 2012 para el ambiente web con la única diferencia que los recursos de procesamiento difieren respecto al ambiente virtual con SQL Server 2017 como se visualiza en la tabla 3.

3.3.3.2. *Requerimientos mínimos de Windows Server 2012*

Antes de instalar Windows Server 2012 es necesario respetar los principales requerimientos mínimos del sistema operativo (BONNET, 2014, pág. 40).

- **Procesador:** 1.4 GHz como mínimo y arquitectura de 64 bits.
- **Memoria RAM:** 512 MB como mínimo, pero se recomienda 1024 MB.
- **Espacio en Disco:** Se requiere al menos 15 GB de almacenamiento.

Por lo tanto, al dar este espacio de memoria y espacio en disco se garantiza un rendimiento adecuado, sin embargo, al ser un servidor con SQL Server 2017 se estableció un mayor recurso de procesamiento.

3.3.3.3. *Requerimientos mínimos de SQL Server 2017*

Una vez instalado el sistema operativo se procedió con la instalación de SQL Server 2017 para lo cual es necesario mencionar los principales requerimientos mínimos del software (William, Randolph, Sven, & Mindy, 2018, pág. 33).

- **Procesador:** 2 GHz como mínimo y arquitectura de 64 bits
- **Memoria RAM:** 3.2 GB como mínimo, pero se recomienda 4 GB.
- **Espacio en Disco:** Se requiere al menos 6 GB de almacenamiento.

3.3.3.4. *Migración de BDD*

Concluida la instalación de SQL Server 2017 se procedió a migrar la base de datos de SICCEC, para lo cual se realizó una copia de seguridad de la BDD como se muestra en la figura 24.

Proceso de Backup BDD

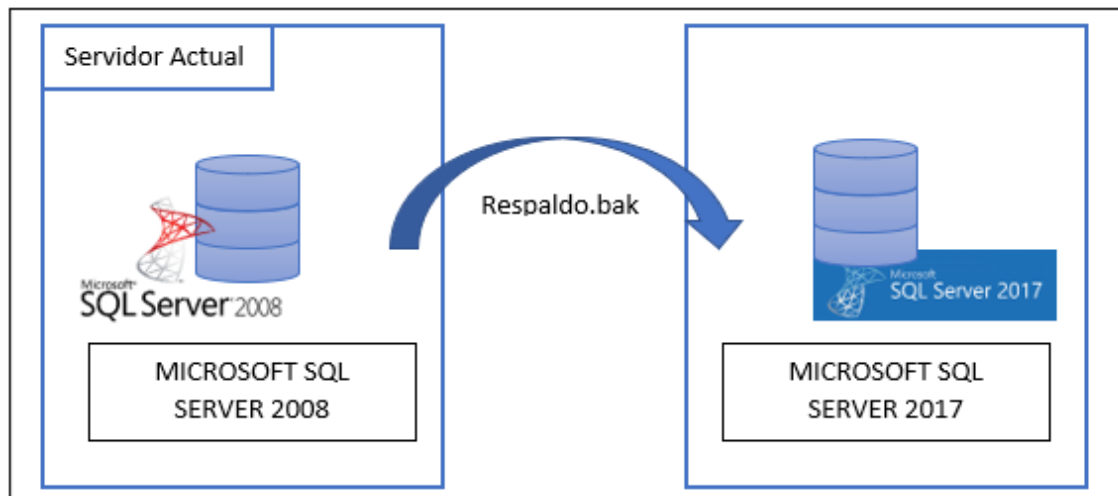


Figura 24. Proceso de Backup BDD
Elaborado por: Williams Valenzuela

3.3.3.5. Backup de la base de datos en producción

Para realizar el Backup de la base de datos de producción se utilizó la herramienta SQL Management Studio la cual es la interfaz de usuario cliente para administrar la base de datos instalada. La figura 25 muestra la herramienta mencionada junto con la base de datos que se encuentra actualmente en producción.

SQL Management Studio

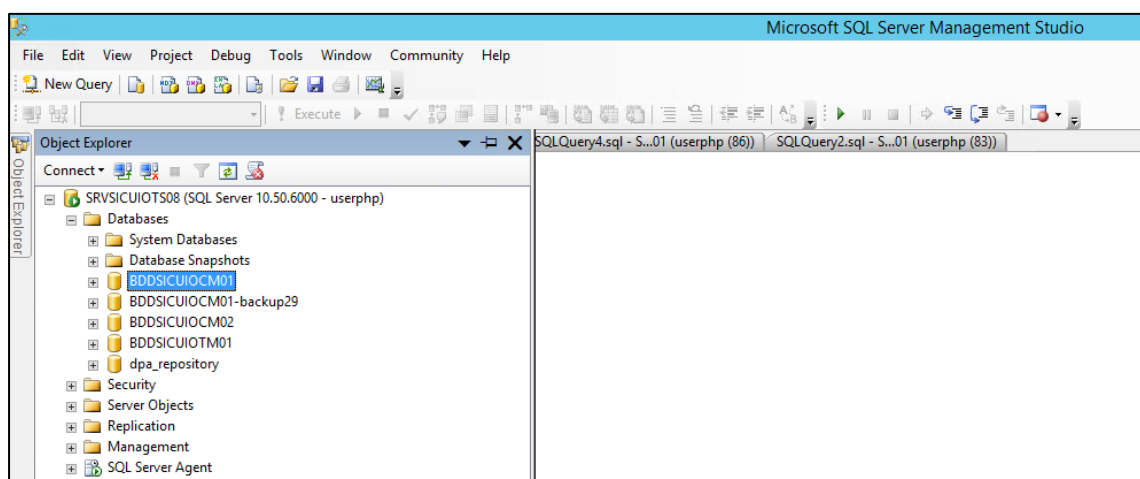
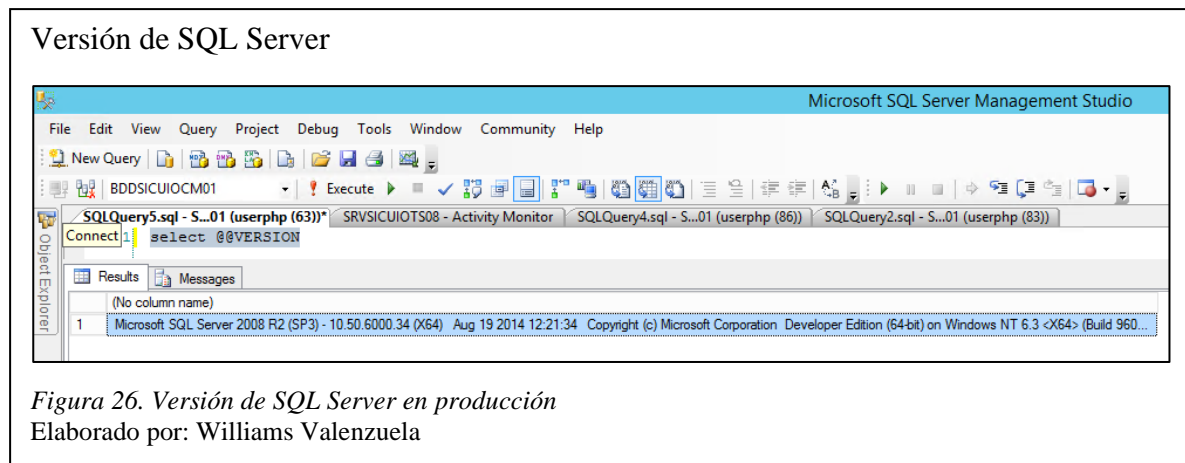
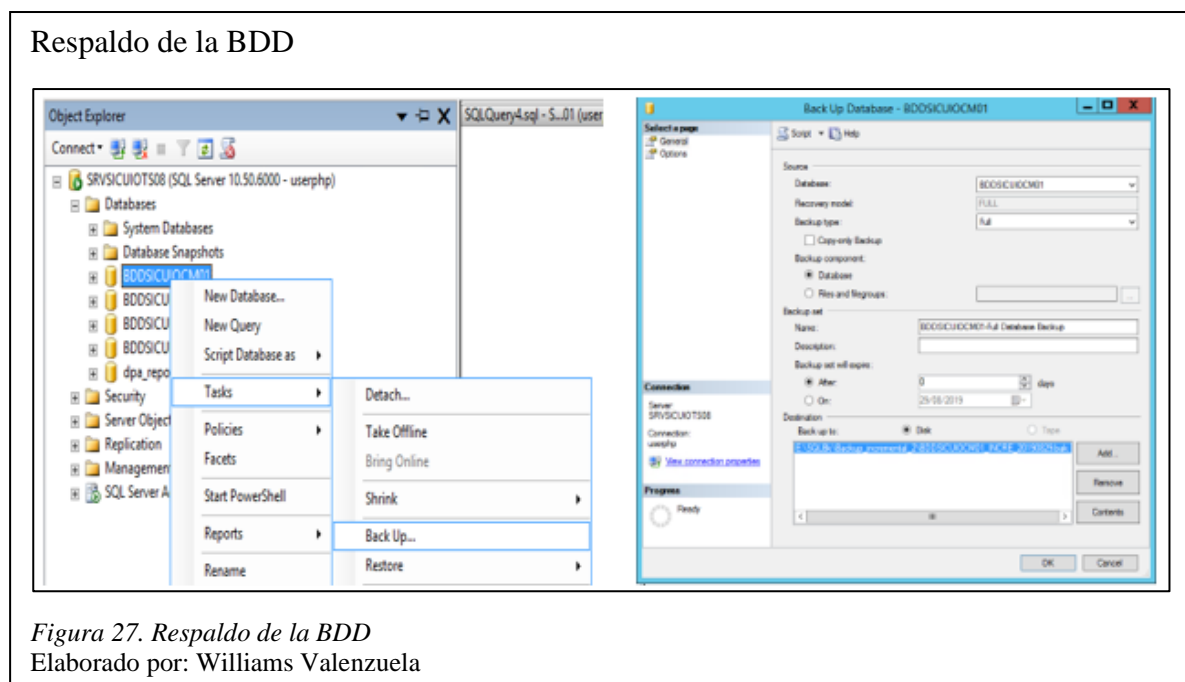


Figura 25. SQL Management Studio
Elaborado por: Williams Valenzuela

La figura 26 muestra la versión del SQL Server instalado en el ambiente de producción.



El respaldo de la base de datos se realizó mediante la interface, para lo cual la figura 27 detalla las opciones que se seleccionaron para generar el mismo.



Al terminar el proceso de copia de seguridad se verificó que pesa aproximadamente 42 GB debido a la cantidad de tablas, registros y procedimientos que esta posee, por lo tanto, el proceso tomo de 30 a 40 minutos aproximadamente.

Archivo BAK

Nombre	Fecha de modificaci...	Tipo	Tamaño
BDDSICUIOCM01_20190601.bak	01/06/2019 1:52	Archivo BAK	41.613.110 ...

Figura 28. Archivo .BAK (respaldo)
Elaborado por: Williams Valenzuela

3.3.3.6. Restauración del backup en el ambiente virtualizado

La restauración del Backup se lo realizó de igual manera mediante la herramienta de administración SQL Management Studio. La figura 29 muestra la versión de SQL Server instalada en el ambiente propuesto.

Versión de SQL Server propuesto



Figura 29. Versión de SQL Server propuesto
Elaborado por: Williams Valenzuela

Para restaurar el Backup se creó una base de datos de pruebas llamada BDDSICUIOCM01_PRUEBAS1 con el fin de evaluar el rendimiento de la misma. En las figuras 30 y 31 se pueden visualizar los pasos que se realizaron para restaurar la copia de seguridad.

Restauración del Backup

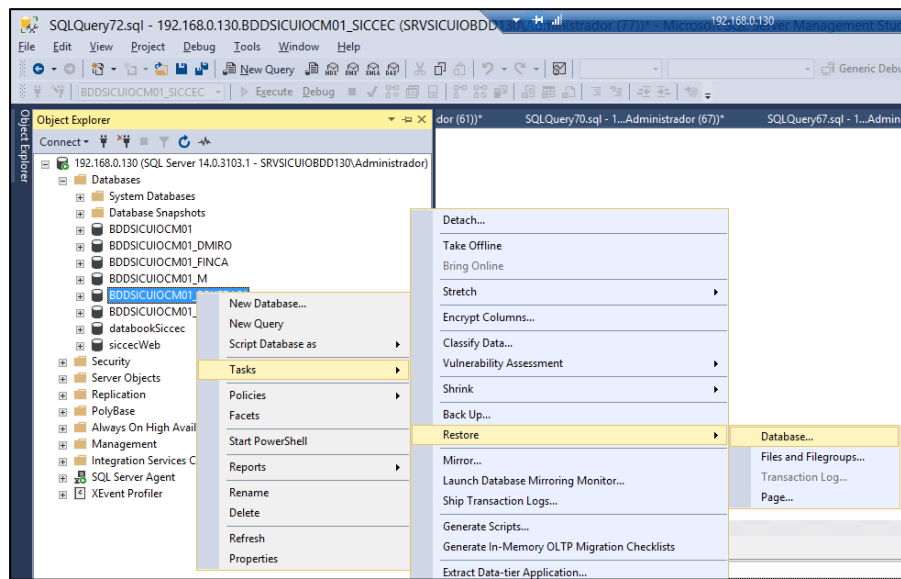


Figura 30. Restauración del Backup respaldado
Elaborado por: Williams Valenzuela

Selección del archivo

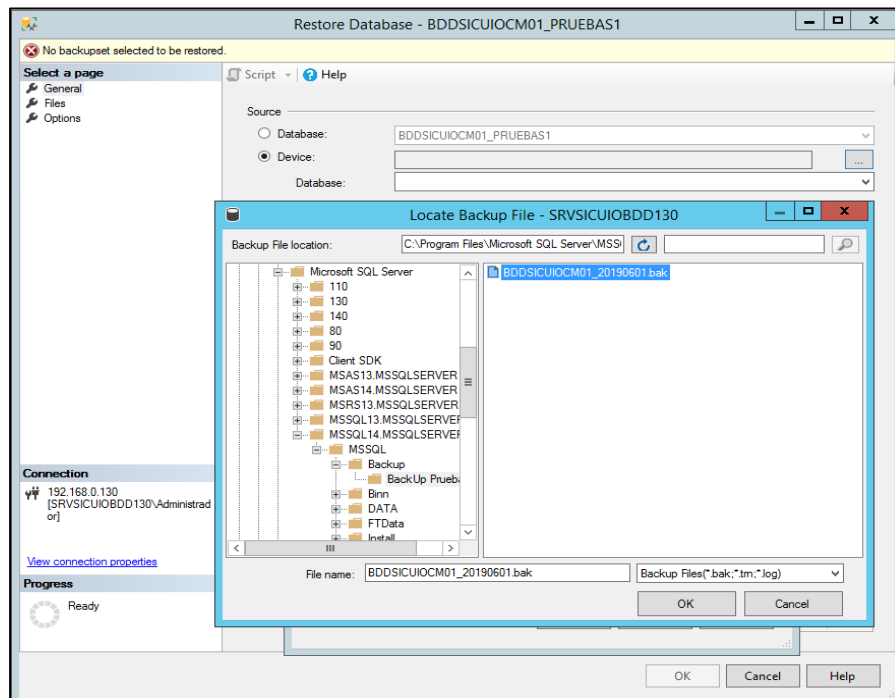


Figura 31. Selección del archivo .bak para la restauración
Elaborado por: Williams Valenzuela

El proceso de restauración tomo alrededor de 15 a 20 minutos, por lo tanto, finalizado el proceso de migración se realizaron pruebas con el fin de evaluar si se optimizaron los procesos que se realizan diariamente en la base de datos como es la actualización de carteras entre otros.

3.4. Diseño de la solución de telefonía IP

Para implementar una solución robusta de comunicaciones telefónicas sobre IP se necesita migrar el servicio de llamadas telefónicas actual hacia un nuevo sistema que continúe siendo de código abierto ofreciendo las mismas características. El sistema de central telefónica Elastix es un sistema de código abierto bajo la licencia GPLv2 que permite el establecimiento de comunicaciones unificadas, el cual funciona sobre cuatro programas importantes como son Asterisk, Hylafax, Openfire y Postfix (Irma & Nancy, 2013, pág. 34). Estos programas en conjunto brindan las diferentes funcionalidades que tiene Elastix como correo, PBX, Fax, Mensajería instantánea, etc.

A finales del año 2016 Elastix la cual era una de las distribuciones más populares de Asterisk, fue adquirida por 3CX, la cual es una empresa que ofrece soluciones de VoIP propietarias, pretendiendo ampliar su presencia en el mercado, por lo tanto, Elastix solo fue desarrollada hasta la versión 4.0 (Elastixtech, ISSABEL PBX, 2018).

3.4.1. Análisis de central telefónica propuesta.

El sistema propuesto para la solución a los inconvenientes con Elastix es Issabel PBX, ya que Elastix al ser adquirido por la empresa 3CX, Asterisk se ve en la necesidad de continuar con el proyecto de donde nace Issabel PBX, manteniendo la puerta abierta al resto de la comunidad para que entren y participen en el proyecto. Issabel PBX se basa en la versión GPL que funciona sobre la versión CentOS 7, diseñada para brindar la capacidad de llamadas simultáneas utilizando la infraestructura de red actual, la misma que se integra a la red telefónica pública ofreciendo comunicación IP dentro y fuera de la ciudad.

Según (Issabel, 2016) las características que se encuentran en Issabel PBX respecto al discontinuado Elastix son:

- Se basa en la versión 4.0 de Elastix.
- Es un drop-in replacement para Elastix, por lo que se puede actualizar de manera semi automatizada (cambiando repositorios).
- El código es más transparente, ya que ahora existe un repositorio abierto de código en Github para el control y monitoreo de cambios.
- Geolocalización de las IP en el firewall.
- Posibilidad de instalar certificados seguros SSL.
- Sistema de videoconferencias.

3.4.2. Diseño de la central telefónica ISSABEL PBX.

La migración de centrales telefónicas se las realizó en un sistema virtualizado que se encuentra en el nuevo servidor adquirido por la empresa, con el fin de contar con un sistema centralizado y administrado por parte de la herramienta de virtualización. Para realizar el proceso de migración de las centrales telefónicas se siguieron los siguientes pasos:

Pasos para la implementación de la nueva central telefónica

1. Se realizó una copia de seguridad de la central telefónica actual Elastix.

2. Descarga de una imagen .ISO de Issabel, ya que en la página oficial de la plataforma se tiene la descarga instantánea.

3. Implementación de una máquina virtual con Issabel en Citrix XenServer.

4. Restauración de la copia de seguridad de Elastix en Issabel.

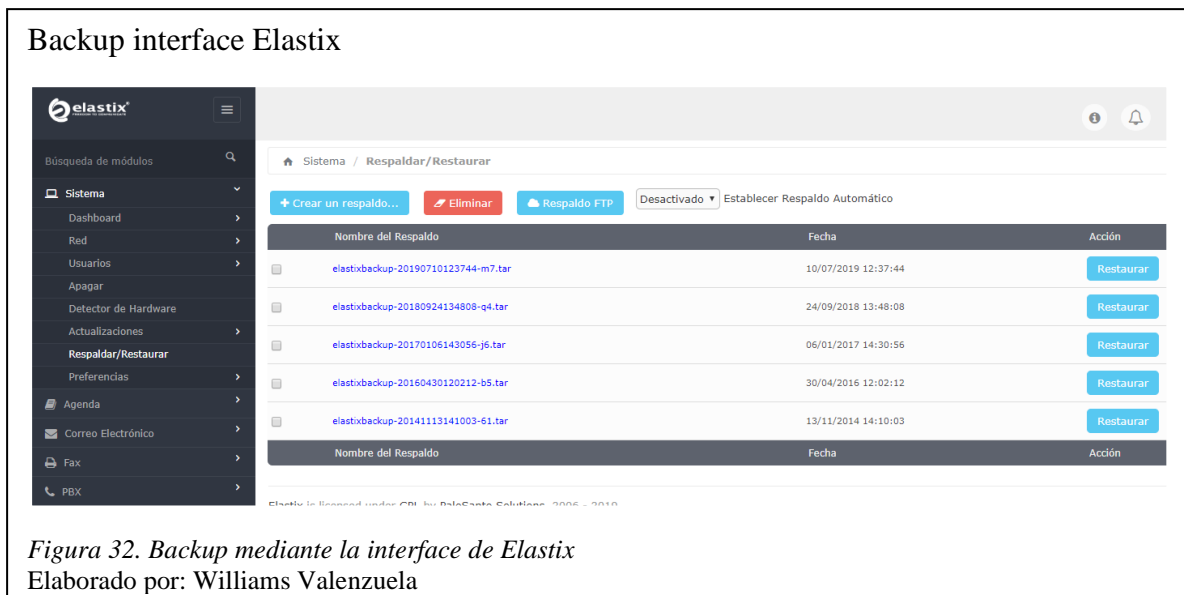
5. Configuraciones de troncales y red.

6. Pruebas de la central telefónica.

3.4.2.1. Backup de central telefónica en ELASTIX.

La central telefónica actual permite generar copias de seguridad de toda la configuración que posee la misma, con el fin de evitar la creación nuevamente de extensiones, troncales, rutas salientes, etc. Por lo tanto, se generó una copia de seguridad durante toda la noche ya que la central telefónica posee varias extensiones y configuraciones debido a la cantidad de personal que maneja SICCEC.

Para realizar la copia de seguridad de la central telefónica se accedió al menú principal donde hay una opción que permite realizar esta función como se visualiza en la figura 32.



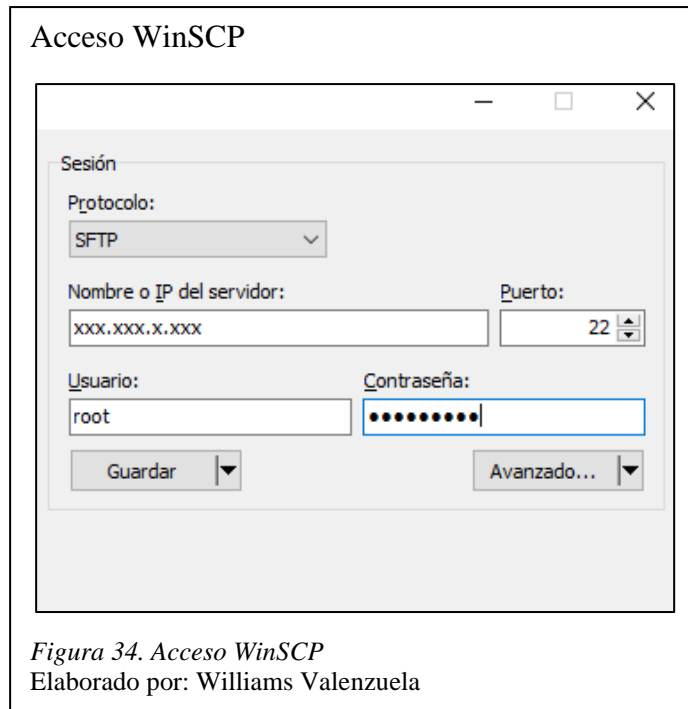
Al seleccionar la opción de crear un respaldo despliega todas las opciones de las cuales podemos seleccionar las que nos interesa sacar una copia de seguridad. Se seleccionaron todas las opciones, esto con el fin de respaldar todas las configuraciones que posee actualmente y así evitar la pérdida de algunos parámetros de configuración.



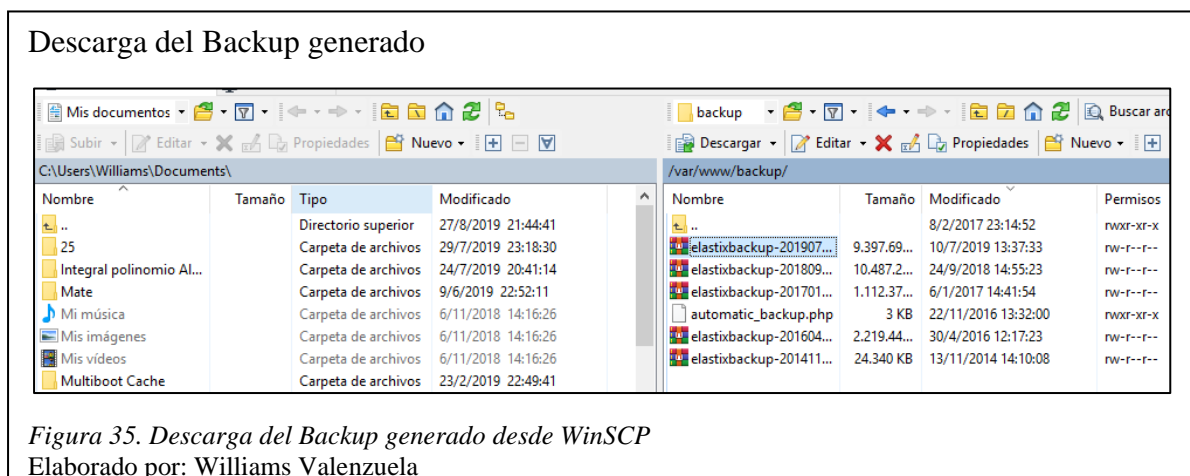
Figura 33. Opciones seleccionadas para realizar el Backup
 Elaborado por: Williams Valenzuela

Una vez seleccionadas todas las opciones junto con el botón procesar, comenzó el proceso de copia de seguridad la cual tomo alrededor de dos horas en completarse. Para visualizar el Backup generado se utilizó WinSCP la cual es una aplicación de software libre que permite la navegación sobre diferentes directorios en diferentes sistemas operativos, además de que permite subir y descargar archivos (Martin, 2014).

La figura 34 muestra la configuración que se necesita poner en la aplicación para conectarse al servidor donde se encuentra alojada la central telefónica, con el fin de acceder a los directorios y descargar el Backup generado.



Una vez colocadas las credenciales correctas se accedió al directorio donde se guardan las copias de seguridad generadas en Elastix. La figura 35 muestra el directorio /var/www/backup con la lista de copias de seguridad generadas, para lo cual se la descargó en un directorio de la computadora local.

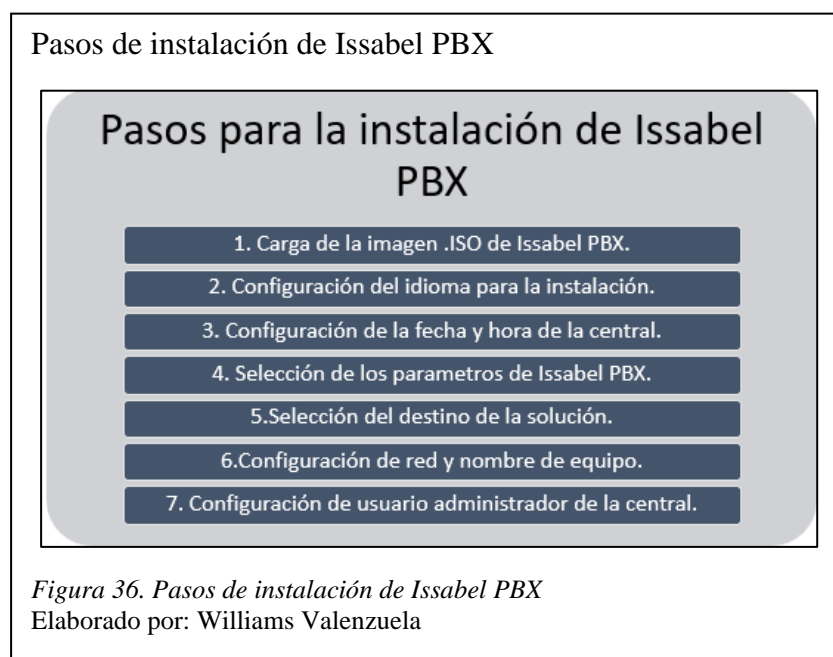


Se escogió la herramienta WinSCP ya que agiliza el proceso de descarga, ya que al ser una copia de seguridad que pesa 10 GB aproximadamente tomo de 50 a 60 minutos en completarse la descarga.

3.4.2.2. Implementación de la central telefónica ISSABEL PBX.

La instalación de la central telefónica se la realizó en un ambiente virtualizado en el servidor adquirido por SICCEC, como se explicó en el punto 3.2.3.1, sin embargo, los recursos asignados a la misma son distintos, como se mencionó en la tabla 3.

A continuación, en la figura 36 se detallan los pasos para la implementación de la central telefónica, ya que la instalación es similar a la de Elastix.



Luego que se realizaron todos los pasos de instalación de la central telefónica, se accedió a la interface de administración en un navegador web mediante la IP asignada a la misma. Al ingresar las credenciales configuradas en el paso 7 de la instalación, despliega la consola de administración de Issabel PBX la cual es muy similar a la de Elastix como se muestra en la figura 37.

Interface de administración de Issabel PBX

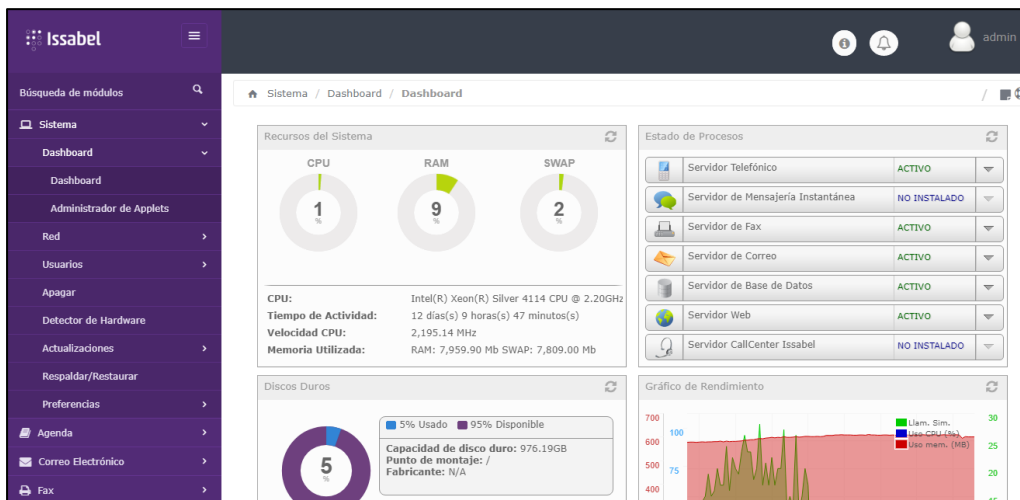


Figura 37. Interface de administración de Issabel PBX desde navegador web
Elaborado por: Williams Valenzuela

3.4.2.3. Restauración del backup de Elastix en ISSABEL PBX.

El proceso de restauración de la copia de seguridad fue similar al de generar la misma, ya que se utilizó la aplicación WinSCP para trasladar el Backup descargado en el directorio local y luego se copió en el directorio de la nueva central telefónica como se visualiza en la figura 38. De tal manera que, al ingresar al apartado de respaldos mediante la interface, muestre el Backup copiado como se visualiza en la figura 40.

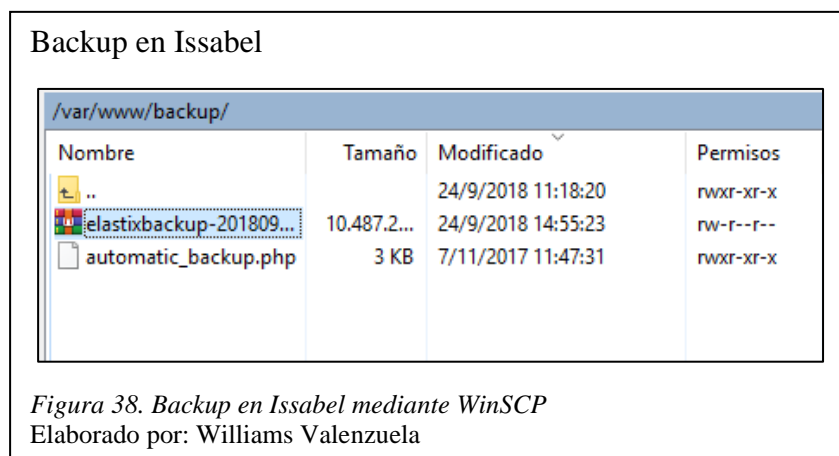


Figura 38. Backup en Issabel mediante WinSCP
Elaborado por: Williams Valenzuela



3.5. Implementación del generador de campañas de IVR

La implementación del generador de campañas del IVR, permite generar llamadas a los clientes automáticamente, con el fin de evitar que un agente del Call Center se comunique directamente con los deudores. Por lo tanto, el objetivo principal de esta propuesta fue modificar las opciones y diseño de la interfaz de las llamadas automáticas, con el fin de optimizar algunos pasos que los supervisores y departamento de sistemas deben realizar para generar las llamadas.

3.5.1. Implementación de AudioElastixDialer.

El autor (Oliva, 2013) ofrece una solución para las llamadas desatendidas, la cual permite generar campañas de llamadas automáticas haciendo uso de las centrales telefónicas Elastix o Issabel PBX. Las campañas se generan mediante una interfaz desarrollada en PHP en donde se carga un archivo con extensión CSV que contiene los números a los cuales se desea contactar, de manera que si la persona contesta se reproduzca una grabación automática previamente grabada y toda esta información se la pueda cargar en una base de datos.

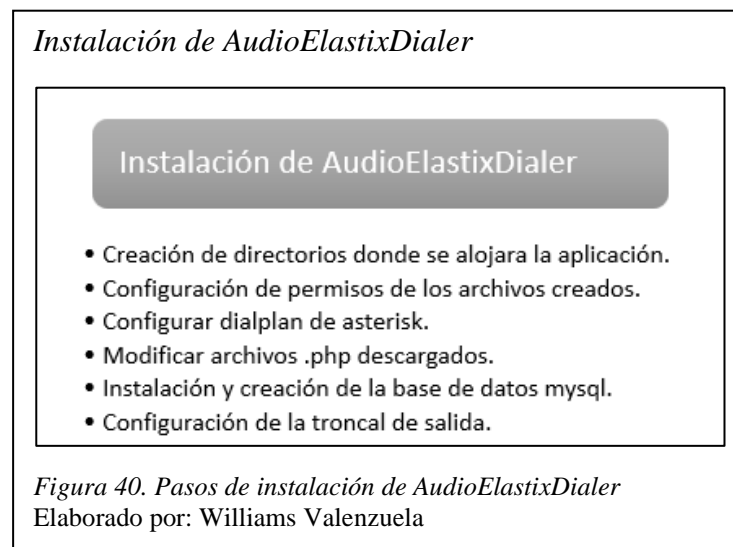
La solución contiene tres archivos los cuales son:

- **Funciones_bd.php:** Contiene la conexión a la base de datos, así como las operaciones a las tablas de la misma.

- **Index.php:** Contiene la interfaz, es decir el formulario en el cual se establece el nombre de la campaña, el tipo de troncal, contexto a usar y la selección del archivo de números a llamar.
- **Audioelastixdialer.php:** Permite subir el archivo hacia el directorio del servidor para que los números se inserten en la base de datos y así generar los archivos.call para que las llamadas puedan ser generadas.

3.5.1.1. *Instalación de AudioElastixDialer.*

La figura 40 detalla los pasos de instalación que se realizaron, estos involucran la descarga y configuración de archivos proporcionados por el autor y archivos propios de Asterisk.



La instalación de AudioElastixDialer se realizó en el ambiente virtual propuesto, en el cual se encuentra instalado Issabel PBX. El primer paso fue crear un directorio dentro de la central para alojar la aplicación, esto con el fin de no mezclar los archivos de configuración.

La carpeta creada se encuentra dentro del siguiente directorio /var/www/html con el nombre AudioElastixDialer

Creación del directorio

```
[root@issabel ~]# mkdir /var/www/html/AudioElastixDialer
[root@issabel ~]#
```

Figura 41. Creación del directorio AudioElastixDialer
Elaborado por: Williams Valenzuela

Se procedió a descargar y descomprimir la aplicación que comparte el autor desde el siguiente

link: <http://www.silcom.com.pe/soft/AudioElastixDialer.zip>

Descarga de AudioElastixDialer

```
[root@issabel ~]# cd /var/www/html/AudioElastixDialer/
[root@issabel AudioElastixDialer]# wget http://www.silcom.com.pe/soft/AudioElastixDialer.zip
--2019-09-24 21:42:37-- http://www.silcom.com.pe/soft/AudioElastixDialer.zip
Resolviendo www.silcom.com.pe (www.silcom.com.pe)... 70.38.123.185
Conectando con www.silcom.com.pe (www.silcom.com.pe) [70.38.123.185]:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 4679 (4,6K) [application/zip]
Grabando a: "AudioElastixDialer.zip"

100%[=====>] 4.679      --.-K/s   en 0s

2019-09-24 21:42:38 (201 MB/s) - "AudioElastixDialer.zip" guardado [4679/4679]

[root@issabel AudioElastixDialer]#
```

Figura 42. Descarga de AudioElastixDialer comprimido en .zip
Elaborado por: Williams Valenzuela

Extracción de archivos

```
[root@issabel AudioElastixDialer]# unzip AudioElastixDialer.zip
Archive:  AudioElastixDialer.zip
  inflating: AudioElastixDialer/audioelastixdialer.php
   creating: AudioElastixDialer/csv/
  inflating: AudioElastixDialer/csv/numerosBD.csv
  inflating: AudioElastixDialer/funciones_bd.php
  inflating: AudioElastixDialer/index.php
   creating: AudioElastixDialer/sql/
  inflating: AudioElastixDialer/sql/AdioElastixDialerBD.sql
[root@issabel AudioElastixDialer]#
```

Figura 43. Extracción de archivos .php
Elaborado por: Williams Valenzuela

Se establecieron permisos a los directorios para que estos puedan interactuar entre sí.

Asignar permisos a directorios

```
[root@issabel AudioElastixDialer]# chmod a+wr /var/www/html/AudioElastixDiale
[root@issabel AudioElastixDialer]# chmod a+wrx /var/spool/asterisk/outgoing/
[root@issabel AudioElastixDialer]# █
```

Figura 44. Crear permisos a directorios

Elaborado por: Williams Valenzuela

Una vez que se asignaron permisos a los directorios, se procedió a configurar el Dial Plan de Issabel, el cual se puede definir como un grupo de reglas que le indican a la central PBX-IP las funciones que debe realizar (Elastixtech, DialPlan o Plan de Marcacion, 2018).

Para configurar el grupo de reglas de marcado se accedió al siguiente directorio `/etc/asterisk/` para editar el archivo `extensions_custom.conf`.

Al acceder al archivo en la parte de `[from-internal-custom]` se añadió la llamada de un método llamado `call-file-test` el cual permitirá definir las acciones que se realizarán luego de contestada la llamada.

Modificación de call-file-test

```
; This file contains the contexts the agents login for the module call center.
; and contains the context conferences for module conferences of elastix 1.0.

[from-internal-custom]
exten => 1234,1,Playback(demo-congrats)           ; extensions can dial 1234
exten => 1234,2,Hangup()
exten => h,1,Hangup()
include => agentlogin
include => conferences
include => calendar-event
include => weather-wakeup
include => call-file-test
```

Figura 45. Modificación de del método call-file-test

Elaborado por: Williams Valenzuela

Al final del archivo se procedió a crear el método o contexto, de tal manera que en este se establezcan las grabaciones que serán reproducidas.

Creación de método para reproducir audio

```
exten => _X.,n,Set(CDR(userfield)=audio:${CALLFILENAME}.${MIXMON_FORMAT})
exten => _X.,n(skiprecord),Dial(${AGENTCHANNEL},300,tw)
exten => h,1,Macro(hangupcall,)

[call-file-test]
exten => s,1,wait(15)
exten => s,2,Playback(demo-congrats)
exten => s,3,Hangup()
-- INSERT --
```

Figura 46. Creación de método para reproducir audio

Elaborado por: Williams Valenzuela

Para que los cambios sean efectuados correctamente hay que generarlos mediante CLI de Asterisk (Asterisk Command Line Interface). La consola de administración de Asterisk permite entender por qué se ha producido un fallo, reiniciar servicios, etc.

Implementación de cambios en Asterisk

```
[root@issabel ~]# asterisk -rvvvvvvvv
Asterisk 13.22.0, Copyright (C) 1999 - 2014, Digium, Inc. and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
S.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
=====
Connected to Asterisk 13.22.0 currently running on issabel (pid = 2132)
issabel*CLI> reload
```

Figura 47. Implementación de cambios en Asterisk (reload)

Elaborado por: Williams Valenzuela

3.5.1.2. Creación de la base de datos de AudioElastixDialer.

La aplicación web se integrará a una base de datos en donde se registran las campañas generadas, junto con las llamadas realizadas a los diferentes números de las distintas campañas. Para lo cual se procedió a crear la base de datos, ya que Issabel PBX cuenta con un MySQL propio predeterminado.

La creación de la base de datos y la asignación de permisos a la base de datos para el usuario root se la realizó mediante comandos como se visualiza en la figura 48.

Creación de BDD

```
[root@issabel ~]# mysql -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 381
Server version: 5.5.56-MariaDB MariaDB Server

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database AudioElastixDialerBD;
Query OK, 1 row affected (0.00 sec)
[root@issabel ~]# mysql -u root -p AudioElastixDialerBD < /var/www/html/AudioElastixDialer/sql/AudioElastixDialerBD.sql
Enter password:
[root@issabel ~]#
```

Figura 48. Creación de BDD AudioElastixDialer
Elaborado por: Williams Valenzuela

3.5.1.3. Modificación de los datos de conexión a la BDD.

El archivo funciones.php contiene la conexión a la base de datos, por lo tanto, se lo modificó con el fin de cambiar la cadena de conexión, la cual apuntara a la nueva base de datos creada en MySQL.

Modificación de Funciones.php

```
[root@issabel ~]# vi /var/www/html/AudioElastixDialer/funciones_bd.php
?php
function conectar_bd()
{
    if(!($conector=mysql_connect("localhost","root","contraseñaBD")))
    {
        echo "Error al conectar al servidor de base de datos";
        exit();
    }

    if(!mysql_select_db("AudioElastixDialerBD",$conector))
    {
        echo "Error al conectarse a la base de datos";
        exit();
    }

    return $conector;
}
```

Figura 49. Modificación de del archivo Funciones.php
Elaborado por: Williams Valenzuela

La función conectar_bd permite realizar la conexión a la base de datos, de tal manera que al poner una condición if permita identificar si la conexión se realizó o si fue fallida.

Se modificaron los siguientes parámetros en la cadena de conexión.

- Nombre de usuario de BDD.
- Contraseña de la BDD.
- Nombre de la BDD.

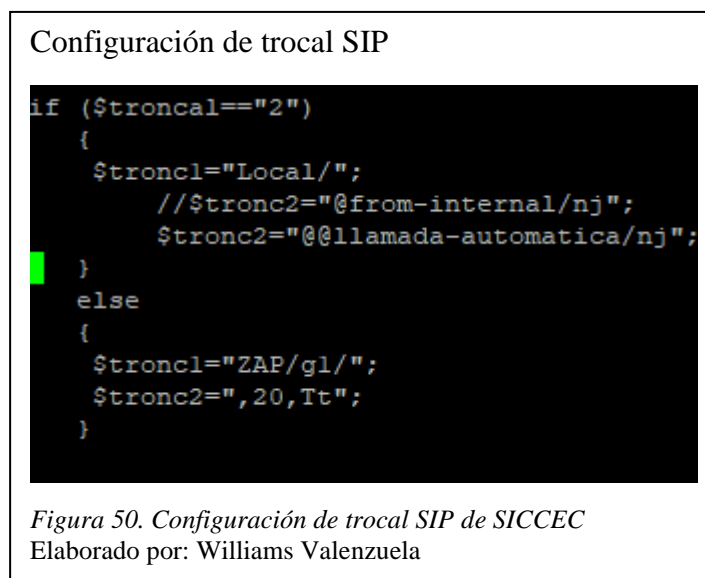
3.5.1.4. Configuración de la troncal de salida.

El archivo audioelastixdialer.php contiene el código hecho en PHP que permite realizar las llamadas, por lo tanto, fue necesario editar dicho archivo con el fin de cambiar las configuraciones de la troncal por donde se realizarán las llamadas a los clientes.

Por defecto están establecidas las siguientes configuraciones

```
$tronc1="SIP/0051";  
$tronc2="@PROVEEDORVOIP";
```

La empresa SICCEC tiene contratada una troncal con un proveedor externo, por lo tanto, se procedió a cambiar los parámetros de configuración para hacer uso de dicha troncal.



Una vez que se realizaron todos los pasos de instalación y configuración se procedió a verificar el funcionamiento de la primera parte de la aplicación web. La interface se la puede abrir desde cualquier navegador web colocando la IP donde se encuentra alojada la aplicación como se visualiza en la figura 51.



La solución propuesta por el autor fue la principal base para partir y modificar la aplicación según las necesidades de SICCEC, ya que se necesitaron agregar campos en los cuales los supervisores puedan escoger el cedente para crear las campañas de llamadas automáticas.

3.6. Caracterización de los activos tecnológicos de la empresa

Los activos tecnológicos de SICCEC se los determinó en base a factores considerados importantes para la producción diaria de la empresa, es decir que, si uno de estos no está disponible, la operatividad de la empresa baja considerablemente. Si bien es cierto con la propuesta de virtualizar los servicios críticos de la empresa, se garantiza de cierta manera la

disponibilidad, al poder restablecer un SnapShot en caso de sufrir un desastre o un ataque, por lo tanto, es necesario proteger este tipo de servicios críticos de la empresa.

Por medio de una entrevista al gerente de sistemas, se ha encontrado que los servicios considerados como los activos tecnológicos más importantes de la empresa son el servidor Web, servidor de base de datos y la central telefónica. Se los considera los más importantes ya que si uno de estos llega a fallar y no hay una intervención oportuna del área de TI, la empresa simplemente no puede realizar su trabajo en cuanto a la gestión de cobranza.

Al considerarlos servicios críticos se los debe proteger de varios factores que puedan afectar su disponibilidad, por lo tanto, es importante detectar las vulnerabilidades que presenten estos tipos de servicios. Se considera como vulnerabilidad a una debilidad en el software o sistema operativo por la cual un atacante puede generar una amenaza y comprometer la integridad, confidencialidad y disponibilidad del sistema o de los datos.

3.6.1. Análisis de vulnerabilidades informáticas.

La mejor solución para mitigar vulnerabilidades en aplicaciones y sistemas operativos es la prevención, para ello se recomienda realizar un inventario de los principales activos tecnológicos de la empresa como servidores, infraestructura, aplicaciones, etc. Para luego realizar un escaneo de vulnerabilidades y pruebas de penetración sobre estos. Finalmente se deben aplicar las medidas correctivas en base a los informes de vulnerabilidades encontradas y así reducir las amenazas considerablemente.

Luego de determinar los servicios críticos de SICCEC se procedió a mitigar las principales vulnerabilidades en el sistema operativo implementado en los servidores. Para esto durante el desarrollo del proyecto de parte de gerencia administrativa y en coordinación con el área de sistemas, se realizó un contrato con una empresa externa que permita realizar un escaneo de vulnerabilidades a los servidores más importantes que tiene la empresa, de tal manera que se

pueda mitigar las principales vulnerabilidades para reducir las probabilidades de recibir algún tipo de ataque informático.

3.6.2. Vulnerabilidades en Windows server 2012.

Según (Gabriel, Danny, & Julio, 2015, pág. 38) El sistema operativo Windows server 2012 desde el año de su lanzamiento hasta el 2015 presento alrededor de 168 vulnerabilidades y exposiciones comunes según la NIST (Instituto Nacional de Estándares y Tecnología) como se puede visualizar en la tabla 5, por lo que al tener este sistema operativo en algunos servidores de la empresa fue necesario realizar un escaneo de vulnerabilidades. Donde los autores recomiendan la administración de actualizaciones de seguridad por parte de Microsoft, las buenas prácticas de Hardening y la correcta administración del Firewall y Active Directory en las empresas.

Tabla 5. Vulnerabilidades en Windows Server 2012

CWE	2012	2013			2014			2015	2012 - 2015	
	September - December	January - April	May - August	September - December	January - April	May - August	September - December	January - April	#	%
Permissions, Privileges and Access Control	1	6	4	2	3	7	4	15	42	25
Buffer Errors	1	3	7	8	3	2	0	2	26	15
Resource Management Errors	2	12	1	2	1	2	1	2	23	14
Code Injection	1	1	2	2	0	1	5	8	20	12
Input Validation	2	2	0	6	1	4	2	2	19	11
Information Leak / Disclosure	0	1	1	1	0	0	1	8	12	7
Other	1	1	1	0	0	1	1	6	11	7
Numeric Errors	2	1	0	2	0	0	0	0	5	3
Race Conditions	0	4	0	0	0	0	0	0	4	2
Insufficient Information	0	2	0	0	0	1	0	1	4	2
Path Traversal	0	0	1	0	0	0	0	1	2	1
Total	10	33	17	23	8	18	14	45	168	100

Fuente: (NIST, 2015)

3.6.3. Escaneo de vulnerabilidades en servidores propuestos.

El realizar escaneos continuos a los servidores y aplicaciones que se alojan en ellos, junto con la implementación de Hardening en los servidores es una de las buenas prácticas para reducir considerablemente los riesgos de recibir un ataque (Gabriel, Danny, & Julio, 2015, pág. 42).

Al realizar el primer escaneo de vulnerabilidades a los servidores propuestos, se corrobora lo mencionado anteriormente, ya que se encontraron una gran cantidad de vulnerabilidades entre estas varias de las indicadas, y las cuales presentan el mayor porcentaje de riesgo frente a un ataque como se visualiza en la tabla 5.

El desarrollo de este tipo de escaneos continuos con un proveedor de seguridad en este tema, facilitó la implementación de las soluciones a las vulnerabilidades, ya que estos proveedores facilitan la herramienta para realizar los escaneos programados y así encontrar la mayor cantidad de vulnerabilidades mediante un informe detallado.

3.6.3.1. Ejemplo de vulnerabilidad encontrada en servidores de prueba.

La figura 52 muestra el ejemplo de una de las vulnerabilidades más concurrentes encontrada en los servidores y la cual pertenece al grupo con mayor porcentaje de riesgo.

Informe de escaneo de vulnerabilidades

5 Microsoft Group Policy Remote Code Execution Vulnerability (MS15-011)

QID: 91017
Category: Windows
CVE ID: [CVE-2015-0008](#)
Vendor Reference: [MS15-011](#)
Bugtraq ID: 72477
Service Modified: 04/13/2018
User Modified: -
Edited: No
PCI Vuln: Yes

SOLUTION:

Refer to MS15-011 (<https://technet.microsoft.com/library/security/ms15-011>) to obtain further patch information.
In some environments, to be completely protected from the vulnerability, additional configuration by a system administrator is required in addition to deploying this security update. Refer to Microsoft Knowledge Base Article KB3000483 (<https://support.microsoft.com/en-us/help/3000483>) to obtain further information.

Patch:

Following are links for downloading patches to fix the vulnerabilities:
MS15-011: Windows Vista Service Pack 2 (<http://www.microsoft.com/downloads/details.aspx?familyid=ddf95df-113d-4e09-9422-d72f1bb3ea01>)
MS15-011: Windows Vista x64 Edition Service Pack 2 (<http://www.microsoft.com/downloads/details.aspx?familyid=ab8a7a65-a0f6-4f79-90ed-4b4cfcbaadfd>)
MS15-011: Windows Server 2008 for 32-bit Systems Service Pack 2 (<http://www.microsoft.com/downloads/details.aspx?familyid=a507236d-0ce1-4e8c-adbe-20186f2c1e1b>)
MS15-011: Windows Server 2008 for x64-based Systems Service Pack 2 (<http://www.microsoft.com/downloads/details.aspx?familyid=5b009bb4-738d-42ce-9e35-5d4580b0ad25>)
MS15-011: Windows Server 2008 for Itanium-based Systems Service Pack 2 (<http://www.microsoft.com/downloads/details.aspx?familyid=7c37a025-81ea-4360-b0de-00b39171202f>)
MS15-011: Windows 7 for 32-bit Systems Service Pack 1 (<http://www.microsoft.com/downloads/details.aspx?familyid=51090490-014f-41c4-a8e5-00706457737f>)
MS15-011: Windows 7 for x64-based Systems Service Pack 1 (<http://www.microsoft.com/downloads/details.aspx?familyid=0f86004d-5870-4204-b30-2f98440e8e0f>)
MS15-011: Windows Server 2008 R2 for x64-based Systems Service Pack 1 (<http://www.microsoft.com/downloads/details.aspx?familyid=b52b259b-5c72-40a9-8559-3d38c0c7a126>)

1

page 3

b52b259b-5c72-40a9-8559-3d38c0c7a126)
MS15-011: Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (<http://www.microsoft.com/downloads/details.aspx?familyid=432b86df-a531-4280-9aaf-0e690e2f096>)
MS15-011: Windows 8 for 32-bit Systems (<http://www.microsoft.com/downloads/details.aspx?familyid=54e7605b-a0b3-4456-9d43-ac3fa037bo47>)
MS15-011: Windows 8 for x64-based Systems (<http://www.microsoft.com/downloads/details.aspx?familyid=374c14fc-82cf-4cfa-94f0-695e99d7c423>)
MS15-011: Windows 8.1 for x64-based Systems (<http://www.microsoft.com/downloads/details.aspx?familyid=29857dc0-5dec-41c1-afee-a898d602d3ef>)
MS15-011: Windows Server 2012 (<http://www.microsoft.com/downloads/details.aspx?familyid=1e6052c8-77a2-4bfd-905f-50e8d6e5efa>)
MS15-011: Windows Server 2012 R2 (<http://www.microsoft.com/downloads/details.aspx?familyid=48248922-d55a-43b7-a564-671d79127ac7>)
MS15-011: Windows Server 2008 for 32-bit Systems Service Pack 2 (<http://www.microsoft.com/downloads/details.aspx?familyid=a507236d-0ce1-4e8c-adbe-20186f2c1e1b>)
MS15-011: Windows Server 2008 for x64-based Systems Service Pack 2 (<http://www.microsoft.com/downloads/details.aspx?familyid=5b009bb4-738d-42ce-9e35-5d4580b0ad25>)
MS15-011: Windows Server 2008 R2 for x64-based Systems Service Pack 1 (<http://www.microsoft.com/downloads/details.aspx?familyid=b52b259b-5c72-40a9-8559-3d38c0c7a126>)
MS15-011: Windows Server 2012 (<http://www.microsoft.com/downloads/details.aspx?familyid=1e6052c8-77a2-4bfd-905f-50e8d6e5efa>)
MS15-011: Windows Server 2012 R2 (<http://www.microsoft.com/downloads/details.aspx?familyid=48248922-d55a-43b7-a564-671d79127ac7>)

Figura 52. Ejemplo de informe de escaneo de vulnerabilidades

Elaborado por: Williams Valenzuela

El informe presentado luego de realizar el escaneo no solo presenta la vulnerabilidad encontrada, si no que presenta las soluciones y como explotarla. Por lo tanto, para el ejemplo que se muestra, se detallan una serie de soluciones propuestas por Microsoft, de donde al acceder a los links se muestran los parches de seguridad de los diferentes sistemas operativos de Windows para dichas vulnerabilidades como se visualizan en la figura 53.


Lista de parches de seguridad

Date	Product	Platform	Article	Download	Details
10/17/2019	Visual Studio Code		Release Notes	Security Update	CVE-2019-1414
10/08/2019	Windows Server 2012		4520007	Monthly Rollup	CVE-2019-1060
			4519985	Security Only	
10/08/2019	Windows 10 Version 1607 for x64-based Systems		4519998	Security Update	CVE-2019-1060
10/08/2019	Windows 10 Version 1607 for 32-bit Systems		4519998	Security Update	CVE-2019-1060
10/08/2019	Windows 10 for x64-based Systems		4520011	Security Update	CVE-2019-1060
10/08/2019	Windows Server 2012 (Server Core installation)		4520007	Monthly Rollup	CVE-2019-1060
			4519985	Security Only	
10/08/2019	Windows Server 2012 R2		4520005	Monthly Rollup	CVE-2019-1060
			4519990	Security Only	
10/08/2019	Windows 10 for 32-bit Systems		4520011	Security Update	CVE-2019-1060
10/08/2019	Windows RT & 1		4520005	Monthly Rollup	CVE-2019-1060
10/08/2019	Windows Server 2016		4519998	Security Update	CVE-2019-1060
10/08/2019	Windows Server 2016 (Server Core installation)		4519998	Security Update	CVE-2019-1060
10/08/2019	Windows 10 Version 1703 for x64-based Systems		4520010	Security Update	CVE-2019-1060
10/08/2019	Windows 10 Version 1703 for 32-bit Systems		4520010	Security Update	CVE-2019-1060
10/08/2019	Windows 10 Version 1709 for 32-bit Systems		4520004	Security Update	CVE-2019-1060
10/08/2019	Windows 10 Version 1709 for 64-based Systems		4520004	Security Update	CVE-2019-1060

Figura 53. Lista de parches de seguridad de acuerdo a la vulnerabilidad
Elaborado por: Williams Valenzuela

Se procedió a descargar el parche de seguridad de la vulnerabilidad de acuerdo al sistema operativo del servidor para luego ser instalada como se visualiza en la siguiente figura.

Aplicación de parche de seguridad

Name	Date modified	Type	Size
 Windows8.1-KB3000483	6/28/2019 8:32 AM	Microsoft Update ...	6,480 KB

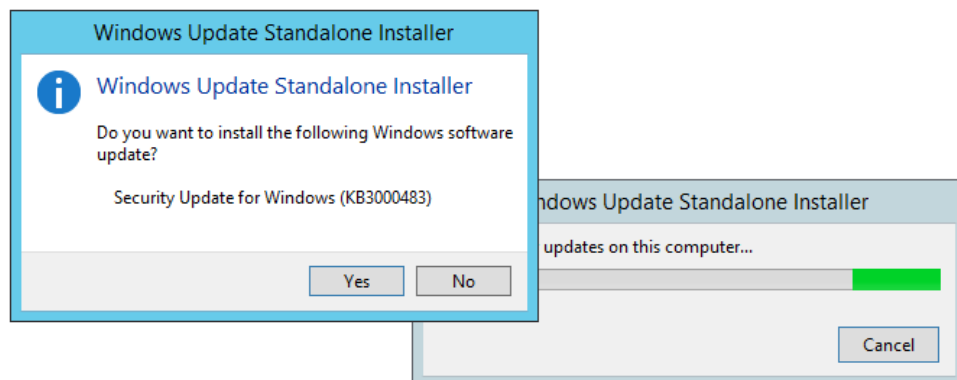


Figura 54. Aplicación de parche de seguridad descargado
Elaborado por: Williams Valenzuela

El parche de seguridad implementado es uno de varios encontrados en los servidores, por lo que fue importante reiniciar el servidor luego de ser instalado para que se apliquen los cambios.

3.7. Análisis de los perfiles de usuario

Para diseñar o modificar las reglas del firewall se analizaron los perfiles de los usuarios que tiene SICCEC, para la cual fue de vital importancia el organigrama de la empresa que se visualiza en la figura 55.

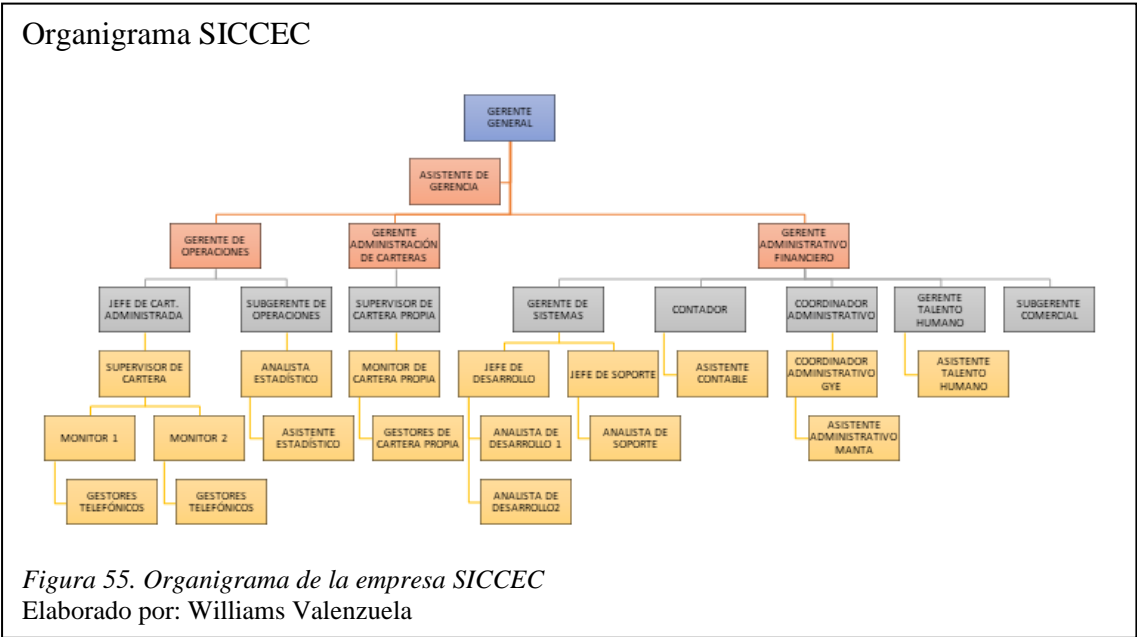
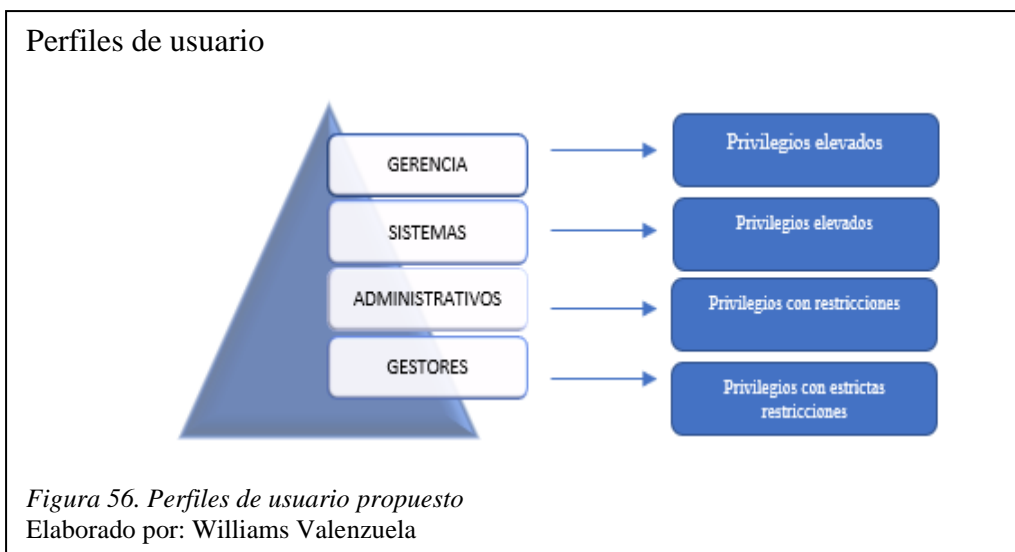


Figura 55. Organigrama de la empresa SICCEC
Elaborado por: Williams Valenzuela

Para diseñar las reglas se categorizaron los usuarios en cuatro grupos: gerencia, administrativos, gestores y sistemas. En base al perfil de cada uno se permitió el acceso a los diferentes servicios que maneja la empresa de acuerdo a las políticas de seguridad, para lo cual en la figura 56 se observa el nivel de cada grupo de usuarios.



- **Perfil de gerencia:** Este perfil de usuario tiene los máximos privilegios a los diferentes servicios que maneja SICCEC, ya que esto se determinó en base a una conversación realizada con el gerente de sistemas, sin embargo, se han utilizado herramientas adicionales para proteger tanto datos como sistemas que maneja el perfil.
- **Perfil de sistemas:** Este perfil de usuarios tiene los máximos privilegios, ya que este tiene acceso a todos los sistemas de la empresa, con el fin de proporcionar una estabilidad de los mismos. Además, es el encargado de proporcionar la seguridad y confidencialidad a los diferentes sistemas y perfiles de usuario.
- **Perfil de administrativos:** Este perfil de usuario tiene privilegios controlados, ya que existe personal administrativo en diferentes áreas por lo que cada uno maneja diferentes páginas y sistemas en la empresa. Por lo tanto, este tipo de perfil es controlado ya que maneja información importante de la empresa.

- **Perfil de gestores:** Este tipo de usuario tiene los privilegios mínimos, ya que solo tiene acceso a las páginas y sistemas que maneja para realizar la cobranza de las carteras asignadas.

3.7.1. Implementación de antivirus empresarial.

Se crearon este tipo de perfiles con el fin de identificar los usuarios que manejan información sensible de la empresa y mediante la adquisición de software, se pueda ofrecer una protección a los diferentes activos o servicios, contra tipos de virus, malware, o incluso ataques como: ransomware, phishing entre otros.

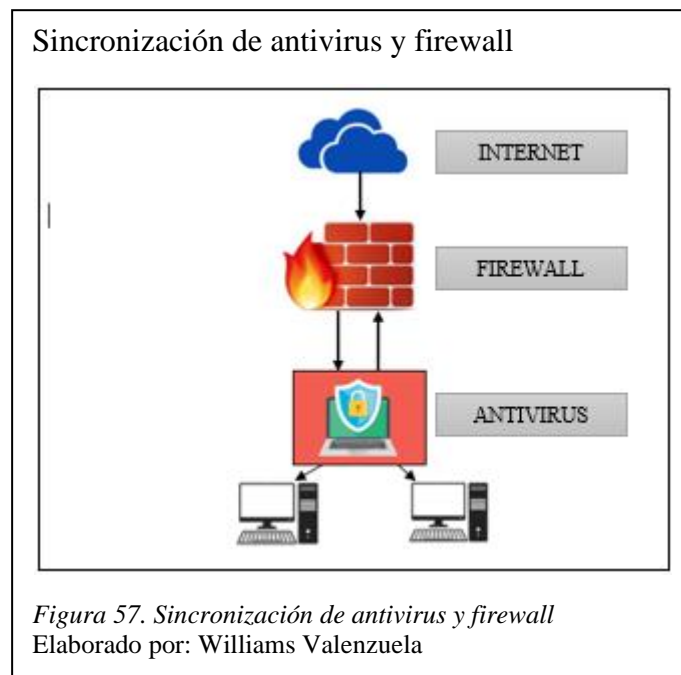
Para proteger los datos y las estaciones de trabajo que manejan los usuarios con perfil de gerencia, sistemas y administrativos, se adquirió un antivirus empresarial, el cual ofrece muy buenas características, que por temas de seguridad no se menciona su nombre comercial, pero sus principales características son.

- Prevención de exploits.
- Detección y respuesta inteligentes para las estaciones de trabajo.
- Limpieza de malware.
- Seguridad sincronizada.

La solución de antivirus implementada ayudó a tener un mejor control, ya que ofrece una administración centralizada de todas las máquinas de los usuarios, ya que ofrece seguridad en tiempo real, es decir que si este encuentra algún tipo de virus lo reporta inmediatamente a la consola de administración y la persona encargada toma las medidas necesarias para remediarlo.

Una de las buenas características que posee el antivirus adquirido es que se puede implementar las reglas de seguridad en las estaciones de trabajo, tanto reglas generales como reglas específicas, de acuerdo al perfil del usuario. Se utilizó este tipo de antivirus ya que se pudo

integrar con el firewall de la empresa, siendo esta una de las buenas características. La figura 57 muestra implementación realizada, en donde el firewall se sincroniza con la consola de administración de antivirus para proteger las estaciones de trabajo de los perfiles de usuario seleccionados.



3.8. Implementación de reglas en el firewall de acuerdo a las políticas de seguridad de la empresa

Con el fin de cumplir con las políticas de seguridad de la información de la empresa SICCEC, se procedió a configurar las reglas en el firewall que actualmente tiene la empresa, de tal manera que se pueda proteger a la misma de una amplia gama de amenazas, a fin de mejorar la disponibilidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de SICCEC.

Se crearon reglas de seguridad en firewall de acuerdo a los perfiles de cada usuario, en donde estos tendrán accesos y permisos solo a lo necesario para desempeñar su trabajo. Lo que se

busca con estas reglas es limitar al usuario el uso de páginas, aplicaciones y sistemas que no sean seguros de los cuales pongan en riesgo a los activos de la empresa.

SICCEC consta de las VLAN implementadas en su infraestructura como se visualizó en la figura 1, lo cual facilitó la creación de los grupos de acuerdo al perfil de usuario, solventando así el inconveniente que se tiene con las reglas creadas actualmente, de tal manera que se pueda segmentar y gestionar de una manera más eficaz la seguridad en la red.

En el firewall de SICCEC se crearon reglas de prueba para cada perfil de usuario, esto con el fin de no afectar a las reglas ya creadas y que se encuentran funcionando actualmente. Lo que se busca es que un futuro con la debida aprobación de gerencia éstas reglas se pongan en funcionamiento, de tal manera que se puedan obtener mayor seguridad y administración en la red de la empresa.

Se limita el acceso al usuario, ya que se considera como el blanco más débil de los atacantes, que lo que buscan es aplicar algún tipo de ataque de ingeniería social sobre los usuarios de manera que por este medio se pueda comprometer algún activo de la empresa.

Se procedió a crear 4 reglas en base a las políticas de seguridad, donde se manifiesta que el usuario debe acatar las políticas implementadas en la red de la empresa, de tal manera que, si este intenta violentar alguna de estas, se deberán aplicar las sanciones correspondientes.

3.8.1. Creación de la regla para el perfil de Gerencia.

Se creó una regla llamada Prueba de perfil de gerencia, para la cual se otorgó privilegios de accesos controlados a todos los sistemas que maneja la empresa, ya que este grupo de usuarios manejan información sensible de acuerdo al giro del negocio. Al ser un usuario crítico se restringió el acceso a páginas de dudosa procedencia mediante la política de navegación web, minimizando el riesgo al que pueden ser comprometidos este tipo de usuarios.

3.8.2. Creación de la regla para el perfil de Sistemas.

Se creó una regla llamada Prueba de perfil de Sistemas, a la que solo pertenecen pocos usuarios al ser un departamento pequeño. Se otorgó accesos a todos los sistemas que maneja la empresa, ya que este perfil los necesita para acceder a ellos y apoyarlos para un correcto funcionamiento, para evitar errores y brindar la mayor disponibilidad posible.

3.8.3. Creación de la regla para el perfil de Administrativos.

Se configuró una regla llamada Prueba de perfil de administrativos con el fin de otorgar los máximos privilegios, pero con restricciones implementadas en la política web de la empresa, en la cual solo se permite el acceso a páginas que no sean de dudosa procedencia las cuales puedan poner en riesgo los activos de la empresa que manejan.

3.8.4. Creación de la regla para el perfil de Gestores.

Se realizó una regla llamada Prueba de perfil de gestores, en la cual se configuró el acceso solo a los sistemas que maneja este grupo de usuarios, limitando el acceso hacia otros que no se encuentren en la regla mencionada. El perfil de gestores tiene acceso a la central telefónica y al sistema de cobranza que maneja la empresa, siempre y cuando este coloque las credenciales correctas para acceder a ellos.

3.9. Política de navegación Web

Esta política está definida para permitir al usuario realizar conexiones WEB o usar los servicios proporcionados por SICCEC para tener acceso a páginas web definidas para el desarrollo de las laborales actividades diarias de los servidores públicos.

En esta política se menciona que SICCEC se reserva el derecho de deshabilitar los sitios de navegación Web que considere como posibles sitios de infección de virus, malware y demás; incluyendo entre éstos, sitios Web de correos personales, almacenamientos masivos externos basados en CLOUD y descargas de cualquier tipo de archivo.

Lo que se busca con la implementación de la política web en el firewall es:

- Habilitar/deshabilitar/bloquear servicios de forma global y granular, incluso a nivel de servicios específicos o aplicaciones asociadas a servicios, como: los de video streaming, audio, redes sociales, etc.
- Mejorar sus niveles de productividad.
- Alarmas preventivas ante situaciones que pueden generar un riesgo o puedan potencialmente afectar la productividad de los funcionarios.

3.9.1. Restricciones generales de sitios de navegación web.

Se mencionan los sitios que se consideran no autorizados y los cuales consumen alto ancho de banda.

- Publicidad.
- Descarga de software gratis.
- Mensajería instantánea.
- Servicios pagados de navegación.
- Servicios de asesoría financiera y manejo de divisas en línea.
- Redes sociales.

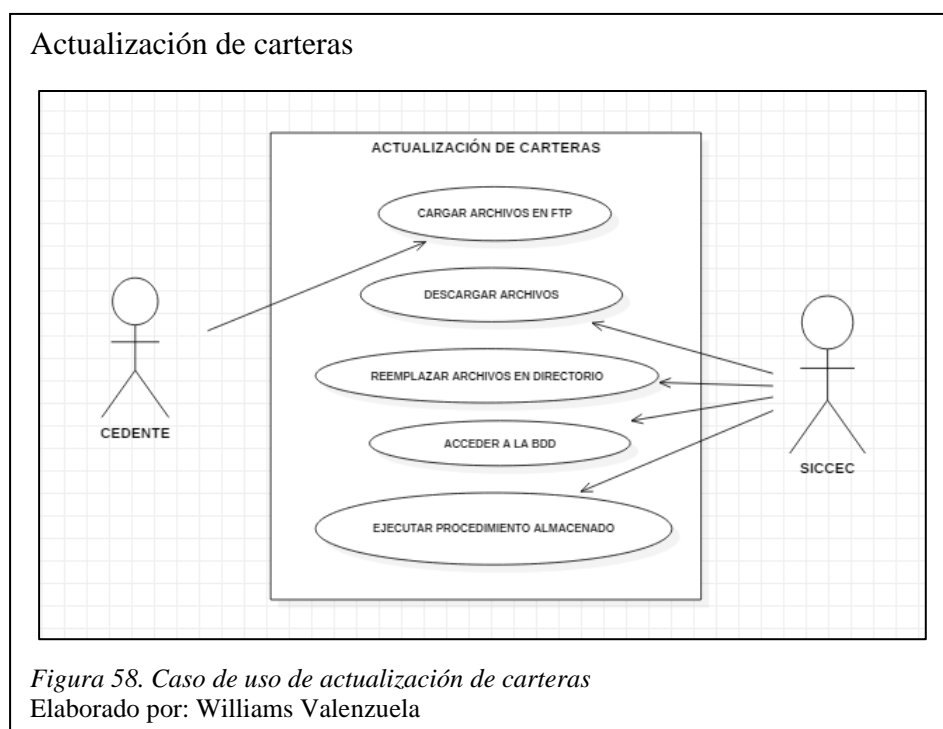
CAPÍTULO 4

4. Análisis de resultados

4.1. Virtualización de la base de datos de SICCEC

Luego de implementar la máquina virtual y migrar la base de datos que se encuentra en producción en SICCEC, se realizaron una serie de pruebas con el fin de comprobar los tiempos de respuesta de la misma, permitiendo comparar si la migración a nivel de hardware y software es factible.

Para realizar las pruebas se escogieron dos procedimientos almacenados de base de datos que la empresa ejecuta diariamente, para lo cual la figura 58 muestra el caso de uso general de este proceso.



- Cargar archivos
 - El cedente deposita los archivos en formato .txt los cuales contienen información referente a la cartera para realizar la cobranza.
- Descargar y reemplazar archivos

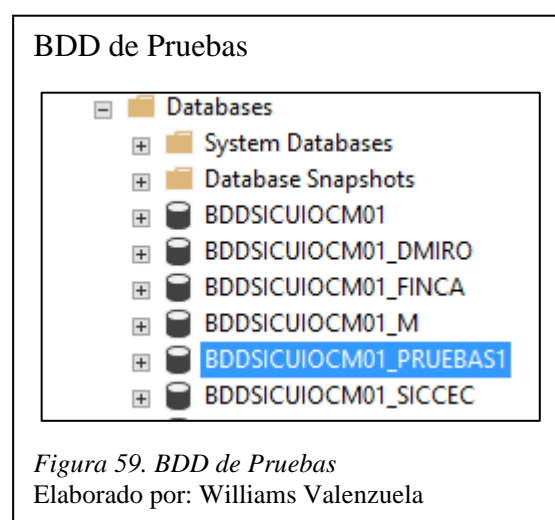
- El encargado de sistemas descarga los archivos depositados y los reemplaza en la ruta correspondiente.
- Acceder a la base de datos y ejecutar el procedimiento almacenado.
 - El encargado de sistemas accede a la base de datos correspondiente para ejecutar el procedimiento almacenado.

El caso de uso muestra el proceso que se ejecuta diariamente, el cual presenta inconvenientes al existir un retardo considerable en la ejecución del procedimiento.

Al analizar todos los procedimientos que se ejecutan en la base de datos se tomaron los que más demoran en realizarse, de tal manera que se puedan comparar los tiempos de respuesta frente a los procedimientos ejecutados en el ambiente propuesto.

- Actualización de la cartera la de Cooperativa JEP.
- Actualización de la cartera de Novacredit.

En el nuevo ambiente de SQL Server 2017 se creó una base de datos de prueba como se muestra en la figura 59, con el fin de realizar pruebas de carga para medir los tiempos de respuesta en los procedimientos seleccionados.



Para tomar el tiempo de respuesta del procedimiento de la base de datos se ejecutaron todos los procesos para tomar el tiempo de cada uno.

4.1.1. Pruebas del procedimiento almacenado de Cooperativa JEP.

A continuación, se describen las pruebas realizadas en el ambiente de producción y en el ambiente propuesto.

4.1.1.1. Pruebas en ambiente de producción.

Luego de realizar el reemplazo de los archivos enviados por el cedente, se procedió a ejecutar el procedimiento almacenado en el servidor de producción median SQL Server Management Studio.

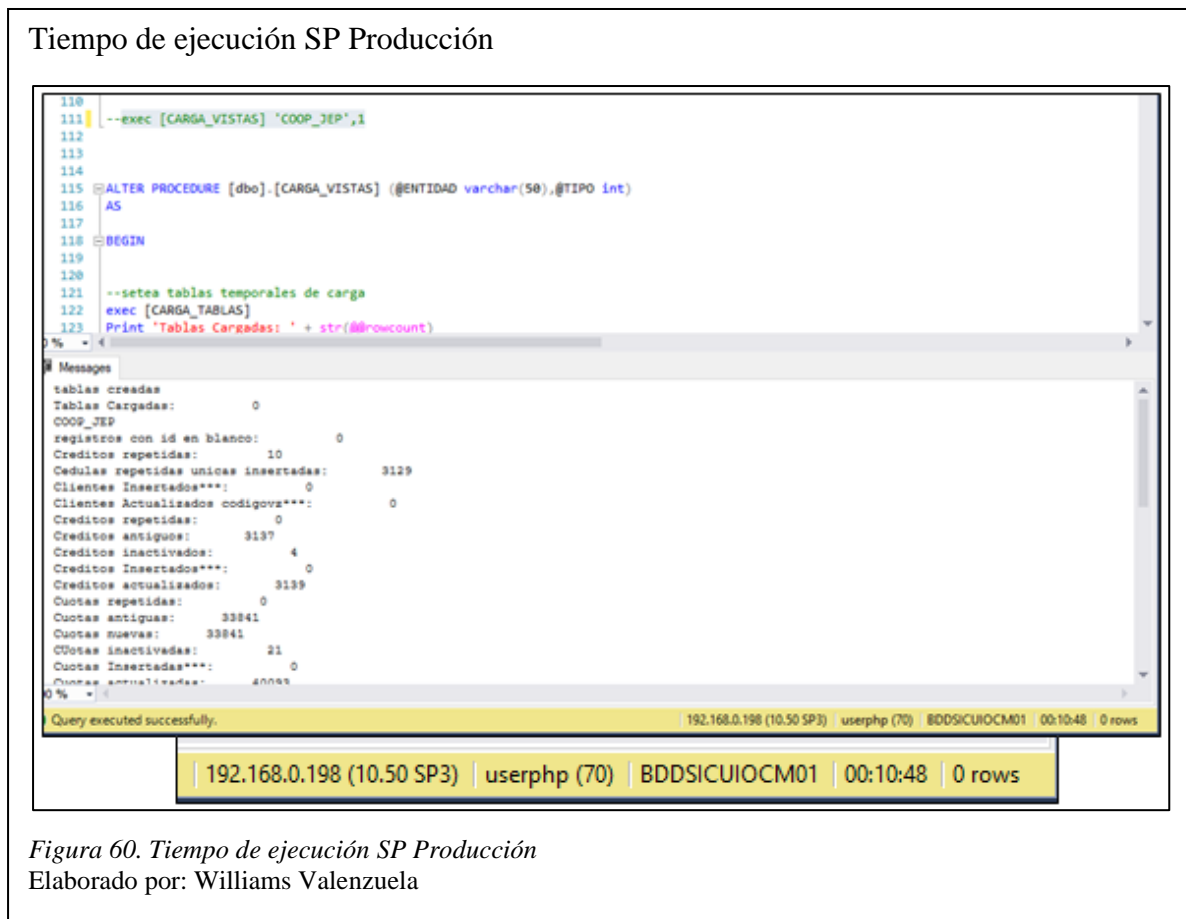


Figura 60. Tiempo de ejecución SP Producción
Elaborado por: Williams Valenzuela

La figura 60 muestra el log de carga luego de ejecutar el procedimiento almacenado para actualizar la cartera de cooperativa JEP, donde se puede visualizar que tomó 00:10:48 minutos en finalizar la actualización de la cartera.

4.1.1.2. Pruebas en ambiente propuesto.

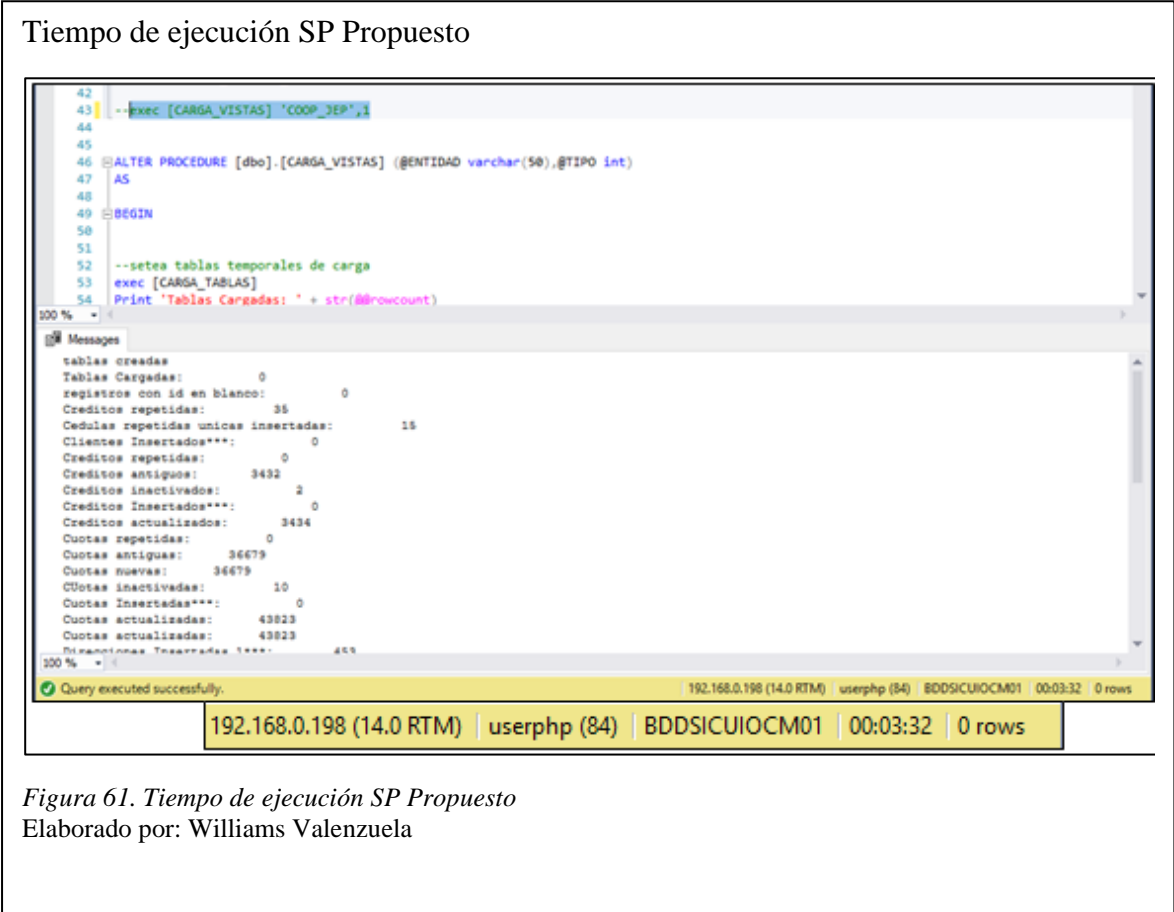


Figura 61. Tiempo de ejecución SP Propuesto
Elaborado por: Williams Valenzuela

En el ambiente propuesto el mismo proceso de actualización de cartera de cooperativa JEP que se ejecuta en el ambiente de producción tomo 00:03:32 minutos, donde se puede visualizar que el tiempo de ejecución disminuyó considerablemente en la figura 61.

4.1.2. Pruebas del procedimiento almacenado de Novacredit.

A continuación, se describen las pruebas realizadas en el ambiente de producción y en el ambiente propuesto.

4.1.2.1. Pruebas en ambiente de producción.

Luego de realizar el reemplazo de los archivos enviados por el cedente, se procedió a ejecutar el procedimiento almacenado en el servidor de producción mediante SQL Server Management Studio.

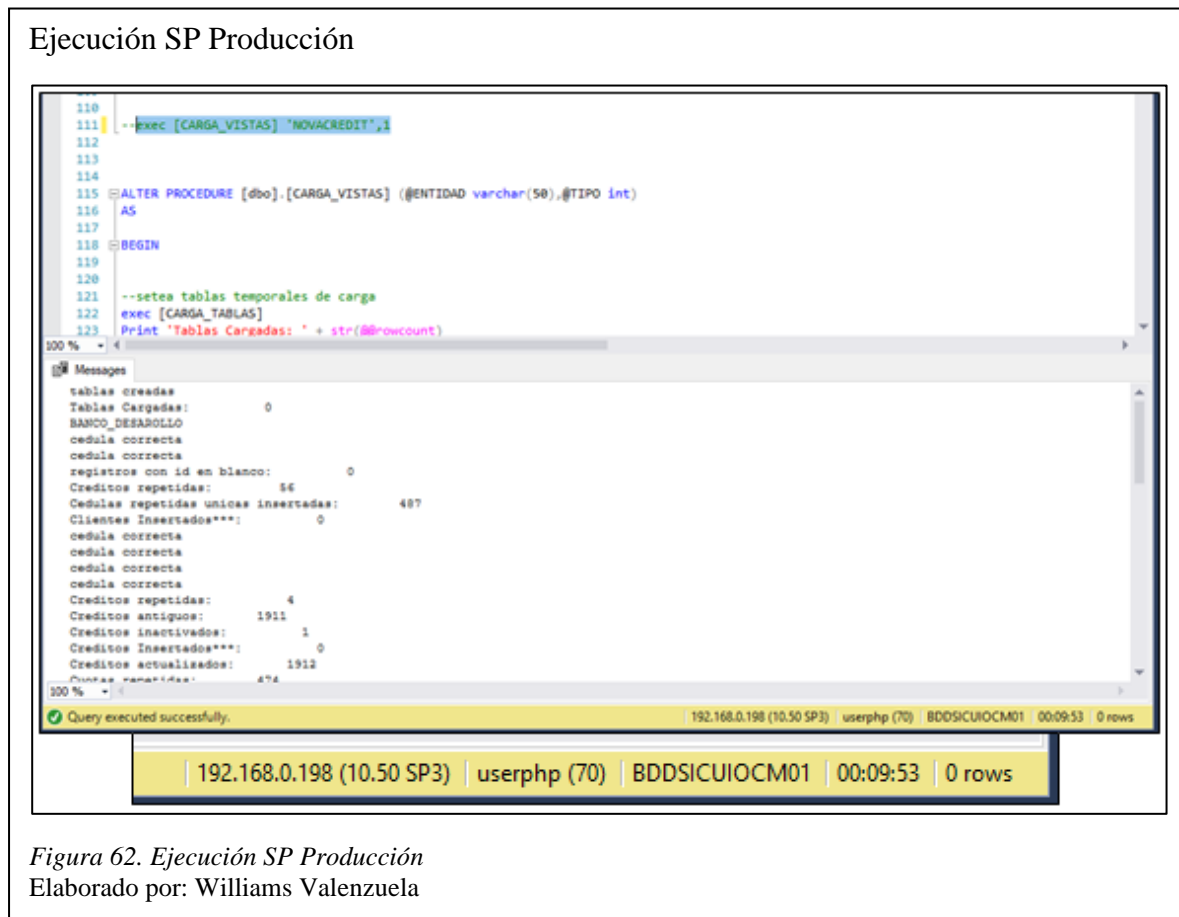


Figura 62. Ejecución SP Producción
Elaborado por: Williams Valenzuela

La figura 62 muestra el log de carga luego de ejecutar el procedimiento almacenado para actualizar la cartera de Novacredit, donde se puede visualizar que tomo 00:09:53 minutos en finalizar la actualización de la cartera.

4.1.2.2. Pruebas en ambiente propuesto.

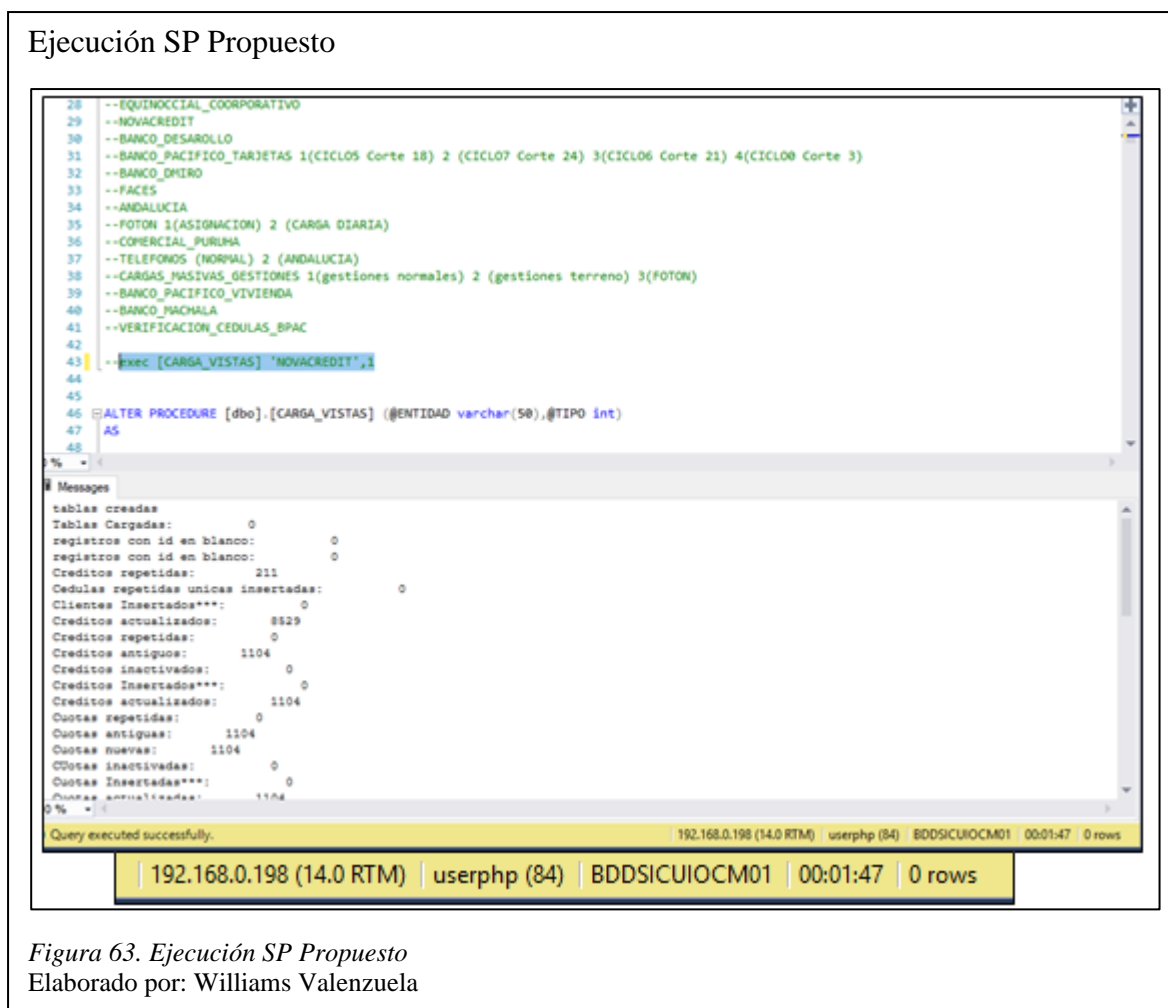


Figura 63. Ejecución SP Propuesto
Elaborado por: Williams Valenzuela

En el ambiente propuesto el mismo proceso de actualización de cartera de Novacredit que se ejecuta en el ambiente de producción tomo 00:01:47 minutos, donde se puede visualizar que el tiempo de ejecución disminuyo considerablemente en la figura 63.

4.1.3. Tiempos de ejecución de procedimientos almacenados en la BDD.

Al realizar las pruebas respecto al tiempo que tomo cada procedimiento en ejecutarse se determinó que no solo se necesitan buenos recursos de hardware y software para el buen funcionamiento de la base de datos, debido a que en un principio los tiempos si disminuyeron, sin embargo, al poner en producción y realizar pruebas de estos, los tiempos del ambiente

propuesto respecto al ambiente de producción no variaron, es por eso que se determinó que la base de datos necesitaba de índices.

Los índices no son más que una estructura de disco asociada a las tablas o vistas de una base de datos, que lo que permiten es que mediante unas claves almacenadas en una estructura de árbol puedan acelerar el proceso de recuperación de los datos que se encuentran en las tablas (Microsoft, 2019).

Luego de implementar dichos índices en las tablas como se muestran en la figura 64 los tiempos de ejecución de los procedimientos disminuyeron considerablemente, de tal manera que la persona encargada de ejecutar dichos procesos puede ahorrarse un tiempo de aproximadamente 00:15:00 minutos en ejecutar dos de todos los procesos que se ejecutan diariamente.

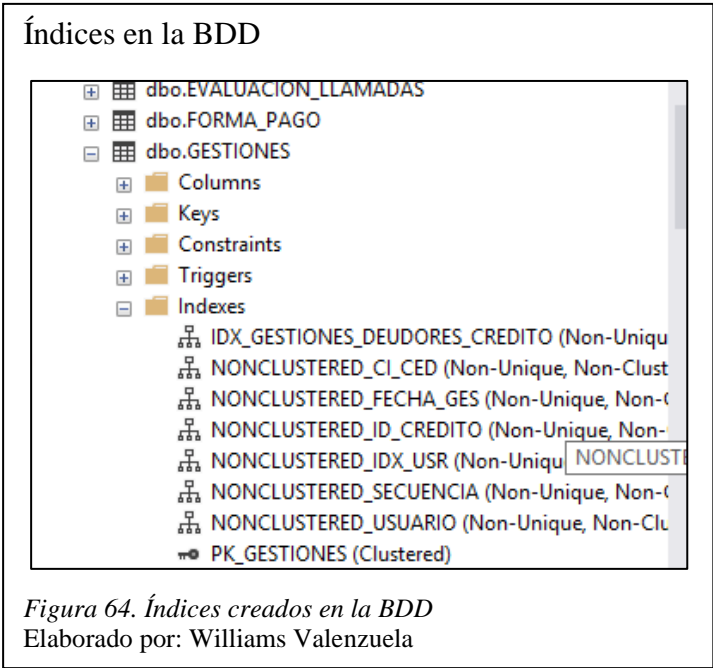


Tabla 6. Tiempos de ejecución de procedimientos almacenados en la BDD

PROCEDIMIENTO ALMACENADO	AMBIENTE DE PRODUCCIÓN (minutos)	AMBIENTE PROPUESTO (minutos)	TIEMPO ESTIMADO DE AHORRO (minutos)
COOPERATIVA JEP	00:10:48	00:03:32	0:07:16

NOVACREDIT	00:09:53	00:01:47	0:08:06
-------------------	----------	----------	---------

Elaborado por: Williams Valenzuela

Al realizar las pruebas en el ambiente virtualizado propuesto se determinó que el procedimiento de actualización de cartea de la cooperativa JEP es aproximadamente 3.5 veces más rápida de lo que se ejecuta en el ambiente de producción. De igual manera la actualización de la cartera de Novacredit es aproximadamente 5.5 veces más rápida en la finalización de ejecución del procedimiento.

4.2. Virtualización de la central telefónica de SICCEC

Luego de implementar una máquina virtual, en la cual se instaló la nueva central telefónica Issabel PBX, se realizaron pruebas para validar su correcto funcionamiento. Cabe recalcar que el cambio se lo hizo en base al soporte y continuidad que esta central telefónica ofrece, ya que como se mencionó en el punto 3.3.1, Elastix se encuentra descontinuada debido a que fue adquirida por otra empresa.

Las pruebas se realizaron en cuanto a procesamiento, funcionamiento y administración. Donde en la figura 65 se puede observar una correcta administración de todas las máquinas virtuales implementadas y en la cual se encuentra Issabel PBX como central telefónica.

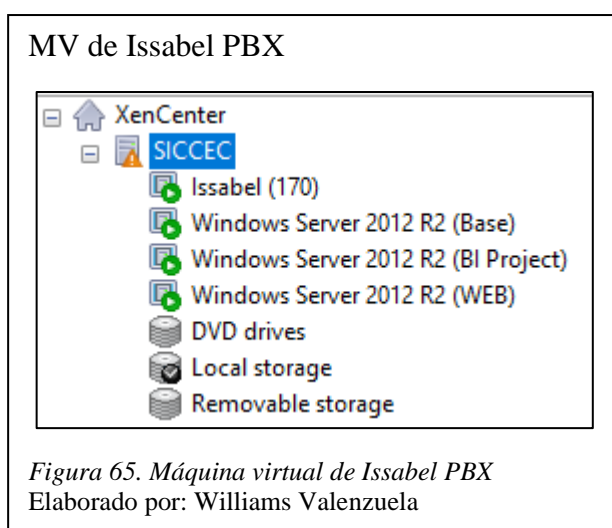
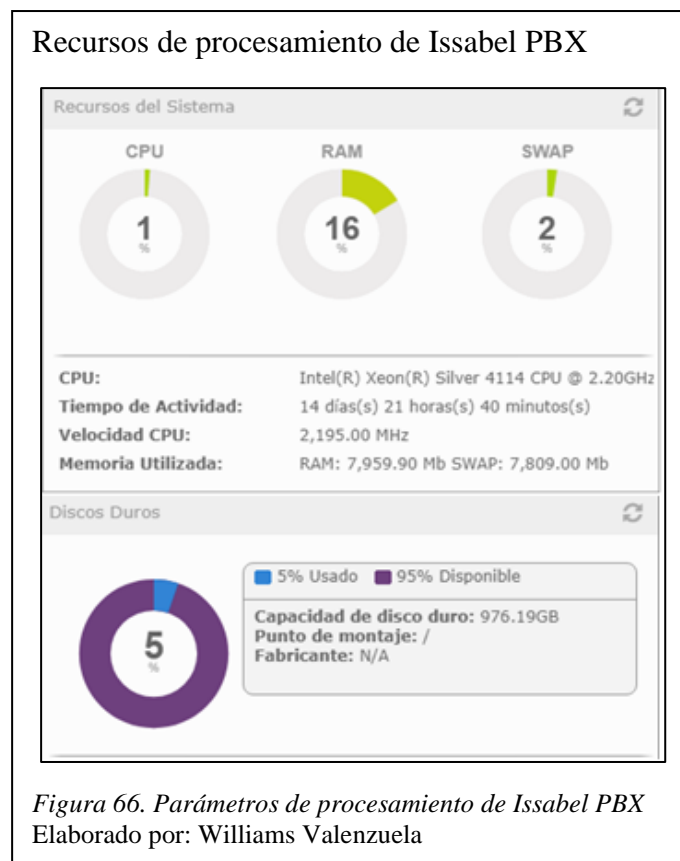


Figura 65. Máquina virtual de Issabel PBX
Elaborado por: Williams Valenzuela

Al ingresar por un navegador web se puede observar el Dashboard que la central telefónica posee, en la cual se muestran los distintos parámetros de procesamiento de la central, como son: los recursos de CPU, RAM y SWAP. Donde SWAP es una forma de liberar carga de la memoria RAM. Además, se muestra la capacidad del disco usado, donde solamente se mantiene en el 5% en uso de toda su capacidad, ya que diariamente las grabaciones que la central almacena se las respalda en un disco diferente, de manera que se puedan eliminar las almacenadas en la central y no ocupar su máxima capacidad.



El funcionamiento y rendimiento de la nueva central telefónica es adecuado, ya que la demanda de llamadas telefónicas es grande al realizarse un aproximado de 12.000 llamadas diarias, en donde existen horas con picos donde las llamadas simultáneas aumentan y la central ha reaccionado correctamente a la cantidad de tráfico generado por este servicio.

Rendimiento de Issabel PBX

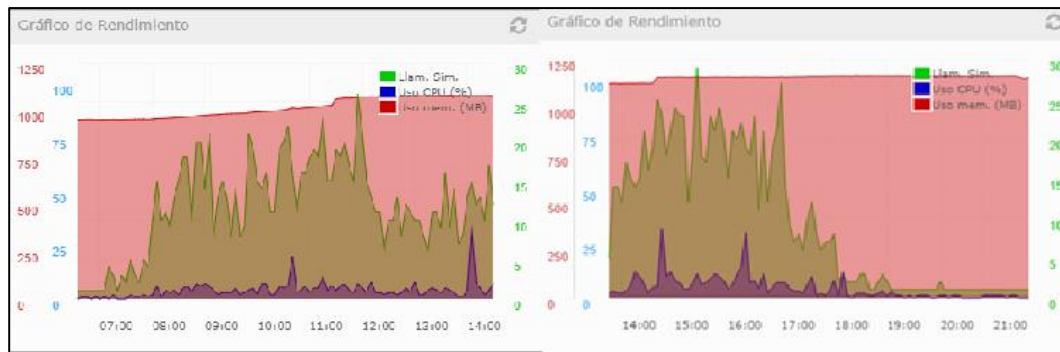
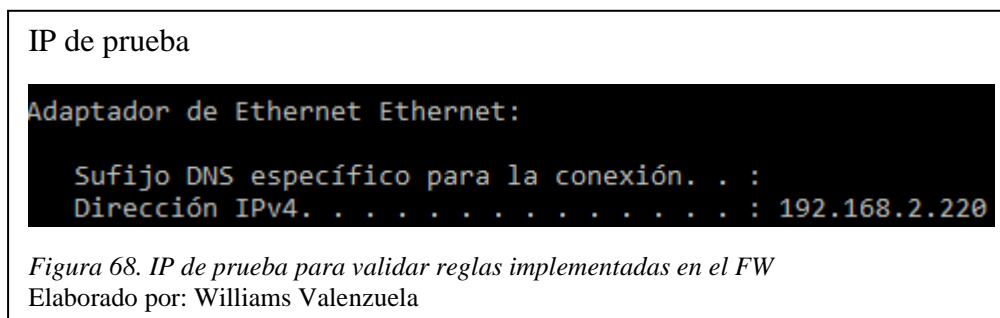


Figura 67. Rendimiento de la central Issabel PBX
Elaborado por: Williams Valenzuela

4.3. Pruebas de reglas de firewall

Con el fin de realizar pruebas de las reglas implementadas en el firewall de la empresa, se tomó como ejemplo una máquina interna con la IP 192.168.2.220 como se visualiza en la figura 68. Al ser una IP interna se la estableció en cada uno de los perfiles creados con el objetivo de verificar el correcto funcionamiento de las reglas.



4.3.1. Perfil Gestores.

La figura 69 muestra la regla implementada de acuerdo a la política del perfil de gestores telefónicos, donde se visualiza el origen de la regla para realizar las pruebas de acceso a los diferentes sistemas y páginas web.

Regla implementada para Gestores

Nombre de regla *

Descripción

Acción

Aceptar
Eliminar
Rechazar

Origen

Zonas de origen *

LAN -

Añadir nuevo elemento

Dispositivos y redes de origen *

Siccec - Williams valenzuela ✎ -

Añadir nuevo elemento

Figura 69. Regla implementada para el perfil de Gestores
Elaborado por: Williams Valenzuela

IP de origen

Siccec - Williams valenzuela

IPv4

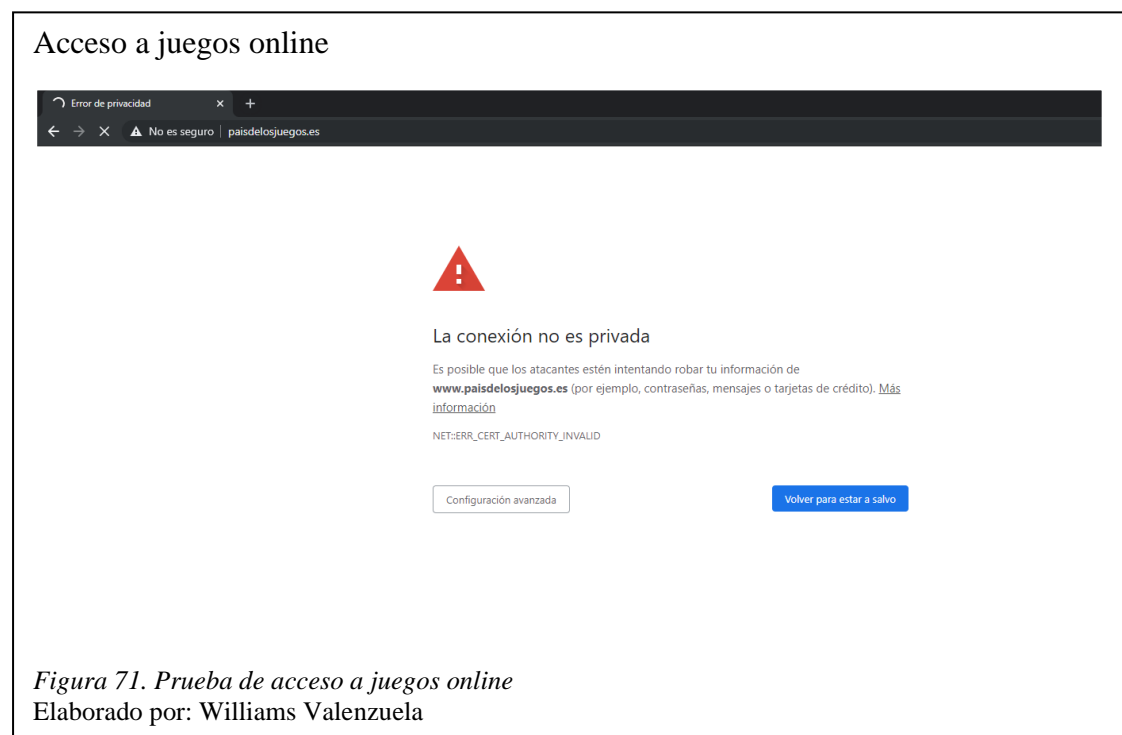
IP

192.168.2.220

Figura 70. IP de origen
Elaborado por: Williams Valenzuela

Para realizar las pruebas se ingresaron a una serie de páginas y sistemas que maneja la empresa con el fin de validar su correcto funcionamiento. Se accedió a páginas de redes sociales, juegos en línea, proxys online, etc.

Al abrir el navegador y tratar de acceder a páginas web a las cuales el perfil de gestor no permite el acceso se despliega el siguiente mensaje.



Al ingresar a páginas y sitios autorizados para el perfil de gestores el acceso es normal como se visualiza en la figura 73, donde al acceder a [sicceec.com.ec](#) la cual es una página informativa de la empresa, el acceso no se restringe al igual que al sistema que los gestores utilizan para realizar la cobranza de las diferentes carteras.

Acceso a siccec.com.ec



Figura 74. Prueba de acceso a siccec.com.ec
Elaborado por: Williams Valenzuela

Acceso a sistema de SICCEC

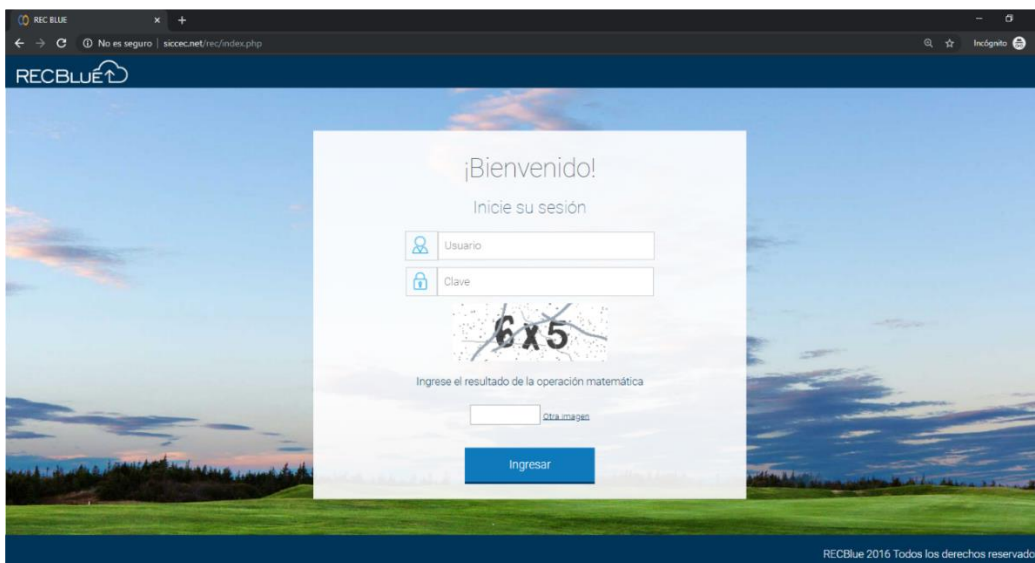


Figura 73. Prueba de acceso a sistema de SICCEC
Elaborado por: Williams Valenzuela

4.3.2. Perfil Sistemas.

El perfil de sistemas posee mínimas restricciones, ya que este necesita accesos para ofrecer la disponibilidad de los distintos sistemas que maneja la empresa, es por eso que se realizaron

pruebas de acceso a diferentes sitios de tal manera que se pueda validar la regla implementada.

La figura 75 muestra las personas del área de sistemas que pertenecen a dicho grupo.

Regla implementada para el perfil de Sistemas



Nombre de regla *

Prueba de perfil Sistemas

Descripción

Introducir Descripción

Acción

Aceptar Eliminar Rechazar

Origen

Zonas de origen *

LAN

Añadir nuevo elemento

Dispositivos y redes de origen *

Siccec - Darwin Tixi

Siccec - Geovanny Muñoz

Siccec - Fernando Pogo

Siccec - Luis Acosta

Siccec - Roberto Gallardo

Siccec - Williams valenzuela

Siccec - Gabriela Channon

Añadir nuevo elemento

Figura 75. Regla implementada para el perfil de Sistemas
Elaborado por: Williams Valenzuela

Al ser mínimas las restricciones al área de sistemas se realizaron pruebas de acceso a sitios de consulta cotidianos que utilizan estas personas como se visualiza en la figura 76, donde al acceder a paginas como GitHub o Facebook el acceso es exitoso sin ningún tipo de restricciones.

Acceso a GitHub

Why GitHub? Enterprise Explore Marketplace Pricing

Search GitHub Sign in Sign up

Built for developers

GitHub is a development platform inspired by the way you work. From **open source** to **business**, you can host and review code, manage projects, and build software alongside 40 million developers.

Username

Email

Password

Make sure it's at least 15 characters OR at least 8 characters including a number and a lowercase letter. [Learn more.](#)

Sign up for GitHub

By clicking "Sign up for GitHub", you agree to our [Terms of Service](#) and [Privacy Statement](#). We'll occasionally send you account related emails.

Figura 77. Prueba de acceso a GitHub
Elaborado por: Williams Valenzuela

Acceso a Facebook

facebook

Facebook te ayuda a comunicarte y compartir con las personas que forman parte de tu vida.

Correo electrónico o número de teléfono

Contraseña

Entrar

[¿Has olvidado los datos de la cuenta?](#)

o

Crear cuenta nueva

[Crea una página](#) para un personaje público, un grupo de música o un negocio.

Figura 76. Prueba de acceso a Facebook
Elaborado por: Williams Valenzuela

Las restricciones se dan si en algún caso alguna persona del departamento de sistemas intenta acceder a sitios no seguros o de dudosa procedencia, ya que la política implementada va

bloquear dichos sitios, ya que estas pueden tener algún tipo de malware por detrás que pueden poner en riesgo los activos de SICCEC.

4.3.3. Perfil Administrativos.

La figura 78 muestra la regla implementada de acuerdo a la política del perfil de administrativos, donde se visualiza el origen de la regla para realizar las pruebas de acceso a los diferentes sistemas y páginas web.

Regla implementada para el perfil de Administrativos

Nombre de regla *	Descripción
<input type="text" value="Prueba de perfil Administrativos"/>	<input type="text" value="Introducir Descripción"/>
Acción	
<input type="button" value="Aceptar"/> <input type="button" value="Eliminar"/> <input type="button" value="Rechazar"/>	
Origen	
Zonas de origen *	Dispositivos y redes de origen *
<input type="text" value="LAN"/> <input type="button" value="Añadir nuevo elemento"/>	<input type="text" value="Siccec - Williams valenzuela"/> <input type="button" value="Añadir nuevo elemento"/>

Figura 78. Regla implementada para el perfil de Administrativos
Elaborado por: Williams Valenzuela

IP de origen

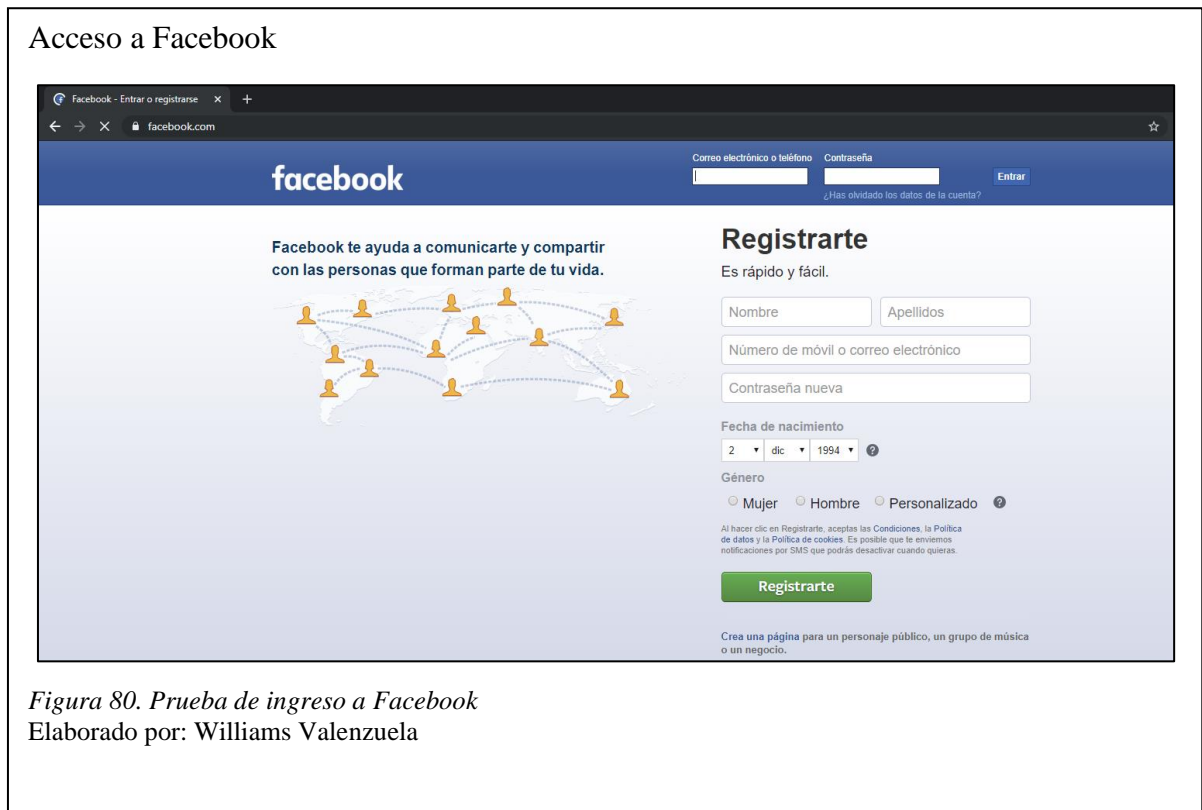
<input type="text" value="Siccec - Williams valenzuela"/>
IPv4
IP
<input type="text" value="192.168.2.220"/>

Figura 79. IP de origen
Elaborado por: Williams Valenzuela

Al ser un perfil al cual las restricciones son mínimas, se realizaron pruebas de acceso a diferentes sitios web, validando la correcta implementación de la regla de seguridad en el

firewall. Para realizar las pruebas se intentó acceder a redes sociales, páginas informativas, juegos en línea, sistemas de la empresa, etc.

La figura 80 muestra un sitio Web a la que el perfil de administrativo si posee acceso, como es Facebook, ya que por orden de gerencia las páginas de redes sociales entre otras no deben estar bloqueadas para dicho perfil.



Al intentar acceder a un sistema que maneja la empresa para realizar la cobranza de las diferentes carteras es exitoso, ya que por orden de gerencia este perfil debe tener acceso a todos los sistemas que maneja SICCEC con el fin de realizar presentaciones entre otros.

Prueba de ingreso a sistema de SICCEC



Figura 81. Prueba de ingreso a sistema de SICCEC
Elaborado por: Williams Valenzuela

Si el perfil de administrativo intenta acceder a sitios de juegos, páginas pornográficas o sitios de dudosa procedencia. La política implementada los va a bloquear, ya que son páginas que pueden tener algún tipo de malware por detrás que pueden poner en riesgo los activos de SICCEC.

Acceso a sitio de juegos

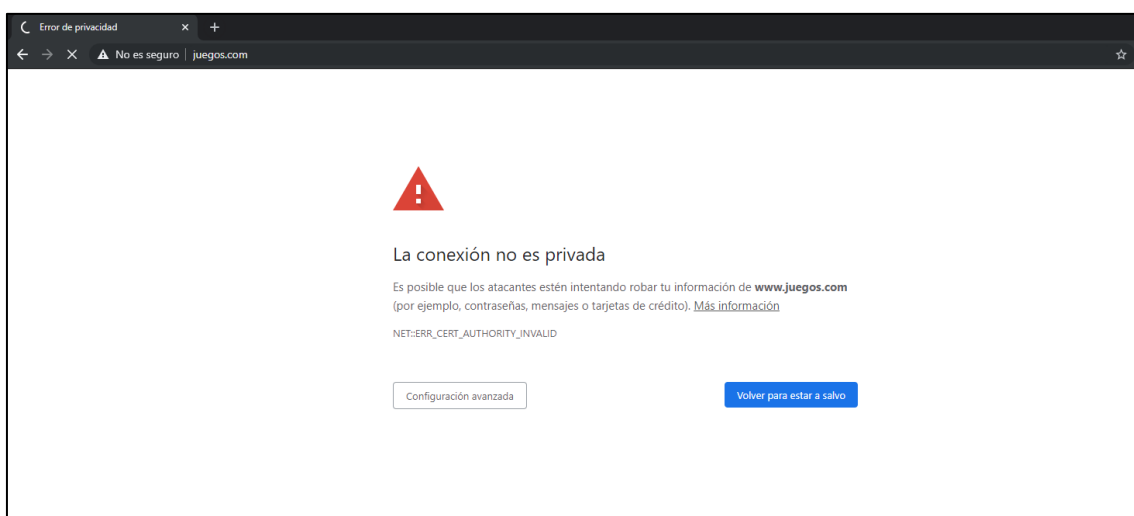


Figura 82. Prueba de ingreso a sitio de juegos
Elaborado por: Williams Valenzuela

Acceso a proxy online

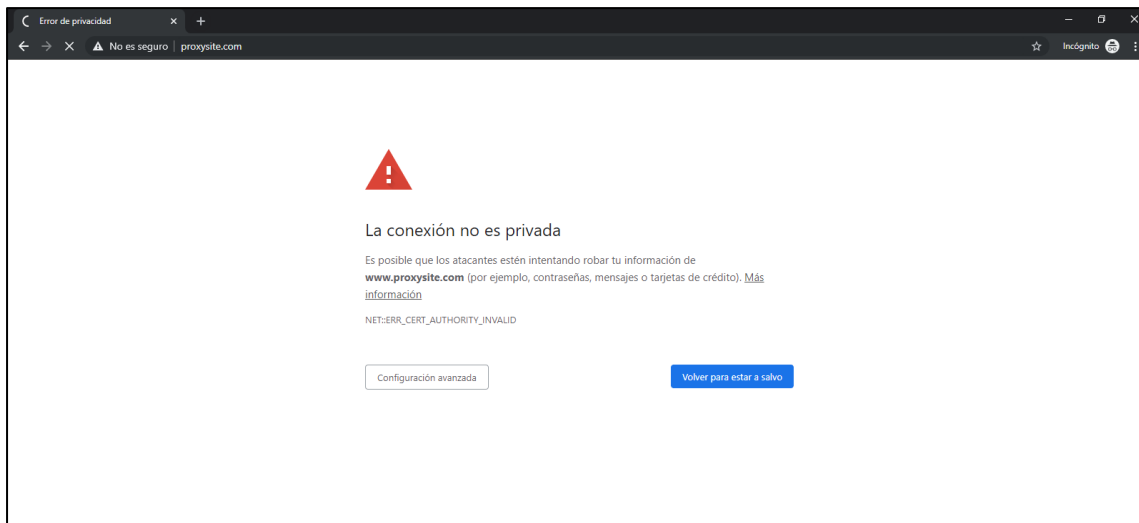
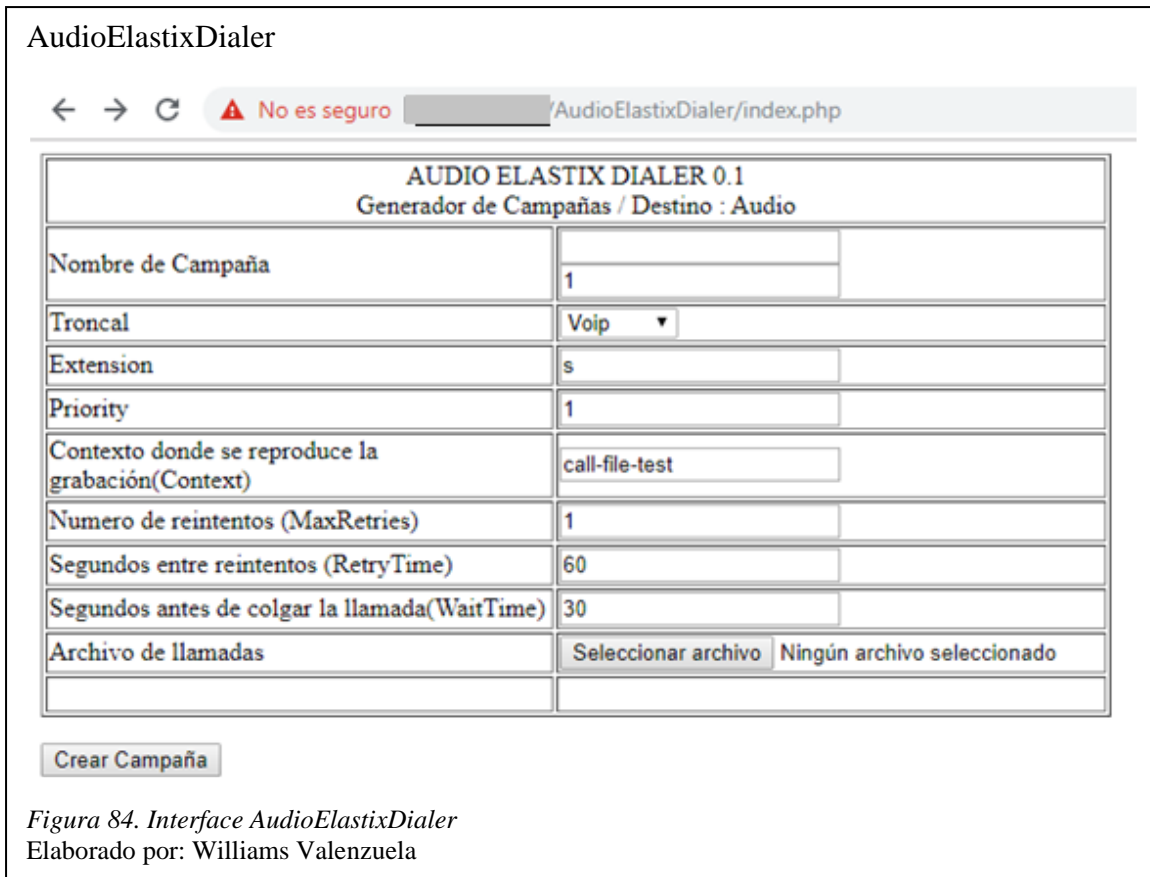


Figura 83. Prueba de acceso a proxy online
Elaborado por: Williams Valenzuela

4.4. Pruebas de IVR de llamadas automáticas

Para realizar pruebas del IVR de llamadas automáticas implementado en la nueva central telefónica Issabel PBX se accedió vía Web al siguiente link desde la red interna de SICCEC <https://xxx.xxx.xxx.xxx/AudioElastixDialer/index.php> donde se muestra la siguiente interface Web.



Se generaron campañas de ejemplo en donde se realizaron llamadas a un grupo de números en un archivo CSV, ya que el programa desarrollado en PHP se encarga de leer dicho archivo y generar las llamadas automáticas. El archivo debe tener dos parámetros los cuales son: número de teléfono y nombre del cliente, ya que el programa se encarga de leer estos datos y junto con los ingresados en la interface de usuario se insertan en la base de datos para luego realizar la llamada.

Archivo CSV

A	B
987906896	WILLIAMS VALENZUELA
984545669	Ejemplo1
963859674	Ejemplo2
986245862	Ejemplo3

Figura 85. Archivo CSV para generar llamadas
Elaborado por: Williams Valenzuela

4.4.1. Generar campaña de llamada automática.

Al llenar todos los campos en la interface como se visualiza en la figura 86 se debe seleccionar el archivo CSV previamente generado.

Generador de campañas automáticas

AUDIO ELASTIX DIALER 0.1 Generador de Campañas / Destino : Audio	
Nombre de Campaña	Prueba 21
Troncal	Voip ▼
Extension	outbound
Priority	1
Contexto donde se reproduce la grabación(Context)	call-file-test
Numero de reintentos (MaxRetries)	2
Segundos entre reintentos (RetryTime)	5
Segundos antes de colgar la llamada(WaitTime)	30
Cedente	BPAC ▼
Fecha ejecución:	2019/12/10
Archivo de llamadas	Seleccionar archivo Prueba IVR OK.csv
<input type="button" value="Crear Campaña"/>	

Figura 86. Generador de campañas automáticas
Elaborado por: Williams Valenzuela

En el archivo audioelastixdialer.php se encuentra la sentencia que se encarga ingresar los datos en la tabla calloutnumeros de la base de datos de AudioElastixDialer.

Inserción de datos en la BDD

```
while (($data = fgetcsv($handle, 1000, ",", "")) !== FALSE) {
    $num = count($data);
    $row++;
    //$cadena = "insert into calloutnumeros(numero,nombre) values(";
    $cadena = "insert into calloutnumeros(campana,telefono,nombre) values('".$nrocampana."','".$;
    //$cadena = "insert into calloutnumeros(campana,fejecucion,cedente,telefono,nombre,identi
    for ($c=0; $c < $num; $c++) {
        if ($c==($num-1))
            $cadena = $cadena."".$data[$c] . """;
        else
            $cadena = $cadena."".$data[$c] . ",";
    }
}
```

Figura 87. Sentencia de inserción de datos en la BDD
Elaborado por: Williams Valenzuela

Una vez creada la campaña los datos se ingresan a la base de datos, de la cual Issabel lee los registros ingresados y se procede a realizar las llamadas automáticamente. Se visualizan los datos ingresados en la tabla calloutcampana mediante la siguiente sentencia.

```
SELECT idcampana, nombre, tipo, troncal, audio, archivo, fechacreacion
FROM AudioElastixDialerBD.calloutcampana;
```

Campaña ingresada en la BDD

19	19	Prueba	2	2	call-file-test	Prueba IVR OK.cs	2019-12-10 00:00:00
20	20	prueba	2	2	call-file-test	Prueba IVR OK.cs	2019-12-10 00:00:00

Figura 88. Campaña ingresada en la BDD

Elaborado por: Williams Valenzuela

De igual manera se pueden visualizar los números a los cuales se realizaron las llamadas automáticamente en la tabla calloutnumeros mediante la siguiente sentencia.

```
SELECT id, campana, telefono, nombre
FROM AudioElastixDialerBD.calloutnumeros;
```

En la figura 89 se puede apreciar todas las llamadas de prueba realizadas.

Llamadas realizadas a la campaña generada

	123 id	ABC campana	123 telefono	ABC nombre
12	12	12	987,906,896	Williams Valenzuela
13	13	13	987,906,896	Williams Valenzuela
14	14	14	987,906,896	Williams Valenzuela
15	15	15	987,906,896	Williams Valenzuela
16	16	16	987,906,896	Williams Valenzuela
17	17	17	987,906,896	Williams Valenzuela
18	18	18	987,906,896	Williams Valenzuela
19	19	19	987,906,896	Williams Valenzuela
20	20	20	987,906,896	Williams Valenzuela
21	21	21	987,906,896	Williams Valenzuela
22	22	21	987,772,013	Pamela Ortiz

Figura 89. Llamadas realizadas de acuerdo a la campaña generada

Elaborado por: Williams Valenzuela

Para visualizar los pasos que se realiza en cada llamada al crear la campaña, se ingresó el comando asterisk -rvvvvvvvv para acceder a la CLI de Asterisk como se muestra en la figura 90.

CLI de Asterisk

```
[root@issabel ~]# asterisk -rvvvvvvvv
Asterisk 13.22.0, Copyright (C) 1999 - 2014, Digium, Inc. and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for detail
s.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
=====
Connected to Asterisk 13.22.0 currently running on issabel (pid = 2132)
issabel*CLI>
```

Figura 90. CLI de Asterisk
Elaborado por: Williams Valenzuela

Cuando se genera una nueva campaña en la consola de Asterisk se puede visualizar y monitorear las llamadas que la central está generando automáticamente como se muestra en la figura 91. Donde se visualiza las llamadas a los distintos números ingresados en el archivo CSV junto con el canal por el cual se está realizando la misma.

Registro de llamadas mediante CLI

```
-- Called 0987720138OpenVox102
== Using SIP RTP TOS bits 184
-- Using SIP RTP CoS mark 5
-- Called 0987906896OpenVox102
> 0x7f7390111470 -- Strict RTP learning after remote address set to: 192.
168.0.102:16900
-- SIP/OpenVox102-00000013 is making progress
> 0x7f73945e7d00 -- Strict RTP learning after remote address set to: 192.
168.0.102:16946
-- SIP/OpenVox102-00000014 is making progress
-- Remote UNIX connection
-- Remove UNIX connection disconnected
> 0x7f73945e7d00 -- Strict RTP learning after remote address set to: 192.
168.0.102:16946
-- SIP/OpenVox102-00000014 answered
-- Executing [outbound@call-file-test:1] NoOp("SIP/OpenVox102-00000014", "")
in new stack
-- Executing [outbound@call-file-test:2] WaitForSilence("SIP/OpenVox102-0000
0014", "2500") in new stack
-- Waiting 1 time(s) for 2500ms of silence with 0s timeout
> 0x7f73945e7d00 -- Strict RTP switching to RTP target address 192.168.0.
102:16946 as source
-- Exiting with 2500ms of silence >= 2500ms required
-- Executing [outbound@call-file-test:3] Playback("SIP/OpenVox102-00000014",
"es/ivrFACES") in new stack
-- <SIP/OpenVox102-00000014> Playing 'es/ivrFACES.slin' (language 'en')
> 0x7f73945e7d00 -- Strict RTP learning complete - Locking on source address 192.168.0.102:16946
> 0x7f7390111470 -- Strict RTP learning after remote address set to: 192.168.0.102:16900
-- SIP/OpenVox102-00000013 answered
-- Executing [outbound@call-file-test:1] NoOp("SIP/OpenVox102-00000013", "") in new stack
-- Executing [outbound@call-file-test:2] WaitForSilence("SIP/OpenVox102-00000013", "2500") in new stack
-- Waiting 1 time(s) for 2500ms of silence with 0s timeout
> 0x7f7390111470 -- Strict RTP switching to RTP target address 192.168.0.102:16900 as source
-- Exiting with 2500ms of silence >= 2500ms required
-- Executing [outbound@call-file-test:3] Playback("SIP/OpenVox102-00000013", "es/ivrFACES") in new stack
-- <SIP/OpenVox102-00000013> Playing 'es/ivrFACES.slin' (language 'en')
> 0x7f7390111470 -- Strict RTP learning complete - Locking on source address 192.168.0.102:16900
-- Executing [outbound@call-file-test:4] Hangup("SIP/OpenVox102-00000014", "") in new stack
-- Spawn extension (call-file-test, outbound, 4) exited non-zero on 'SIP/OpenVox102-00000014'
[2019-12-11 20:10:42] NOTICE[23392][C-00000010]: pbx_spool.c:460 attempt_thread: Call completed to SIP/0987906896OpenVox102
-- Executing [outbound@call-file-test:4] Hangup("SIP/OpenVox102-00000013", "") in new stack
[2019-12-11 20:10:51] NOTICE[23393][C-00000011]: pbx_spool.c:460 attempt_thread: Call completed to SIP/0987720138OpenVox102
issabel*CLI>
```

Figura 91. Registro de llamadas mediante CLI
Elaborado por: Williams Valenzuela

Lo que se busca con esta implementación es disminuir el tiempo que toma a varios gestores comunicarse con una serie de clientes, para recordarles que tienen una deuda pendiente, de tal manera que este proceso lo puede realizar un solo gestor generando una campaña automática de IVR.

4.5. Análisis de la solución propuesta de manera técnica y económica

La tabla 7 muestra el valor total, pagado cuando se adquirió el servidor, donde se implementó la plataforma de virtualización. A continuación, se muestran las características generales del mismo.

Tabla 7. Características de servidor para virtualizar

CARACTERÍSTICAS
Servidor HPE ProLiant DL360 Gen10 Intel Xeon-S 4114
Embedded 1Gb 4-port Ethernet Adapter
Fuente de poder HPE 500w flex Slot Platinum
4 discos duros SAS 10K SFF SC DS HDD 1,2 TB
4 memorias RAM 16gb
\$7.235.00

Elaborado por: Williams Valenzuela

En el desarrollo de la virtualización se implementaron tres máquinas virtuales con diferentes recursos de procesamiento como se visualiza en la tabla 3, donde se migraron los servicios más relevantes de la empresa.

A continuación, se analiza la propuesta de implementación para determinar el ahorro que genera la virtualización en SICCEC, donde se visualizan cotizaciones generales de servidores físicos que la empresa tendría que adquirir en caso de no implementar ambientes virtuales sobre un mismo hardware, por lo tanto, se muestran las características de cada servidor de acuerdo al servicio que necesita ser implementado junto con el precio estimado.

Tabla 8. Precio de servidores físicos de acuerdo al servicio

CARACTERÍSTICAS	SERVIDOR PARA LA BDD DE SICCEC	SERVIDOR PARA EL SERVICIO WEB DE SICCEC	SERVIDOR PARA LA CENTRAL TELEFÓNICA ISSABEL PBX
Marca	HPE 800075-S01	HPE ProLiant DL360 Gen10 3106 85	HPE ProLiant DL20 Gen9
Procesador	3.4 GHz Intel Xeon	Intel Xeon (8 núcleos, 1,7 GHz, 85 W)	Intel Xeon E3-1220
RAM		16 GB	8 GB
Disco Duro	SATA 1 TB	SATA 1 TB	SATA 1 TB
Descripción de la tarjeta de red	Embedded 1Gb 4-port Ethernet Adapter	Embedded 2-port Ethernet Adapter	Embedded 2-port Ethernet Adapter
Precio	\$4,295.00	\$2,211.00	\$1,110.00

Elaborado por: Williams Valenzuela

La tabla 8 muestra el precio estimado de cada servidor físico de acuerdo a los requerimientos del servicio de SICCEC, mientras que la tabla 9 muestra el costo total de la inversión en caso de que se decida adquirir un servidor para cada servicio.

Tabla 9. Costo total de servidores físicos

SERVICIO	COSTO
SERVIDOR PARA LA BDD DE SICCEC	\$4,295.00
SERVIDOR PARA EL SERVICIO WEB DE SICCEC	\$2,211.00
SERVIDOR PARA LA CENTRAL TELEFÓNICA ISSABEL PBX	\$1,110.00
RECURSOS PARA UN SERVICIO ADICIONAL	\$1,110.00
TOTAL	\$8,726.00

Elaborado por: Williams Valenzuela

La propuesta de implementación de ambientes virtuales como servicio sobre una misma plataforma es factible, ya que al utilizar un solo servidor físico la empresa ahorra un estimado de \$1,401.00. Además, con esta implementación optimiza recursos de mantenimiento, espacio, electricidad y operatividad al tener todos los ambientes centralizados con una correcta administración.

El análisis de la implementación del sistema que permite generar campañas automáticas de IVR sin duda es factible, ya que se tomó como ejemplo que diariamente se realizan 500 llamadas a los deudores solo con el fin de notificar sus deudas pendientes, asumiendo que cada llamada toma un tiempo de 2 minutos aproximadamente y que estas llamadas las generan 100 gestores telefónicos de la empresa. Por lo que cada gestor tiene que realizar 5 llamadas tomándole un tiempo de aproximadamente 10 minutos en completar estas.

Con la implementación del IVR automático el tiempo no es un problema, ya que la campaña automática la genera el supervisor con N número de deudores, donde los gestores ya no realizarían este trabajo, más bien aprovecharían el tiempo que se gasta en realizar las 5 llamadas en realizar gestiones de cobranza plenamente.

CONCLUSIONES

- El recolectar información del estado actual de la red junto con el análisis de los perfiles de usuario, ayudó a determinar las herramientas y reglas que fueron implementadas de acuerdo a los requerimientos de la empresa, con el fin de solucionar los inconvenientes de seguridad y mejorar la disponibilidad de los servicios.
- La implementación de la virtualización en el nuevo servidor de SICCEC fue bastante útil, ya que solucionó uno de los mayores inconvenientes al implementar uno o más servicios dentro de un mismo servidor físico, con una correcta administración de las máquinas virtuales, monitoreo constante y correcto manejo de recursos de procesamiento en una solución libre como es XenServer.
- La virtualización de la BDD de SICCEC favoreció en el aprovechamiento de los recursos del servidor, ya que al realizar las pruebas de la actualización de carteras el tiempo disminuyó considerablemente respecto a la BDD de producción. Sin embargo, se necesitó de la creación de índices en las tablas, ya que al poner el ambiente propuesto en producción los procedimientos aumentaron su tiempo de ejecución.
- Al transcurrir un mes de la implementación de Issabel PBX y la misma puesta en producción, la central telefónica abastece correctamente la gran demanda de llamadas telefónicas. Además, la migración de la central telefónica es un requerimiento que se lo realizó debido al soporte y continuidad que ofrece Issabel PBX, ya que es uno de los servicios más importantes que posee SICCEC de acuerdo al giro de negocio.
- Las reglas implementadas en el Firewall de la empresa ayudarán a tener un mejor control en cuanto a los accesos de cada perfil de usuario, ofreciendo seguridad en la red, optimizando recursos de ancho de banda y sobre todo responder a lo mencionado en las políticas de seguridad de SICCEC.

- La aplicación de parches de seguridad a los sistemas operativos reduce considerablemente el riesgo de recibir algún tipo de ataque informático, por lo cual los servidores deben ser sometidos a escaneos de vulnerabilidades continuos junto con la aplicación de Hardening a los mismos.
- La implementación de campañas de IVR automáticas ayuda en la recuperación de cartera, ya que permite la gestión automática hacia un grupo de clientes con el fin de recordar sus obligaciones de pago, ahorrando el tiempo que le toma a varios gestores realizar dicho trabajo diariamente.

RECOMENDACIONES

- La flexibilidad es una de las principales características de la virtualización, por lo tanto, se recomienda que una vez implementadas las máquinas virtuales se programen SnapShots automáticos, con el fin de tener una contingencia en caso de que exista algún error o desastre con las máquinas virtuales.
- Para obtener una base de datos óptima no solo se necesita de un servidor o máquina virtual con buenos recursos de procesamiento, sino que se recomienda implementar una base de datos bien estructurada, de tal manera que se puedan crear índices en las tablas, ya que estos ayudan a minorizar el tiempo de respuesta de las consultas.
- Se recomienda realizar un inventario de los principales activos tecnológicos de la empresa como servidores, infraestructura, aplicaciones, etc. Para luego realizar un escaneo de vulnerabilidades y pruebas de penetración sobre estos, con el fin de aplicar las medidas correctivas en base a los informes de vulnerabilidades encontradas y así reducir las amenazas considerablemente.
- La implementación de un generador de campañas de IVR automático sin duda ayuda a recordar a los clientes sus obligaciones de pago, sin embargo, se recomienda a futuro implementar sobre AudioElastixDialer un TTS (Text to Speech) la cual es una tecnología capaz de recibir un texto y reproducirlo con una voz artificial humana, con el fin de notificar a los clientes sus valores a pagar de forma personalizada.

REFERENCIAS

- Andrés, N., Juan, F., & Jonathan, M. (2013). *A review of agile methodologies for software development*. Obtenido de <https://www.redalyc.org/pdf/4962/496250736004.pdf>
- BONNET, N. (2014). *Windows Server 2012 R2 Las bases imprescindibles para administrar y configurar su servidor*. Obtenido de https://books.google.com.ec/books?hl=es&lr=&id=464Hd3t0CsIC&oi=fnd&pg=PA13&dq=querimientos+minimos+para+instalar+server+2012&ots=9RIh08EC2F&sig=2O2osvIhj9_iNPCKSvpKgVEhPMI#v=onepage&q=querimientos%20minimos%20para%20instalar%20server%202012&f=false
- Doña, J. (2010). *Virtualización de Servidores*. Obtenido de http://www.redtauros.com/Clases/Gestion_SO/Sistemas_paravirtuales.pdf
- Elastixtech. (2018). *DialPlan o Plan de Marcacion*. Obtenido de <http://elastixtech.com/dialplan-o-plan-de-marcacion/>
- Elastixtech. (2018). *ISSABEL PBX*. Obtenido de <http://elastixtech.com/que-es-issabelpbx/>
- Gabriel, L., Danny, G., & Julio, C. (2015). *Windows Server 2012 vulnerabilities and security*. Obtenido de <http://ingenieria.ute.edu.ec/enfoqueute/index.php/revista/article/view/67/71>
- García, E. (2017). *PROPUESTA PARA IMPLEMENTACIÓN DE UN SERVICIO DE TELEFONÍA IP PARA EL HOSPITAL DR. RAFAEL RODRÍGUEZ ZAMBRANO DE LA CIUDAD DE MANTA*. Obtenido de <http://repositorio.puce.edu.ec/bitstream/handle/22000/14126/CASO%20DE%20ESTUDIO%20FINAL%20-%20EDER%20GARCIA.pdf?sequence=1&isAllowed=y>
- Irma, C., & Nancy, C. (2013). *DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE ENTRENAMIENTO EN COMUNICACIONES CENTRALIZADAS BASADAS EN TECNOLOGÍA ELASTIX EN EL LABORATORIO DE COMUNICACIONES DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE EXTENSIÓN LATACUNGA*. Obtenido de <http://repositorio.espe.edu.ec/handle/21000/7111>
- Issabel. (2016). <https://www.issabel.com/>. Obtenido de <https://www.issabel.com/>
- Jácome, G. (2013). *IMPLEMENTACION DE UN SISTEMA IVR AUTOMATIZADO PARA LA ADMINISTRACIÓN DE CITAS PARA LOS TALLERES DE COMERCIAL HIDROBO*

- TOYOTA. Obtenido de <http://repositorio.utn.edu.ec/bitstream/123456789/1825/1/TESIS.pdf>
- José, C., Patricio, L., & Carmen, P. (2012). *Métodologías Ágiles en el Desarrollo de Software*. Obtenido de <http://roa.ult.edu.cu/bitstream/123456789/476/1/TodoAgil.pdf>
- Kelly, M., Javys, P., & Zúñiga, I. (2009). *Firewall – Linux: Una Solución De Seguridad Informática Para*. Obtenido de <https://www.redalyc.org/pdf/5537/553756879003.pdf>
- Landivar, E. (2009). *Comunicaciones unificadas con Elastix*. Obtenido de https://s3.amazonaws.com/academia.edu.documents/35593728/Comunicaciones_Unificadas_con_Elastix_Volumen_1_29Mar2009.pdf?AWSAccessKeyId=AKIAIWOWY YGZ2Y53UL3A&Expires=1556597375&Signature=511dAh39tRhGDdeILdzULt4GBiU%3D&response-content-disposition=inline%3B%2
- Lara, A. (2011). *ESTUDIO E IMPLEMENTACIÓN DE LA TÉCNICO DE VIRTUALIZACIÓN EN LA DIRECCIÓN CENTRAL DE SERVICIOS COMPUTACIONALES, UTFSM*. Obtenido de <http://telematica.usm.cl/telematica/site/artic/20121008/asocfile/20121008171131/laraalejandro.pdf>
- Llumiquinga, D. (2012). *análisis, diseño y construcción de un portal web de gestion comercial para la empresa farmacored integrando herramientas de voip sobre elastix*. Obtenido de <https://dspace.ups.edu.ec/bitstream/123456789/3535/1/UPS-ST000779.pdf>
- Mariana, M. (2015). *EL PHISHING*. Obtenido de http://repositori.uji.es/xmlui/bitstream/handle/10234/127507/TFG_Leguizam%C3%B3n_Mayra.pdf?sequence=1&isAllowed=y
- Martin. (17 de 09 de 2014). *WinSCP*. Obtenido de <https://winscp.net/eng/docs/lang:es#caracteristicas>
- Mena, E. (2009). *DISEÑO E IMPLEMENTACIÓN DE UN IVR BASADO EN CÓDIGO LIBRE ORIENTADO A TRONCALES SIP E INTERACTUANDO CONTRA BASES DE DATOS MySQL*. Obtenido de <http://repositorio.espe.edu.ec/bitstream/21000/193/1/T-ESPE-026219.pdf>
- Mero, J., & Gallegos, H. (2015). *La edición gratuita de XenServer comienza con un hipervisor de 64 bits y una gestión centralizada, migración en vivo y herramientas de conversión*

- para crear una plataforma virtual que maximice el rendimiento y la densidad del cliente.* Obtenido de <https://dspace.ups.edu.ec/bitstream/123456789/10324/1/UPS-GT001232.pdf>
- Microsoft. (10 de 02 de 2019). *Indices agrupados y no agrupados descritos.* Obtenido de <https://docs.microsoft.com/es-es/sql/relational-databases/indexes/clustered-and-nonclustered-indexes-described?view=sql-server-ver15>
- Moposita, P. (2012). *"MEDIDAS DE PROTECCIÓN INFORMÁTICA PARA EVITAR EL ROBO DE de identidad provocado por el Ataque Phishing "The Tabnabbing Attack" para la Facultad de Ingeniería en Sistemas Electrónica e Industrial.* Obtenido de <http://repositorio.uta.edu.ec/handle/123456789/2378>
- NIST. (2015). *National Vulnerability Database.* Obtenido de <http://web.nvd.nist.gov/view/vuln/search-advanced>
- Obando, G. (2009). *ESTUDIO DE IVR (RESPUESTA INTERACTIVA DE VOZ) CON.* Obtenido de <http://repositorio.utn.edu.ec/bitstream/123456789/607/1/Tesis%20de%20Grado.pdf>
- Oliva, J. (2013). *Sistema de llamadas desatendidas para Elastix – AudioElastixdialer 0.1.* Obtenido de <https://jroliva.net/2013/06/13/sistema-de-llamadas-desatendidas-para-elastix-audioelastixdialer-0-1/>
- Paola Noreña, S. R. (2018). *PROTECTION TECHNIQUE FOR AUTHENTICATION CREDENTIALS ON SOCIAL NETWORKS AND EMAIL FROM PHISHING ATTACKS.* Obtenido de <http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/2960/3014>
- Principado, S. d. (2015). *Qué Es La Virtualización y Cuáles Son Sus Beneficios.* Obtenido de <http://sistemasdeoficinadelprincipado.blogspot.com/2015/06/que-es-la-virtualizacion-y-cuales-son.html>
- Quispe, H. (2014). *VIRTUALIZACIÓN EN LOS CENTROS DE DATOS.* Obtenido de <http://dspace.unitru.edu.pe/bitstream/handle/UNITRU/2419/QUISPE%20GANOZA%20HECTOR%20JAVIER%20.pdf?sequence=1&isAllowed=y>
- SICCEC. (2009). *Servicio Integral de Créditos y Cobranzas.* Obtenido de <http://www.siccec.com.ec/>

- Smyth, D. (2017). *Smyth SysIT Consulting*. Obtenido de <https://www.smythsys.es/8690/elastix- parece-haber-muerto-desgraciadamente-nacen-issabel-openelx/>
- Sophos. (2012). *Sophos Essential*. Obtenido de <https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophosessentialnetworkfirewallldsna.pdf>
- Velasquez, P. (2004). *DISEÑO E IMPLEMENTACIÓN DE SISTEMA*. Obtenido de <http://cybertesis.uach.cl/tesis/uach/2004/bmfciv434d/sources/bmfciv434d.pdf>
- William, A., Randolph, W., Sven, A., & Mindy, C. (2018). *SQL Server 2017 Administration*. Obtenido de https://books.google.com.ec/books?id=eJdNDwAAQBAJ&pg=PT28&dq=introducing+microsoft+sql+server+2017&hl=es&sa=X&ved=0ahUKEwizx_GhtOfiAhVtuVkkHRBxBjsQ6AEIKjAA#v=snippet&q=system%20requirements&f=false
- Yépez, J. (2018). *HARDENING Y ALTA DISPONIBILIDAD EN SISTEMAS TELEFÓNICOS*. Obtenido de <http://repositorio.ug.edu.ec/bitstream/redug/27904/1/B-CINT-PTG-N.283%20Y%c3%a9pez%20Jim%c3%a9nez%20Jes%c3%bas%20Armando.pdf>