

UNIVERSIDAD DE LAS CIENCIAS INFORMÁTICAS

Facultad 1

Centro de Software Libre



“Estrategia para la migración de servicios de correo electrónico en Cuba”

Presentado en opción al título de Máster en Informática Aplicada.

Autor

Ing. Amaury Viera Hernández

Tutor

MSc. Iván Pérez Mallea

La Habana. Diciembre de 2014.

“Año 56 de la Revolución”

Declaración de autoría

Yo, Amaury Viera Hernández, con carné de identidad 85062613305, declaro que soy el autor del trabajo “Estrategia para la migración del servicio de correo electrónico en Cuba” para optar por el título de Máster en Informática Aplicada.

Este trabajo fue desarrollado durante el período 2012 - 2014 en colaboración con mis colegas de equipo Yadiel Pérez Villazón, Yasiel Pérez Villazón y Jesús Castañeda Valdés, quienes me reconocen la autoría de los resultados expuestos en el mismo.

Autorizo a la Universidad de las Ciencias Informáticas a hacer el uso que estime pertinente de los resultados aquí presentados, como propietaria de los derechos legales de este proyecto.

Finalmente declaro que todo lo anteriormente expuesto se ajusta a la verdad, y asumo la total responsabilidad moral y jurídica que se derive de este juramento profesional.

Y para que así conste, firmo la presente declaración jurada de autoría en La Habana a los 18 días del mes de diciembre del año 2014.

Ing. Amaury Viera Hernández
Autor

MSc. Iván Pérez Mallea
Tutor

Agradecimientos

En especial a mi amigo y tutor Mallea.

A Miguel Jaeger Rodríguez Lazo, Yoandy Pérez Villazón, Mideisy Trevejo Guevara, Grettel Barrio Marshall, Yurenia Hernández Blanco, Eduardo Alejandro Cuesta LLanes, Yadiel Pérez Villazón, Yasiel Pérez Villazón y Jesús Castañeda Valdés por sus constantes consejos y ayudas.

A mi madre por formarme cada segundo de mi vida.

A todos mis amigos y compañeros de trabajo del departamento SIMAYS del centro CESOL de la UCI. Sin ustedes hubiera sido mucho más difícil.

Dedicatoria

A mi padre: Todos los días de mi vida te recuerdo.

A la mujer más bella del mundo, mi madre.

Al departamento SIMAYS del centro CESOL de la UCI: Son muchos años aprendiendo entre todos y dando lo mejor de cada uno; entre comandos, errores y lenguajes. Ahí he pasado los mejores años de mi vida estudiantil y profesional.

Resumen

A través de esta investigación se presentó una estrategia para la migración de los servicios de correo electrónico en las instituciones cubanas. La misma cuenta con 13 etapas, donde se especifica el orden de realización de cada una de ellas. Varias etapas de la estrategia fueron automatizadas en una aplicación informática. La estrategia planteada y la automatización de varias de sus etapas, permiten el ahorro de tiempo durante la implantación de un servicio de correo electrónico en una institución, evitando los tiempos de caída de los servicios y aumentando la calidad con que se brindan los mismos. También se contribuye a la adaptación de las tecnologías libres implantadas durante la ejecución de los proyectos de migración de servicios de correo electrónico a las condiciones tecnológicas existentes en las entidades, permitiendo que se aprovechen los recursos existentes. La solución propuesta fue validada mediante la ejecución de dos proyectos de migración de los servicios de correo electrónico ejecutados por el departamento “Servicios Integrales de Migración, Asesoría y Soporte” del Centro de Software Libre de la Universidad de las Ciencias Informáticas durante el período comprendido entre los meses de marzo y octubre del 2014.

Índice

Introducción.....	1
CAPÍTULO 1	8
1.1. Servicio de correo sobre <i>Windows</i>	8
1.2. Servidor de correo <i>MDaemon</i>	9
1.3. Tecnologías asociadas a los servicios de correo electrónico	11
1.4. Agentes de transferencia de correo (MTA)	11
1.5. Agentes de entrega de correo (MDA)	14
1.6. Clientes web a utilizar como MUA.....	16
1.7. Filtrado de correos spam	19
1.8. Herramientas para antivirus.....	21
1.9. Técnica utilizada para la selección de las herramientas investigadas	22
1.10. Comparación entre las herramientas investigadas	24
1.11. Resultados sobre las tecnologías investigadas	26
1.12. Tecnologías adicionales a utilizar en los servicios de correo electrónico ...	26
1.13. Estrategias de migración de los servicios de correo electrónico	29
1.14. Conclusiones del capítulo	33
CAPÍTULO 2	34
2.1. Fundamentación de las etapas de la estrategia de migración	36
2.2. Propuesta de automatización de la estrategia para la migración del servicio de correo electrónico	50
2.3. Conclusiones del capítulo	53
CAPÍTULO 3	54
3.1. Misión de ambas empresas.....	54
3.2. Objetivos estratégicos de ambas empresas	54
3.3. Términos utilizados	54
3.4. Información sobre los servicios de correo brindados en ambas empresas ...	55
3.5. Servicios de correo brindados en la ECOAIND3	57
3.6. Comparación de los resultados de las pruebas realizadas a ambas empresas	58
3.7. Conclusiones del capítulo	59
Conclusiones	60
Recomendaciones	61
Referencias Bibliográficas	62
Anexos	66

Introducción

Los servicios telemáticos están presentes en la mayoría de las organizaciones, y en muchos casos son de importancia estratégica para las mismas. Actualmente, a nivel mundial existe un gran número de empresas que brindan estos servicios sobre sistemas operativos de la familia Microsoft Windows; sin embargo para muchas de estas, la migración hacia plataformas GNU/Linux es de suma importancia, debido a un amplio conjunto de características como la reducción de los costos de licencias, tanto por el sistema operativo instalado como por las aplicaciones que se ejecutan en el mismo, el poder alcanzar una alta disponibilidad y tiempo efectivo de funcionamiento, el aseguramiento de una mayor estabilidad, fiabilidad, seguridad, entre otros.

Debido a que se tiene acceso al código fuente de las aplicaciones, se garantiza la soberanía tecnológica, previniéndose el quedar atrapado en un proveedor privativo y facilitándose el diseñar y construir exactamente lo que los clientes necesitan, logrando una alta interoperabilidad y conformidad con estándares abiertos.

Según investigaciones de la *Evans Data Corporation*¹, un 90% de los sistemas GNU/Linux nunca ha sido infectado por virus, y el 78% de los sistemas GNU/Linux nunca ha sido violado por usuarios en la red, algo que demuestra la confiabilidad de estas plataformas (EVANS DATA, 2004).

A nivel global en toda la empresa, tanto por el personal administrativo, como los empleados, debe observarse y traducirse el cambio hacia una nueva plataforma en un mejor control de los procesos de negocio, donde se logrará mantener o incluso aumentar el cumplimiento de los objetivos de la institución, con un mayor rendimiento y reducción de los tiempos de caída de servicios, potenciándose la innovación y aumentando las ventajas competitivas, mejorando de esta forma la seguridad y las relaciones entre los clientes, así como la facilidad de adaptación de las tecnologías a las necesidades de la empresa.

Frente a esto, una de las soluciones recurrentes es la migración de los sistemas operativos, servicios y aplicaciones que se encuentran instalados en las empresas hacia otros nuevos que abarquen los requerimientos actuales, comprendiendo además, que en los cambios realizados puedan surgir nuevos requerimientos y permitiendo la incorporación de nuevas tecnologías en el momento en que sea necesario.

¹ Firma de investigaciones de mercado sobre el desarrollo de *software*.

Actualmente se hace mucho más complicado diseñar soluciones para el cambio de plataformas en ambientes de producción, debido a que en la actualidad, los sistemas tienen que estar funcionando prácticamente las 24 horas, por lo que la solución más viable no sería realizar grandes cambios teniendo en cuenta sólo los horarios donde posiblemente el flujo de trabajo sea menor, pues de esta forma se estarían obviando varias variables que de no ser tenidas en cuenta, podrían provocar que determinada información se pierda, o que algún servicio deje de funcionar durante algún tiempo, lo cual atrasaría determinados procesos que no se podrían ejecutar en el momento deseado o necesitado, disminuyendo los ingresos e incidiendo en la reputación de la empresa y atentando contra el éxito de la migración (IBM, 2007).

Cabe señalar, que antes de decidirse a comenzar una migración de los servicios en una empresa, los directivos deben estar impulsados por varios motivos fuertes, que de estar bien claros, de acuerdo a investigaciones previas, permitirán que se logre con éxito todo lo planeado. Entre ellos pueden mencionarse motivos de negocio, análisis de costo y beneficio realizados exhaustivamente, requisitos de seguridad o no menos importante, la reducción de costos.

Algo importante a destacar, es que estas decisiones nunca deben estar motivadas solamente por ideas, como por ejemplo, es gratis o libre de virus y que además señala Stefan Werden, líder del equipo de arquitectura de SUSE Novell en Europa, Medio Oriente y África, cuando afirma (traducido del inglés): “Vas a fracasar si comienzas una migración impulsado por el lado filosófico” (KAREN D, 2004).

A nivel mundial existe una gran cantidad de empresas que brindan herramientas y servicios para la puesta en marcha de una infraestructura de servicios sobre plataformas GNU/Linux, pero la escasa comunicación de un país como Cuba con estas agencias, bloqueado por leyes que impiden el comercio con muchas de estas empresas y principalmente por los altos costos que implicaría contratar estos servicios no sería conveniente utilizarlos.

Para comenzar la migración de los servicios que se ejecutan en los servidores en una organización, es necesario tener como premisa, que el cambio de plataforma aunque no será totalmente transparente al usuario, debe intentarse que lo sea en lo mayor posible y sin pérdidas de información. Esto permitirá ahorrar bastante tiempo a cada usuario o trabajador, lo cual puede traducirse también en disminución de costos durante la migración del servicio, pues las personas que le den uso a los sistemas, tendrán que conocer o investigar lo menos posible sobre la nueva forma de acceder a la información que necesitan.

Específicamente en Cuba, en muchas de las instituciones se brindan los servicios telemáticos principales sobre plataformas privativas de la familia de sistemas operativos Microsoft Windows, de los cuales muchos son copias ilegales que no han sido pagadas a esta gran multinacional, debido a que el bloqueo impuesto por los Estados Unidos impide comerciar con la Microsoft, empresa proveedora y desarrolladora de estos sistemas operativos.

Es necesario tener en cuenta que si en algún momento Cuba tiene que pagar por cada una de estas copias, muchos de los organismos pueden verse inmersos en una gran deuda, sin mencionar el riesgo diario que existe de que estos sistemas operativos envíen información sobre las aplicaciones instaladas en los mismos, así como el uso que se les da, invadiendo la información personal de los usuarios, de lo cual Windows 8, una de las últimas versiones de estos sistemas, no está exento y ha sido planteado en varias ocasiones por Richard Stallman, presidente de la *Free Software Foundation* (FSF) en múltiples conferencias y en la dirección web oficial de la FSF (FSF, 2012).

Como estrategia a la situación planteada anteriormente, en el año 2004 y por consenso del Consejo de Ministros de la República de Cuba se anuncia el acuerdo 084, el cual orienta una migración paulatina de los Organismos de la Administración Central del Estado cubano hacia aplicaciones de *software* libre y código abierto.

Desde el año 2005, en la Universidad de las Ciencias Informáticas, específicamente en la antigua Facultad 10, actual Facultad 1, se viene trabajando sobre la investigación de herramientas y soluciones para realizar la migración de entornos sobre Microsoft Windows hacia plataformas GNU/Linux. En este sentido se han logrado identificar las principales estrategias durante la migración de estos entornos, habiéndose creado una Guía de migración a *Software* Libre, que define un procedimiento para la migración hacia *Software* Libre en los OACE, aunque aún no brinda soluciones lo suficientemente prácticas para la migración de los servicios telemáticos desde plataformas *Microsoft Windows Server*.

Debido a que el departamento Servicios Integrales de Migración, Asesoría y Soporte (SIMAYS) del Centro de Software Libre (CESOL) tiene como misión principal brindar servicios y desarrollar aplicaciones de apoyo a la migración, es que se han investigado y probado diferentes alternativas en el área de los servicios telemáticos que permiten realizar el cambio de plataforma de los servicios de una institución. Así mismo se han ideado soluciones basadas en tecnologías existentes y adaptado a los requerimientos necesarios, así como construido determinadas herramientas e identificado otras que pueden ser de gran utilidad para realizar la migración de varios servicios telemáticos,

pero se ha detectado que la gran cantidad de escenarios existentes, herramientas con propósitos diferentes, así como las características propias de los entornos en las instituciones cubanas hacen mucho más complicado tanto la migración de los servicios telemáticos, como el mantenimiento de los mismos una vez migrados.

Dentro de los servicios telemáticos, los asociados al servicio de correo electrónico juegan un papel crucial ya que los mismos se han convertido en uno de los principales medios de comunicación para la mayoría de las organizaciones y constituyen una de las herramientas de comunicación de las que los usuarios menos pueden prescindir.

Puesto que el correo electrónico en las empresas se utiliza constantemente, durante el horario laboral y en ocasiones cuando los empleados están en su casa, debe permanecer disponible en todo momento, sin importar la hora o el día de la semana del que se trate. Un tiempo de inactividad de incluso 30 minutos puede ocasionar consecuencias graves para la productividad de los empleados y los ingresos de las instituciones, por no mencionar incidentes de tiempo de inactividad que pueden durar días o semanas debido a inconvenientes graves que pueden presentarse, por ejemplo, problemas de telecomunicaciones o de red de área extensa que pueden hacer que los sistemas de correo electrónico se desactiven tan rápidamente como los problemas internos (TECHNET, 2005).

En muchos de los organismos en Cuba se utilizan servicios de correo electrónico como una de las vías principales para la comunicación, el cual constituye uno de los servicios que requiere especial atención cuando se necesita cambiar hacia las plataformas GNU/Linux, por las razones que se mencionan a continuación:

- Los servicios de correo electrónico en muchas de las instituciones cubanas cuentan con características específicas debido a las limitaciones de ancho de banda y *hardware* existentes en el país.
- La gestión de los servicios de correo sobre los sistemas operativos GNU/Linux en las instituciones cubanas resulta compleja, pues muchas veces se hace necesario la introducción de comandos en consola y cambios en los ficheros de configuración de los servicios.
- Se necesitan migrar grandes volúmenes de datos desde las plataformas *Windows Server* hacia GNU/Linux.

Según las condiciones planteadas anteriormente es necesario tener en cuenta que aunque existen algunas herramientas que permiten la gestión de los servicios de correo en los sistemas operativos GNU/Linux y varias realizan la instalación y

configuración de estos, permitiendo la gestión de los mismos una vez instalados y configurados, una de las dificultades que existen es que estas no han sido diseñadas teniendo en cuenta las características que actualmente existen en muchas de las instituciones cubanas, pues mientras en países como Australia, Bangladesh, Reino Unido, Italia o Estados Unidos, las personas pueden acceder a un servicio de alta velocidad (DSL²) con una transferencia directa de hasta 24 Mbps y en otros como Noruega o Japón, por ejemplo, algunos usuarios tienen conexiones de fibra óptica tan rápidas que sobrepasan los 100 Mbps, Cuba apenas tiene autorizados, vía satélite, para Internet 65 Mbps de ancho de banda para la salida y 124 Mbps para la entrada (JUVENTUD REBELDE, 2006).

Este es uno de los motivos por los cuales, en muchos casos para enviar los correos en las instituciones cubanas se hace necesario la utilización de servicios de correos que brinden la posibilidad de hacer envíos hacia otros servidores de correos, de esta forma los organismos no tienen la necesidad de contar con una conexión directa. Así mismo, se brindan servicios de almacenamiento remoto de buzones de correos electrónicos, los cuales son lugares donde los servicios de correo comparten buzones remotos, que son descargados por los diferentes servidores de correo que utilizan estos servicios sin necesidad de contar con una conexión hacia Internet. También se hace necesario determinadas restricciones de envío de correos por dominios, entre otras, que no solo permiten un ahorro del canal de navegación, sino que posibilitan la configuración del servicio para lograr bajos consumos de recursos, pues en muchas instituciones se utilizan computadoras convencionales con bajas prestaciones de *hardware* para brindar servicios en la red.

Las condiciones explicadas anteriormente hacen que las herramientas existentes se queden muy por debajo de las necesidades actuales en los organismos cubanos, por lo que para utilizarlas se hace necesario la introducción de muchos comandos en consola y configuraciones en los servicios de correo electrónico para lograr los propósitos deseados, de tal forma que a los administradores de sistemas se les hace muy difícil la gestión de los mismos utilizando sistemas operativos GNU/Linux.

Para la migración de los servicios de correo, actualmente hay varias vías, una de ellas, es manual, lo cual es extremadamente engorroso e inseguro debido a los grandes volúmenes de datos que son necesarios transferir desde una plataforma hacia otra. Existen herramientas en modo consola, que hacen difícil el manejo de la migración de los datos y no comprenden aspectos importantes como listas de contacto, así como

² *Digital Subscriber Line* (Línea de abonado digital)

algunas que permiten la migración, pero mediante el pago del servicio a compañías extranjeras, lo cual no es viable actualmente para nuestro país. También existen herramientas que pudieran ser utilizadas, pero requieren de un alto consumo de recursos y no se pueden descargar desde las direcciones de Internet asignadas a Cuba, lo que imposibilitaría el acceso a sus actualizaciones, siendo poco viable utilizar estas alternativas en la actualidad.

Ante tal situación se plantea el siguiente **problema científico**:

¿Cómo garantizar la migración de los servicios de correo electrónico hacia GNU/Linux en las instituciones cubanas, de forma que se reduzca el tiempo y se garantice el rendimiento teniendo en cuenta las condiciones tecnológicas del país?

El **objetivo general** de este trabajo se centra en **la obtención de una estrategia que permita la migración de los servicios de correo electrónico hacia sistemas GNU/Linux, reduciendo el tiempo y garantizando el rendimiento de acuerdo a las condiciones tecnológicas del país.**

Para cumplir el objetivo general de la investigación se trazaron los siguientes **objetivos específicos** que se exponen a continuación:

- Fundamentar aspectos teóricos conceptuales de las soluciones, estrategias y herramientas para la gestión y migración de los servicios de correo electrónico.
- Obtener una estrategia que permita la gestión y migración de los servicios de correo electrónico desde plataformas Windows hacia sistemas GNU/Linux.
- Desarrollar una herramienta que permita la gestión y migración de los servicios de correo electrónico.
- Validar la propuesta de solución.

De esta forma se determinó como **objeto de estudio**: **el área de los servicios telemáticos** y como **campo de acción**: **los servicios de correo electrónico.**

Como **hipótesis** de la investigación se plantea que: **el desarrollo de una estrategia que permita migrar los servicios de correo electrónico hacia sistemas GNU/Linux, que tenga en cuenta las condiciones tecnológicas en Cuba, reducirá el tiempo utilizado en la migración y garantizará el rendimiento.**

La investigación realizada como parte del trabajo se sustenta en el empleo de los **métodos científicos siguientes**:

Análisis Histórico - Lógico: se utilizó para determinar los antecedentes históricos

relacionados con los servicios de correo, así como las herramientas para la gestión y migración de los mismos.

Analítico - Sintético: se utiliza en la investigación de los servicios de correo, así como las herramientas y tecnologías para la gestión y migración de los servicios de correo electrónico. Ayuda a escoger los más apropiados para utilizarlos en el desarrollo de la aplicación propuesta.

Inductivo Deductivo: teniendo en cuenta el funcionamiento de los servicios de correo y las necesidades para realizar la migración de estos en Cuba, se evalúa la problemática existente, para determinar aspectos particulares y desarrollar una propuesta de solución.

Hipotético Deductivo: se utiliza para el análisis de la información derivada del uso de otros métodos y de los componentes que conforman el objeto de investigación. Se utiliza en la definición de la hipótesis para arribar a conclusiones mediante el uso de procedimientos deductivos.

Observación: mediante este método se puede conocer la manera en que se llevan a cabo los servicios de correo electrónico en Cuba. De esta forma se identifican las necesidades y se valoran los distintos flujos de trabajos en los que se encuentra inmerso el proceso a mejorar.

El **principal aporte** asociado a esta investigación viene dado por la obtención de una estrategia para la gestión y migración de los servicios de correo electrónico hacia GNU/Linux en los organismos cubanos materializada en una herramienta informática.

Para mostrar el desarrollo de la investigación y los resultados, el trabajo se ha estructurado en 3 capítulos, además de las Conclusiones, Recomendaciones, Referencias Bibliográficas y Anexos.

En el primer capítulo, se realiza un análisis del estado del arte referente a la migración de los servicios de correo electrónico, así como las principales soluciones, estrategias y herramientas para este fin.

En el segundo capítulo, se traza la estrategia que permitirá la gestión y migración de los servicios de correo electrónico en las instituciones cubanas y se realiza la propuesta de automatización de varias etapas de la misma en una herramienta.

En el tercer capítulo se realiza la valoración del sistema propuesto mediante la evaluación de dos casos de estudio, uno donde se realizó la documentación de un proceso de migración de los servicios de correo electrónico sin haber aplicado una estrategia y el otro mediante la utilización de la estrategia investigada.

CAPÍTULO 1

SERVICIOS DE CORREO ELECTRÓNICO

Los servicios de correo electrónico constituyen uno de los servicios proporcionados en Internet y a nivel empresarial que más auge han presentado en los últimos tiempos, incluso se consideran uno de los factores que han popularizado el uso de Internet. Ideados sobre la típica arquitectura cliente-servidor son utilizados para la transferencia de mensajes de forma rápida y eficiente. Algo importante a destacar es que no constituyen simplemente un programa cliente que se comunica con un servidor mediante un protocolo de aplicación, sino que están compuestos por varios subsistemas, cada uno con una funcionalidad determinada que interaccionan entre sí mediante distintos protocolos de aplicación (ADMIN S. O., 2013). A menudo realizan diferentes funciones según sea el uso que se les planifique (ECURED, 2013). Esto unido a la gran cantidad de tecnologías o subsistemas que son necesarios utilizar para lograr un funcionamiento adecuado, de acuerdo al uso que se necesite de los mismos hace que la gestión y administración sea una tarea de vital importancia durante su utilización.

1.1. Servicio de correo sobre *Windows*

A continuación se hará una investigación sobre uno de los principales servicios de correo para plataformas *Windows* utilizado en los organismos cubanos. Su utilización ha sido detectada por el equipo de migración del departamento Servicios Integrales de Migración, Asesoría y Soporte del Centro de Software Libre de la Universidad de las Ciencias Informáticas. Es necesario destacar que aunque existen varios servicios de correo, en esta investigación se hará referencia al *MDaemon*, debido a que las soluciones homólogas encontradas para plataformas libres son compatibles con todos, ya que los protocolos utilizados son los mismos generalmente. El objetivo principal es identificar las funcionalidades que presenta, teniendo en cuenta cuales de ellas son las más utilizadas en las instituciones cubanas. Esto permitirá evaluar la solución que cumpliendo con los mismos requisitos permite sobre plataformas GNU/Linux la migración de los datos necesarios.

1.2. Servidor de correo *MDaemon*

El Servidor de Mensajería *MDaemon* está disponible en tres versiones: *MDaemon Standard*, *PRO*, y *FREE*. Con las potentes funcionalidades de *MDaemon Standard*, se puede hospedar el correo electrónico de la red en el servidor SMTP³ de *MDaemon*, o recolectar el correo electrónico para todo un dominio desde POP3⁴ a través de la funcionalidad incluida de dominio pop. Puede hospedar múltiples listas de correo, permitir a sus usuarios acceder al correo a través del componente de correo web y utilizar muchas otras funcionalidades.

MDaemon PRO está equipado con todas las opciones de la versión *Standard*, además de soporte para IMAP4⁵, múltiples dominios, dominios compartidos, puertas de enlace, listas de correo extendidas. También añade calendario y programación de grupos, un sistema de mensajería instantánea, soporte múltiple de idiomas para el cliente de correo web, creación automática de puertas de enlace y mucho más.

Soporta los protocolos SMTP y POP3 e incluye soporte para administración remota y algunas otras funcionalidades. Mediante el soporte y protección completa para el escaneo de virus provee una potente protección. Los mensajes pueden ser escaneados en busca de virus y limpiados o borrados automáticamente antes de llegar a los destinatarios, así como ser configurado para que envíe un mensaje al administrador, al remitente y al destinatario del mensaje infectado notificándoles del virus.

Incluye varias funciones de listas de correo y gestión de grupos que permiten la formación de un número ilimitado de listas de distribución que pueden contener miembros locales y/o remotos. Las listas se pueden configurar para permitir o rechazar peticiones de suscripción, ser públicas o privadas, enviar respuestas a la lista o bien al origen del mensaje, ser enviadas en formato resumen, y para ser configuradas usando muchas otras funcionalidades.

Un componente integrado en *MDaemon* es el cliente de correo web. Este producto hace posible a sus usuarios acceder a su correo utilizando su navegador web favorito en lugar de hacerlo desde una estación de trabajo que dependa de un cliente de correo. Esta herramienta es ideal para empleados con mucha movilidad y usuarios que

³ *Simple Mail Transference Protocol* (Protocolo simple de transferencia de correos.)

⁴ *Post Office Protocol* por sus siglas en inglés. Protocolo que permite descargar los correos electrónicos, moviendo los mismos desde los agentes de entrega de correo hacia los clientes de correo de usuario.

⁵ *Internet Message Access Protocol* por sus siglas en inglés. Protocolo que permite descargar los correos electrónicos, copiando los mismos desde los agentes de entrega de correo hacia los clientes de correo de usuario.

CAPÍTULO 1: SERVICIOS DE CORREO ELECTRÓNICO

no disponen de una máquina dedicada desde la que puedan acceder a su correo. Está equipado con un conjunto completo de funcionalidades de cliente de correo. Puede enviar y recibir correos, comprobar la ortografía de los mensajes, gestionar su correo en múltiples carpetas personales, mostrar la interfaz en cualquiera de los 18 lenguajes con que cuenta, programar reuniones, citas, compartir calendarios y tareas con otros usuarios, así como gestionar sus preferencias de cuenta. Presenta muchas funcionalidades diseñadas para ayudar a proteger los sistemas de correo electrónico. Las funcionalidades de filtro de correo basura y lista negra son utilizados para eliminar la recepción de la mayoría de los mensajes de correo *spam*⁶ que se tratan de enrutar a través de los dominios. Para la autenticación de los usuarios permite utilizar un directorio activo o un servidor *ldap*⁷ como base de datos de cuentas de *MDaemon*, en lugar del sistema local *userlist.dat*. De esta forma, puede configurar múltiples servidores *MDaemon* en múltiples localizaciones para que compartan la misma base de datos de cuentas.

Puede ser configurado para mantener su libreta de direcciones de *Windows* o un almacén de contactos de *Microsoft Outlook* actualizado con la información de los usuarios. Esto provee otro modo de conseguir una libreta de direcciones global disponible para los usuarios.

Los alias de direcciones proveen la habilidad de enrutar mensajes de correo electrónico dirigidos a buzones de correo ficticios a cuentas o listas de correo válidas. Esto hace posible que cada cuenta individual o lista de correo posea múltiples direcciones en uno o más dominios.

Provee la posibilidad de establecer dominios separados para varios departamentos o grupos que pueden ser locales en la red o ubicados en otro lugar de Internet. Utilizando esta funcionalidad, todas las direcciones de correo dirigidas a un dominio para el cual *MDaemon* esté actuando de puerta de enlace serán colocadas en el buzón de dicho dominio por *MDaemon*. Puede ser posteriormente recolectado por el servidor *MDaemon* de dicho dominio o por un cliente de correo, y distribuido a los usuarios del dominio. Esta funcionalidad también se puede usar para habilitar *MDaemon* como servidor de copia de seguridad para otros dominios.

Cuenta con una administración integrada basada en web, integrada con *MDaemon* y el cliente de correo web, permitiendo a sus usuarios revisar y editar sus configuraciones de cuenta a través de su navegador web.

⁶ Mensajes no solicitados, habitualmente de tipo publicitario, enviados en forma masiva.

⁷ Protocolo Ligero de Acceso a Directorios.

CAPÍTULO 1: SERVICIOS DE CORREO ELECTRÓNICO

Mediante un sistema de filtro de contenido altamente versátil se hace posible personalizar el comportamiento del servidor basándose en el contenido de los mensajes entrantes y salientes. De esta forma permite insertar y eliminar cabeceras de mensajes, añadir pies, eliminar adjuntos, enrutar copias a otros usuarios, así como hacer que un mensaje instantáneo se envíe a alguien (ALT-NTECHNOLOGIES I. N. C., 2013).

1.3. Tecnologías asociadas a los servicios de correo electrónico

Para el correcto funcionamiento del servicio de correo influyen un conjunto de tecnologías básicas las cuales están relacionadas entre sí.

Cuando se envía un correo electrónico, éste se enruta mediante un agente de transferencia de correos (MTA) usando el protocolo simple de transferencia de correos, conocido también como SMTP (Paso 1), la próxima etapa es realizar un escaneo del mensaje mediante un filtro *antispam* para determinar si es un correo basura y luego a través del antivirus se comprueba si el mensaje está infectado (Paso 2), posteriormente se devuelve el correo al MTA (Paso 3), en caso de haber alguna dificultad se notifica al remitente, sino el MTA del destinatario entrega el correo electrónico al agente de entrega de correos, MDA (Paso 4), el cual almacena el correo electrónico. La obtención del mensaje de correo por el usuario final se logra a través de un agente de usuario de correo, MUA (Paso 5). La Figura 1 ilustra el proceso descrito (YADIEL PÉREZ y YASIEL PÉREZ, 2013).



Figura 1 Interacción entre tecnologías en servicio de correo

1.4. Agentes de transferencia de correo (MTA)

Actualmente existen varias aplicaciones que implementan el protocolo SMTP, siendo utilizadas como agentes de transferencia de correo. A continuación se describen las

CAPÍTULO 1: SERVICIOS DE CORREO ELECTRÓNICO

principales herramientas que realizan esta función, describiéndose las principales funcionalidades, ventajas y desventajas de cada una.

1.4.1. Qmail

Qmail es un *software* que brinda la posibilidad de configurar un servicio de correo electrónico que implementa el protocolo SMTP y ha sido construido para GNU/Linux y *Unix*. Utiliza uno de los formatos más eficientes para almacenar sus mensajes, el cual es el formato *maildir* (DAVE, 2002a).

Una de las desventajas que presenta es que no está optimizado para todos los posibles escenarios y fue diseñado para la comunicación entre aquellas computadoras que estén conectadas directamente y tengan una alta conectividad, por lo que en computadoras con baja conectividad o ancho de banda, su rendimiento puede verse afectado (DAVE, 2002b).

1.4.2. Sendmail

Sendmail es un programa de transferencia de correo electrónico a través de la red. Cuando las arquitecturas de red que compiten dieron paso a la Internet basada en TCP/IP⁸, las grandes posibilidades de configuración de *Sendmail* le permitieron mantener su punto de apoyo como servidor predeterminado para el correo electrónico. Muchos años más tarde, sigue siendo el estándar por defecto para el correo de Internet, y es utilizado por muchos sitios de gran tamaño, como Yahoo⁹, Earthlink¹⁰ y AOL¹¹. Se ha calculado que si se envía un mensaje de correo electrónico a través de Internet, existe de un 75 a 80 por ciento de posibilidades de que va a tocar *Sendmail* en algún punto de su viaje (MICHAEL y STEVE, 2003a).

Los autores Michael Turner y Steve Shah en su libro "*Red Hat Linux Administration A beginner's Guide*" plantean que entre las desventajas que presenta *Sendmail* está la de ser el programa más difícil que tendrá que configurar alguien como administrador de *Unix*, además que el archivo de configuración principal es tan difícil de entender que no se considera adecuado tratar de editarlo directamente.

La estructura y diseño interno de *Sendmail* son complejas y requieren una atención considerable durante el desarrollo, por lo que a lo largo de su dilatada historia, ha tenido un historial de seguridad irregular. En los últimos años, los desarrolladores han

⁸ Conjunto de protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre computadoras.

⁹ Es una empresa global de medios con sede en Estados Unidos. Posee un portal de Internet, un directorio web y una serie de servicios, incluido el popular correo electrónico.

¹⁰ Proveedor de servicios de tecnologías de la información, redes y comunicaciones.

¹¹ Empresa de servicios de internet y medios.

CAPÍTULO 1: SERVICIOS DE CORREO ELECTRÓNICO

adoptado un enfoque muy paranoico a su diseño para ayudar a aliviar estos problemas. Básicamente, se envía el paquete en un modo de seguridad bastante alto y dejan al administrador de sistemas la responsabilidad de utilizarlo según sus necesidades, lo cual resulta difícil en muchas ocasiones debido a los parámetros colocados por defecto para lograr una mayor seguridad (MICHAEL y STEVE, 2003b).

1.4.3. Exim

Exim es un MTA que surge en el año 1995 y fue desarrollado por Philip Hazel en la universidad de Cambridge. Al igual que *Sendmail*, se ejecuta como un solo proceso que lleva a cabo todas las tareas de correo.

Cuando se compila con soporte para análisis de contenido, es capaz de comunicarse con herramientas de escaneo de virus y *spam* tales como Clamav¹² y *SpamAssassin*¹³. Las políticas de control se llevan a cabo a través de ACLs¹⁴ que pueden aceptar o rechazar mensajes y pasarlos a herramientas de escaneo. Muchos aspectos de la configuración de Exim se especifican en tiempo de compilación (EVI NEMETH y TOBI, 2011a).

Esto constituye una gran desventaja pues se hace necesaria la compilación del mismo cada vez que se necesita un determinado tipo de configuración en el servicio de correo que se necesite utilizar, desaprovechando la comodidad de poder utilizar los binarios distribuidos para la comunidad en dependencia del sistema operativo que se utilice.

1.4.4. Postfix

Postfix es un agente de transferencia de correo, que permite transportar mensajes desde un cliente de correos a un servidor de correo remoto mediante el protocolo SMTP. Además acepta mensajes de servidores de correo remotos para reenviarlos a otros agentes de transferencia de correo o entregarlos a buzones de correo locales. Después de transmitir o entregar los mensajes de correo electrónico, el trabajo de Postfix termina (RALF y PATRICK, 2005a).

Entre las metas en el diseño de Postfix se encuentran no sólo la seguridad, que es la primera y más importante, sino también una política de distribución de código fuente abierto, de rápido rendimiento, así como una gran robustez y flexibilidad. Las principales distribuciones de GNU/Linux incluyen Postfix, y desde la versión 10.3, Mac OS X ha utilizado Postfix en lugar de *Sendmail* como su sistema de correo electrónico.

¹² Antivirus ampliamente utilizado en sistemas GNU/Linux.

¹³ Filtro de correos *antispam* utilizado en servidores de correo.

¹⁴ *Access Control Lists* (Listas de control de acceso).

Entre los aspectos más importantes de Postfix se encuentran que funciona correctamente como mismo se distribuye y que los archivos de configuración más simples son sólo de una o dos líneas de largo (EVI NEMETH y TOBI, 2011b).

Postfix fue desarrollado por Wietse Venema, quien es un experto en sistemas *Unix*, por lo que en el diseño de este MTA no se incluye ninguna funcionalidad que *Unix* provea por defecto (RALF y PATRICK, 2005b). Esto es algo que puede verse como una gran ventaja teniendo en cuenta que permite que Postfix sea lo más ligero posible, ya que aprovecha al máximo las funcionalidades del sistema operativo.

1.5. Agentes de entrega de correo (MDA)

Actualmente existen varias aplicaciones que implementan los protocolos POP e IMAP, siendo utilizados como agentes de entrega de correo. A continuación se describen las principales herramientas que realizan esta función, describiéndose las principales funcionalidades, ventajas y desventajas de cada una.

1.5.1. Courier IMAP

El servidor Courier IMAP es un servidor rápido y escalable que implementa los protocolos POP3 e IMAP permitiendo almacenar los mensajes de correo en los buzones en varios formatos, entre ellos lo más conocidos y eficientes. Ambos protocolos también pueden ser compartidos mediante SSL¹⁵/TLS¹⁶, utilizando los puertos 995 y 993. Muchos proveedores que brindan servicios de correo electrónico utilizan el servidor Courier IMAP debido a que soporta el manejo de miles de cuentas de correo, además las cuentas se pueden mover entre diferentes servidores, para lograr un uso óptimo de los recursos. Permite almacenar los datos de autenticación de los usuarios no solo en el sistema operativo, sino en bases de datos ldap, mysql, postgresql.

Uno de los problemas que presenta Courier es la poca documentación que dispone en los sitios en línea ya que no hay suficiente información y estadísticas acerca de su funcionamiento, configuración y formas de administración, así como características y requisitos funcionales que cumple, aunque también ha sido fuertemente criticado por el grado de complejidad para realizar la autenticación segura utilizando SASL¹⁷ (PEER y PEER, 2007).

¹⁵ *Secure Sockets Layer* (Capa de Conexión Segura).

¹⁶ *Transport Layer Security* (Seguridad de la Capa de transporte).

¹⁷ *Simple Authentication and Security Layer* (Capa de Seguridad y Autenticación Simple).

1.5.2. Cyrus IMAP

Cyrus IMAP proporciona acceso al correo personal y de todo el sistema a través del protocolo IMAP. Se diferencia de otras implementaciones del servidor IMAP en que se ejecuta en servidores donde los usuarios normalmente no están permitidos entrar a la base de datos del buzón de correo ya que se almacenan en las partes del sistema de archivos que son privadas para el sistema. El diseño de la base de datos del buzón privado ofrece las ventajas de servidores de gran tamaño para la eficiencia, escalabilidad y administración. Permite almacenar los datos de autenticación de los usuarios no solo en el sistema operativo, sino en bases de datos ldap, mysql y postgresql. Para la administración cuenta con una herramienta, que utiliza una interfaz web, llamada Cyradm, la cual facilita el trabajo a los administradores de sistemas. La autenticación segura utilizando SASL se puede realizar de forma sencilla. En Cyrus se puede utilizar el lenguaje de filtros de correo Sieve, contando además con un sistema de permisos para las carpetas compartidas, que facilita la implementación de las políticas de control de acceso, así como sistemas de cuotas para el almacenamiento de los buzones de correo. Uno de los problemas que presenta Cyrus es la escasa documentación de la que dispone ya que no hay suficiente información y estadísticas acerca de su funcionamiento, configuración y formas de administración (PEER y PEER, 2007).

1.5.3. Dovecot

Dovecot es una herramienta de código abierto que implementa los protocolos IMAP y POP3 para sistemas GNU/Linux y UNIX. Fue escrito pensando primeramente en la seguridad. Es una excelente opción para pequeñas y grandes instalaciones, y también muy rápido y simple de configurar, por lo que no requiere de grandes conocimientos para su administración. Consume muy poca memoria y cuenta con un gran conjunto de funcionalidades (OFFICIAL DOVECOT, 2013).

Algunas de sus características más notables son:

- Es el servidor IMAP de mayor rendimiento entre todos, sin dejar de soportar los formatos de correo *mbox* y *maildir*. Los buzones de correo son transparentemente indexados, proporcionándole un gran desempeño y ofreciendo total compatibilidad con las herramientas de manejo de buzones existentes
- Cumple con facilidad los estándares, por lo que pasa todas las pruebas de estandarización para servidores IMAP, mientras que la mayoría de los

servidores fallan.

- Los índices están propiamente optimizados, ya que contienen exactamente lo que los usuarios necesitan, ni más ni menos.
- Permite la auto recuperación de sus índices, solucionando la mayoría de los problemas automáticamente, aunque quedan registrados por lo que el administrador puede más tarde averiguar lo que los ha causado y de esta forma quedar informado.
- Trata en lo mayor posible de tener una administración amigable y los mensajes de error comunes se registran de una forma comprensible.
- Los sistemas de autenticación con que cuenta son extremadamente flexibles, siendo rico en funciones y con soporte para la mayoría de las bases de datos existentes como ldap, postgresql y mysql.
- Dovecot soporta una fácil migración desde servidores IMAP y POP3, lo que permite que el cambio sea transparente para los usuarios existentes.
- El diseño e implementación de Dovecot está muy centrado en la seguridad, y se utilizan métodos eficientes para solucionar las vulnerabilidades cada vez que alguien las informa.
- Es fácilmente extensible debido a la gran cantidad de componentes con que cuenta (OFFICIAL DOVECOT, 2013).

1.6. Clientes web a utilizar como MUA

Actualmente existen varias aplicaciones que cumplen la función de cliente web, siendo utilizados como clientes de correo electrónico en la web. A continuación se describen las principales herramientas que realizan esta función, detallándose las principales funcionalidades, ventajas y desventajas de cada una.

1.6.1. SquirrelMail

SquirrelMail es una herramienta de correo web basada en estándares y escrito en PHP¹⁸. Incluye soporte integrado para los protocolos IMAP y SMTP. Tiene casi todas las funcionalidades que se desea de un cliente de correo electrónico (OFFICIAL SQUIRRELMAIL, 2013). Entre sus desventajas principales se encuentra que no cuenta con una interfaz amigable, principalmente por la decisión del equipo de *SquirrelMail* de no utilizar *JavaScript*, algo que aunque aumenta su compatibilidad con

¹⁸ Lenguaje de código abierto muy popular especialmente adecuado para el desarrollo web.

la mayoría de los navegadores web existentes, disminuye la posibilidad al usuario de lograr una mejor interacción con la aplicación.

Algunas de sus características más notables son:

- Está licenciado bajo GNU/GPL¹⁹.
- Fácil de configurar e instalar.
- Soporte a tipos MIME²⁰.
- Libreta de direcciones.
- Manipulación de carpetas.
- Basado en componentes (249 disponibles agrupados en 14 categorías) (OFFICIAL SQUIRRELMAIL, 2013).

1.6.2. Horde Groupware Webmail Edition

El proyecto *Horde Groupware Webmail Edition* es una *suite* de comunicación libre basada en navegador, utilizada como cliente web de correo. Mediante él, los usuarios pueden leer, enviar y organizar los mensajes de correo electrónico, así como gestionar y compartir calendarios, contactos, tareas y notas mediante componentes que cumplen con los estándares del proyecto Horde (OFFICIAL HORDE GROUPWARE, 2013). Una de las desventajas con que cuenta el mismo es que aunque la interfaz es bastante amigable, aún no se ha logrado que esté a la altura de otras soluciones como Roundcube, debido a que ha sido en la versión reciente que se comenzó a enfocar en estos aspectos (OFFICIAL HORDE GROUPWARE, 2014), algo que para el proyecto Horde es mucho más difícil, pues los aspectos del cliente de correo web no pueden verse independientes de la solución de *Groupware* de Horde, siendo más difícil lograr este objetivo que en proyectos que solo desarrollan un cliente de correo web como *SquirrelMail* y Roundcube.

Algunas de sus características más notables son:

- Soporte para IMAP y POP3.
- Filtrado de mensajes.
- Búsqueda de mensajes.
- Composición de mensajes en formato HTML²¹.
- Corrección ortográfica.
- Cifrado y firma de mensajes de correo.
- Soporte de cuotas.

¹⁹ *General Public License* (Licencia Pública General).

²⁰ *Multipurpose Internet Mail Extensions* (Extensiones Multipropósito de Correo de Internet).

²¹ *Hypertext Markup Language* (Lenguaje de Marcado de Hipertexto).

CAPÍTULO 1: SERVICIOS DE CORREO ELECTRÓNICO

- Soporte completo de caracteres para los nombres de carpetas y mensajes de correo electrónico.
- Flexibilidad con las direcciones y alias.
- Suscripciones a carpetas IMAP.
- Adjuntos enviados como enlaces (OFFICIAL HORDE GROUPWARE, 2013).

1.6.3. Roundcube

Este proyecto es una solución de cliente de correo web gratuita y de código abierto con una interfaz de usuario fácil de instalar y configurar. Utiliza interfaces que cuentan con un diseño basado en los últimos estándares web como XHTML²² y CSS²³, así como bibliotecas sofisticadas de código abierto. Está escrito en PHP y requiere una base de datos relacional, por lo que se ejecuta en un servidor LAMP²⁴ estándar. La interfaz de usuario es totalmente personalizable, algo de gran utilidad en muchas ocasiones (OFFICIAL ROUND CUBE, 2013).

Algunas de sus características más notables son:

- Disponible en más de 70 idiomas.
- Gestión de mensajes para arrastrar y soltar.
- Soporte completo para mensajes MIME y HTML.
- Sofisticada protección de privacidad.
- Libreta de direcciones completa con grupos y conectores ldap.
- Integración de búsquedas con la libreta de direcciones y lo que se escriba.
- Composición de mensajes de texto enriquecido con HTML.
- Búsqueda de mensajes y contactos.
- Soporte para Internacionalización de Nombres de Dominio en Aplicaciones.
- Corrección ortográfica.
- Administración de carpetas IMAP.
- Compartición global de carpetas IMAP.
- Soporte para listas de control de acceso.
- Construcción de caché para acceso rápido al buzón de correo
- Usuarios y mensajes ilimitados.
- Sistema de plantillas para temas personalizados.
- Basado en componentes (Cuenta con un gran número de componentes

²² *Extensible Hypertext Markup Language* (Lenguaje de Marcado de Hipertexto Extensible).

²³ *Cascading Style Sheets* (Hojas de Estilo en Cascada).

²⁴ Acrónimo usado para describir un sistema de infraestructura de Internet que usa las herramientas Linux, Apache, MySQL y Perl, PHP o Python.

agrupados en 10 categorías) (OFFICIAL ROUND CUBE, 2013).

1.7. Filtrado de correos spam

Actualmente existen varias aplicaciones que cumplen la función de filtrar los correos electrónicos y determinar si los mismos son correos no deseados, siendo utilizados como filtros de correo *spam*. A continuación se describen las principales herramientas que realizan esta función, detallándose las principales funcionalidades, ventajas y desventajas de cada una.

1.7.1. DSPAM

Esta aplicación es un escalable filtro de *spam* basado en contenidos. Es de código abierto y ha sido diseñado para los sistemas empresariales multiusuarios. Soporta varios agentes de transferencia de correos y ha sido probado en muchos sistemas, tanto grandes como pequeños, en total, en alrededor de 350000 buzones de correo.

DSPAM es un filtro adaptativo que es capaz de aprender y adaptarse al correo electrónico de cada usuario. En lugar de trabajar mediante una lista de reglas para identificar el *spam*, examina el contenido de cada mensaje y aprende qué tipo de contenido el usuario considera como *spam* o no (OFFICIAL, DSPAM WEB, 2013a). Entre sus desventajas se encuentra la de no poder utilizar a una interfaz para la comunicación con el MTA, sino que se comunica directamente con el mismo.

Algunas de sus características más notables son:

- Es un sistema ampliamente libre de mantenimiento. El agente *DSPAM* se puede integrar en casi cualquier red e incluso puede ser implementado como una puerta de enlace SMTP.
- Utiliza de forma sencilla el mecanismo de aprendizaje.
- Tiene soporte para gran variedad de implementaciones de almacenamiento.
- Ha sido desarrollado en el lenguaje de programación C para la velocidad, el rendimiento y la escalabilidad.
- Funciona muy bien con *Sendmail*, *Postfix*, *Qmail*, *Exim* y debería funcionar bien con muchos otros MTA (OFFICIAL, DSPAM WEB, 2013a).

1.7.2. Bogofilter

Bajo los principios del *software* libre, *Bogofilter* es un filtro para clasificar los mensajes de correo electrónico como *spam* o no, desarrollado en el lenguaje C, que hace uso de un análisis estadístico de la cabecera y el contenido del mensaje. De esta forma es capaz de aprender de la clasificación de los usuarios y sus correcciones. Actualmente

CAPÍTULO 1: SERVICIOS DE CORREO ELECTRÓNICO

soporta las plataformas Linux, *FreeBSD*, Solaris, OS X, HP-UX, AIX, RISC OS, SunOS. Entre sus desventajas se encuentra la de no poder utilizar a una interfaz para la comunicación con el MTA, sino que se comunica directamente con el mismo.

Algunas de sus características más notables son:

- Puede ser integrado con los clientes de correo gráficos como *KMail* de KDE, *Evolution* de Gnome o *Claws Mail*.
- Puede ser ejecutado mediante un agente de entrega de correo, permitiendo clasificar un mensaje entrante como *spam* o no.
- Proporciona procesamiento de texto plano y HTML (OFFICIAL BOGOFILTER, 2013).

1.7.3. SpamAssassin

SpamAssassin utiliza una variedad de normas para identificar el *spam* y captura esencialmente todo el *spam* real. Utiliza un sistema de puntos para categorizar los mensajes, por lo que si un mensaje acumula demasiados puntos, es etiquetado como *spam* y si se cuenta con un filtro para su MDA puede almacenar los mensajes sospechosos en una carpeta específica. Utilizando a *SpamAssassin* se le pueden enseñar los mensajes buenos y malos mediante el uso de su función de filtro bayesiano y de esta forma se realizará un aprendizaje supervisado para que mensajes similares sean categorizados de acuerdo a los mensajes de muestra (EVI NEMETH y TOBI, 2011c).

Algunas de sus características más notables son:

- **Amplio espectro:** Utiliza una amplia variedad de pruebas locales y de red para identificar firmas de correos no deseados.
- **Es software libre:** Se distribuye bajo los mismos términos y condiciones que los otros paquetes de *software* de código abierto populares.
- **Fácil de ampliar:** Las pruebas y la configuración de correo no deseado se almacenan en texto plano, por lo que es fácil de configurar y poner nuevas reglas.
- **Flexible:** Encapsula su lógica en una API²⁵ bien diseñada, por lo que se puede integrar en cualquier flujo de correos electrónico.
- **Amplio soporte para servidores SMTP:** Puede ser utilizado en una amplia variedad de sistemas de correo electrónico incluyendo Sendmail, Postfix, *Qmail*, y muchos otros.

²⁵ *Application Programming Interface* (Interfaz de programación de aplicaciones).

- **Fácil configuración:** Requiere muy poca configuración y no se necesita actualizar continuamente con los detalles de sus cuentas de correo electrónico, listas de correos y demás.
- **Permite portar las políticas:** Las políticas una vez clasificado el sitio y el usuario específico, pueden ser aplicadas tanto en otros servidores de correo como en una aplicación propia de agente de usuario de correo del usuario (OFFICIAL SPAMASSASSIN, 2013).

1.8. Herramientas para antivirus

Actualmente existen varias aplicaciones que cumplen la función de detectar en los servicios de correo si un mensaje contiene virus, siendo utilizados como antivirus en estos servicios. A continuación se describen las principales herramientas que realizan esta función, detallándose las principales funcionalidades, ventajas y desventajas de cada una.

1.8.1. Kaspersky Security for Linux Mail Server

Kaspersky Security for Linux Mail Server ofrece funciones esenciales de seguridad del correo electrónico, incluyendo *antimalware*, *antispam* y filtrado de contenido, en un paquete fácil de administrar. Al combinar los motores *antimalware* y *antispam* de *Kaspersky Lab*, además del poder de la nube, *Kaspersky Security for Linux Mail Server* proporciona detección de *malware* y *spam* mejorada con una baja tasa de falsos positivos (OFFICIAL KASPERSKY, 2014).

Algunas de sus características más notables son:

- **Detección de *spam* mejorada con menos falsos positivos:** Las últimas tecnologías de *Kaspersky Lab* ofrecen detección de *spam* mejorada para asegurarse de que una cantidad cada vez menor de mensajes de *spam* consiga alcanzar su sistema de correo electrónico.
- **Detección *antimalware* y hora cero mejorada:** El último motor antivirus de Kaspersky ofrece un escaneo mejorado y una mayor tasa de detección, lo que permite una detección más rápida y exacta de archivos adjuntos de correo electrónico maliciosos.
- **Alta utilidad y alto rendimiento:** Está diseñado para entregar una alta utilidad sin un efecto significativo en el rendimiento del sistema.
- **Fácil de integrar:** *Kaspersky Security for Linux Mail Server* se puede integrar con populares agentes de transferencia de correo basados en Linux (MTA), incluidos *Postfix*, *Sendmail*, *Exim*, *Qmail* y *CommuniGate Pro*, así como

CAPÍTULO 1: SERVICIOS DE CORREO ELECTRÓNICO

también con sistemas de correo basados en Linux a través de Amavis (OFFICIAL KASPERSKY, 2014).

1.8.2. SAVUnix

Es un antivirus desarrollado por la empresa cubana Segurmática, el cual es capaz de detectar programas malignos que se ejecuten sobre *Microsoft Windows* y GNU/Linux (OFFICIAL, SAVUNIX WEB, 2013b). Cuenta con una herramienta para la comunicación con agentes de transferencia de correos llamada SaVUnix Milter, que permite la integración con Sendmail 8.12.0 o superior y Postfix 2.3.0 o superior. Mediante información intercambiada con los desarrolladores de esta aplicación se informó que aún no está lo suficientemente estable como para ser desplegada en un entorno real.

1.8.3. ClamAV

ClamAV es un motor antivirus de código abierto licenciado bajo GPL y diseñado para la detección de troyanos, virus, *malware* y otras amenazas. Es el estándar por excelencia para escanear servidores de correo. Proporciona un demonio de escaneo de alto rendimiento, así como utilidades de línea de comandos para el análisis de archivos en demanda y una herramienta inteligente para las actualizaciones automáticas de firmas. La biblioteca central de ClamAV ofrece numerosos mecanismos de detección de formatos de archivo (OFFICIAL CLAM A. V. ANTIVIRUS, 2013).

Es utilizado en entornos de producción en muchas empresas privadas, grandes universidades y agencias gubernamentales, tales como: *Barracuda Networks*, la Universidad Estatal de Michigan, la Universidad de Brandeis, Webmail.us, *Slashmail*, y el estado de Vermont en los Estados Unidos de América (YOUSEF, 2006).

1.9. Técnica utilizada para la selección de las herramientas investigadas

Para establecer las comparaciones entre aplicaciones de código abierto son muy utilizados los modelos de madurez referentes a este tipo de aplicaciones también denominados OSMM²⁶ por sus siglas en inglés. En la presente investigación para seleccionar los criterios de comparación entre las herramientas se utiliza el método de calificación y selección de *software* QSOS²⁷. El proceso consiste en cuatro pasos:

²⁶ *Open Source Maturity Model* (Modelo de madurez de código abierto).

²⁷ *Qualification and Selection of Open Source software* (Calificación y selección de software de código abierto).

CAPÍTULO 1: SERVICIOS DE CORREO ELECTRÓNICO

definición, evaluación, calificación, y selección. Cuenta con dos alternativas, la estricta y la amplia. Este método permite seleccionar la aplicación más idónea según los parámetros definidos por el propio modelo de madurez.

Para la selección de las herramientas adecuadas se presentará una comparación entre las aplicaciones anteriormente descritas teniendo en cuenta los aspectos siguientes:

- Licencia: La licencia bajo la cual se distribuye posee viralidad, herencia y *copyleft*.
 0. Si no posee dos o tres de las cualidades, dos cualidades son parciales y no posee la tercera.
 1. Las tres cualidades las posee parcialmente o posee dos.
 2. Posee las tres cualidades.
- Facilidad de administración: Referido a la facilidad de administración del *software*.
 0. El *software* es difícilmente administrable.
 1. Cuenta con niveles de administración medios.
 2. Es una de las herramientas que con mayor facilidad se administra entre sus homólogas.
- Documentación: Abundancia y accesibilidad de documentación sobre el *software*.
 0. No se dispone de documentación para los usuarios.
 1. Documentación escasa u obsoleta o sujeta a un único lenguaje o contiene pocos detalles.
 2. Actualizada, disponible en varios idiomas y adaptado a varios lectores (administradores, usuarios, etc).
- Flexibilidad: Nivel de configuración del *software*.
 0. Constituye una herramienta demasiado rígida.
 1. Puede ser cambiada, aunque no como se necesita.
 2. Es altamente configurable.
- Rendimiento: Efectividad para utilizar de la forma más eficiente posible los recursos en el entorno en el que se encuentra.

CAPÍTULO 1: SERVICIOS DE CORREO ELECTRÓNICO

- 0. Alto consumo de recursos.
 - 1. El consumo de recursos es mediano.
 - 2. Bajo consumo.
- Seguridad: Seguridad con que cuenta el *software*.
 - 0. Es totalmente vulnerable.
 - 1. Cuenta con niveles de seguridad básicos.
 - 2. Se considera un *software* seguro.
- Soporte: Respuesta de cambio del *software* ante nuevas necesidades o problemas que surjan.
 - 0. No cuenta con soporte.
 - 1. Se actualiza poco, en ocasiones mucho después de lo necesitado por la comunidad.
 - 2. Cuenta con un soporte activo.
- Interfaz: Presentación del *software* al usuario.
 - 0. Cuenta con una interfaz muy pobre.
 - 1. La interfaz es medianamente usable.
 - 2. Entre sus homólogos, el *software* cuenta con una de las interfaces de mayor usabilidad.
- Componentes: Cantidad de componentes con que cuenta el *software*
 - 0. No cuenta con componentes.
 - 1. Cuenta con menos de 100 componentes.
 - 2. Cuenta con más de 100 componentes.
- Interfaz de comunicación: Referido a la comunicación indirecta con un MTA
 - 0. No utiliza interfaz de comunicación.
 - 1. Utiliza interfaz de comunicación.

1.10. Comparación entre las herramientas investigadas

Las aplicaciones investigadas serán comparadas utilizando la técnica QSOS, explicada anteriormente. Aquellas herramientas que obtengan en su totalidad un mayor puntaje serán las seleccionadas como las más adecuadas de acuerdo a los

CAPÍTULO 1: SERVICIOS DE CORREO ELECTRÓNICO

parámetros comparados.

1.10.1. Agentes de transferencia de correo

Tabla 1. Comparación entre Agentes de transferencia de correo.

	<i>Qmail</i>	<i>Sendmail</i>	<i>Exim</i>	<i>Postfix</i>
Licencia	2	2	2	2
Facilidad de administración	0	0	1	1
Documentación	0	2	2	2
Flexibilidad	1	2	1	2
Rendimiento	2	2	1	2
Seguridad	1	0	1	1
Soporte	2	2	2	2
Total	8	10	10	12

1.10.2. Agentes de entrega de correo

Tabla 2. Comparación entre Agentes de entrega de correo.

	<i>Courier IMAP</i>	<i>Cyrus IMAP</i>	<i>Dovecot</i>
Licencia	2	2	2
Facilidad de administración	1	1	2
Documentación	0	0	2
Flexibilidad	0	1	2
Rendimiento	2	2	2
Seguridad	1	2	2
Soporte	2	2	2
Total	8	10	14

1.10.3. Clientes web de correo

Tabla 3. Comparación entre clientes web de correo.

	<i>SquirrelMail</i>	<i>Horde</i>	<i>Roundcube</i>
Licencia	2	2	2
Interfaz	0	1	2
Componentes	2	0	2
Rendimiento	1	1	2
Flexibilidad	2	0	2
Soporte	2	2	2
Total	9	6	12

1.10.4. Filtrado de correos *spam*

Tabla 4. Comparación de filtros de correo *spam*.

	<i>DSPAM</i>	<i>Bogofilter</i>	<i>Spamassassin</i>
Licencia	2	2	2
Interfaz de comunicación	0	0	2
Rendimiento	2	2	2
Flexibilidad	1	1	2
Soporte	2	2	2
Total	7	7	10

1.10.5. Herramientas para antivirus

Tabla 5. Comparación entre herramientas para antivirus

	Kaspersky	SAVUnix	ClamAV
Licencia	0	0	2
Interfaz	2	0	2
Rendimiento	2	2	2
Flexibilidad	2	1	2
Soporte	2	2	2
Total	8	5	10

1.11. Resultados sobre las tecnologías investigadas

Luego de haber investigado y comparado las tecnologías principales para el montaje de una infraestructura de servicios de correo utilizando la técnica de Calificación y selección de *software* de código abierto (QSOS) se decide que como agente de transferencia de correo, Postfix se adapta en mayor medida a los requisitos necesitados. De esta misma forma fueron seleccionados Dovecot como agente de entrega de correo, Roundcube como cliente de correo web, *SpamAssassin* para la detección de correos *spam* y ClamAV como antivirus.

1.12. Tecnologías adicionales a utilizar en los servicios de correo electrónico

En toda infraestructura para los servicios de correo electrónico es necesario contar con un conjunto de tecnologías que complementan la correcta interacción de varios componentes permitiendo todos ellos la eficiencia, seguridad y estabilidad de los servicios de correo electrónico. A continuación se expondrán cada una de estas tecnologías y las características y funcionalidades de las mismas (YADIEL PÉREZ y YASIEL PÉREZ, 2013).

1.12.1. Amavis

Amavis es una interfaz entre los servidores de correo (MTA) y las herramientas que chequean contenido como escáneres de virus y *spam*. Está escrito en Perl²⁸, lo que garantiza una alta fiabilidad, portabilidad y facilidad de mantenimiento, sin que nada de esto signifique sacrificar su rendimiento, el cual es muy bueno.

Aunque presenta varias características, algunas de las más notables son:

- **Seguro:** Se ejecuta mediante un usuario con permisos específicos (no root o *mail*)
- **No deja pasar correos sin chequear:** Cuando ocurren errores impredecibles,

²⁸ Lenguaje de programación.

CAPÍTULO 1: SERVICIOS DE CORREO ELECTRÓNICO

la responsabilidad siempre recae en el MTA.

- **Mecanismos de Autenticación de Correo Electrónico:** Soporta Mecanismos de Autenticación de Correo Electrónico (DKIM) y firmas de llaves de dominio.
- **Amplio soporte para antivirus:** La lista actual soporta más de 40 antivirus y puede ser fácilmente extendida.
- **Rendimiento:** Posee un rendimiento elevado por lo que es adecuado su uso en computadoras con escasos recursos de *hardware* (OFFICIAL AMAVIS, 2013).

1.12.2. Sieve

Sieve es un lenguaje para el filtrado de mensajes de correo electrónico. Está diseñado para poder aplicarse ya sea en un cliente de correo o servidor de correo. Es extensible, simple e independiente del protocolo de acceso, arquitectura del servicio de correo y sistema operativo. También es adecuado para ser ejecutado en un servidor de correo donde los usuarios no tienen permitido ejecutar programas arbitrarios (OFFICIAL SIEVE, 2013).

1.12.3. Cluebringer

La versión 2 de Policyd fue renombrada a cluebringer, el cual es un servidor de políticas multiplataforma para agentes de transferencia de correos. Ha sido diseñado para el trabajo en ambientes hostiles con servidores de correo y su principal objetivo es el combate de correos *spam* y la clasificación y detección de los diferentes tipos de listas blancas, negras y grises, manteniendo al mismo tiempo la portabilidad, estabilidad y el rendimiento requerido en los servicios de correo actuales. Es muy útil ya que brinda una parte importante de la seguridad que se necesita en la mayoría de los servidores de correo actuales (POLICYD, 2014).

1.12.4. Fail2ban

Fail2ban es un lector de bitácoras del sistema licenciado bajo GPL. Su objetivo principal es bloquear las direcciones ip que fallan un determinado número de veces, lo cual se realiza actualizando el cortafuegos en los sistemas GNU/Linux. Permite la lectura de bitácoras de diferentes tipos de servicios como ssh, dovecot, postfix, apache, vsftpd, proftpd, qmail, exim y muchos más. Funciona para todas las distribuciones de GNU/Linux, lo cual lo ha convertido en una herramienta muy popular y poderosa, pues evita que determinados usuarios traten de obtener la contraseñas de otros usuarios en determinados servicios como aplicaciones web, de correo y más (FAIL2BAN, 2014).

1.12.5. **Altermime**

Altermime es una aplicación usada para la modificación de los mensajes entrantes y salientes en los servidores de correo electrónico de una organización. Es utilizada también para eliminar adjuntos, para lo cual se basa en el nombre del archivo o el tipo de contenido, así como reemplazar los adjuntos que se deseen (ALTERMIME, 2014).

1.12.6. **Awstats**

Awstats es una poderosa herramienta que genera estadísticas sobre el uso de servidores de correo, ftp, web, brindando los reportes graficados mediante páginas web. Este analizador de bitácoras es distribuido bajo la licencia GPL y funciona a la perfección en todas las distribuciones GNU/Linux. Muestra estadísticas sobre el número de visitas y su duración, los usuarios autenticados, sistemas operativos utilizados, tipos de navegadores, lista de máquinas que han visitado los servicios, los usuarios que más envían correos graficados por días, semanas, meses, el flujo de correos en la organización por días, semanas, meses, los dominios a los que se envían correos y desde donde se reciben y muchos más (AWSTATS, 2014).

1.12.7. **Mailman**

Mailman es utilizado para la distribución masiva de mensajes a múltiples usuarios de forma simultánea. Es un proyecto distribuido bajo la Licencia Pública General. Se ha escrito en los lenguajes de programación Python y C y a diferencia de otros productos similares asigna una página a cada lista de correo; además puede ser administrado en su totalidad a través de la web. Integra pasarelas de noticias, correo, incluyendo el archivado, manejo automatizado de rebotes, prevención de *spam*, tiene también soporte integrado para la web (incluyendo el archivado basado en la web), cuenta con varios idiomas y permite la sincronización de las listas mediante el protocolo ldap (MAILMAN, 2014).

1.12.8. **Davical**

Davical es un servidor para compartir el calendario. Está distribuido bajo la licencia GNU/GPL. Es una implementación del protocolo CalDAV²⁹, que está diseñado para el almacenamiento de los recursos de calendario en un servidor compartido remoto. Utiliza una base de datos relacional para el almacenamiento de los datos de los eventos y es compatible con WebDAV³⁰. Es muy útil para la gestión empresarial de las

²⁹ Protocolo para compartir calendarios y tareas.

³⁰ Conjunto de extensiones para el protocolo HTTP, que permite a los usuarios manejar y editar archivos de servidores web.

tareas y calendarios de una organización, por lo que es un agregado necesario en la mayoría de los servicios de correo (DAVICAL, 2014).

1.12.9. Fetchmail

Fetchmail es una herramienta completa y robusta de obtención y reenvío de correos electrónicos. Cuenta con una buena documentación y es compatible con todos los protocolos de obtención de correo electrónico remoto que están en uso en Internet como POP2, POP3, RPOP, APOP, KPOP, así como todas las implementaciones y versiones de IMAP, ETRN y ODMR. Recupera los correos de los servidores remotos y lo reenvía a través de SMTP, siendo entonces leídos por los agentes de correo de usuario normales. Ofrece mejor protección contra la detección de contraseñas por la red que cualquier otro cliente de correo electrónico remoto. Puede ser configurado para admitir el cifrado de extremo a extremo a través de un túnel con SSH (OFFICIAL FETCHMAIL, 2014).

1.13. Estrategias de migración de los servicios de correo electrónico

Una vez investigadas las tecnologías existentes para la gestión de los servicios de correo sobre plataformas GNU/Linux y haber determinado las que más se adaptan a las características existentes en varias de las instituciones cubanas, se procederá a investigar las estrategias existentes a nivel mundial para realizar la migración de los servicios de correo electrónico.

1.13.1. Migración sencilla desde servidores Lotus hacia Exchange

Este tipo de estrategia de migración implica la migración de todos los usuarios de forma simultánea. Incluye varios pasos, los cuales se mencionan a continuación:

- Seleccionar las herramientas de migración adecuadas.
- Crear objetos de destinatario en el servicio de directorio.
- Realizar los procedimientos de migración en un laboratorio de pruebas.
- La implementación del servicio de correo.
- Instalar el cliente de correo más adecuado y capacitar a los usuarios.
- Migrar los datos de usuario.
- Poner fuera de servicio los servidores que serán migrados para activar definitivamente los nuevos servicios de correo (MICROSOFT, 2014).

Ventajas de la migración sencilla

- Todos los usuarios migran al mismo tiempo, lo cual produce resultados rápidos.
- Se ahorra tiempo ya que no se necesita una fase de planificación porque la convivencia no tiene que ser probada.
- No hay ningún requisito para el mensaje o la conectividad del calendario entre los dos entornos de mensajería.
- Preservar las direcciones de correo electrónico existentes es más sencillo (MICROSOFT, 2013b).

Desventajas de la migración sencilla

- La migración de un gran número de usuarios o grandes cantidades de datos puede resultar en el tiempo de inactividad inaceptable.
- Se debe configurar la totalidad del entorno del servicio antes de migrar los usuarios.
- Es más difícil controlar el ritmo de la migración, pues no se puede optar por migrar divisiones o departamentos por separado.
- Se limita la flexibilidad debido a que no es posible dejar un grupo particular de usuarios en el sistema de correo que se necesite por alguna razón (MICROSOFT, 2013b).

1.13.2. Migración en varias fases desde servidores Lotus hacia Exchange

En las migraciones en varias fases, se utilizan los mismos procedimientos de migración que los empleados en las de una sola fase, pero estos procedimientos se realizan varias veces. En consecuencia, muchas de las cuestiones estratégicas que debe responder al diseñar una migración en una fase también son importantes al diseñar una migración en varias fases. No obstante, existen varios problemas adicionales relacionados con la coexistencia que se deben solucionar antes de migrar a los usuarios. Además de los pasos definidos para las migraciones en una fase, se debe:

- Conservar las rutas de los mensajes para mantener una transferencia de mensajes ininterrumpida. Durante la coexistencia, los usuarios deben poder enrutar y recibir correos electrónicos de otros usuarios corporativos y destinatarios de Internet. Debe asegurarse que los mensajes se transfieran a los destinos correctos, independientemente de la plataforma de correo del destinatario.
- Sincronizar la información de los directorios para que la información de la

CAPÍTULO 1: SERVICIOS DE CORREO ELECTRÓNICO

libreta de direcciones esté siempre actualizada y sea consistente. Cuando los usuarios envían mensajes de correo electrónico, tienen acceso a la dirección de correo electrónico actual de otros usuarios. Como resultado de este requisito, durante la coexistencia, los usuarios y las listas y grupos de distribución se deben mantener en ambos directorios.

- Sincronizar la información del calendario para proporcionar a todos los usuarios información actualizada de la disponibilidad. Muchas empresas utilizan el componente de calendario del sistema de mensajería como medio principal para programar reuniones. Esta funcionalidad debe estar disponible durante la coexistencia. De esta manera, los usuarios podrán ver cuándo otros usuarios están disponibles para una reunión y enrutar convocatorias de reunión entre entornos de correo (MICROSOFT, 2013a).

Ventajas de la migración en fases.

- La migración se realiza en pasos graduales y manejables. En una empresa grande, deben migrarse departamentos, unidades comerciales o equipos simultáneamente, así como a los usuarios que necesiten acceso a los calendarios y bases de datos de correo de cada uno de los otros durante la misma fase de migración.
- Se reducen los riesgos. Si una operación concreta de la migración en varias fases no se realiza correctamente, resultan afectadas un menor número de personas y es posible deshacer la operación con bastante rapidez. Si la migración de un grupo de usuarios no se realiza correctamente por cualquier razón, los usuarios pueden seguir trabajando hasta que se solucione el problema.
- Puede sincronizar la reconfiguración del cliente de mensajería y la formación del usuario final con la migración de buzones.
- Se tiene control sobre el ritmo de la migración. No es necesario establecer todo el entorno antes de migrar los usuarios. Se pueden realizar las implementaciones en el servidor y los clientes por etapas, según sus fases de migración (MICROSOFT, 2005).

Desventajas de la migración en fases.

- Comparadas con las migraciones en una fase, las migraciones en varias fases requieren más tiempo y por consiguiente son más costosas en cuanto a esfuerzo y precio del servicio.

CAPÍTULO 1: SERVICIOS DE CORREO ELECTRÓNICO

- La nueva infraestructura de mensajería no puede reflejar las direcciones de correo electrónico existentes. Es difícil mantener las direcciones de correo electrónico existentes, ya que los procesos de transferencia de mensajes utilizan la información de direcciones
- Ambos sistemas de mensajería se deben mantener y se les debe prestar soporte técnico durante un período de tiempo (MICROSOFT, 2005).

1.13.3. Migración utilizando tecnologías similares

Este tipo de migración de los servicios de correo comprende la migración de los mismos, pero no tiene en cuenta el cambio de las tecnologías, pues asume que los nuevos servicios tendrán las mismas tecnologías que las existentes en el servidor antiguo.

Se divide en 5 pasos, los cuales se mencionan a continuación:

1. Configurar el nuevo servicio de correo, creando los buzones de correos, reenviadores y registros de dns³¹ necesarios.
2. Crear un subdominio en el nuevo servidor y crear los reenviadores necesarios desde ese subdominio al dominio actual.
3. Una vez que los registros dns para el subdominio creado se han propagado se mueven todos los datos necesarios hacia el nuevo servidor.
4. Configurar los reenviadores en el sistema antiguo hacia el nuevo subdominio. De esta manera, al llegar los correos al subdominio en el nuevo servidor los correos son reenviados nuevamente hacia el dominio requerido de manera local.
5. Cambiar los registros dns del antiguo servidor para el dominio requerido en el nuevo servidor. Esto permitirá que todo el tráfico generado hacia ese dominio vaya hacia el nuevo servidor directamente (EDGE OF WEB, 2013).

1.13.4. Estrategia de migración de correo de la compañía *Connected software*

La compañía *Connected software* es un *partner* certificado de Microsoft que brinda soluciones de migración de los servicios de correo, ya basadas en su experiencia de más de 8 años con migraciones en más de 70 países. Entre sus investigaciones se encuentra la concepción del planeamiento e implementación de un proyecto de migración de correo.

Para ello, los autores plantean que se deben dividir las tareas en 5 partes

³¹ Sistema de nombres de dominio.

fundamentales:

1. Inventario de la información a ser migrada.
2. Hacer coincidir el inventario de información con las posibilidades de migración de datos con que cuentan las herramientas de migración.
3. Evaluar y seleccionar el *software* al que se migrará el nuevo servicio de correo.
4. Llevar a cabo un proyecto piloto y solicitar retroalimentación de los usuarios.
5. Llevar a cabo la migración completa.

1.14. Conclusiones del capítulo

Sobre las estrategias de migración analizadas en este capítulo se detectó que a pesar de que cuentan con un conjunto de etapas comunes y útiles, las mismas no brindan toda la información necesaria para que puedan ser utilizadas. Otro aspecto clave es que no comprenden la migración hacia aquellas tecnologías de software libre que mejor se adaptan a las condiciones de hardware y ancho de banda como la existente en algunos organismos en Cuba. Luego de haber investigado las tecnologías para el montaje de una infraestructura de servicios de correo se pudo percibir que como agente de transferencia de correo, Postfix se adapta en mayor medida a los requisitos necesarios, también Dovecot como agente de entrega de correo, Roundcube como cliente de correo web, *SpamAssassin* para la detección de correos spam y ClamAV como antivirus. Fueron identificadas las siguientes tecnologías adicionales: Amavis, Sieve, Cluebringer, *Fail2ban*, Altermime, Awstats, *Mailman*, Davical y *Fetchmail*.

CAPÍTULO 2

ESTRATEGIA PARA LA MIGRACIÓN DE LOS SERVICIOS DE CORREO ELECTRÓNICO EN CUBA

En muchas ocasiones las tareas de migración de los servicios de correo son enfrentadas confiando en la experiencia de los ejecutores. Es de vital importancia utilizar una estrategia (Proceso regulable, conjunto de las reglas que aseguran una decisión óptima en cada momento (RAE, 2014)) que contemple las acciones que serán necesarias realizar para que la migración de los servicios de correo electrónico sea un éxito. Las mismas permiten un ahorro de tiempo, la adecuación a entornos específicos y evitan la introducción de errores en el proceso. Después de revisar diferentes estrategias y concluir que existen un grupo de aspectos comunes que no deben dejarse de valorar en los procesos de migración de los servicios de correo se hace el planteamiento de una estrategia para migración de los servicios de correo en Cuba. La misma cuenta con varias etapas y son mencionadas a continuación:

- Recogida de información.
- Elección del sistema operativo a usar.
- Investigación de alternativas para GNU/Linux.
- Formación.
- Montaje de la solución.
- Investigación sobre migración de los servicios de correo de la empresa.
- Pruebas de migración sobre los servicios de correo de la empresa.
- Realizar salvadas de seguridad de los datos.
- Migración de los servicios de correo electrónico.
- Monitoreo de los servicios.
- Seguridad en los servicios colocados.
- Definir políticas de salvadas automáticas de los servicios migrados.
- Planificación del soporte.

La siguiente figura muestra la relación entre la ejecución y continuidad de cada una de estas etapas. Obsérvese que en algunas ocasiones no es necesario que una etapa culmine para comenzar la otra, mientras que en otras sí. Así mismo, hay etapas que pueden realizarse de manera simultánea con otras.

CAPÍTULO 2: ESTRATEGIA PARA LA MIGRACIÓN DE LOS SERVICIOS DE CORREO ELECTRÓNICO EN CUBA

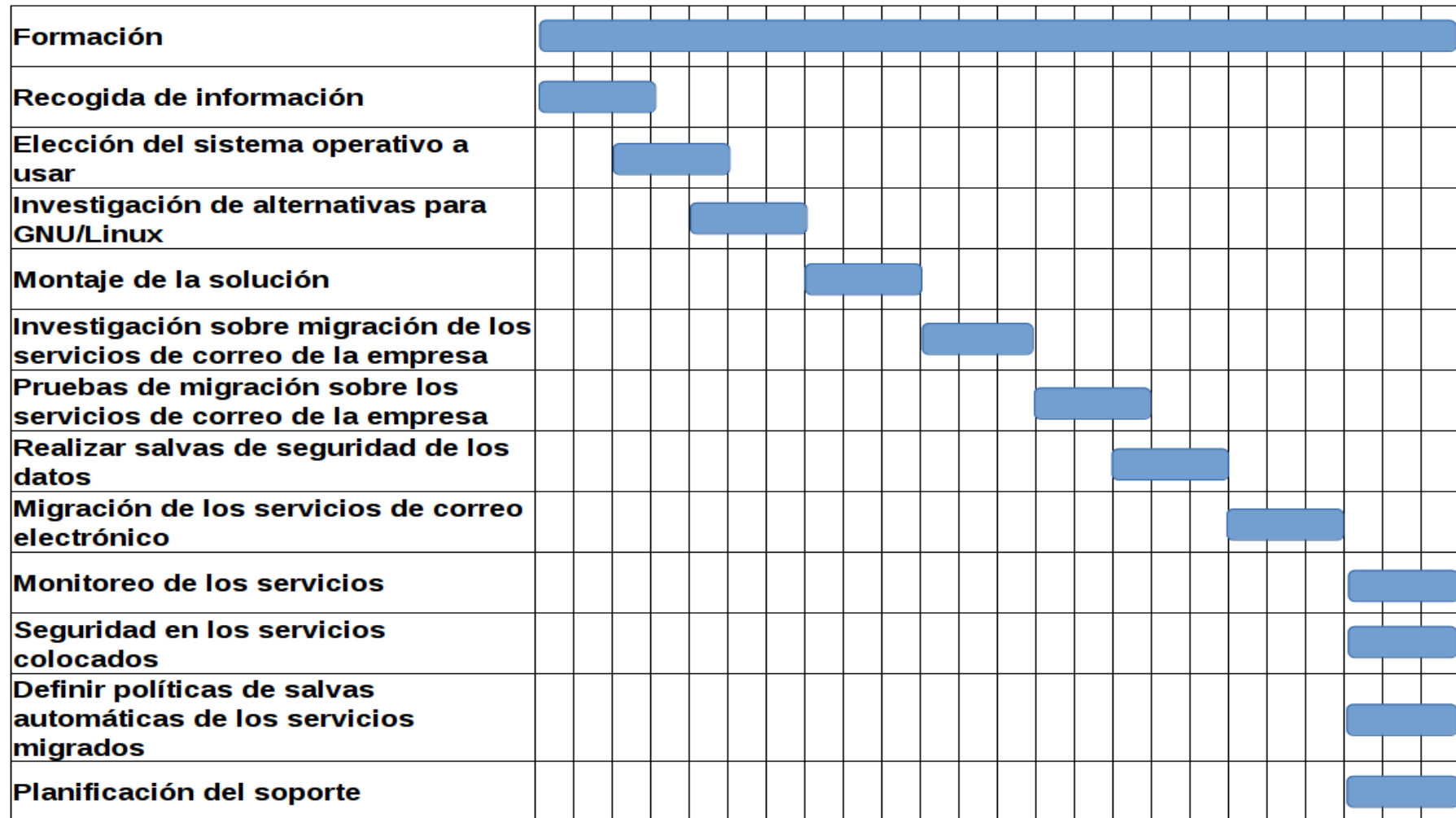


Figura 2. Relación entre las etapas de la estrategia de migración de los servicios de correo electrónico.

CAPÍTULO 2: ESTRATEGIA PARA LA MIGRACIÓN DE LOS SERVICIOS DE CORREO ELECTRÓNICO EN CUBA

2.1. Fundamentación de las etapas de la estrategia de migración

A continuación se realizará una explicación más detallada de cada una de las etapas de la estrategia propuesta:

2.1.1. Recogida de información

Cuando se desea enfrentar el cambio de plataforma de los servicios de correo electrónico en los servidores de una empresa, lo primero que deberán realizar los encargados de esta tarea, debe ser la recogida de información del servidor o los servidores que cumplen esta función, teniendo en cuenta, que tanto el *software* como el *hardware* instalado, son de suma importancia para tomar varias decisiones durante el transcurso de la migración.

Para ello, debe realizarse un documento que identifique cada servidor por su nombre, en el que se reflejen los aspectos principales de *hardware* y *software* de cada uno. Cabe aclarar que esta recogida de información debe ser realizada de la forma más eficiente posible, ya que una vez que se haya terminado este proceso, el equipo de migración, podrá comenzar a tomar acciones y tendrá una visión bastante precisa de la complejidad del proceso de migración. Para más detalles remitirse a los [anexos](#).

A continuación se expondrá mediante explicaciones y en forma de ejemplos la mayoría de los aspectos que se consideran necesarios recoger para cumplir este objetivo:

2.1.2. Elección del sistema operativo a usar

El autor opina que desde varios puntos de vista, no existe una diferencia sustancial entre alguna de las distribuciones de GNU/Linux que se usan para brindar cualquier tipo de servicio en un organismo determinado, ya sea Debian GNU/Linux, Ubuntu GNU/Linux, Nova GNU/Linux, Centos GNU/Linux, Fedora GNU/Linux, OpenSUSE GNU/Linux, o cualquier otra de las muchas distribuciones existentes. En este punto, se debe tener en cuenta, que algunas de estas distribuciones brindan soporte, lo cual puede ser visto como una gran ventaja, que permitiría tener a quien acudir en caso de ocurrir algún problema en un momento determinado, incluso, algunas de estas distribuciones, pueden brindar un soporte inmediato y en el caso de Cuba, la única distribución que brinda soporte es la distribución cubana Nova GNU/Linux, que además cuenta con una edición para servidores, por lo que constituye una muy buena opción a la hora de analizarse un candidato de distribución de GNU/Linux para brindar los servicios de correo.

CAPÍTULO 2: ESTRATEGIA PARA LA MIGRACIÓN DE LOS SERVICIOS DE CORREO ELECTRÓNICO EN CUBA

El manejo y comodidad sobre estos sistemas mencionados, tanto del personal de la institución como del equipo de migración pudiera ser otra razón fuerte para decidirse por una de ellas. Es necesario tener en cuenta que estas razones anteriores, deben estar sujetas además a un estudio de compatibilidad de *hardware* y *software* minucioso.

Como se ha visto hasta el momento, la elección de la distribución de GNU/Linux que se usará, pudiera tomarse debido al conocimiento previo de algunos de los implicados en el proceso de migración o del equipo de migración que está trabajando en la tarea con una de ellas, también por las ventajas que brinda el soporte sobre algunos de estos sistemas o por el buen o mejor funcionamiento de algún tipo de *software* o controlador en alguna de estas distribuciones.

2.1.3. Investigación de alternativas para GNU/Linux

Las alternativas recomendadas para la gestión y migración de los servicios de correo electrónico en varias de las instituciones cubanas son las siguientes:

- Agente de transferencia de correo: Postfix.
- Agente de entrega de correo: Dovecot.
- Filtro de correos *spam*: *SpamAssassin*.
- Antivirus: ClamAV.
- Interfaz de comunicación con Agente de transferencia de correo: Amavis.
- Descarga de correos en buzones remotos: *Fetchmail*.
- Cliente de correo web: Roundcube.
- Herramienta para la detección de intentos de hackeo: *Fail2ban*.
- Herramienta para la obtención de estadísticas del envío de correos: Awstats.
- Servidor de políticas para postfix: Cluebringer.
- Envío masivo de listas de correo: *Mailman*.
- Gestión de calendarios y tareas: Davical.
- Modificación de correos entrantes y salientes: Altermime.
- Lenguaje para filtrado de mensajes de correo electrónico: Sieve.

Debe ser destacado, que aunque estas tecnologías han sido investigadas, sería importante retomar las investigaciones realizadas cada vez que se inicia un proyecto de migración, pues de esta forma se potenciará la posibilidad de que alguna nueva tecnología aparezca, o algunas de las competencias a las soluciones ya investigadas haya superado a las que en tiempos anteriores hayan sido las candidatas seleccionadas, lo cual suele suceder en ocasiones.

CAPÍTULO 2: ESTRATEGIA PARA LA MIGRACIÓN DE LOS SERVICIOS DE CORREO ELECTRÓNICO EN CUBA

A pesar de que el personal encargado de atender los servicios de correo pueda no estar capacitado para trabajar con sistemas operativos GNU/Linux, es necesario destacar la importancia de la preparación de los mismos en los temas relacionados con los servicios telemáticos, pues de no cumplirse esto, el colocar una solución bastante completa y que haga un uso bastante extensivo de los protocolos implicados, pudiera traer complicaciones innecesarias en el manejo de ese servicio en la empresa.

Siempre será importante analizar cuan necesario le es a la empresa contar con niveles de seguridad altos, o sencillamente aceptables, pues las alternativas buscadas y sus configuraciones específicas pueden variar en dependencia de la compañía. Desde este punto de vista, pueden ocurrir variaciones si se maneja información clasificada, donde se debe tener en cuenta una definición detallada de los accesos a cada servicio o si se trabaja en un organismo donde haya menor riesgo y manejo de información.

Es posible que quienes administren los servicios y soluciones encontradas, no serán los que mayor peso tuvieron en la decisión de colocarlos, por lo que otro de los puntos a tener en cuenta es la documentación existente, siendo necesario de esta forma que la solución investigada e implantada en los servidores cuente con un amplio conjunto de información en la web, que le pueda servir a quienes se enfrenten a un problema específico, solucionarlo lo más rápido posible.

En ocasiones, algunas de las soluciones encontradas, no cuentan con un soporte activo, y muchas veces, solo las sigue una comunidad pequeña de desarrolladores, siendo una muy buena práctica, seguir de cerca y tratar de escoger soluciones que tengan una comunidad grande que les de soporte continuamente, evitando de esta forma el riesgo a que se quede descontinuada la solución implantada durante la investigación y el servidor se quede con los servicios colocados, sin actualizaciones, prácticamente obsoletos con el paso del tiempo.

Es necesario señalar que ciertamente, a simple vista puede observarse un conjunto elevado de variables a tener en cuenta, y que por tal motivo es muy aconsejable que el personal que se encuentre enfrentando la tarea cuente con un equipo de migración o varios miembros de experiencia en tareas de este tipo, de esta forma la posibilidad de tener éxito será mucho mayor, pues personas expertas en estas áreas tendrán claro siempre que la solución más rápida, sencilla, y fácil, puede no ser la más segura, confiable y flexible.

De esta forma durante la ejecución del proyecto de migración deben tenerse en cuenta varios parámetros en cada uno de las tecnologías investigadas. A continuación se exponen los que se pueden aplicar de forma general:

CAPÍTULO 2: ESTRATEGIA PARA LA MIGRACIÓN DE LOS SERVICIOS DE CORREO ELECTRÓNICO EN CUBA

- Licencia.
- Facilidad de administración.
- Documentación.
- Flexibilidad.
- Rendimiento.
- Seguridad.
- Soporte.

2.1.4. Formación

El personal de la institución que se involucrará en el proyecto, junto a los expertos de migración, deben trabajar en conjunto. Esto permitirá un mejor entendimiento entre las partes implicadas, pues internamente es donde mayor conocimiento se tiene de los procesos que a diario se llevan a cabo en los servicios de correo, para lo cual es importante formar parte del equipo de trabajo a los administradores de red de la empresa, así como a todos trabajadores que se determine que sea necesario incluir. La formación comienza desde el inicio del proyecto de migración, durante las primeras reuniones realizadas con los principales cuadros de dirección y administradores de red de la empresa hasta la finalización del mismo y para lograr que se realice con la mayor calidad posible, es importante realizar varias acciones, que asegurarán el éxito en todo el proceso.

De esta manera y con intencionalidad formativa se pueden planificar encuentros cada cierto tiempo con determinadas áreas donde se explique el estado en que se encuentra la migración, las acciones a realizar, se preparen y discutan materiales y documentos que ayuden a todos los usuarios de la red a informarse de los cambios que se están realizando.

Es una buena práctica haber iniciado un proceso gradual de información a los usuarios de la institución desde el inicio del proyecto a través de los medios con que cuenta la empresa para estos fines, los cuales pudieran ser el correo electrónico, la intranet de la institución, matutinos o reuniones periódicas que se realicen.

Cuando el proyecto de migración haya avanzado completamente en sus investigaciones y pruebas, se deben tener claros, todos los cambios que pueden ocurrir a la vista del usuario en la nueva plataforma con respecto a la antigua, pues aunque la premisa debe ser mantener los datos, informaciones y configuraciones transparentes al usuario, no siempre se podrá cumplir este objetivo.

Entre estos cambios pueden mencionarse la interfaz del nuevo cliente de correo web,

CAPÍTULO 2: ESTRATEGIA PARA LA MIGRACIÓN DE LOS SERVICIOS DE CORREO ELECTRÓNICO EN CUBA

nuevos clientes de correo, posibles nuevas configuraciones en los protocolos de los clientes de correo existentes, acciones a tomar para que los usuarios no vayan a perder algún tipo de datos, algún nuevo nombre de dominio que se incluirá, nuevas direcciones ip a las que los usuarios accederán, así como nuevas formas de realizar determinadas tareas en la red.

Para ello pudiera realizarse un conjunto de materiales en formato digital y enviarse por correo o publicarse en lugares accesibles por todos. También puede ser de mucha ayuda la elaboración y publicación en la intranet u otro medio existente en la organización, de video tutoriales y multimedias que expliquen la utilización de las nuevas tecnologías para que el cambio sea lo más sencillo posible y quienes utilicen los servicios de correo se adapten lo más pronto posible a la nueva plataforma de servicios una vez migrada, permitiendo que se pierda la menor cantidad de horas de trabajo.

La capacitación tiene una gran importancia en la futura interacción de los trabajadores con el sistema operativo y las nuevas aplicaciones que se utilizarán en la institución, así como con los servicios y tecnologías que se brindarán. Si esta no resulta lo más completa posible y no les es realmente provechosa a quienes la reciban, es muy posible que en un futuro no puedan enfrentarse a los nuevos problemas o requerimientos que puedan surgir.

Una de las acciones que deben tomarse para cumplir el propósito anteriormente mencionado debe ser impartir un paquete de cursos de entrenamiento al personal involucrado. Dicha formación debe estar enfocada en impartir los contenidos que son estrictamente necesarios en la institución, estando acorde con los servicios y aplicaciones detectadas durante la recogida de información y con las alternativas a los servicios privados que se determinó que se utilizarían para sustituir los servicios sobre las plataformas privadas.

Una vez encontradas las alternativas a los servicios de correo que se desean migrar, conocer el sistema operativo sobre el cual se soportarán las nuevas tecnologías y tener claro todas las funcionalidades que se utilizan en la empresa, tanto directamente los usuarios, como las relacionadas directamente con los servidores, se puede elaborar una capacitación que tenga en cuenta todas las funcionalidades que se requerirán utilizar una vez implantado el nuevo servicio.

De esta forma se agilizaría el proyecto posibilitando que quienes asistan a los cursos no reciban conocimientos que a corto plazo no necesitarán. Lo anterior no significa, que los entrenamientos solo se enfoquen en la instalación, configuración,

CAPÍTULO 2: ESTRATEGIA PARA LA MIGRACIÓN DE LOS SERVICIOS DE CORREO ELECTRÓNICO EN CUBA

administración, seguridad y optimización de los servicios de correo, pues en la mayoría de los casos puede ser muy útil comenzar la capacitación impartiendo cursos sobre el *software* libre y las ventajas que este puede traer en el ámbito que se usará, o sobre la instalación y configuración de los clientes de correo con los nuevos servicios que se colocarán, así como cursos del sistema operativo elegido para el despliegue de las soluciones, un aspecto de importancia teniendo en cuenta que el adecuado manejo del sistema operativo sobre el cual se investigará y desplegarán las soluciones será la base para el mejor entendimiento de las tecnologías que se usarán.

2.1.5. Montaje de la solución

Durante la recogida de la información y el estudio de las alternativas y tecnologías, los especialistas encargados de realizar la migración de los servicios de correo electrónico deben haber investigado y probado varias herramientas y tecnologías y finalmente haberse decidido por una de ellas teniendo en cuenta los diferentes parámetros que se mencionaron anteriormente y que en muchos casos, tienen mayor peso en algunas organizaciones que en otras.

Es un buen momento, para de una forma más pausada, ejecutar estas soluciones sobre servidores u ordenadores destinados con este fin. Esta etapa servirá para realizar pruebas más precisas de cada una de las funcionalidades necesitadas, siendo oportuno que tanto todos los involucrados en la migración, como la administración de la empresa y muy importante, una parte de los usuarios puedan probar las nuevas tecnologías que se utilizarán y compararlas con las actuales, permitiendo de paso comprobar la estabilidad y comportamiento de los servicios instalados.

De esta forma se podrán realizar cambios de acuerdo a las sugerencias recibidas por todos los involucrados en esta tarea. Sería recomendable colocar nuevas funcionalidades en los servicios que se brindarán que hagan al usuario notar que el cambio de plataforma de los servicios de correo también les será beneficioso a ellos. También sería la ocasión ideal para presentarle a la administración las soluciones encontradas, reafirmando la adecuación de las alternativas y tecnologías que se usarán en la institución objetivo.

Para esta etapa puede ser necesario utilizar servidores para realizar dicha tarea, aunque en ausencia de esta posibilidad, pudieran usarse ordenadores con prestaciones inferiores y de igual forma se podrán realizar pruebas y mantener los servicios activos durante el tiempo que se necesite mantenerlos en línea.

En caso de no disponerse de recursos para adquirir servidores o utilizar otros ordenadores con este fin, siempre tendrá la alternativa de realizar estas pruebas en los

CAPÍTULO 2: ESTRATEGIA PARA LA MIGRACIÓN DE LOS SERVICIOS DE CORREO ELECTRÓNICO EN CUBA

puestos de trabajo del personal enfrascado en la tarea, aunque debe tenerse en cuenta siempre, que mientras más alejado esté el *hardware* utilizado en las pruebas del escenario en que se usará, más lejos estará el desempeño real del *software* en el ambiente donde se desplegará.

2.1.6. Investigación sobre migración de los servicios de correo de la empresa

Llegado este punto se instalarán y configurarán sobre ordenadores destinados para este fin los servicios de correo privados presentes en la institución para comenzar la realización de pruebas de migración. Debe mencionarse que las configuraciones y escenarios sobre los servicios de correo privados se realizará lo más similar posible al entorno real donde se encuentran los servicios de la compañía.

Para este fin se utilizará toda la información obtenida durante la recogida de las funcionalidades presentes en los servicios de correo. Una vez con el entorno de servicios privados ejecutándose y datos introducidos en los mismos lo más similar posible al entorno real, se comenzará la investigación sobre la migración hacia cada una de las alternativas encontradas.

Es importante destacar que no se debe comenzar la realización de estas pruebas sobre los propios servicios de correo de la institución, pues algún descuido o mal entendimiento de los procedimientos de migración podría provocar pérdida o daño en la información de los usuarios.

Inicialmente se debe tener una idea de las maneras en que se realizará la migración de los datos, pues ya se deben haber realizado algunas investigaciones iniciales sobre este tema durante la evaluación de las alternativas a los servicios privados o al menos estar seguros de que una migración hacia la alternativa es factible, pero es importante destacar que en muchas ocasiones se necesitará ser creativo e innovador para adecuar los mecanismos que existen para trasladar los datos necesarios desde los servidores con plataformas privadas hacia las plataformas deseadas. De esta forma puede ser útil el trabajo con potentes lenguajes interpretados como Python, Bash y Perl, los cuales son muy eficientes tanto en el trabajo en la red, como con ficheros y comandos en los sistemas operativos GNU/Linux.

Es importante chequear que ninguno de los procedimientos necesarios para realizar la migración afecta de alguna forma, las configuraciones y datos sobre los servicios privados, ya que siempre se debe tener la posibilidad de regresar hacia atrás en caso de que algo salga mal durante la migración de los servicios y no se tenga que depender de solucionar algún problema que pueda tardar varias horas o incluso días

CAPÍTULO 2: ESTRATEGIA PARA LA MIGRACIÓN DE LOS SERVICIOS DE CORREO ELECTRÓNICO EN CUBA

para resolverse.

Debe tenerse en cuenta que este paso es bastante crucial, debido a que la migración de los servicios de correo debe ser lo más transparente posible al usuario aunque no siempre se pueda lograr totalmente, valorando que aunque los usuarios no noten el cambio de servicio, tampoco los nuevos que se colocarán deben sacrificar el buen funcionamiento soportado y heredar errores o problemas de seguridad de los antiguos servicios.

La solución encontrada para la migración de los servicios de correo privados en una empresa variará en dependencia de varios factores, los cuales son principalmente:

- El *software* utilizado para brindar los servicios de correo privados de la institución.
- Las funcionalidades utilizadas del servicio de correo privado.
- El *hardware* existente para la migración del mismo hacia tecnologías libres.

Ante la imposibilidad de migración de algún tipo de datos, sí se debe tener claro que los buzones de correo de todos los usuarios deben ser migrados en su totalidad y en dependencia de la tecnología privada y las herramientas existentes en el momento de la migración debe tratarse de migrar en lo posible la mayor cantidad de datos y funcionalidades hacia las alternativas libres deseadas, haciendo mayor énfasis en aquellas que más utilizan los usuarios, como pudieran ser listas de correo, calendarios, tareas, contactos. Esto no quiere decir que no se puedan migrar datos de manera manual, pues si no es considerable el esfuerzo siempre será una buena opción la migración de la mayor cantidad de datos posible, pues lo más importante es la satisfacción de los usuarios durante la implantación de las nuevas tecnologías.

2.1.7. Pruebas de migración sobre los servicios de correo de la empresa

Una vez realizadas todas las pruebas de migración desde los servicios de correo privados hacia la plataforma GNU/Linux escogida, tratando de reflejar en lo mayor posible el mismo escenario existente en la institución, debe haber una seguridad casi total del correcto funcionamiento de la migración de los datos de los usuarios. Además deben haberse tomado acciones para mitigar el riesgo de perder información y configuraciones en los servicios sobre la plataforma privada en caso de haberse detectado alguna posibilidad de pérdida o variación en la información.

Es el momento adecuado para comenzar a realizar las pruebas de migración de los

CAPÍTULO 2: ESTRATEGIA PARA LA MIGRACIÓN DE LOS SERVICIOS DE CORREO ELECTRÓNICO EN CUBA

datos y configuraciones sobre los servicios privativos instalados en los servidores de correo de la institución. Para ello se tendrá en cuenta que a pesar de haberse realizado sobre otros servicios privativos con las mismas características que los que se están usando, estas pruebas comprenden la interacción con los servicios que están siendo explotados en la institución, por lo que cualquier precaución que se tenga es poca y debe realizarse con extrema responsabilidad, teniendo en cuenta los posibles cambios que pudieran provocarse en algunos de los servicios durante el proceso de traslado de información.

Estas pruebas pueden tener como resultado final, la presentación de los servicios migrados a la dirección de la empresa y la discusión de cada uno de los logros obtenidos por el equipo de migración. Será el momento idóneo para dejar todo listo como mismo se tendrá una vez migrados los servicios.

También se podrá escoger determinado conjunto de usuarios e informarles de la dirección donde se encuentran los servicios que están siendo migrados a modo de prueba, para que estos puedan darle uso a los mismos, lo cual le permitirá al equipo de migración verificar que los datos han sido migrados correctamente, y además retroalimentarse con sus opiniones sobre las soluciones probadas.

2.1.8. Realizar salvas de seguridad de los datos

Es importante partir del concepto de que aunque el objetivo principal del proyecto es la migración hacia servidores GNU/Linux, los datos e informaciones que se encuentren sobre los servidores en las plataformas privativas deben almacenarse al menos por un año, debido a que aunque se migrará la información de los usuarios y sus datos, no será necesario migrar las trazas de los usuarios en los servicios, las cuales pueden servir para auditar en un momento dado el comportamiento de los usuarios en la red en tiempos anteriores. También la Oficina de Seguridad de Redes Informáticas de Cuba lo exige y puede solicitar una auditoría durante ese tiempo, así como cualquier otra información que pudiera ser útil para los administradores de la red. Además, durante los días iniciales sería una garantía tener estos servicios a mano, pues pueden llegar a ser necesitados con urgencia para realizar una regresión en el menor tiempo posible hacia ellos en caso de algún problema serio que pudiera ocurrir.

La recomendación principal para realizar esta salva de los servicios es nunca eliminar la información de los discos duros de los servidores con las tecnologías privativas y además realizar copias enteras a la información de los discos duros, y guardarlos en lugares seguros, una vez que se coloquen los servicios sobre las plataformas migradas, aunque todo esto siempre dependerá de la forma en que se estén

CAPÍTULO 2: ESTRATEGIA PARA LA MIGRACIÓN DE LOS SERVICIOS DE CORREO ELECTRÓNICO EN CUBA

realizando las salvadas en la organización por lo que pudiera ser innecesario guardar la información debido a que en todas las organizaciones deben existir salvadas automáticas de todos los servicios que se brindan.

2.1.9. Migración de los servicios de correo electrónico

Una vez esté todo preparado en la organización y el equipo de migración está seguro de que todos los pasos realizados con anterioridad se han cumplido satisfactoriamente y además las personas encargadas de permitir los cambios sobre las plataformas han dado su autorización se puede proceder con la migración de los servicios de correo privados en la empresa.

Para ello debe tener en cuenta, que comenzará a realizarse el proceso más importante y sensible durante todo el proyecto, pues es el que involucra directamente el objetivo principal por el que se inició. La migración de los servicios de correo se realizará utilizando una de las dos siguientes maneras:

- Instalación y migración de los servicios de correos en un nuevo servidor.
- Instalación y migración de los servicios de correos en un disco duro, en caso de que no se cuente con un servidor para este fin.

En ambas se debe proceder a realizar la instalación y configuración de todas las tecnologías libres de los servicios de correo electrónico. Para ello se tendrá en cuenta las pruebas realizadas en los entornos de prueba anteriores y no se dejará pasar por alto que se soporten todas o la mayoría de las funcionalidades detectadas durante la recogida de información y que fueron probadas durante las etapas anteriores.

Luego que el entorno se encuentre listo se procederá a migrar los datos existentes en los servicios privados de la organización. El orden expresado anteriormente no tiene necesariamente que ser así, pues después de la migración de los datos puede ser necesario realizar algunas configuraciones a los servicios de correo electrónico. Por su importancia cabe destacar que deben crearse todos los usuarios de los servicios de correos o tomarlos de algún lugar de la red donde se encuentren centralizados como una base de datos mysql, ldap o directorio activo y la dirección de los buzones de cada uno debe coincidir con la ubicación de cada uno de sus antiguos buzones ya en el nuevo servidor.

Al haberse colocados todos estos datos será necesario realizar pruebas de funcionamiento a los nuevos servicios de correo migrados, para lo cual hay que detener los servicios de correo actuales, y realizar pruebas de envío y recepción de correos una vez se desconecte el antiguo servicio y se conecte el nuevo. Estas

CAPÍTULO 2: ESTRATEGIA PARA LA MIGRACIÓN DE LOS SERVICIOS DE CORREO ELECTRÓNICO EN CUBA

pruebas deben realizarse con correos enviados dentro y hacia afuera de la organización. Cuando se haya comprobado que los nuevos servicios funcionan a la perfección para lo primordial que deben funcionar que es el envío y recepción de correos, se puede conectar nuevamente el antiguo servicio de correos y se pasa a asegurarse que cada una de las funcionalidades que se desea que estén en el nuevo servicio efectivamente funcionen bien, esto incluye, tanto los datos migrados de los usuarios en el servidor, configuraciones existentes en el antiguo servidor o nuevas configuraciones que se hayan requerido realizar. De manera general deberán probarse:

- Listas de correo.
- Contactos.
- Gestión de calendarios y tareas.
- Envío de correos mediante el cliente de correo web.
- Envío de correos mediante los clientes de escritorio.
- Funcionamiento de la detección de correos enviados con virus en la organización.
- Funcionamiento de la detección de correos *spam* y la gestión de listas blancas, negras y grises.
- Las claves no se envían en texto plano por la red.
- No se pueden enviar correos con tamaño mayor que el establecido en el servidor.
- Solamente se pueden enviar correos con los adjuntos que tengan las extensiones permitidas en el servidor de la organización.
- La cuota de cada usuario funciona bien y se envían los correos deseados cuando esta alcanza los límites establecidos.
- No se permite el envío de correos ofensivos en la organización y esto no interfiere en el envío de correos permitidos de la organización.
- Se toman acciones en los servicios de correo para prevenir el espionaje corporativo y la contrarrevolución en la organización.
- Cada vez que se envía un correo se le envía una copia a un usuario encargado de almacenar todos los correos de la organización.

CAPÍTULO 2: ESTRATEGIA PARA LA MIGRACIÓN DE LOS SERVICIOS DE CORREO ELECTRÓNICO EN CUBA

- Se mantienen los permisos de los usuarios para enviar correos a determinados dominios.
- Una vez que se realiza una determinada cantidad de intentos de acceso fallidos, se bloquea esa dirección por un tiempo determinado.
- Funcionan los reportes sobre las estadísticas del uso del servicio de correo.
- Los usuarios definidos con anterioridad pueden acceder a cualquier buzón de la organización
- Los usuarios pueden compartir carpetas de su buzón a otros usuarios dentro de la organización.
- Funcionamiento de los alias en el servidor.
- Se pueden adjuntar mensajes a todos los correos de la organización enviados por los usuarios.
- El firewall se encuentra activado mientras todas las pruebas se realizaban.

Posterior a la realización de todas estas pruebas, en el caso de haber instalado las tecnologías en un nuevo servidor solamente queda apagar los servicios privativos y dejar el nuevo servidor en funcionamiento. Es posible que haya habido que crear o cambiar algún registro en el dns para los clientes de escritorio o con otro fin, aunque puede analizarse la posibilidad de colocar la misma dirección ip al nuevo servidor de correos, algo que siempre deberá ser valorado.

En caso de solamente haber contado con discos duros, puede proceder a colocar el disco o los discos duros con las configuraciones realizadas y las tecnologías migradas en el servidor de correos y remover el disco duro con las tecnologías privativas.

En ambos casos debe estar preparado para una posible regresión, pues aunque se hayan realizado muchas pruebas, la prueba de mayor importancia se lleva a cabo en el momento de la sustitución de los viejos servicios por los nuevos en el entorno real.

A partir de ese momento comenzarán las pruebas reales de los usuarios y deberán existir mecanismos de retroalimentación directos para ir solucionando los problemas que puedan presentarse, teniendo en cuenta que ante una falla que no se pueda solucionar rápidamente es preferible regresar por unos días a los antiguos servicios hasta que se solucione el problema encontrado.

Para asegurarse de que los procesos de migración no se vean comprometidos debido a configuraciones con altos niveles de seguridad, y se logre agilizar el proceso, algunos aspectos de seguridad pueden no ser necesarios tenerse en cuenta, algo que

CAPÍTULO 2: ESTRATEGIA PARA LA MIGRACIÓN DE LOS SERVICIOS DE CORREO ELECTRÓNICO EN CUBA

es recomendable en la mayoría de las instituciones en que no se requieran altos niveles de seguridad.

2.1.10. Monitoreo de los servicios

Los momentos iniciales a la ejecución de los servicios de correo electrónico pueden ser útiles para realizar un monitoreo del estado de los servicios migrados, comprobando el consumo del procesador, memoria RAM, carga en la red, accesos a disco; algo importante a tener en cuenta, considerando la gran cantidad de procesos de lectura y escritura que se realizan en los servidores de correo.

También debe monitorearse el uso de las tecnologías presentes en los servicios de correo, tomando las acciones correspondientes para enfrentar los momentos en que mayor sobrecargado se encuentre el servidor y las tecnologías utilizadas en el mismo. De esta forma se pueden ir ajustando los parámetros que permitirán continuar brindando el servicio de la forma más estable y eficiente posible, pues es importante explotar al máximo las capacidades de las tecnologías utilizadas y las prestaciones de *hardware* con que cuenta el servidor.

2.1.11. Seguridad en los servicios colocados

De acuerdo al tipo de organización, se puede necesitar determinados niveles de seguridad, lo cuales pueden variar entre niveles aceptables donde un cortafuegos puede ser suficiente para establecer el acceso a sus recursos y otros, donde sea necesario colocar sistemas de detección de intrusos basados en *hosts*, basados en red y cortafuegos con políticas de accesos bien definidas y restricciones a los servicios lo más controladas posible.

Una vez realizada la migración de los servicios de correo, haber verificado su estabilidad, así como la información migrada desde las plataformas privativas y haberse monitoreado los mismos es un buen momento para explotar al máximo las potencialidades que brindan las distribuciones GNU/Linux para establecer las políticas de seguridad de acuerdo a las necesidades de la organización y a las políticas establecidas por los organismos competentes.

A medida que se trabaje en la seguridad de los servicios, debe irse realizando un proceso de pruebas en el acceso a los mismos, tanto para estar seguros de que no se puede acceder a los lugares restringidos, como para comprobar que se puede acceder a los lugares que se requiere que sean accesibles por los usuarios, lográndose la confidencialidad, disponibilidad e integridad de la información en todos los casos.

CAPÍTULO 2: ESTRATEGIA PARA LA MIGRACIÓN DE LOS SERVICIOS DE CORREO ELECTRÓNICO EN CUBA

2.1.12. Definir políticas de salvallas automáticas de los servicios migrados

Una vez migrados los servicios, se establecerá una política de salvallas para el servidor o los servidores de correo de la organización.

El equipo de migración en conjunto con los trabajadores que se encargarán de administrar los servidores debe definir los puntos de acceso en la red donde se realizarán las salvallas del servidor de correos de la organización y la periodicidad de los mismos.

Es recomendable guardar al menos la siguiente información:

- Sistema operativo del servidor con tecnologías funcionando.
- Buzones de correo de la organización.
- Configuraciones de cada una de las tecnologías utilizadas en el servidor.

De esta forma se asegurará que en un momento dado los servicios en la organización puedan dejar de funcionar o incluso pueda dañarse el *hardware* en los servidores y la información quede almacenada en lugares en la red y se podrá enfrentar con mayor rapidez situaciones de pérdida de datos.

Tenga en cuenta que en este paso puede necesitarse realizar reajustes en las configuraciones de seguridad establecidas en cada uno de los servicios. Aun así, realizarlo antes del aseguramiento de los servicios podría tener consecuencias negativas, ya que retrasaría el aseguramiento final de los servicios, por lo que es preferible tener que realizar ajustes en su cortafuegos durante el establecimiento de la política de salvallas.

2.1.13. Planificación del soporte

Al haber terminado la migración de los servicios de correo y sus principales configuraciones puede ser necesario que los miembros del equipo de migración trabajen para responder a los principales problemas que puedan ocurrir durante el transcurso de los primeros días tras haber realizado la migración total de los servicios de correo privados de la empresa.

Es el momento adecuado para que los administradores de los servicios de correo vayan enfrentándose a los problemas o tareas diarias que se necesitan realizar, como pueden ser la gestión de usuarios, el cambio de cuotas y muchos más, pues aunque deben haber recibido los cursos de entrenamiento necesarios para enfrentarse a las eventualidades que puedan ocurrir, la práctica diaria puede ser un poco diferente de los contenidos recibidos durante las capacitaciones y pruebas realizadas durante el proceso de migración de los servicios de correo electrónico.

CAPÍTULO 2: ESTRATEGIA PARA LA MIGRACIÓN DE LOS SERVICIOS DE CORREO ELECTRÓNICO EN CUBA

Siempre será una precaución contar con una estrategia de soporte, la cual inicialmente debe ser inmediata, siendo necesario que el equipo de migración trabaje durante algún tiempo brindando respuestas a las posibles situaciones que puedan ocurrir una vez realizada la migración, configuración, administración, optimización y adecuación de los servicios a las necesidades de la empresa. Transcurrido el tiempo necesario, se podrá pasar a brindar un soporte en línea, dejándose el protagonismo al personal encargado de administrar los servicios instalados en la empresa.

2.2. Propuesta de automatización de la estrategia para la migración del servicio de correo electrónico

Los problemas existentes durante la ejecución de un proyecto de migración de los servicios de correo electrónico en las instituciones cubanas, pueden ser resueltos mediante la utilización de la estrategia planteada anteriormente, la cual contempla las características propias de estos, pero la automatización de varias de las etapas de esta estrategia, permite agilizar la implantación de estos servicios, disminuyendo los tiempos de caída de los mismos.

Para ello se presenta a continuación una aplicación que se integra a la Herramienta para la Migración y Administración de Servicios Telemáticos (HMAST), que está siendo desarrollada en el departamento “Servicios Integrales de Migración, Asesoría y Soporte” del Centro de Software Libre de la Universidad de las Ciencias Informáticas que ya se encuentra en la fase de pruebas y utilización. Las principales etapas de la estrategia que se automatizan en el mismo son:

- Investigación de alternativas para GNU/Linux
- Montaje de la solución
- Realizar salvadas de seguridad de los datos
- Migración de los servicios de correo electrónico
- Monitoreo de los servicios
- Seguridad en los servicios colocados
- Definir políticas de salvadas automáticas de los servicios migrados

2.2.1. Concepción inicial

La aplicación permitirá la instalación, administración y migración de una infraestructura de correos de manera remota. Implementa componentes y clases que posibilitan la gestión y comunicación entre las tecnologías Postfix (MTA), Dovecot (MDA), Amavis (Interfaz entre MTA y herramientas de filtrado de contenidos), *Spamassassin* (Filtro *antispam*), ClamAV (Antivirus), *Fetchmail* (Obtención de correo remoto), Cluebringer (Servidor de políticas para Agentes de transferencia), *Mailman* (Distribución masiva de

CAPÍTULO 2: ESTRATEGIA PARA LA MIGRACIÓN DE LOS SERVICIOS DE CORREO ELECTRÓNICO EN CUBA

mensajes), Awstats (Generación de estadísticas sobre el uso de los servidores de correo), *Fail2ban* (Reescritura de reglas en el firewall) y varias tecnologías adicionales que fortalecen una infraestructura de correos electrónico. Además brinda interfaces que proveen los servicios necesarios para el acceso desde la capa de presentación.

2.2.2. Arquitectura

La arquitectura que presenta la herramienta HMAST y que además es heredada por la aplicación, propone el diseño de una arquitectura N-Capas orientada al dominio, compuesta por cinco capas. La capa de presentación es la que presenta al usuario los conceptos de negocio mediante una interfaz de usuario. La capa de aplicación realiza las llamadas a servicios de la capa inferior y tiene la responsabilidad de adaptar la información que le llega a los requerimientos de los servicios del dominio. La capa de dominio es responsable de las validaciones, define las interfaces de persistencia a datos (contratos de repositorio) pero no los implementa y está compuesta por entidades del dominio que representan objetos del dominio y están definidas fundamentalmente por su identidad, servicios de dominio que contienen la lógica que trata a las entidades como un todo y los contratos de repositorios que son interfaces que especifican las operaciones que deben implementar los repositorios. La capa de persistencia es responsable de contener el código necesario para persistir los datos, contiene como componente los repositorios que son clases que implementan los contratos de repositorios definidos en la capa de dominio. Finalmente la capa Infraestructura transversal es responsable de promover la reutilización de código, ella albergará las operaciones de seguridad, autenticación, monitoreo del sistema, mecanismos de persistencia reutilizables, validadores genéricos y todas aquellas operaciones que se puedan utilizar desde otras capas (CÉSAR DE LA TORRE LLORENTE, 2010). A continuación puede observar un diagrama donde se muestra la arquitectura de la aplicación:

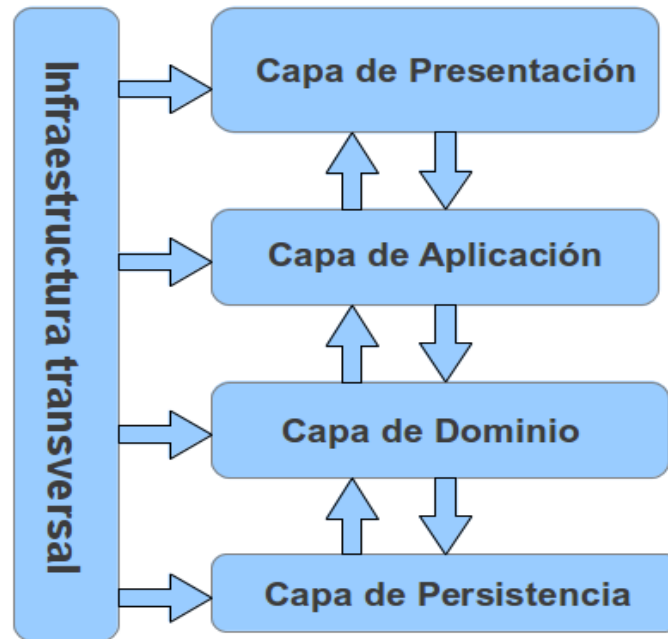


Figura 3. Arquitectura de la aplicación.

2.2.3. Consideraciones para realizar la integración de la aplicación a HMAST

La integración a la herramienta HMAST se logra a través de la llamada de funciones las cuales devuelven las conexiones asociadas a servidores lógicos y permiten un mecanismo para trabajar con las configuraciones de estos. Es necesario tener en cuenta que:

- La lógica de la aplicación no debe incluir ninguna lógica del dominio, solo tareas de coordinación relativas a requerimientos técnicos de la aplicación, como conversiones de formatos de datos de entrada a entidades del dominio, llamadas a componentes de la capa infraestructura para que realicen tareas complementarias.
- Se debe garantizar que no viajen hacia y desde la capa de presentación objetos de dominio, en su lugar deben viajar objetos DTO (*Data Object Transfer*).
- Las entidades solo pueden tener dependencias de componentes de la capa de dominio.
- Las clases de servicios deben ser las únicas responsables (vías de acceso) de acceder a los repositorios, no se puede implementar código de persistencia a datos en la capa de dominio.

CAPÍTULO 2: ESTRATEGIA PARA LA MIGRACIÓN DE LOS SERVICIOS DE CORREO ELECTRÓNICO EN CUBA

- Solo se puede acceder a la información almacenada en los servidores haciendo uso de los repositorios.
- Es importante que todo el código reutilizable por más de un repositorio se ponga a disposición de todos en la capa de infraestructura transversal.

2.2.4. Tecnologías asociadas al desarrollo de la aplicación

Para el proceso de desarrollo se seleccionaron un conjunto de tecnologías y herramientas que ayudan a diseñar, modelar e implementar la solución propuesta, las cuales se corresponden con las que quedaron definidas en los estudios iniciales referentes al desarrollo de HMAST, aspectos que se encuentran especificados en el documento Plantilla de Concepción del Sistema HMAST, recogido en el expediente de proyecto de mismo. Para el desarrollo de la lógica del negocio se utiliza el lenguaje de programación Java. El lenguaje XML es empleado para la persistencia temporal de la información en la computadora donde se encuentra el servidor de aplicaciones mientras se mantiene establecida una conexión. Como marco de trabajo para el desarrollo se utiliza Spring. Entre las características reutilizadas que provee el mismo para el desarrollo se utilizó el módulo de inyección de dependencias con XML para establecer la instanciación de los objetos. Como entorno para desarrollar se usa Netbeans, así como Visual Paradigm para el modelado, siendo guiado todo el proceso de desarrollo por la metodología SXP (PEÑALVER ROMERO, 2008).

2.2.5. Relativo a los artefactos de ingeniería y pruebas

Referente a los artefactos de ingeniería y pruebas, en el expediente se pueden encontrar las especificaciones de un total de 270 funcionalidades, organizadas para conformar un total de 16 historias de usuario. Se describe el diagrama de paquetes y despliegue, las tareas de ingenierías, los requisitos funcionales y no funcionales, las tareas de ingenierías, patrones de diseño utilizados, así como las pruebas realizadas.

2.3. Conclusiones del capítulo

La estrategia de migración de los servicios de correo electrónico para las instituciones cubanas cuenta con un conjunto de 13 etapas, con un orden para la ejecución de las mismas, de las cuales han sido automatizadas 7 en una herramienta informática, lo cual permitirá reducir el tiempo durante la implantación de los servicios de correo electrónico, evitando los tiempos de caída de los servicios, la introducción de errores en el proceso y garantizando el rendimiento de las tecnologías implantadas en el hardware colocado, así como la adecuación a entornos específicos de manera general.

CAPÍTULO 3

ANÁLISIS DE LOS RESULTADOS

Para la validación de la estrategia concebida en el capítulo de la presente investigación se realizan un conjunto de pruebas. Para ello se brindarán los datos necesarios sobre dos empresas en las que se realizó la migración de los servicios de correo por el departamento Servicios Integrales en Migración, Asesoría y Soporte del Centro de Software Libre: La Empresa Constructora de Obras para la Arquitectura número 24 (ECO A24), donde no se aplicó una estrategia específica y la Empresa Constructora de Obras de Arquitectura e Industriales número 3 (ECO AIND3) donde se utilizó la estrategia para la migración de los servicios de correo electrónico adecuada a las instituciones cubanas. Sería importante acotar que se escogieron estas dos empresas debido a que los datos sobre las mismas son los más recientes con los que se cuenta y a que las empresas ECO A24 y ECO AIND3 cuentan con características similares que permiten la comparación de ambos escenarios.

3.1. Misión de ambas empresas

La misión de ambas empresas consiste en ejecutar obras con niveles competitivos de calidad, compromiso y trabajo en equipo, que satisfacen a sus clientes, sustentados en el desarrollo del capital humano, elevando los valores políticos e ideológicos.

3.2. Objetivos estratégicos de ambas empresas

Como objetivos estratégicos se encuentran:

- Brindar servicios de construcción civil y montaje de nuevas obras, edificaciones e instalaciones.
- Demolición, desmontaje, remodelación, reconstrucción y/o rehabilitación de edificaciones, instalaciones y otros objetivos existentes.
- Reparación y mantenimiento constructivo.
- Construcción de áreas verdes.
- Servicios integrales de impermeabilización de cubiertas.

3.3. Términos utilizados

Tiempo de caída de servicios: Espacio de tiempo en el que los servicios deben

estarse ejecutando, pero debido a problemas de los mismos, los usuarios no puedan acceder al correo electrónico.

Tiempo necesitado para la implantación del servicio de correos: Tiempo durante el cual se están colocando los servicios de correo en la empresa. Es muy posible que los usuarios no puedan utilizar los servicios de correo, pero se debe haber planificado previamente que los servicios de correo no estén disponibles.

3.4. Información sobre los servicios de correo brindados en ambas empresas

Tabla 6. Información sobre hardware y software en las empresas ECOA24 y ECOAIND3

Empresa	CPU	RAM (Mb)	Disco Duro (Gb)	Tarjeta de red (Mb/s)	Cantidad de usuarios	Cantidad de usuarios concurrentes	Sistema Operativo	Software privativo
ECOA24	P IV	1024	160	100	70	65	Windows Server 2003	MDaemon 10.0
ECOAIND3	Intel Dual Core	1024	320	100	85	76	Windows Server 2003	MDaemon 10.0

3.4.1. Pasos y procedimientos realizados de la migración de la ECOA24

Para la migración del servidor de correo de la institución se utilizaron las siguientes etapas:

- Inventario de la información a ser migrada.
- Seleccionar las herramientas de migración adecuadas.
- Realizar los procedimientos de migración en un laboratorio de pruebas.
- Llevar a cabo un proyecto piloto y solicitar retroalimentación de los usuarios.
- Implementación del servicio de correo.
- Instalar el cliente de correo más adecuado y capacitar a los usuarios.
- Llevar a cabo la migración completa.

3.4.2. Tiempo de caídas durante la implantación y migración de los servicios de correo

A pesar de que la implantación final de los servicios de correo se hizo en los horarios en que el flujo de información era menor, tuvieron que hacerse pruebas durante 3 días consecutivos en los horarios donde el personal se encontraba almorzando. Esto ocasionó alrededor de 3 horas de inactividad de los mismos, principalmente debido a que en la recogida de información no se obtuvieron todos los datos necesarios para la implantación del nuevo servicio de correos.

3.4.3. Problemas enfrentados en el proyecto

- Fallas en el transporte hacia la institución.
- No se recogió toda la información necesaria referente al servicio brindado.
- Se colocaron funcionalidades existentes en el antiguo servidor de correo sin haber sido probadas en el nuevo servicio de correo.
- Se produjeron alrededor de 3 horas de inactividad.
- Pérdida de más de 100 correos.
- Descontento inicial de algunos de los usuarios de la ECOA24.

3.4.4. Pruebas de rendimiento realizadas en la ECOA24

A ambos servidores, tanto sobre *Windows* como sobre GNU/Linux en ambas empresas, se le realizaron pruebas de estrés, midiéndose el desempeño de los mismos antes de comenzar a realizar el envío masivo de correos y durante la ejecución de las pruebas. Las mismas fueron realizadas con la aplicación *SMTP Stress Tool* (SMTP STRES TOOL, 2014), realizando un envío masivo de 5000 mensajes de correo electrónico, uno cada 10 milisegundos. Para ello se enviaron 3000 mensajes de 1Kb y 2000 de 25Kb.

A continuación se muestran los resultados de los servicios sobre ambos sistemas operativos en la empresa ECOA24 antes y durante la realización de las pruebas:

Tabla 7. Consumo de recursos en los servicios de correo de la ECOA24.

Sistema Operativo	Memoria RAM consumida antes de la prueba (Mb)	Utilización de la CPU antes de la prueba (%)	Memoria RAM consumida durante la prueba (Mb)	Utilización de la CPU durante de la prueba (%)
<i>Windows Server</i> 2003	625	32	890	75
<i>Ubuntu Server</i> 12.04	560	24	720	62

3.4.5. Tiempo necesitado para la implantación del servicio de correos

Debido a que no se utilizó una herramienta que automatizara la implantación del servicio de correos y a que no se tuvieron en cuenta aspectos importantes como una recogida de información detallada, pruebas a gran escala sobre los servicios de correo a colocar, un adecuado monitoreo de los mismos, una capacitación, entre otros, se necesitaron aproximadamente 19 horas para poner en marcha el servicio de correos electrónico con la calidad requerida.

3.5. Servicios de correo brindados en la ECOAIND3

A continuación se brindarán los datos necesarios sobre la empresa ECOAIND3, donde se utilizó la estrategia para la migración de los servicios de correo electrónico para las instituciones cubanas.

3.5.1. Tiempo de caídas durante la implantación y migración de los servicios de correo

Los tiempos de caídas durante la implantación y migración de los servicios de correo en la institución fueron los mínimos y estuvieron asociados solamente al cambio de teléfono de las cuentas ancladas en los antiguos servidores de la empresa.

3.5.2. Problemas enfrentados en el proyecto

- Fallas en el transporte hacia la institución

3.5.3. Pruebas de rendimiento realizadas

Tabla 8. Consumo de recursos en servicios de correo de la ECOAIND3.

Sistema Operativo	Memoria RAM consumida antes de la prueba (Mb)	Utilización de la CPU antes de la prueba (%)	Memoria RAM consumida durante la prueba (Mb)	Utilización de la CPU durante de la prueba (%)
<i>Windows Server</i> 2003	585	18	805	38
<i>Ubuntu Server</i> 12.04	500	10	650	21

3.5.4. Tiempo necesitado para la implantación del servicio de correos

Debido a la utilización de la estrategia investigada y a la automatización de partes importantes de la misma, el tiempo necesitado para la implantación del servicio en su totalidad no llegó a la hora.

3.6. Comparación de los resultados de las pruebas realizadas a ambas empresas

Tabla 9. Comparación del consumo de recursos en ambas empresas durante la migración de los servicios de correo electrónico desde Windows hacia GNU/Linux.

Empresa	Memoria RAM consumida sobre Windows (Mb)	Utilización de la CPU sobre Windows (%)	Memoria RAM consumida sobre GNU/Linux (Mb)	Utilización de la CPU sobre GNU/Linux (%)
ECO24	625	32	560	24
ECOAIND3	585	18	500	10

CAPÍTULO 3: ANÁLISIS DE LOS RESULTADOS

Tabla 10. Comparación del consumo de recursos en ambas empresas utilizando tecnologías libres.

Empresa	Memoria RAM consumida antes de la prueba (Mb)	Utilización de la CPU antes de la prueba (%)	Memoria RAM consumida durante la prueba (Mb)	Utilización de la CPU durante la prueba (%)
ECO24	560	24	720	62
ECOIND3	500	10	650	21

Tabla 11. Comparación del consumo de tiempo durante la implantación del servicio de correo electrónico en ambas empresas utilizando tecnologías libres.

Empresa	Tiempo necesitado (Horas)	Tiempo de caída de servicios (Horas)
ECO24	16	3
ECOIND3	1	0

3.7. Conclusiones del capítulo

Mediante la migración de los servicios de correo electrónico que se realizaron en las empresas ECO24 y ECOIND3 se puede apreciar que existen marcadas diferencias en cuanto al tiempo y el aprovechamiento de los recursos tecnológicos de una institución donde se aplique una estrategia que no tenga en cuenta las características de los entornos cubanos (ECO24), en la cual se utilizaron 19 horas para implantar los mismos y una donde sí se tengan en cuenta los aspectos de una estrategia que contemple estas características (ECOIND3) y que tuvo como resultados principales que el tiempo de despliegue de los servicios de correo no llegara a 1 hora, disminuyendo en 18 horas el tiempo total necesitado. Además se redujo el consumo del procesador de un 24% de uso a un 10% y la memoria RAM utilizada de 560Mb a 500Mb, por lo que se mejoró el rendimiento de las tecnologías implantadas en el hardware existente.

Conclusiones

Como resultado de la presente investigación se obtuvo una estrategia para realizar la migración de los servicios de correo electrónico en las instituciones cubanas. Sobre la base de los resultados obtenidos se arribó a las siguientes conclusiones:

- La estrategia investigada reduce el tiempo en que se realizan los procesos de migración de los servicios de correo electrónico y permite aprovechar los recursos existentes.
- La aplicación informática desarrollada automatiza varias de las etapas de la estrategia propuesta e influye positivamente en la reducción del tiempo de despliegue de los servicios de correo electrónico.
- La adecuada selección de las alternativas influye positivamente en el correcto desempeño de los servicios de correo electrónico sobre plataformas libres.
- Las pruebas realizadas durante la investigación demuestran que la estrategia propuesta cumple con los objetivos para los que se diseñó.

Recomendaciones

- Integrar a la plataforma cubana de migración a software libre y código abierto la etapa “Recogida de Información” de la estrategia propuesta.
- Incorporar a la aplicación desarrollada funcionalidades referentes a las pruebas de funcionamiento y carga de los servicios de correo electrónico.

Referencias Bibliográficas

1. ADMIN S. O. (2013). *Aspectos básicos del servidor de correo electrónico - ASO* Última actualización: 2013/04/26/14:07:28. Disponible en: http://www.adminso.es/index.php/Aspectos_b%C3%A1sicos_del_servidor_de_correo_electr%C3%B3nico.
2. ALT-NTECHNOLOGIES I. N. C. (2013). *Mail Server | MDaemon Messaging Server | System Requirements* Última actualización: 2013. 2013/05/23/22:57:51. Disponible en: <http://www.altn.com/Products/MDaemon-Email-Server-Windows/System-Requirements/>.
3. ALTERMIME (2014). Modificación de mensajes en servidores de correo. 08/05/2014 2014, nº Disponible en: <http://www.pldaniels.com/alternmime/>.
4. ANDREE, M. (2002). *Postfix vs. qmail-Performance*. 2002,
5. AWSTATS (2014). AWStats logfile analyzer. 04/04/2014 2014, nº Disponible en: <http://awstats.sourceforge.net/>.
6. BERNSTEIN, D. J. (2007). Some thoughts on security after ten years of qmail 1.0. En *Proceedings of the 2007 ACM workshop on Computer security architecture*. 2007. p. 1-10.
7. CÉSAR DE LA TORRE LLORENTE, U. Z. C., MIGUEL ANGEL RAMOS BARROS, JAVIER CALVARRO NELSON (2010). *Arquitectura N-Capas orientada al Dominio con .NET 4.0*. 2010, nº ISSN 978-84-936696-3-8.
8. COSTALES, B. (2002). *Sendmail*. " O'Reilly Media, Inc.", 2002. ISBN 0596550529.
9. DAVE, S. (2002a). What is Qmail. En *The Qmail Handbook*. Apress, 2002a,
10. --- (2002b). Why Not Use qmail. En *The Qmail Handbook*. Apress, 2002b,
11. DAVICAL (2014). Davical for calendar. 09/05/2014 2014, nº Disponible en: <http://www.davical.org/>.
12. DENT, K. D. (2003). *Postfix: the definitive guide*. " O'Reilly Media, Inc.", 2003. ISBN 144937879X.
13. DESTAILLEUR, L. (2005). AWStats Logfile Analyzer Documentation. *NLTechno*, 2005, vol. 7, nº p. 3.
14. ECURED (2013). *Servidor de correo - EcuRed* Última actualización: 2013/04/26/15:01:58. Disponible en: http://www.ecured.cu/index.php/Servidor_de_correo.
15. EDGE OF WEB (2013). *Email migration strategy - plans & tips* Última actualización: 2013/12/05/11:46:43. Disponible en: <http://www.edgeoftheweb.co.uk/blog/2011/11/08/email-migration-strategy-plans-tips/>.
16. EVANS DATA, C. (2004). *Evans Data Corporation | More Than 90% Of Linux Systems Have Never Been Infected By A Virus, New Evans Data Survey | Press*

REFERENCIAS BIBLIOGRÁFICAS

- Release. publicado el: 2004/07/28/ de 2004, última actualización: 2004/07/28/. [Consultado el: 2013/04/01/18:31:03]. Disponible en: <http://www.evansdata.com/press/viewRelease.php?pressID=41>.
17. EVI NEMETH, G. S. T. R. H. B. W. T. M. N. M. R. J. D. S. y TOBI, O. (2011a). Exim. En *Unix and Linux System Administration Handbook*. Prentice Hall, 2011a, p. 807-827.
 18. --- (2011b). Postfix. En *Unix and Linux System Administration Handbook*. Prentice Hall, 2011b, p. 828-844.
 19. --- (2011c). Spamassassin. En *Unix and Linux System Administration Handbook*. 2011c,
 20. FAIL2BAN (2014). Fail2ban para GNU/Linux. 04/04/2014 2014, nº [Consultado el: 14/04/2014]. Disponible en: <http://www.fail2ban.org/>.
 21. FSF (2012). *Windows 8: No caigas en la publicidad exagerada — Free Software Foundation — working together for free software* Última actualización: 2012/09/. 2013/04/01/18:56:52. Disponible en: <http://www.fsf.org/es/windows8>.
 22. HAZEL, P. (2001). *The Exim SMTP Mail Server*. O'Reilly, 2001, nº
 23. HEINLEIN, P. y HARTLEBEN, P. (2008). *The book of IMAP: building a mail server with Courier and Cyrus*. No Starch Press, 2008. ISBN 1593271778.
 24. IBM (2007). *Best practices for data migration*. IBM Global Technology Services, publicado el: 2007/06/ de 2007, última actualización: 2007/06/.
 25. JUVENTUD REBELDE (2006). *Estados Unidos bloquea Internet en Cuba (I) - Cuba - Juventud Rebelde - Diario de la juventud cubana* Última actualización: 2013/04/01/19:07:43. Disponible en: <http://www.juventudrebelde.cu/cuba/2006-11-02/estados-unidos-bloquea-internet-en-cuba-i/>.
 26. KAREN D, S. (2004). *Windows to Linux Migration Guide* Última actualización: 2004/07/. 2013/04/01/16:00:11. Disponible en: <http://www.linux.com/learn/new-user-guides/328340-windows-to-linux-migration-guide>.
 27. MAILMAN (2014). Mailman, the GNU Mailing List Manager. 15/02/2014 2014, nº [Consultado el: 15/04/2014]. Disponible en: <http://list.org/>.
 28. MCGREGOR, C. (2007). Controlling spam with SpamAssassin. *Linux J*, 2007, vol. 153, nº 1,
 29. MICROSOFT (2005). *Multiple-Phase Migration. Advantages and disadvantages* Última actualización: 2013/12/05/08:42:42. Disponible en: [http://technet.microsoft.com/en-us/library/bb124309\(v=exchg.65\).aspx](http://technet.microsoft.com/en-us/library/bb124309(v=exchg.65).aspx).
 30. --- (2013a). *Multiple-Phase Migration Steps* Última actualización: 2013/12/05/08:43:51. Disponible en: [http://technet.microsoft.com/en-us/library/bb123987\(v=exchg.65\).aspx](http://technet.microsoft.com/en-us/library/bb123987(v=exchg.65).aspx).
 31. --- (2013b). *Single-Phase Migration. Advantages and disadvantages* Última actualización: 2013/12/05/06:30:25. Disponible en: [http://technet.microsoft.com/en-us/library/aa998904\(v=exchg.65\).aspx](http://technet.microsoft.com/en-us/library/aa998904(v=exchg.65).aspx).

REFERENCIAS BIBLIOGRÁFICAS

32. --- (2014). *Single-Phase Migration Steps* Última actualización: 2013/12/05/06:26:18. Disponible en: [http://technet.microsoft.com/en-us/library/bb123656\(v=exchg.65\).aspx](http://technet.microsoft.com/en-us/library/bb123656(v=exchg.65).aspx).
33. MICHAEL, T. y STEVE, S. (2003a). Exploring Sendmail. En *Red Hat Linux Administration A beginner's Guide*. The McGraw-Hill Companies, 2003a,
34. --- (2003b). Security Implications. En *Red Hat Linux Administration A beginner's Guide*. The McGraw-Hill Companies, 2003b,
35. OFFICIAL AMAVIS, W. (2013). *amavisd-new* Última actualización: 2013/04/28/12:13:39. Disponible en: <http://www.ijs.si/software/amavisd/>.
36. OFFICIAL BOGOFILTER, W. (2013). *Bogofilter Official Documentation* Última actualización: 2013. 2013/04/28/09:09:03. Disponible en: <http://bogofilter.sourceforge.net/>.
37. OFFICIAL CLAM A. V. ANTIVIRUS (2013). *Clam AntiVirus* Última actualización: 2013. 2013/04/28/11:23:40. Disponible en: <http://www.clamav.net/lang/en/>.
38. OFFICIAL DOVECOT, W. (2013). *Dovecot Official Documentation* Última actualización: 2013. 2013/04/27/20:42:47. Disponible en: <http://www.dovecot.org/>.
39. OFFICIAL, D. W. (2013a). *DSPAM Official Documentation* Última actualización: 2013. 2013/04/28/08:30:43. Disponible en: <http://dspam.nuclearelephant.com/>.
40. OFFICIAL FETCHMAIL, W. (2014). *Fetchmail* Última actualización: 2013/04/28/12:27:21. Disponible en: <http://fetchmail.berlios.de/index.html>.
41. OFFICIAL HORDE GROUPWARE, W. (2013). *Horde Groupware Webmail Edition* Última actualización: 2013. 2013/04/28/05:02:02. Disponible en: <http://www.horde.org/apps/webmail>.
42. --- (2014). *The Horde Project* Última actualización: 2013/04/28/05:03:20. Disponible en: <http://www.horde.org/>.
43. OFFICIAL KASPERSKY, W. (2014). *Kaspersky Security for Linux Mail Server | Kaspersky Lab América Latina* Última actualización: 2013/04/28/10:49:17. Disponible en: <http://latam.kaspersky.com/productos-para-empresas/linux-mail-server-antivirus>.
44. OFFICIAL ROUND CUBE, W. (2013). *Roundcube webmail* Última actualización: 2013. 2013/04/28/04:02:45. Disponible en: <http://roundcube.net/about#features>.
45. OFFICIAL SIEVE, W. (2013). *start - Sieve.Info* Última actualización: 2013/04/28/12:17:45. Disponible en: <http://sieve.info/>.
46. OFFICIAL SPAMASSASSIN, W. (2013). *Spamassassin Official Documentation* Última actualización: 2013. 2013/04/28/09:52:42. Disponible en: <http://spamassassin.apache.org/>.
47. OFFICIAL SQUIRRELMAIL, W. (2013). *SquirrelMail Official Documentation* Última actualización: 2013. 2013/04/28/00:14:09. Disponible en: <http://squirrelmail.org/about/>.
48. OFFICIAL, S. W. (2013b). *SAVUnix Milter Official Documentation* Última

REFERENCIAS BIBLIOGRÁFICAS

- actualización: 2013/04/28/10:14:23. Disponible en: <http://www.segurmatica.cu/laboratorio/lab1.jsp>.
49. PEER, H. y PEER, H. (2007). Comparing Courier and Cyrus. En *The book of Imap*. William Pollock, 2007, p. 20-21.
 50. PEÑALVER ROMERO, S. J. G. D. L. P. A. A. M. (2008). SXP, metodología de desarrollo de software. 2008, n°
 51. POLICYD (2014). Mail Policy Daemon. 15/03/2014 2014, n° Disponible en: <https://www.policyd.org/>.
 52. RAE (2014). Concepto de estrategia. 2014, n° [Consultado el: 09/12/2014]. Disponible en: <http://lema.rae.es/drae/?val=estrategia>.
 53. RALF, H. y PATRICK, K. (2005a). An Introduction to Postfix. En *The Book of Postfix*. William Pollock, 2005a, p. 1-2.
 54. --- (2005b). Preparing your host and environment. En *The Book of Postfix*. 2005b,
 55. RAYMOND, E. S. (2005). *Bogofilter: A fast open source bayesian spam filters*. 2005,
 56. SIRAINEN, T. *Dovecot Design/Memory*.
 57. SMTP STRES TOOL (2014). Tool to Test the SMTP mail Servers. 2014, n°
 58. SURMACZ, T. (2007). Reliability of e-mail delivery in the era of spam. En *Dependability of Computer Systems, 2007. DepCoS-RELCOMEX'07. 2nd International Conference on. 2007*. p. 198-204.
 59. TECHNET (2005). *Importancia creciente de la continuidad del correo electrónico* Última actualización: 2005. 2013/04/26/18:15:50. Disponible en: [http://technet.microsoft.com/es-es/library/cc164341\(v=exchg.80\).aspx](http://technet.microsoft.com/es-es/library/cc164341(v=exchg.80).aspx).
 60. THOMASON, A. (2007). Blog Spam: A Review. En *CEAS. 2007*.
 61. VENEMA, W. (2008). *The Postfix home page*. 2008,
 62. YADIEL PÉREZ, V. y YASIEL PÉREZ, V. (2013). *Módulo de administración de correo electrónico para HMAST*. UCI, 2013.
 63. YOUSEF, O. (2006). *Free Software Magazine*. publicado el: 2006 de 2006, última actualización: 2006. ISBN 1746-8752 1.

Anexos

Anexo 2.1

Nombre identificativo: Tiene que ser un nombre que identifique a este servidor solamente, por ejemplo: HP Proliant DL380G5 o simplemente Servidor de correo.

Procesador: Características del procesador, ejemplo: Intel Xeon Dual Core a 2.6 GHz. En el caso que haya más de un procesador, también debe especificarse.

Memoria RAM: Características de la memoria RAM instalada, ejemplo: Memoria RAM DDR2 de 2Gb a 800 MHz o Memoria RAM DDR3 de 2Gb a 1066 MHz.

Disco duro: Características del disco o los discos duros del servidor, ejemplo: Disco duro de 160 Gb de capacidad, con 16 Mb de caché del búfer, a 7200 RPM³². En el caso que haya más de un disco duro, y haya algún nivel de redundancia entre ellos, también debe especificarse.

Tarjeta de red: Características de la tarjeta de red, ejemplo: Tarjeta de red Broadcom *Fast Ethernet* a 1 Gbps. En el caso que haya más de una tarjeta de red, y exista algún nivel de redundancia entre ellos debe especificarse.

Observaciones de *hardware*: En este aspecto se informará de *hardware* específico instalado en cada uno de los servidores y que pudieran necesitar de controladores en los sistemas operativos GNU/Linux, tal es el caso de una UPS³³ a la que esté conectada al servidor, tarjetas para el almacenamiento en dispositivos SAN³⁴ y demás dispositivos que se entienda son necesarios colocar durante la recogida de información.

Sistema operativo y versión sobre el cual se ejecuta: La variante del sistema operativo desde la cual se desea realizar la migración, ejemplo: Sistema operativo *Windows Server 2003*.

Arquitectura del sistema operativo: La arquitectura del sistema operativo que se encuentra instalado en el servidor, ejemplo: Arquitectura de 32 bits o de 64 bits.

Software utilizado para brindar los servicios de correo: Debe especificarse el *software* utilizado en la organización para brindar los servicios de correo electrónico, y la versión del mismo, por ejemplo: *MDaemon* en su versión 10.0.0.

³² Revoluciones por minuto.

³³ Fuente de suministro eléctrico que posee baterías con el fin de dar energía a uno o varios dispositivos.

³⁴ Red de área de almacenamiento.

Funcionalidades utilizadas en el servicio de correo electrónico:

En este paso se recogerá la información relacionada con los servicios de correo de la empresa, preferiblemente de la siguiente manera de acuerdo al *software* utilizado en la organización:

- Funcionalidades que se encuentran habilitadas en el servicio de correo privativo.
- Funcionalidades que se encuentran habilitadas y se utilizan en el momento de la recogida de información y un aproximado de los usuarios que la utilizan en caso de ser necesario.
- La importancia de la funcionalidad. Esta se pudiera dar en términos de la necesidad (baja, media o alta) de esa funcionalidad para el servicio de correo de la organización.

La utilización de estas funcionalidades debe ser dividida en funcionalidades que son utilizadas mayormente por los usuarios y funcionalidades que son llevadas a cabo directamente por el servidor. El motivo principal de dividir esta información es que aunque todas las funcionalidades son de suma importancia, sí deben estar bien identificadas cuales utilizan directamente los usuarios y cuales se utilizan en el servidor, pues las funcionalidades de los usuarios deben cambiar lo menos posible y a las identificadas como utilizadas por el servidor se les puede buscar una alternativa sobre los entornos libres, tratando siempre que los cambios realizados no sean visibles a los usuarios. A continuación se exponen ejemplos de los dos tipos de funcionalidades que se deben reflejar durante el proceso de recogida de la información de las funcionalidades.

Funcionalidades utilizadas directamente por los usuarios:

- Listas de correo.
- Gestión de calendarios y tareas.
- Utilización de cliente web y funcionalidades del mismo como completamiento de los usuarios, filtros de correos, gestión de calendarios y tareas, creación de listas de correo y contactos, así como todas aquellas que se considere necesario destacar.
- Utilización de cliente de escritorio, protocolos utilizados para la comunicación con el servidor y funcionalidades utilizadas del mismo.
- Tipo de autenticación utilizada en el servidor, si es con un directorio activo, una

base de datos relacional, usuarios locales.

- Todas las acciones realizadas por los usuarios que se encuentren relacionadas con el servicio de correo.

Funcionalidades utilizadas en el servidor:

- Formato de almacenamiento de los buzones de correo.
- Dominios virtuales en la organización.
- Detección de virus en tiempo real.
- Detección de correos *spam* y la gestión de listas blancas, negras y grises.
- Configuraciones de optimización realizadas al servidor para ahorrar el ancho de banda y lograr el funcionamiento eficiente del *hardware* del servidor de correos en la organización.
- Cifrado de la autenticación utilizada en el servidor.
- Tamaño de los mensajes enviados.
- Tipos de adjuntos permitidos a enviar en el servidor de la organización.
- Cuota definida para el tamaño de los buzones en la organización.
- Envío de correos a los usuarios cuando la cuota alcanza determinados límites.
- Configuraciones de la cola del servidor de correos.
- Utilización de servidor *relay* para el envío de correos de la organización.
- Utilización del servidor como *relay* para que otras organizaciones envíen correos a través de él.
- Descarga de correos de la organización en servidor remoto.
- Almacenamiento de buzones de correos de otras organizaciones para que estas lo puedan descargar.
- Filtrado de correos de la organización.
- Copia de todos los correos de la organización.
- Salvas de los correos de la organización.
- Restricciones en el envío de correos por dominio.
- Detección de intentos de hackeo.
- Obtención de estadísticas sobre el uso del servicio de correo.

- Protocolos utilizados para brindar los servicios de correo y funcionalidades presentes en cada uno de ellos.
- Usuarios que pueden acceder a cualquier buzón de la organización o posibilidad de acceder a cualquier buzón de la organización.
- Posibilidad de compartir carpetas o buzones enteros dentro de la organización.
- Utilización de alias en el servidor.
- Posibilidad de modificaciones a los correos de la organización enviados por los usuarios.
- Configuraciones realizadas en el servidor sean o no características del *software* de servidor utilizado, que influyan en el funcionamiento del servicio de correos.
- Utilización de cortafuegos.

Datos específicos sobre el servicio de correo:

Las funcionalidades utilizadas directamente por los usuarios en la organización y en el servidor, servirán al equipo de migración de los servicios de correo para tener una visión global de las posibles tecnologías a utilizar una vez implantado el nuevo servicio, pero es importante recoger la información necesaria de cada una de las configuraciones realizadas en el servicio de correo. Estos datos incluyen todos los aspectos relacionados con las funcionalidades, como por ejemplo de las listas de correo, todas las listas de correo de la organización, pero si se le hace *relay* a algún servidor de correo, debe reflejarse la dirección ip a la que se le hace *relay*, o si se descargan los correos, los datos de autenticación con que se realizan estas tareas, y así sucesivamente, especificarse con el mayor nivel de detalles la información de cada una de las funcionalidades utilizadas. Es muy posible que haya información que sea necesaria colocar que no venga reflejada dentro de las funcionalidades detectadas y también deberá colocarse en el documento, pues con toda esta información podrá obtenerse en un futuro un escenario lo más similar posible al de la organización.

Cantidad de usuarios concurrentes: Será un aproximado de la máxima cantidad de usuarios o peticiones que en un momento dado usarán concurrentemente el servidor.