

UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE ARQUITECTURA E INGENIERÍAS

Trabajo de fin de carrera titulado:

“DISEÑO DE UN MODELO DE COMUNICACIONES SEGURAS BASADO EN RIGHTS MANAGEMENT SERVICES (RMS), BAJO EL DOMINO 10 DE LA NORMA ISO/IEC 27002:2013 APLICADO EN UNA INFRAESTRUCTURA MICROSOFT.”

Realizado por:

DANILO JOSÉ NINABANDA OCAMPO

Director del proyecto

ING. JUAN SEBASTIÁN GRIJALVA LIMA, MSc.

Como requisito para la obtención del título de:

INGENIERO DE SISTEMAS EN DISEÑO Y MULTIMEDIA

Quito, Julio del 2016

DECLARACION JURAMENTADA

Yo, DANILO JOSÉ NINABANDA OCAMPO, con cédula de identidad #020183115-3, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado o calificación profesional; y, que ha consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

Danilo José Ninabanda Ocampo

C.C: 020183115-3

DECLARATORIA

El presente trabajo de investigación titulado:

“DISEÑO DE UN MODELO DE COMUNICACIONES SEGURAS BASADO EN RIGHTS MANAGEMENT SERVICES (RMS), BAJO EL DOMINO 10 DE LA NORMA ISO/IEC 27002:2013 APLICADO EN UNA INFRAESTRUCTURA MICROSOFT.”

Realizado por:

DANILO JOSÉ NINABANDA OCAMPO

Como requisito para la obtención del título de:

INGENIERO DE SISTEMAS EN DISEÑO Y MULTIMEDIA

Ha sido dirigido por el docente:

ING. JUAN SEBASTIÁN GRIJALVA LIMA, MSc

Quien considera que constituye un trabajo original de su autor

Ing. Juan Sebastián Grijalva, MSc

DIRECTOR

PROFESOR INFORMANTE

ING. DANIEL RIPALDA, MSC

Después de revisar el trabajo presentado,
lo he calificado como apto para su defensa oral ante
el tribunal examinador

Ing. Daniel Ripalda, MSC

Quito, Julio 2016

PROFESOR INFORMANTE

ING. VERÓNICA RODRÍGUEZ, MSC

Después de revisar el trabajo presentado,
lo he calificado como apto para su defensa oral ante
el tribunal examinador

Ing. Verónica Rodríguez, MSC

Quito, Julio 2016

DEDICATORIA

Dedico el presente trabajo principalmente a mi padre porque nunca ha dejado de apoyarme, por su esfuerzo constante para sacar adelante a su familia y ser un gran ejemplo para mi.

A mi madre por su inmenso cariño, por su ayuda y consejos en los momentos más difíciles, pero sobretodo por educarme con principios y valores que guiarán mi vida.

A mis hermanas que con sus ocurrencias han hecho que mi vida este llena de felicidad, las amo.

AGRADECIMIENTO

Agradezco a mi familia por sus palabras de aliento, consejos y enseñanzas; son todo para mí.

A todos mis profesores por haber compartido sus conocimientos durante toda la carrera, los cuales han permitido realizar este trabajo.

A mis amigos, por brindarme su sincera amistad y haber compartido conmigo esta etapa de mi vida.

A la Universidad Internacional SEK que me permitió desarrollar y culminar mis estudios universitarios.

ÍNDICE DE CONTENIDO

CAPÍTULO I	18
INTRODUCCIÓN	18
1.1. El Problema de investigación	18
1.1.1. Planteamiento del Problema	18
1.1.2. Objetivos	19
1.1.3. Justificación	20
1.2. Marco Teórico	21
1.2.1. Estado actual de conocimiento sobre el tema	21
1.2.1.1. Sistema Operativo	21
1.2.1.2. Sistemas Operativos de Servidor	22
1.2.1.3. Active Directory	23
1.2.1.4. Rights Management Services (RMS)	26
1.2.1.5. Sistemas Operativos de Computadora Personal	27
1.2.1.6. Correo Electrónico	28
1.2.1.7. ISO/IEC 27002:2013	29
1.2.1.8. Criptografía – Cifrado	30
1.2.1.9. Criptografía Clásica	32
1.2.1.10. Cifrado del César	32
1.2.1.11. El Disco de Alberti	33
1.2.1.12. Cifrado de Vernam	33
1.2.1.13. La Máquina Enigma	34
1.2.1.14. Criptografía Moderna	37
1.2.1.15. Criptografía Simétrica	37
1.2.1.16. Algoritmo Simétrico DES	38
1.2.1.17. Algoritmo Simétrico IDEA	41
1.2.1.18. Algoritmo Simétrico Rijndael (AES)	42
1.2.1.19. Criptografía Asimétrica	47

1.2.1.20.	Algoritmo Asimétrico Diffie-Hellman	48
1.2.1.21.	Algoritmo Asimétrico RSA (Rivest, Shamir, Adleman)	50
1.2.1.22.	Algoritmo Asimétrico Gamal	51
1.2.1.23.	Funciones Hash	52
1.2.1.24.	Controles Criptográficos.....	55
1.2.1.25.	Política de Uso de los Controles Criptográficos.....	56
1.2.1.26.	Gestión de Claves.....	57
1.2.2.	Marco Conceptual.....	58
1.2.2.1.	Seguridad de la Información.	58
1.2.2.2.	Documentos Electrónicos.....	59
1.2.2.3.	Confidencialidad.....	59
1.2.2.4.	Integridad	60
1.2.2.5.	Disponibilidad.....	60
1.2.2.6.	No Repudio.....	60
CAPÍTULO II		62
MÉTODO		62
2.1.	Análisis.....	62
2.1.1.	Estudio Preliminar.....	62
2.1.2.	Estudio de Factibilidad.....	68
2.1.2.1.	Factibilidad Operativa	68
2.1.2.2.	Factibilidad Tecnológica	70
2.1.2.3.	Factibilidad Económica.....	71
2.2.	Diseño.....	73
2.2.1.	Esquema General de la Solución	73
CAPÍTULO III		77
RESULTADOS		77
3.1.	Construcción.....	77
3.1.1.	Generalidades.....	77
3.1.2.	Descripción de Componentes.....	78
3.1.3.	Levantamiento Máquinas Virtuales.....	79
3.1.4.	Configuración red virtual en VMware Workstation 12.....	85

3.1.5. Instalación Active Directory.	94
3.1.6. Instalación Microsoft Exchange.	108
3.2. Implementación	119
3.2.1. Implementación de RMS	119
3.2.2. Creación de plantillas de directivas de derechos distribuidos.	132
3.2.3. Configuración de Terminal de Usuarios de RMS.	137
CAPÍTULO IV	139
DISCUSIÓN	139
4.1. Conclusiones	139
4.2. Recomendaciones	141
BIBLIOGRAFÍA	142
ANEXOS	146
ANEXO #1. ESTRUCTURA DE UNA POLITICA DE PROTECCION DE CLAVES ENCRIPTADAS PARA USUARIOS FINALES ELABORADO POR SANS	146
ANEXO #2. COTIZACIÓN DE LICENCIAS PARA EL USO DEL SERVICIO RMS DE MICROSOFT	151

ÍNDICE FIGURAS

Figura #1. Estructura básica de un sistema operativo	21
Figura #2. Estructura Cliente – Servidor.....	23
Figura #3. Estructura física de Active Directory	24
Figura #4. Estructura lógica de Active Directory	25
Figura #5. Origen de la criptografía.....	30
Figura #6. Ejemplo cifrado del César con desplazamiento de 4	32
Figura #7. Disco de Alberti.....	33
Figura #8. Código Baudot.....	34
Figura #9. Ejemplo simplificado de la máquina Enigma.....	36
Figura #10. Demostración cifrado simétrico.....	38
Figura #12. Estructura de funcionamiento de algoritmo de cifrado IDEA	42
Figura #14. Matriz de estados algoritmo de cifrado AES	44
Figura #13. Estructura de funcionamiento de algoritmo de cifrado AES	46
Figura #14. Demostración cifrado asimétrico.....	47
Figura #15. Funcionamiento algoritmo asimétrico Diffie-Hellman	49
Figura #16. Estructura función Hash	53
Figura #17. Estructura certificado digital.....	55
Figura #18. Estadísticas sobre las preocupaciones en materia de seguridad de la información en las empresas de Latinoamérica.	64
Figura #19. Estadísticas sobre los controles de seguridad utilizados en las empresas de Latinoamérica.	67
Figura #20. Diseño general del modelo de comunicaciones seguras.....	73
Figura #21. Diagrama de secuencias del modelo de comunicaciones seguras	74
Figura #22. Diagrama de actividades del modelo de comunicaciones seguras	75
Figura #23. Creación de un documento protegido por RMS	76
Figura #24. Modelo de Implementación.	78
Figura #25. Asistente de instalación de nueva máquina virtual.....	80
Figura #26. Medio de instalación.....	80
Figura #27. Usuario del sistema operativo.....	81
Figura #28. Alerta de serial de activación.....	81

Figura #29. Nombre y ubicación de la máquina virtual.....	82
Figura #30. Espacio de disco de máquina virtual	83
Figura #31. Finalización del asistente de creación de máquinas virtuales.....	83
Figura #32. Instalación de Windows Server 2008 R2.....	84
Figura #33. Windows Server 2008 R2 Standard instalado e iniciado.....	85
Figura #34. Menú editar de VMware Workstation	86
Figura #35. Creación de la nueva red virtual	87
Figura #36. Nueva red virtual	87
Figura #38. Selección adaptador de red de máquina virtual	89
Figura #39. Selección de adaptador de red para máquinas virtuales	90
Figura #40. Estado de conexión de área local.....	92
Figura #41. Funciones de red.....	93
Figura #42. Direccionamiento IP	93
Figura #43. Asistente de configuración de Active Directory.....	94
Figura #44. Inicio del asistente de instalación de Active Directory	95
Figura #45. Compatibilidad de sistema operativo.....	96
Figura #46. Configuración de DNS	97
Figura #47. Configuración de implementación.....	98
Figura #48. Nombre al dominio raíz del bosque.....	99
Figura #49. Nivel funcional del bosque	100
Figura #50. Nivel funcional del dominio	101
Figura #51. Opciones adicionales del controlador de dominio.....	102
Figura #52. Alerta sobre servicio DNS	103
Figura #53. Ubicación de la base de datos, los archivos de registro y SYSVOL ...	104
Figura #54. Contraseña de administrador para restauración de servicios de directorio	105
Figura #55. Resumen	106
Figura #56. Proceso de instalación de Active Directory.....	106
Figura #57. Finalización del asistente de instalación de Active Directory	107
Figura #58. Asistente de instalación de Filter Pack 1.0	108
Figura #59. Windows PowerShell.....	109
Figura #60. Ejecutando comandos en PowerShell.....	110

Figura #61. Servicios de Windows	110
Figura #62. Servicios de Windows	111
Figura #63. Inicio del servicio	112
Figura #64. Inicio del asistente de instalación de Exchange.....	113
Figura #65. Acuerdo de licencia de Microsoft Exchange	113
Figura #66. Reporte de errores.....	114
Figura #67. Tipo de instalación Microsoft Exchange	115
Figura #68. Organización Exchange	115
Figura #69. Configuración clientes Outlook 2003	116
Figura #71. Programa de mejora de la experiencia del cliente	117
Figura #72. Comprobación de disponibilidad	118
Figura #73. Asistente para agregar roles.....	119
Figura #74. Servicios de rol requeridos para RMS	120
Figura #75. Servicios de rol	121
Figura #76. Crear un clúster de AD RMS.....	121
Figura #77. Base de datos de configuración de políticas de RMS.....	122
Figura #78. Cuenta de servicio de RMS	123
Figura #79. Almacenamiento de la clave de clúster de AD RMS	124
Figura #80. Contraseña de la clave de clúster de AD RMS.....	125
Figura #81. Dirección de clúster	126
Figura #82. Nombre Para el Certificado Emisor de Licencias de Servidor	127
Figura #83. Punto de conexión de servicio de AD RMS	128
Figura #84. Seleccionar servicios de rol	129
Figura #85. Lista de selecciones para instalación	130
Figura #86. Proceso de instalación.....	130
Figura #87. Resultados de la instalación.....	131
Figura #89. Direccionamiento de plantillas de directivas de derechos	133
Figura #90. Crear plantilla de directiva de derechos distribuidos.....	134
Figura #91. Agregar nueva información de identificación de la plantilla.....	135
Figura #92. Agregar usuario o grupo	136
Figura #93. Servicios de RMS en terminales de usuarios.....	137

Figura #94. Creación de nueva clave	138
Figura #95. Creación de valor de cadena expandible	138

INDICE TABLAS

Tabla #1. ISO/IEC 27002:2013 Dominio 10	29
Tabla #2. Ejemplo operación XOR	34
Tabla #3. Ejemplo cifrado de Vernam.....	34
Tabla #4. Tipos de factibilidad.	68
Tabla #5. Perfil de competencias necesarias para la operación del proyecto.	69
Tabla #6. Requisitos de hardware para aplicar RMS de Microsoft.....	70
Tabla #7. Requisitos de software para aplicar RMS de Microsoft.....	70
Tabla #8. Cuadro de costos para la implementación de RMS en una infraestructura Microsoft	72
Tabla #9. Direccionamiento IP del proyecto	91

RESUMEN

El presente documento es la descripción del análisis, diseño e implementación en un ambiente de pruebas de un modelo de comunicaciones seguras basadas en Rights Management Services de Microsoft bajo el dominio 10 (Cifrado) de la norma ISO/IEC 27002:2013. Este modelo de comunicaciones seguras permitirá a las empresas que tengan una infraestructura Microsoft para proteger todos sus documentos de varias amenazas, como por ejemplo: malos empleados o ciberdelincuentes, que aprovechan ciertas brechas de seguridad de la información para cometer este y otros delitos que afectan a muchas empresas y que en ocasiones causan grandes pérdidas para las mismas. Este proyecto se desarrolló en base a las técnicas de cifrado, usando los servicios que RMS, Active Directory y Exchange Server que Microsoft ofrece. El modelo de comunicaciones seguras desarrollado en este documento es una solución que usa tecnologías poco usadas, como el cifrado, por lo que significa una gran ventaja para las empresas en cuanto a la protección de sus documentos ya que se garantiza la confidencialidad y la integridad de los mismos.

Palabras Claves:

Cifrado, Rights Management Services, Seguridad de la Información, Confidencialidad, Integridad, Amenazas.

ABSTRACT

This document is a description of the analysis, design and implementation of a secure communication model in a test environment. This model is based on Microsoft Rights Management Services under the rule 10 (encryption) of ISO / IEC 27002: 2013. This model of secure communications will allow companies to have a Microsoft infrastructure for protecting their documents from threats, for example a bad employee, or cyber criminals who take advantage of certain breaches of security information to commit this and other crimes that affect the companies, and sometimes it causes enormous losses for them. This project was developed according with the encryption techniques using RMS services, Active Directory and Microsoft Exchange Server offers. The model is a solution that applies underused technologies, such as encryption. This represent a big advantage for companies in order to protect their documents, because this model guarantee the confidentiality and integrity of the documents.

Keywords:

Encryption, Rights Management Services, Information Security, Confidentiality, Integrity, Threats.

CAPÍTULO I

INTRODUCCIÓN

1.1.El Problema de investigación

1.1.1. Planteamiento del Problema

La información es un recurso que todas las empresas grandes o pequeñas tienen y es de vital importancia para su funcionamiento y es considerada como un activo más, por lo que se convierte en un objetivo muy valioso para ser robado. Algunas organizaciones no toman las medidas adecuadas para preservar la integridad, confidencialidad de su información, y esto las convierte en víctimas de ciberdelincuentes que se dedican a descubrir vulnerabilidades para luego aprovecharlas y acceder de manera ilegal a sus redes y extraer toda la información que este a su alcance; ocasionando problemas de producción, operación de la empresa, pero principalmente pérdidas económicas significativas que pueden ser en algunos casos irreparables.

1.1.2. Objetivos

Objetivo General

Diseñar un modelo de comunicación segura que impida la pérdida de información valiosa para las empresas, mediante la aplicación de controles criptográficos basados en la Norma ISO/IEC 27002:2013.

Objetivos Específicos

- Realizar un estudio bibliográfico de los principales algoritmos criptográficos que se usan para la protección de la información.
- Desarrollar una solución para preservar la integridad de la información en base al domino 10 de la norma ISO/IEC 27002:2013 a través de herramientas de software en una infraestructura Microsoft.
- Implementar en un ambiente de pruebas el modelo de comunicaciones seguras basado en Rights Management Services (RMS) de Microsoft.
- Establecer una comunicación que permita la aplicación de confidencialidad para el servicio de correo electrónico interno aplicando el uso de Microsoft Exchange y RMS de Microsoft.

1.1.3. Justificación

Con el pasar del tiempo las empresas han desarrollado sistemas de comunicación internos, como las redes de área local, que facilitan los flujos de trabajo y permiten que se comparta todo tipo de información, optimizando costos, agilizando la comunicación que mejoran el funcionamiento de las empresas, pero en algunos casos puede presentar fallos de seguridad, por lo que es necesario que se establezcan de manera eficiente políticas y soluciones eficientes para así, proteger la información importante de personas no autorizadas que quieran utilizarla con fines dañinos y poco éticos que perjudicarán a la empresa.

Así surge la necesidad de usar técnicas de cifrado que protejan y garanticen la confidencialidad e integridad de toda la información que transite por la red de la empresa, para la aplicación de esta solución existen varias herramientas de encriptación; una de ellas es la aplicación de RMS (Rights Management Services) de Microsoft que se presente en este proyecto.

1.2. Marco Teórico

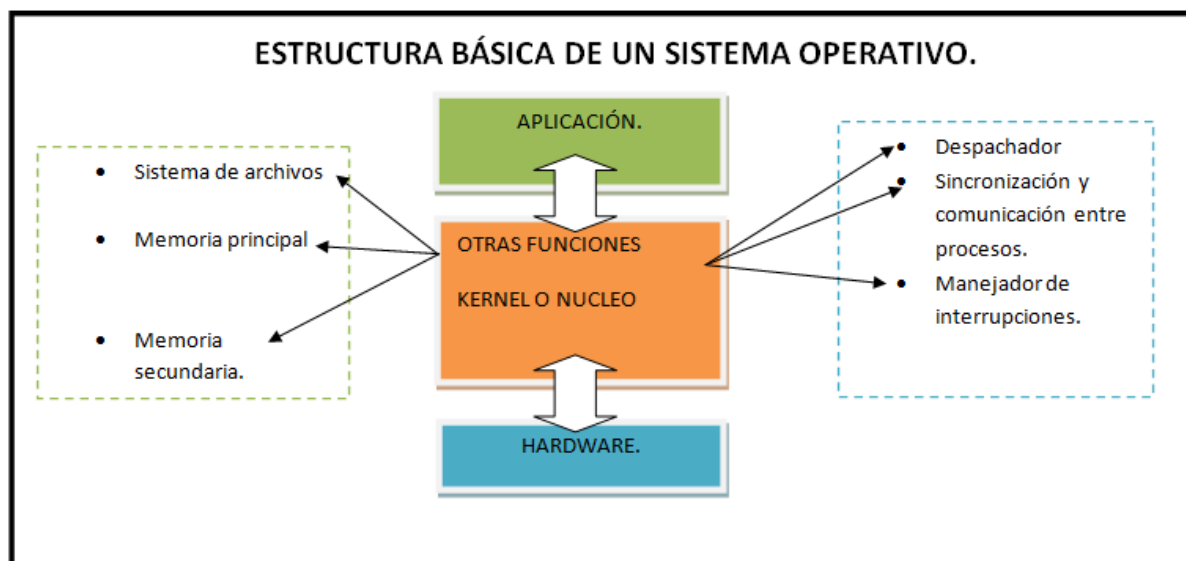
1.2.1. Estado actual de conocimiento sobre el tema

1.2.1.1. Sistema Operativo

“El sistema operativo es el software que se ejecuta en modo kernel, y se encarga de dos funciones básicas: proporcionar a los programadores de aplicaciones un conjunto abstracto de recursos simples, en vez de los complejos conjuntos de hardware; y administrar estos recursos de hardware.”. (Tanenbaum, Andrew S. 2009)

Figura #1. Estructura básica de un sistema operativo

Fuente: Theira Irasema Samperio Monroy



Los sistemas operativos en la actualidad son dinámicos, y con entornos gráficos amigables con el usuario, pero antes que estos se muestren así tuvieron que pasar por una evolución muy grande, y van ligadas con la evolución de la arquitectura de las computadoras. Existen cuatro generaciones de computadores; y en la última generación nacen las computadoras personales con el sistema operativo DOS (Sistema operativo de Disco) y este a su vez da paso a lo que hoy conocemos. (Tanenbaum, A. S. 2009)

Tanenbaum (2009) en su libro Sistemas Operativos Modernos menciona nueve tipos de sistemas operativos de los cuales dos forman parte del presente proyecto y estos son:

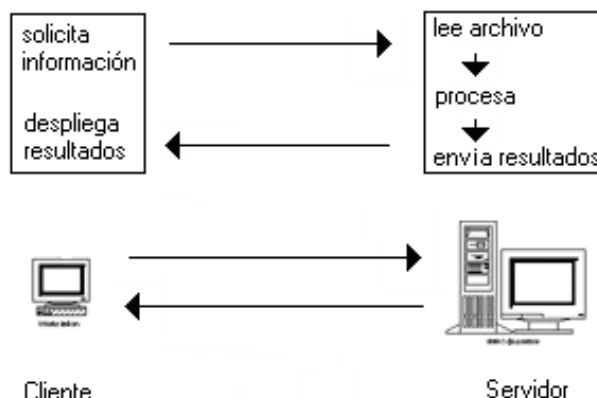
- Sistemas Operativos de Servidor
- Sistemas Operativos de Computadora Personal

1.2.1.2.Sistemas Operativos de Servidor.

Éstos se ejecutan en servidores, que son computadores personales muy grandes, estaciones de trabajo o incluso mainframes, dan servicio a múltiples usuarios a través de una red, permitiéndoles compartir recursos de hardware y software. Los servidores pueden prestar servicios de impresión, de archivo o de Web. Los proveedores de Internet operan muchas máquinas servidoras para atender a sus clientes, y los sitios Web emplean servidores para almacenar páginas Web y manejar las solicitudes que llegan. Entre los sistemas operativos de servidor típicos están UNIX y Windows 2000. (Tanenbaum, A. S. 2009)

Figura #2. Estructura Cliente – Servidor

Fuente: Sistemas operativos para redes cliente/servidor de oocities.org



En este proyecto se utilizó el sistema operativo de servidor de la compañía Microsoft, Windows Server 2008 R2, que en este momento es uno de los sistemas operativos para servidores más avanzados, y que se encuentra diseñado para aplicaciones y servicios web. Con este sistema operativo se podrá ofrecer una infraestructura de red muy segura y se aumentará la eficiencia de la organización. (Microsoft, 2016)

1.2.1.3.Active Directory

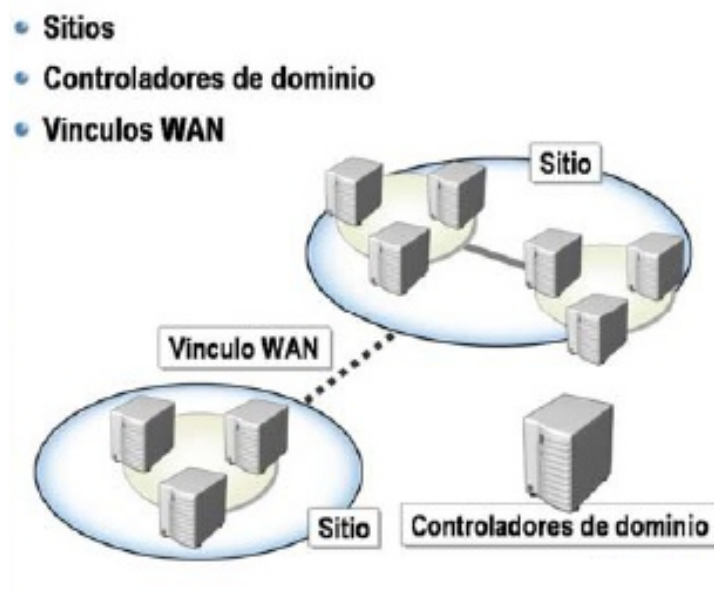
Active Directory es un servicio de Microsoft Sever que almacena información sobre los objetos de la red y facilita la búsqueda de esta información para los usuarios y administradores, además utiliza un almacén de datos estructurado como base para una organización lógica y jerárquica de la información del directorio, este almacén de datos o directorio, contiene información sobre los objetos de Active Directory en los que se incluyen todos los recursos compartidos como servidores, volúmenes, impresoras, cuentas de usuario de red y cuentas de equipo. (Microsoft, 2016)

Active Directory se divide en dos tipos de estructuras: estructura física y estructura lógica. La estructura física es la que configura y administra todo el tráfico de red. Los elementos de esta estructura son:

- Controladores de dominio que son servidores ejecutando Windows Server 2008 R2, Directorio Activo.
- Sitios que son los grupos de equipos conectados en distintas áreas y pertenecen al dominio principal. (Gómez Gómez, A. 2015).

Figura #3. Estructura física de Active Directory

Fuente: Introducción a las infraestructuras de Active Directory – Fausto Arias

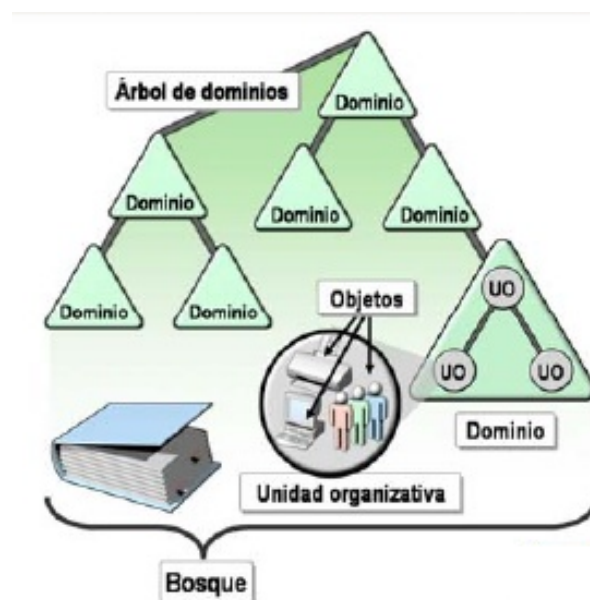


La estructura lógica es la que administra los recursos de la red de una empresa u organización, esto de manera independiente de donde se encuentren físicamente dichos recursos, y de la topología de las demás redes. Los elementos que intervienen en la estructura lógica son:

- Dominios: es el que representa un límite administrativo que puede almacenar objetos, y estos objetos son productos que los miembros de la red necesitan para su correcto funcionamiento. Los dominios pueden expandirse en más de una localización física.
- Árboles: un árbol es una agrupación de uno o más dominios que se pueden crear añadiendo uno o más dominios secundarios a un dominio principal existente.
- Bosque: es una agrupación o configuración jerárquica de uno o más árboles de dominio distintos y completamente independientes entre sí.
- Unidades organizativas: es el contenedor que se utiliza para organizar objetos dentro de un dominio en grupos administrativos lógicos que reflejan la estructura funcional y de negocios de una empresa. (Gómez Gómez, A. 2015).

Figura #4. Estructura lógica de Active Directory

Fuente: Introducción a las infraestructuras de Active Directory – Fausto Arias



1.2.1.4.Rights Management Services (RMS)

Rights management Services son todas las tecnologías de servidor y de cliente necesarias para la administración de permisos de acceso a la información en una organización. Los servidores de certificación y de licencias de RMS de la organización, junto con los servicios de RMS que están alojados por Microsoft certifican las entidades de confianza que se encuentran en el sistema RMS. Estos servidores de licencias de RMS de la organización emiten licencias de publicación y de uso que controlan la forma en que las aplicaciones cliente de RMS utilizan el contenido protegido. Las tecnologías de cliente y las aplicaciones compatibles con RMS, se ejecutan en los equipos clientes y permiten a los usuarios crear, publicar y utilizar contenido protegido con RMS. (Microsoft, 2016)

Las funciones que RMS permite son:

- **Creación de contenido protegido con RMS.** “Los usuarios que son entidades de confianza de un sistema RMS pueden crear y administrar fácilmente archivos protegidos utilizando aplicaciones y herramientas que incorporen las características de la tecnología de RMS.”
- **Emisión de licencias y distribución de contenido protegido con RMS.** Los certificados emitidos por los servidores de un sistema RMS identifican a las entidades de confianza que pueden publicar y utilizar contenido protegido con RMS. Los usuarios que son entidades de confianza de un sistema RMS asignan permisos y condiciones de uso al contenido que crean y desean proteger, estas directivas de uso especifican quién puede usar el contenido y qué se puede hacer con él. Los autores que utilizan el servicio

de RMS solicitarán licencias de publicación, que enlazan las directivas de uso con el contenido especificado. Así el contenido se distribuirá por toda la organización o empresa.

- **Adquisición de licencias para descifrar información protegida con RMS y aplicar directivas de uso.** “Los usuarios que son entidades de confianza pueden utilizar contenido protegido con RMS mediante clientes de confianza. Esos clientes son equipos y aplicaciones compatibles con RMS que permiten a los usuarios ver y trabajar con contenido protegido con RMS, para conservar la integridad del contenido e imponer directivas de uso. Cuando los usuarios intentan obtener acceso al contenido protegido con RMS, las solicitudes se envían a un servidor de RMS para emitir licencias de uso para que el usuario pueda utilizar ese contenido.” (Microsoft, 2016)

1.2.1.5.Sistemas Operativos de Computadora Personal.

Su misión consiste en presentar una buena interfaz a un solo usuario. Se les usa en forma amplia para procesamiento de texto, hojas de cálculo y acceso a Internet. Ejemplos comunes son Windows 98, Windows 2000, el sistema operativo Macintosh y Linux. Los sistemas operativos de computadora personal son tan conocidos que con toda seguridad no necesitan mucha presentación. (Tanenbaum, A. S. 2009.)

En la implementación de este proyecto se usó, Windows 8.1, que es un sistema operativo de computadora personal y se instalará para la demostración del rol de usuario o cliente en la

empresa u organización; este sistema operativo tiene compatibilidad con los servicios de RMS y también es donde se instalaron herramientas compatibles con RMS como por ejemplo Microsoft Word, Excel, PowerPoint, Outlook que pertenecen al paquete Microsoft Office.

1.2.1.6. Correo Electrónico

El correo electrónico es un servicio de internet que permite la comunicación entre dos o más personas a través del intercambio de textos escritos digitalizados; pero el correo electrónico no solo ofrece la posibilidad del envío de texto, sino también la posibilidad de enviar archivos adjuntos, por tanto la estructura básica de un correo electrónico consta de: el texto del mensaje, los archivos adjuntos, y el encabezado que es donde se encuentra los destinatarios que recibirán el mensaje, y quienes recibirán copia del mensaje, etc. (Vela C, 2006)

El correo electrónico fue creado por un ingeniero de la empresa BBN, Ray Tomlinson, que tuvo la idea de crear un programa que permitiera depositar mensajes en máquinas remotas. Dando así como resultado en 1971 la introducción del primer sistema de correo electrónico. (Vela C, 2006)

El sistema de comunicación de correo electrónico, es importante en el desarrollo de este proyecto, ya que es el medio por el cual los usuarios o clientes intercambiaran sus documentos electrónicos. Para la comunicación mediante correo electrónico se usaron los servicios de

Microsoft Exchange 2010, y Microsoft Outlook 2010 como herramienta para envío, recepción y archivo de correos electrónicos.

1.2.1.7.ISO/IEC 27002:2013

ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional), son parte de un sistema especializado para la normalización de estándares en todo el mundo. Los organismos que son miembros de ISO e IEC participan en el desarrollo de normas internacionales a través de comités técnicos que se establecen por la organización respectiva, para hacer frente a campos particulares de diferentes actividades técnicas. (ISO/IEC Directives, Part 2, 2014)

ISO/IEC 27002:2013 es una guía de buenas prácticas para mejorar la seguridad de la información en las empresas. Posee 14 dominios, 35 objetivos de control y 114 controles, de los cuales, para la ejecución de este proyecto se tomará como referencia el dominio número 10 que trata el tema de Cifrado, con su objetivo “Controles Criptográficos”, en donde los controles a aplicar son: política de uso de los controles criptográficos y gestión de claves. (ISO27000.es, 2016)

Tabla #1. ISO/IEC 27002:2013 Dominio 10

Elaborado por: Danilo Ninabanda.

10. CIFRADO
10.1 Controles criptográficos
10.1.1 Política de uso de los controles criptográficos
10.1.2 Gestión de claves

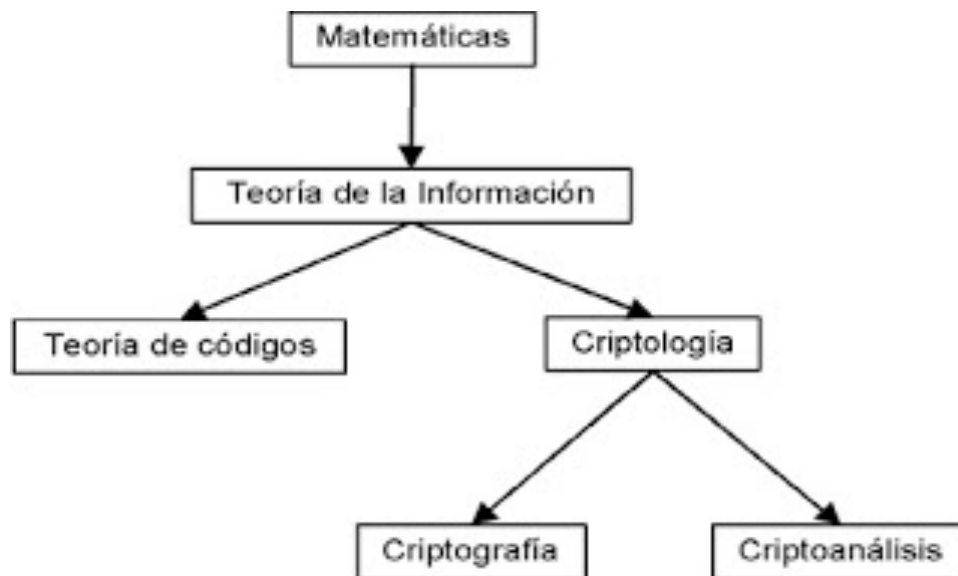
1.2.1.8.Criptografía – Cifrado

“La palabra criptografía proviene en un sentido etimológico del griego Kriptos=ocultar, Graphos=escritura, lo que significaría ocultar la escritura, o en un sentido más amplio sería aplicar alguna técnica para hacer ininteligible un mensaje”. (Paredes, G. 2006)

Dentro de las matemáticas, la criptografía se encuentra en la rama denominada “Teoría de la información”, y esta rama de las ciencias se divide en “Teoría de los códigos” y en “Criptología”. Y a su vez la Criptología en Criptoanálisis y Criptografía, así como se muestra en la siguiente gráfica. (Paredes, G. 2006)

Figura #5. Origen de la criptografía

Fuente: Introducción a la criptografía - Gibran Granados Paredes



“En un sentido más amplio, la Criptografía es la ciencia encargada de diseñar funciones o dispositivos, capaces de transformar mensajes legibles o en claro a mensajes cifrados de tal

manera que esta transformación (cifrar) y su transformación inversa (descifrar) sólo pueden ser factibles con el conocimiento de una o más llaves. En contraparte, el criptoanálisis es la ciencia que estudia los métodos que se utilizan para, a partir de uno o varios mensajes cifrados, recuperar los mensajes en claro en ausencia de la(s) llave(s) y/o encontrar la llave o llaves con las que fueron cifrados dichos mensajes”. (Paredes, G. 2006)

La criptografía se clasifica en dos grupos grandes, la criptografía clásica y moderna, para el desarrollo del proyecto se tomó en cuenta los conceptos de la criptografía moderna, porque en la solución planteada que es el servicio RMS de Microsoft hace uso del cifrado asimétrico, firmas digitales, creación de certificados de confianza y entre otras características. (Paredes, G. 2006)

Mario Paguay en su trabajo sobre Criptografía señala que para el estudio de los diferentes tipos de algoritmos es indispensable tener conocimiento de la notación que cada uno de ellos utiliza. A continuación citamos los elementos que componen los algoritmos.

M: conjunto de todos los mensajes sin cifrar.

C: conjunto de todos los posibles mensajes cifrados, o criptogramas.

K: conjunto de claves que se pueden emplear en el criptosistema.

E: conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de M para obtener un elemento de C.

D: conjunto de transformaciones de descifrado, análogo a E.

1.2.1.9.Criptografía Clásica

La criptografía clásica es la que se aplicaba hasta antes del siglo XX con algoritmos simétricos para mantener los mensajes que se enviaban en la época fuera del alcance de “miradas indiscretas”. Todos los tipos de cifrados que se han creado hasta antes de la II Guerra Mundial se consideran como clásicos. Todas estas técnicas tienen algo en común y es que estas pueden ser aplicadas y analizadas nada más con lápiz y papel. (Lucena, 2015)

1.2.1.10. Cifrado del César

Llamado así en honor al emperador Julio César, en el siglo I a.C. Este tipo de cifrado aplica al texto original un desplazamiento fijo de tres caracteres, para simular una transformación. La desventaja de este cifrado es que como la técnica usada para la encriptación era conocida (desplazamiento fijo de tres espacios), descifrarla no era ningún problema. (Pacheco F, 2014)

Como este algoritmo era un tanto inseguro para su uso se aplicaron algunas variantes una de ellas es que las personas que intervienen se pueden poner de acuerdo con la cantidad de espacios para el desplazamiento. (Pacheco F, 2014)

Figura #6. Ejemplo cifrado del César con desplazamiento de 4

Elaborado por: Danilo Ninabanda

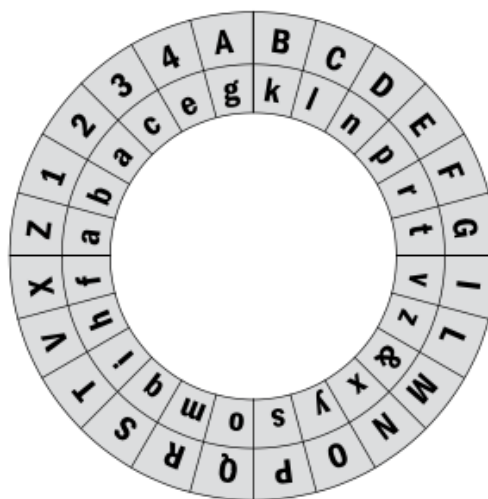
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V

1.2.1.11. El Disco de Alberti

Este método de cifrado fue inventado en el siglo XVI por el sacerdote León Battista Alberti que diseñó un disco para cifrar textos. “Este método, dependiendo de una clave, cada letra podía ser cifrada con un carácter diferente. Estaba compuesto por un disco exterior con veinte caracteres en latín más los números 1, 2, 3 y 4 en caso de necesitar el uso de códigos especiales, y un disco interior con los caracteres latinos más el signo & y las letras H, K e Y.” (Pacheco F, 2014)

Figura #7. Disco de Alberti

Fuente: Criptografía de Federico Pacheco



1.2.1.12. Cifrado de Vernam

Esta técnica de cifrado se propuso en 1917, consistía en la sustitución binaria que usaba el código de los teletipos (Baudot, de 5 bits). El sistema aplica la operación XOR y una secuencia aleatoria S obtenida en base a una clave (K) que era compartida entre las partes. (Pacheco F, 2014)

Figura #8. Código Baudot

Fuente: Libro Electrónico Seguridad Informática y Criptografía de Jorge Ramíó

Código Binario	Carácter	Código Binario	Carácter
00000	Blanco	10000	T
00001	E	10001	Z
00010	=	10010	L
00011	A	10011	W
00100	Espacio	10100	H
00101	S	10101	Y
00110	I	10110	P
00111	U	10111	Q
01000	<	11000	O
01001	D	11001	B
01010	R	11010	G
01011	J	11011	↑
01100	N	11100	M
01101	F	11101	X
01110	C	11110	V
01111	K	11111	↓

Tabla #2. Ejemplo operación XOR

Elaborado por: Danilo Ninabanda

XOR		BITS DE SALIDA
MENSAJE	CLAVE	
0	0	0
0	1	1
1	0	1
1	1	0

Tabla #3. Ejemplo cifrado de Vernam

Elaborado por: Danilo Ninabanda

Criptograma	11010	00000	01010	10110	10100	10101	10010
Clave	10100	00110	00111	11100	10111	11100	01010
Mensaje	01110	00110	01101	01010	00011	01001	11000
	C	I	F	R	A	D	O

1.2.1.13. La Máquina Enigma

Una de las herramientas más emblemáticas a lo largo de la historia que representa a la criptografía clásica, es la máquina Enigma, ya que este artefacto tuvo una participación muy

alta en la Segunda Guerra Mundial. Además Enigma dio paso al estudio de una nueva ciencia como lo es el criptoanálisis, y sobretodo dio paso al nacimiento de los que hoy conocemos como las computadoras.

La máquina Enigma fue patentada por el inventor alemán Arthur Scherbius en 1918, su parecido a una máquina de escribir tradicional facilitaba su uso entre los comerciantes que usaban este aparato para comunicarse de manera secreta. En sus inicios Enigma no tuvo mucho éxito comercial por lo que fue ofrecida a militares los que en una primera ocasión desestimaron la idea, en ese momento Enigma contaba con 2 versiones una con siete rotores o 6 billones de combinaciones y otra versión con treinta rotores o 100 trillones de combinaciones. Según los cálculos que hizo Scherbius se necesitaban 1000 operadores trabajando 24 horas durante 14 años para descifrar un mensaje. (Pérez C, 2008)

En 1923 después de algunas mejoras el ejército cambio su decisión y convirtió a Enigma como su canal de comunicación, en ese momento la máquina contaba con rotores mejorados que podían extraerse y cambiar su orden, se añadió un nuevo anillo a cada rotor que se podía poner en cualquiera de las 26 posiciones (una por cada letra). (Pérez C, 2008)

La máquina Enigma se encontraba compuesta por:

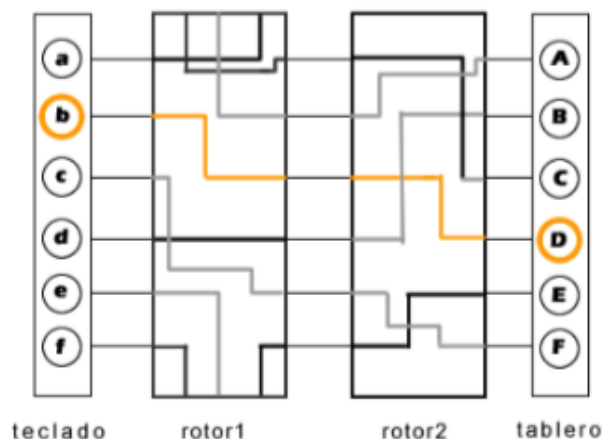
- Un teclado de 26 letras, tipo máquina de escribir
- “Lampboard” o Tablero luminoso de 26 bombillas para cada letra.
- “Steckerboard” o un frontal donde se podían hacer 13 conexiones para emparejar letras mediante unas clavijas.

“El funcionamiento de Enigma consistía que cuando se pulsaba una letra la corriente pasaba primero por el steckerboard. Supongamos que se pulsa la B y esta está intercambiada en el steckerboard por la A. La corriente pasaba de la B a la A y llegaba al primer rotor por el contacto correspondiente a esta letra en el lado derecho y su cableado interno la llevaba hasta un contacto diferente de su lado izquierdo, por ejemplo G. La corriente entonces pasaba de G a un contacto del lado derecho del segundo rotor y éste la llevaba de nuevo mediante el cableado interno hasta el otro lado, dando la señal W. Desde este contacto pasaba hasta la cara derecha del tercer rotor y se volvía a repetir el proceso. Supongamos que la salida del tercer y último rotor será la C. Cuando la corriente salía por el lado izquierdo del último rotor entraba en lo que llamamos reflector, que nos la retornaba también al lado izquierdo del tercer rotor pero en un contacto diferente, por ejemplo S.” (Pérez C, 2008)

Para realizar este proceso era necesario de dos operadores, uno se encargaba de escribir el mensaje en claro y el segundo operador copiaba las letras del tablero luminoso que se encendían y correspondían a cada letra del mensaje ya cifrado. (Pérez C, 2008)

Figura #9. Ejemplo simplificado de la máquina Enigma.

Fuente: Desarrollo de una máquina Enigma - Carlos Pérez.



1.2.1.14. Criptografía Moderna

Federico Pacheco, en su libro publicado en el año 2014 denominado “Criptografía” señala que la criptografía moderna nace con los avances tecnológicos de la matemática y de las ciencias de la información junto con el planteamiento de Claude Shannon sobre la teoría de la matemática de la información. Pacheco también indica que la criptografía moderna se basa en tres pilares:

- Teoría de la información
- Teoría de los números
- Teoría de la complejidad numérica

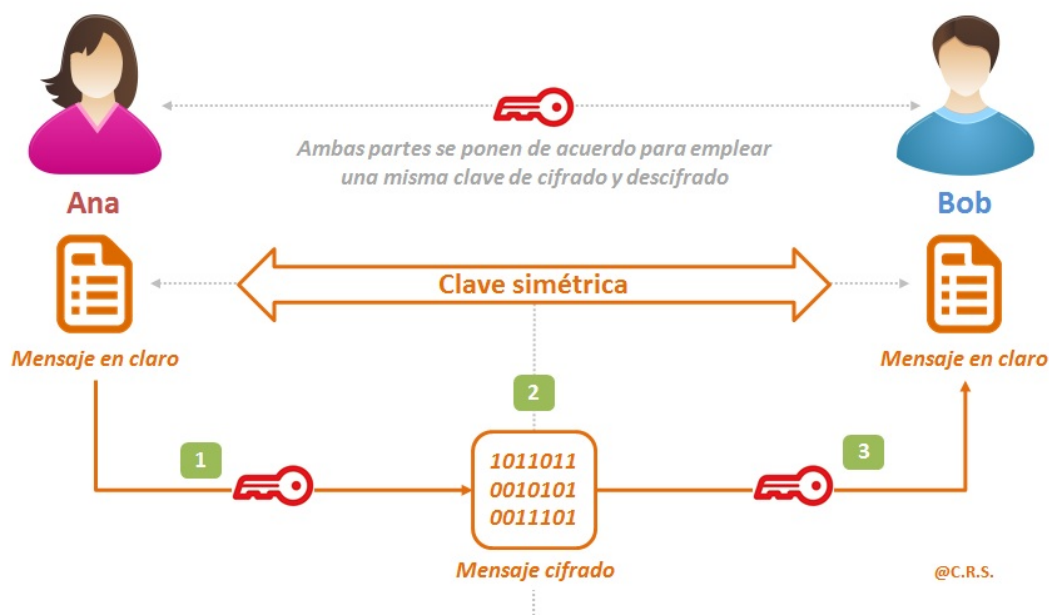
1.2.1.15. Criptografía Simétrica

“La criptografía simétrica se refiere al conjunto de métodos que permiten tener comunicación segura entre las partes siempre y cuando anteriormente se hayan intercambiado la clave correspondiente que llamaremos clave simétrica. La simetría se refiere a que las partes tienen la misma llave tanto para cifrar como para descifrar”. (Ángel, A. 2000)

“Este tipo de criptografía también es conocida como criptografía de llave privada, ya que esta utiliza la misma clave para cifrar y descifrar el mensaje de datos, es decir se basa en un secreto compartido.” (Mendoza, T. & César, J. 2008)

Figura #10. Demostración cifrado simétrico

Fuente: Criptografía de clave privada por secur-IT



1.2.1.16. Algoritmo Simétrico DES

DES (Data Encryption Standard) es el algoritmo más conocido mundialmente se basa en Lucifer un algoritmo creado por IBM a principios de los setenta, este algoritmo fue el primero en usar la red Feistel. En 1976 este algoritmo fue considerado como un estándar por el Gobierno de los Estados Unidos de Norteamérica para comunicaciones no clasificadas. (Lucena M, 2015)

El cifrado DES fue un producto comercial de IBM, ya que podía ser implementado en un solo chip, con un tamaño de llave de 56 bits con 8 bits de paridad. Esto fue muy controversial ya que en la primera versión poseía 128 bits de longitud de llave y los expertos consideraban

que la segunda versión del logaritmo no era lo suficientemente fuerte para soportar un ataque de fuerza bruta. (Carreño Castelló, M., & Valenzuela Ramírez, J. E. 2015)

“En cuanto al funcionamiento DES operaba de la siguiente manera:

- El texto plano se divide en bloques fijos de 64 bits a los cuales se les aplica una permutación inicial IP.
- Los bits salientes de la IP se dividen en 2 bloques de 32 bits denotados como L_i y R_i respectivamente, los cuales intercambian su lugar en cada ronda
- Para cada ronda el bloque L_i es el bloque R_{i-1} excepto en la última.
- Para cada ronda el bloque R_i es el resultado de función XOR entre el bloque L_{i-1} y la salida de cada función Feistel f excepto en la última.
- En cada ronda la función Feistel f desarrolla su funcionamiento con el bloque R_i y la respectiva llave K_n .
- Concluidas las 16 rondas se concatenan los 2 bloques de 32 bits y se les aplica la permutación IP^{-1} .
- La salida generada será el primer bloque de texto cifrado repitiendo el proceso hasta cifrar todos los bloques que forman el texto claro.” (Morales, A. 2012).

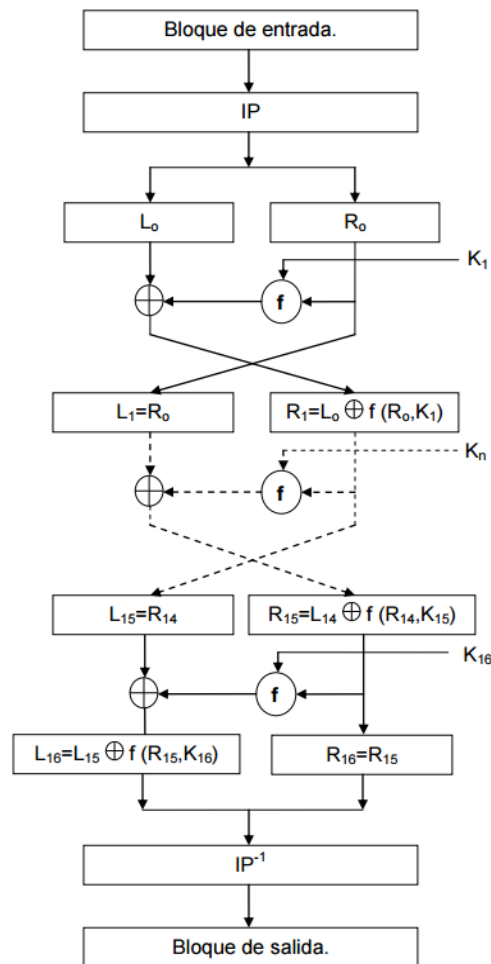
“Las operaciones que se mencionan en el funcionamiento del algoritmo DES son:

- Permutación Inicial IP: es la que genera difusión mediante la permutación de los 64bits de entrada como indica la tabla IP. La salida de este proceso es conocida como pre entrada.

- Función Feistel f: el objetivo de este proceso es generar difusión y confusión mediante la permutación de bits, expansión, contracción de bloques y ocho tablas diferentes de sustitución conocidas como tablas S_n . La función de Feistel consta de cuatro pasos que son:
 1. Expansión: es cuando ingresan 32 de los 64 bits del bloque de pre entrada a los cuales se les efectúa una permutación con expansión mediante la tabla E, generando un bloque saliente de 48 bits de los cuales algunos de ellos son duplicados.
 2. Mezcla: aquí el bloque saliente del paso anterior se ingresa para realizar una operación XOR con la subllave K_n generada en cada ronda obteniéndose así un nuevo bloque saliente de 48 bits.
 3. Sustitución: Los 48 bits obtenidos a la salida del paso mezcla, se dividen en 8 grupos de 6 bits procesándose cada uno con su respectiva tabla de sustitución $S_1, S_2, \dots, S_8$. Para ello, en cada grupo se toma el primer y último bit que indicara el número de fila de la tabla y los cuatro bits intermedios darán el número de columna. El valor de salida de la tabla es el elemento, representado en 4 bits, que se encuentra en la intersección de la fila con la columna. De esta forma los 4 bits de salida al ser concatenados generan un bloque de salida de 32 bits.
 4. Permutación: Los 32 bits obtenidos en el paso 3, se reordenan mediante la tabla de permutación P constituyendo el bloque de salida de la ronda Feistel.
- Permutación inversa IP^{-1} : consiste en una nueva permutación pero usando la inversa de la tabla IP.
- Generación de subllaves: aquí el algoritmo genera las 16 subllaves para emplearse en cada una de las rondas Feistel.” (Morales, A. 2012).

Figura #11. Funcionamiento del cifrado DES

Fuente: Análisis de los algoritmos de cifrado de llave secreta y su uso dentro de una organización pública



1.2.1.17. Algoritmo Simétrico IDEA

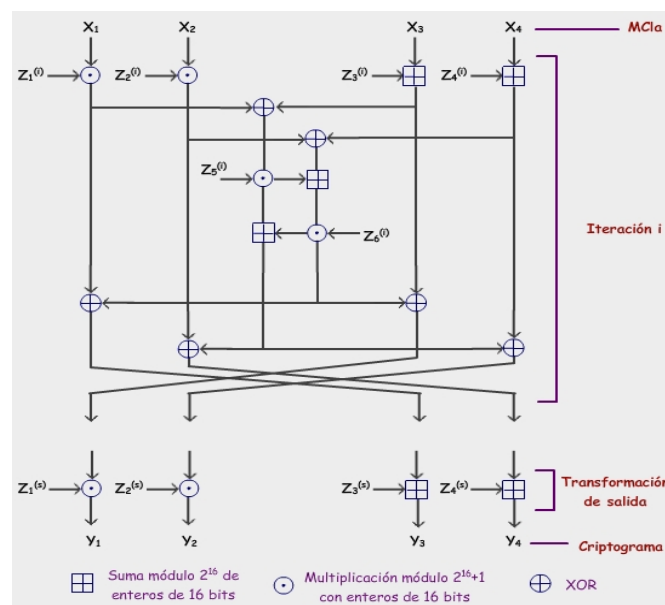
Este algoritmo fue diseñado en 1991 por Xuejia Lai y James Massey bajo el nombre de IDEA (International Data Encryption Algorithm), no usa la red de Feistel como DES, este algoritmo opera con bloques de 64 bits pero la clave que usa es de 128 bits, lo que asegura su fortaleza con espacio de claves de 2^{128} , es decir más de 3,4 cuatrillones de claves. (Pacheco F, 2014)

Jorge Ramío en su publicación llamada, “Seguridad informática y Criptografía”, expone las características básicas del funcionamiento del algoritmo IDEA que son:

- El mensaje en claro es dividido en cuatro bloques de 16 bits.
- Cifra los bloques de 64 bits en ocho vueltas.
- Genera 52 subllaves de 16 bits a partir de la clave maestra de 128 bits.
- Usa seis claves por vuelta.
- Hay una transformación final con cuatro claves para invertir la operación inicial.

Figura #12. Estructura de funcionamiento de algoritmo de cifrado IDEA

Fuente: Principales algoritmos simétricos – IDEA por Universidad Autónoma de México



1.2.1.18. Algoritmo Simétrico Rijndael (AES)

Este algoritmo fue creado en base a un concurso que organizó NIST (National Institute of Standards and Technology) en 1997, para que fuera usado como estándar de protección de datos, este algoritmo sería llamado AES (Advanced Encryption Standard) y debía cumplir con

algunas condiciones. Debía ser de dominio público, su estructura por bloques debía ser de mínimo 128 bits, con la opción que las llaves de cifrado puedan ser entre 128, 192, 256 bits, además este algoritmo debía ser compatible con la mayor parte de hardware y software. Después de que todos los algoritmos fueron analizados y sometidos a votación resultando ganador el algoritmo Rijndael de los criptólogos belgas Joel Daemen y Vincent Rijmen. Este algoritmo fue escogido ya que presentó la mejor combinación de seguridad, velocidad, eficiencia, sencillez y flexibilidad. Por tal motivo ahora AES es considerado como estándar de cifrado que utilizan los gobiernos, bancos, y algunas empresas privadas. (Morales, A. 2012)

El algoritmo de cifrado asimétrico AES, realiza el cifrado por bloques de 128 bits fijos y sus llaves pueden ser de 128, 192 o 256 bits, realizando n rondas según el uso del tamaño de su llave pudiendo ser 10, 12 o 14 rondas. (Morales, A. 2012)

El funcionamiento de AES comprende de una ronda inicial, $n-2$ rondas estándar y una ronda final que la realiza de la siguiente manera:

- El texto claro se divide en bloques de entrada de 128 bits para ingresar a la ronda inicial.
- En ésta ronda el bloque es operado con la llave inicial en la función AddRoundKey para luego ingresar a las rondas estándar.
- Las rondas estándar una por una operan al bloque con las funciones en el siguiente orden entendiendo que la salida de una es la entrada a la siguiente: ByteSub, ShiftRow, MixColumns y AddRoundKey con la K_i subllave siendo $1 \leq i \leq n-1$.
- Cuando las rondas estándar terminan, es la señal para que se inicie la ronda final considerando las funciones ByteSub, ShiftRow y AddRoundKey con la subllave K_n .

- El resultado de esta última ronda es el primer bloque ya cifrado, y este proceso se repite hasta que se logre cifrar todo el texto original. (Morales, A. 2012)

El cifrado AES se basa en una matriz de estados, que consiste que la unidad de información de cada una de sus celdas corresponde a un byte. Esta matriz se divide en: matriz inicial, matriz intermedia y matriz final. (Morales, A. 2012)

Figura #14. Matriz de estados algoritmo de cifrado AES

Fuente: Análisis de los algoritmos de cifrado de llave secreta y su uso dentro de una organización pública



La matriz inicial es la que indica como inicia el funcionamiento del algoritmo cifrador. La matriz intermedia mediante las funciones AddRoundKey, ByteSub, ShiftRow y MixColumns muestran el proceso de transformación. Por último y no menos importante la matriz final muestra el resultado de cada uno de las funciones. (Morales, A. 2012)

AddRoundKey

Esta función aplica la operación XOR al bloque de entrada con la llave pública en la ronda inicial. En las rondas que siguen la operación se hace con cada una de las subllaves obtenidas. El resultado de AddRoundKey será el bloque de entrada para la nueva función. (Morales, A. 2012)

“En la primera ronda la operación XOR es entre el bloque de texto original o claro y su llave de cifrado será K_0 , en las rondas estándar la operación XOR es entre el bloque de salida de la función MixColumns y la subllave K_i generada, en la ronda final la operación XOR es con el bloque de salida de la función MixColumns y la subllave final K_n . Cuando esta función termina de ejecutarse, el bloque de salida se convierte en el primer bloque de texto cifrado.” (Morales, A. 2012)

ByteSub

“Para esta función se sustituye de manera no lineal cada byte del resultado de la función AddRoundKey para generar un nuevo byte. La sustitución de cada byte resulta de la aplicación de la tabla de sustituciones S-box donde el primer valor de byte de entrada corresponde al número de fila y el segundo valor a la columna.” (Morales, A. 2012)

ShiftRow

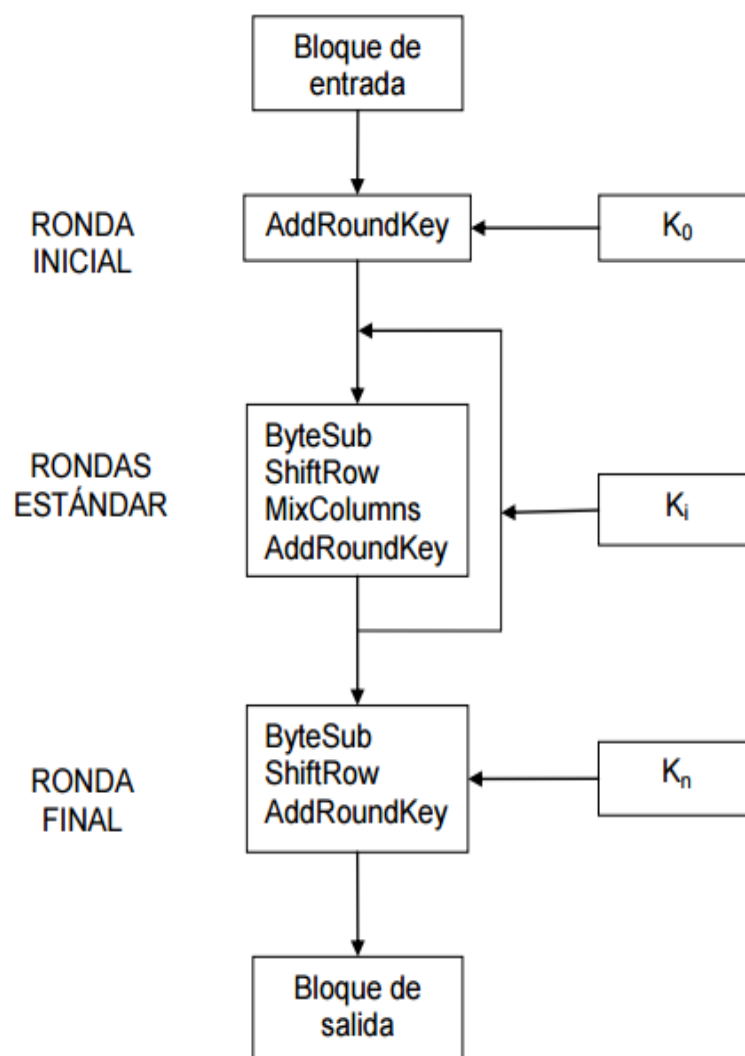
“Esta función rota a la izquierda los bytes de las filas de la matriz de estados de la función ByteSub. Los valores de rotación varían conforme a la longitud de la llave empleada. Para una llave de 128 bits, la primera fila siempre permanece igual, la segunda rota un byte, la tercera dos bytes y la cuarta 3 bytes.” (Morales, A. 2012)

MixColumns

“Actúa sobre los bytes de una misma columna de la matriz de estados de la función anterior lo cual permite una mezcla de los bytes de las columnas. Es decir, esta función consiste en una multiplicación en un campo de las columnas de la matriz de estados con una matriz polinomial. Dicha matriz está dada en el estándar.” (Morales, A. 2012)

Figura #13. Estructura de funcionamiento de algoritmo de cifrado AES

Fuente: Análisis de los Algoritmos de Cifrado de Llave Secreta y su uso Dentro de una Organización Pública



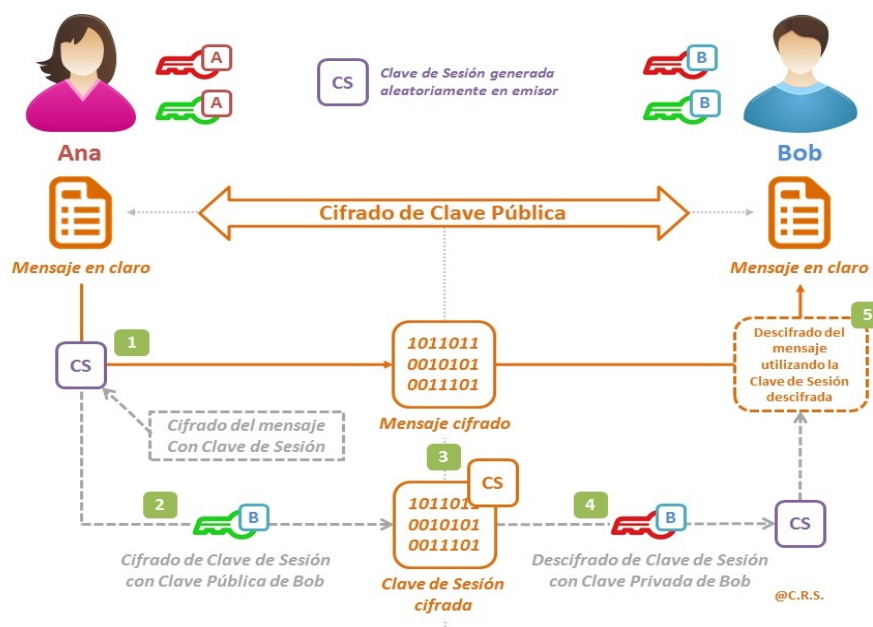
1.2.1.19. Criptografía Asimétrica

La criptografía asimétrica aparece por primera vez en 1976 de la mano de Diffie-Hellman, se la conoce también como criptografía de llave pública, basándose en el uso de dos claves diferentes, estas tienen la propiedad de que una clave puede descifrar lo que la otra ha encriptado. Estos algoritmos se basan en funciones matemáticas fáciles de resolver en un sentido, pero muy complicadas de realizar en sentido inverso, a menos que la clave privada su potencia y logaritmo sean descifrados. (Carreño, M. & Valenzuela, E. 2015)

El servicio de RMS se basa en la criptografía asimétrica y esta funciona de la siguiente manera: Si A desea mandar un mensaje que sólo B pueda ver, entonces A debe cifrar la información con la llave pública de B y solo B será capaz de descifrar la información con su llave privada, así como se muestra en la figura. (Velasco, V. 2006)

Figura #14. Demostración cifrado asimétrico

Fuente: Criptografía de Clave Privada por secur-IT



1.2.1.20. Algoritmo Asimétrico Diffie-Hellman

Este algoritmo es el método que permite el intercambio de claves entre el emisor y receptor para encriptar la información de los mensajes, tomando en cuenta que los usuarios no se han contactado para compartir dichas claves, y se comunican por un medio no seguro por lo que se podría decir que no se define si el usuario que emite el mensaje es el real. (Paguay Cuvi, H. 2015)

El funcionamiento de este algoritmo son necesarios los datos “g” y “p” que son dos numero primos grandes base y modulo respectivamente (mínimo 300 dígitos). Por otro lado también se necesita de las variables “a” y “b” que son números secretos de emisor y receptor. (Paguay Cuvi, H. 2015)

Para la obtención de datos este algoritmo realiza las siguientes operaciones:

- El emisor envía los datos g y p.
- Emisor y receptor generan un número secreto a y b respectivamente.
- El emisor realiza la siguiente operación y envía su resultado.

$$x = g^a \text{ mod } p$$

Envía el valor de x

- El receptor realiza la misma operación.

$$y = g^b \text{ mod } p$$

Envía el valor de y

- Emisor y receptor cambian a las bases Y y X respectivamente y obtienen la clave genérica de la siguiente forma.

Emisor realiza la operación $C = y^a \bmod p$

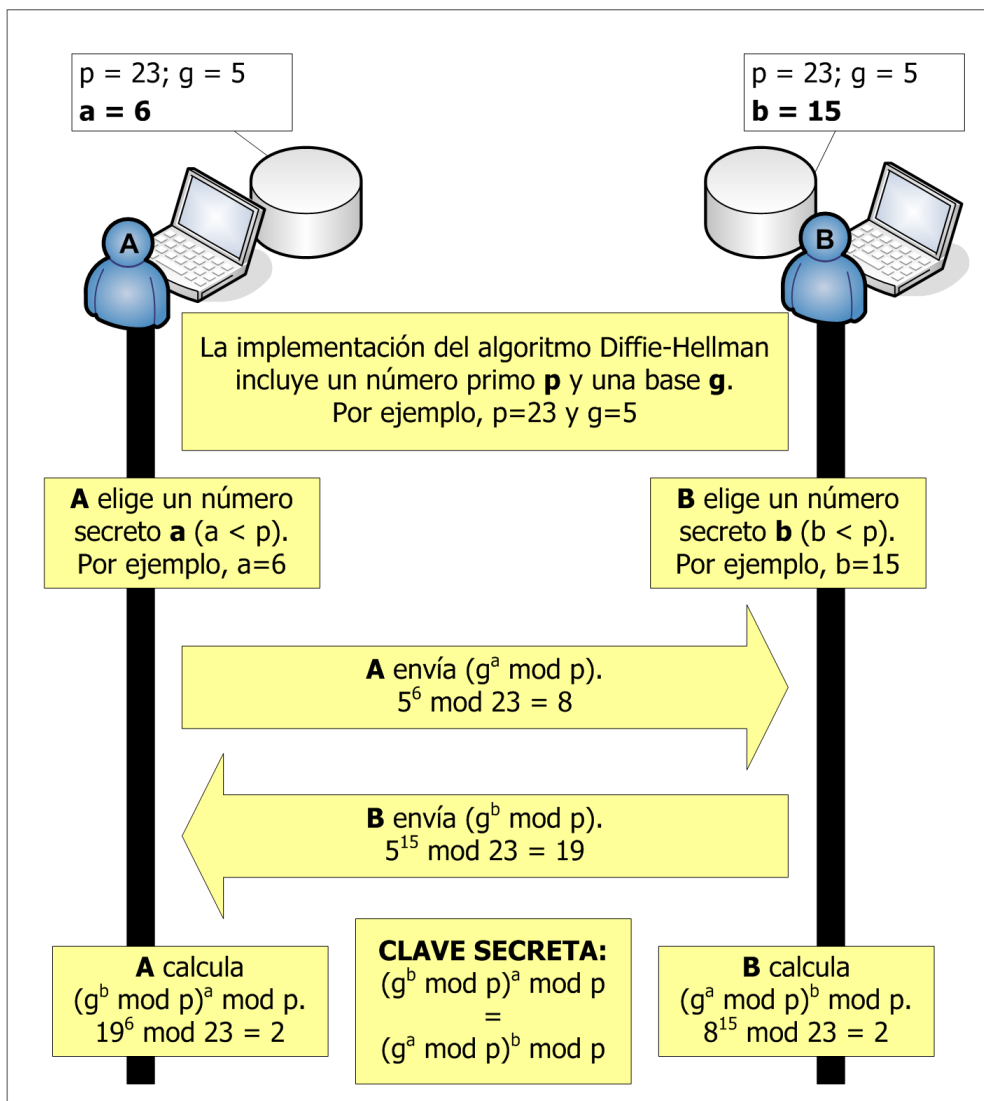
Receptor realiza la operación $C = x^b \bmod p$

La clave C obtenida sirve de llave privada para cifrar la información con métodos de cifrado.

(Paguay Cuvi, H. 2015)

Figura #15. Funcionamiento algoritmo asimétrico Diffie-Hellman

Fuente: El Algoritmo de Diffie-Hellman por Javier Campos.



1.2.1.21. Algoritmo Asimétrico RSA (Rivest, Shamir, Adleman)

RSA es un algoritmo de cifrado de información y firmas digitales se hizo público en 1977 sus creadores fueron Ron Rivest, Adi Shamir y Leonar Adleman. La principal característica de este algoritmo es que posee dos claves, pública y privada, con estas claves se puede cifrar y descifrar los mensajes. Es decir se cifra con la clave pública que puede ser de conocimiento de cualquier individuo y la clave privada se utiliza para descifrar el mensaje que se ha enviado. (Paguay Cuvi, H. 2015)

Una característica de RSA es que cuando se utiliza para enviar mensajes estos se representan con caracteres numéricos y el proceso de funcionamiento es en base al resultado de dos cifras que son primos grandes que se eligen aleatoriamente para así formar la clave que posteriormente descifrá el mensaje enviado. Además este algoritmo permite aparte de cifrar información; el intercambio de llaves y autenticación. (seguinfo. 2007)

Seguinfo en su publicación sobre el algoritmo RSA indica de manera simple su funcionamiento, el cual es el siguiente:

- Obligatoriamente se inicia con generar aleatoriamente dos números primos grandes, los que toman como nombre de variables p y q.
- Se calcula n como producto de p y q: $n = p * q$
- Continúa con el cálculo de ϕ : $\phi(n) = (p - 1) (q - 1)$
- Se calcula un número natural “e” de manera que $MCD(e, \phi(n)) = 1$, es decir debe ser primo relativo de $\phi(n)$.

- Mediante el algoritmo extendido de Euclides se calcula d : $e * d \bmod \phi(n) = 1$, puede realizarse el cálculo $d = ((Y * \phi(n)) + 1) / e$ para $Y = 1, 2, 3, \dots$ hasta encontrar un “ d ” entero.
- El par de números (e, n) son la clave pública.
- El par de números (d, n) son la clave privada.
- La función de cifrado es $C = M^e \bmod n$
- La función de descifrado es $M = C^d \bmod n$

1.2.1.22. Algoritmo Asimétrico Gamal

Es un algoritmo creado por Taher ElGamal en 1985, en sus inicios se usó para la generación de firmas digitales y con el pasar del tiempo se utilizó también para cifrar mensajes, la seguridad de este algoritmo está basada en el problema del logaritmo discreto. (Paguay Cuvi, H. 2015)

El funcionamiento de este algoritmo consiste primero en generar las claves en base a un grupo multiplicativo de enteros módulo p , con el siguiente proceso:

- Eligiendo un primo p tal que $(p - 1)$ tenga un factor primo grande.
- Se elige aleatoriamente un generador g (valor público)
- Se elige un valor a mayor que 2 y menor que $(p - 1)$, que será la clave privada, que debería ser grande.
- Se calcula $A = g^a \bmod p$, que resulta ser la clave pública (p, g, a) . (Pacheco F. 2014)

Al momento de cifrar información de un mensaje M el algoritmo funciona de la siguiente manera:

- Se convierte M en un elemento m del grupo G.
- Se elige un numero b aleatorio, mayor que 2 y menor que (p - 1).
- Se calcula $y1 = g^b \pmod{p}$ y $y2 = A^b m \pmod{p}$.
- Se obtiene como criptograma la tupla (secuencia ordenada de objetos): $C^b(m, b) = (y1, y2)$
- Para descifrar el criptograma se hace $y1^{xy2} \pmod{p}$ donde $x = p-1-a$. Si se aplica el teorema de Fermat quedaría la expresión: $y1^{(p-1-a)y2} = m \pmod{p}$. (Pacheco F. 2014)

1.2.1.23. Funciones Hash

Después que el mensaje o la información ha sido cifrada con una llave privada la criptografía simétrica tiene disponible una ventaja y es que esta proporciona un tipo de aplicación que se llama función de resumen o función de hash, que son fragmentos del mensaje encriptado, que dependen totalmente del mismo, si se cambia el mensaje cambia el resultado de la operación. (Velasco, V. 2006)

“Basta entonces, para garantizar autenticidad, cifrar el resultado de la función de resumen con la llave privada. Si el mensaje es auténtico, entonces tendrá el mismo resultado de la función de resumen y se compara con el resumen descifrado con la llave pública, si son iguales se garantizan dos cosas: el mensaje es auténtico (lo envió quien dice enviarlo) y es íntegro (no se modificó). Si no son iguales entonces puede suceder dos cosas: el mensaje no lo

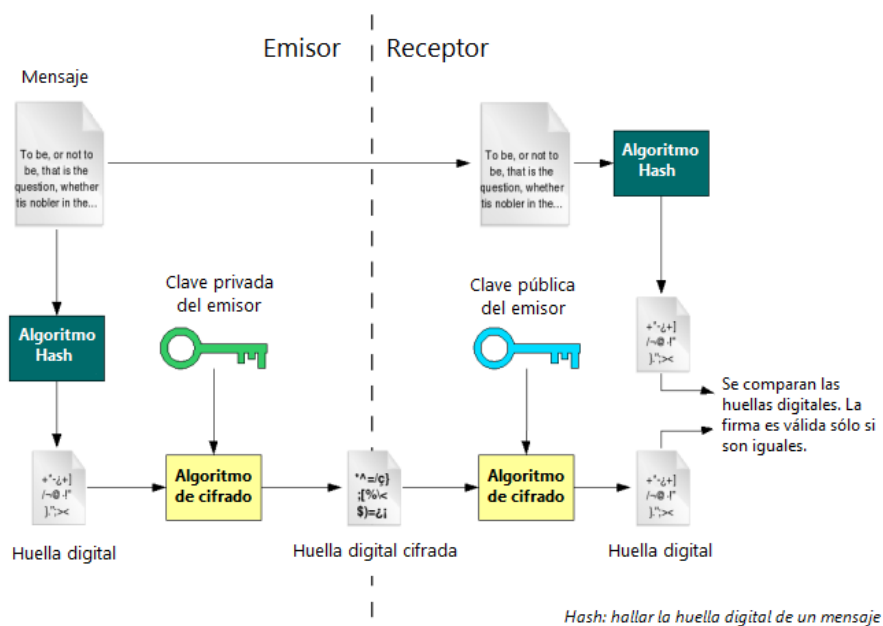
envió quien dice enviarlo (no es auténtico) o alguien lo modificó en el camino, de cualquier manera, sabemos que no podemos confiar en esa información.” Así el proceso de la función hash trabaja para cuidar la integridad de la información. (Velasco, V. 2006)

Existen varios tipos de funciones hash y todas tienen como objetivo proteger la integridad de la información, entre los tipos de hashes criptográficos se tiene: Message Digest, Secure Hash Algorithm, Tiger, Whirlpool, entre otros. (Pacheco F. 2014)

Uno de los hashes más usados es el Secure Hash Algorithm o SHA que fue creada por la NSA (National Secure Agency) de Estados Unidos de Norteamérica y publicada por el NIST, la primera versión de este algoritmo salió en 1993, y el segundo que fue el más conocido fue SHA-1. (Pacheco F. 2014)

Figura #16. Estructura función Hash

Fuente: En qué consiste la firma de un APK por humanos.uci.cu



Certificados Digitales.

Los certificados digitales son llamados así a los documentos con un formato especial, firmado digitalmente por una autoridad certificante, permitiendo vincular a una entidad con los datos de verificación de una firma que están incluidos en el certificado, validando así la procedencia e identidad del documento. Estos certificados pueden ser de varios tipos dependiendo de la información que maneja y la entidad que lo relaciona. (Pacheco F. 2014)

“VeriSign define clases como se puede indicar a continuación.

- Clase 1: para personas (email)
- Clase 2: para organizaciones (requiere prueba de identidad)
- Clase 3: para servidores y firma de software (requiere distintas verificaciones)
- Clase 4: para transacciones comerciales online entre empresas.
- Clase 5: para organizaciones privadas o seguridad gubernamental.” (Pacheco F. 2014)

Comúnmente se puede encontrar el uso de certificados digitales en los servidores web con HTTPS, que son los que permiten que el navegador verifique la identidad del usuario, algo que es fundamental en el comercio electrónico y en otras aplicaciones que usan datos sensibles. Para saber si estos certificados son válidos existe un listado de números de serie de certificados que están validos o que se encuentran revocados, esta lista se denomina CRL (Certificate Revocation List). (Pacheco F. 2014)

Los certificados digitales siempre se emiten con un período de validez, asegurando así que no corra el riesgo de ser falsificado, otros motivos por los que los certificados han sido revocados pueden ser que la clave privada haya sido perdida o robada, que se pierda la condición que permitió expedirlo, algún dato incorrecto o erróneo o por una orden judicial. Un CRL debe estar firmado digitalmente por la autoridad certificadora, para así permitir constatar la validez de dicho certificado. (Pacheco F. 2014)

Figura #17. Estructura certificado digital

Fuente: Certificado Digital por Andrea Hernandez



1.2.1.24. Controles Criptográficos.

Según la norma ISO/IEC 27002:2013, los controles criptográficos tienen el objetivo de proteger la confidencialidad, autenticidad o integridad de la información por medio de las técnicas criptográficas. Toda organización debería utilizar controles criptográficos para la protección de claves, datos y servicios, inclusive para la transmisión de información clasificada. (ISO27000.es. 2016)

La norma también manifiesta que es necesario el desarrollo de procedimientos y asignación de funciones respecto de la administración de contraseñas, recuperación de desastres con información cifrada, y en cuanto al cambio de claves. (ISO27000.es. 2016)

El uso del cifrado y las longitudes de claves deberán ser evaluadas periódicamente, esto con el fin de que las técnicas de descifrado avancen y puedan aumentar el riesgo de que la información pueda ser descifrada. (ISO27000.es. 2016)

En cuanto a las firmas digitales se conoce que ayudan con la protección de la autenticidad e integridad de los documentos electrónicos, pero en ocasiones, se necesitará del asesoramiento legal para establecer acuerdos especiales que respalden su uso. (ISO27000.es. 2016)

1.2.1.25. Política de Uso de los Controles Criptográficos

ISO/IEC 27002:2013 en su control 10.1.1, Política de uso de controles criptográficos, señala que se debe desarrollar e implementar una política para regular el uso de los controles criptográficos para la protección de la información. (ISO27000.es. 2016)

La política de seguridad de información según la norma, luego de ser desarrollada, debe ser aprobada por la dirección principal de la organización y debe ser publicada para el

conocimiento de todos los empleados y partes externas relevantes. (ISO27002.wiki.zoho.com. 2016)

Según SANS instituto de investigación cooperativa, donde varios expertos de seguridad de la información de todo el mundo comparten sus conocimientos, proponen una política para la protección de claves cifradas. Esta política tiene el objetivo de indicar cuales son los requisitos para proteger las claves que se encuentran en uso por los usuarios finales; estos requisitos están diseñados para evitar la divulgación no autorizada y su mal uso posterior. Los métodos que propone son: procedimientos de copia de seguridad, claves de cifrado bajo una clave y el uso de hardware resistente a la manipulación. (SANS Consensus Policy Resource Community. 2014)

En el ANEXO 1 se pone en consideración la estructura de la política de cifrado aceptable creada por SANS, en la que cualquier empresa podrá tener una guía clara de cuáles son los puntos que debe tomar en cuenta para la creación de políticas de encriptación.

1.2.1.26. Gestión de Claves

“Una política de gestión de claves es un conjunto de reglas que establecen el modo de generación, almacenamiento, distribución, borrado, actualización, recuperación, protección y aplicación de claves en una red, en dicha política también se establece quién es la persona o grupo de personas autorizadas a realizar cada una de estas acciones.” (Universidad Autónoma de México – Facultad de Ingeniería. 2016)

Existen varios motivos por los que es importante implementar una política de gestión de claves, entre los cuales se puede citar:

- Renovar claves cada cierto tiempo prudente ya que cada vez que se usan estas quedan expuestas.
- Aplicar diferentes claves para los distintos servicios que los usuario manejan, esto con el fin de que si en algún momento la clave ha sido vulnerada se pueda controlar los daños que esto pueda causar.
- Se debe asignar diferentes claves para cada uno de los usuarios o grupos de trabajo que acceden a la red, de forma que solo los usuarios autorizados tengan acceso a información clasificada. (Universidad Autónoma de México – Facultad de Ingeniería. 2016)

1.2.2. Marco Conceptual

1.2.2.1.Seguridad de la Información.

Cuando se menciona a la seguridad de la información se está haciendo referencia a toda información que tiene cierto grado de importancia que hay que proteger, por lo tanto se puede definir a la seguridad de la información como el conjunto de medidas técnicas, organizativas y

legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su sistema. (Mifsud E. 2012)

1.2.2.2.Documentos Electrónicos.

Son el conjunto de documentos producidos, recibidos o reunidos por una persona natural o jurídica, de modo espontáneo como apoyo de la actividad que realiza, haciendo uso de la electrónica. Los mismos se conservan y transmiten también mediante medios electrónicos, con medidas de autenticación y de preservación adecuadas, con el fin de garantizar su valor informativo, legal y cultural así como de permitir su acceso y uso también mediante las tecnologías de la información. (Navarro, E. 2001)

1.2.2.3.Confidencialidad.

La confidencialidad es considerada de extrema importancia. Su objetivo principal es que la información privada no se revele a personas no autorizadas, la confidencialidad debe ser tomada en cuenta en la información almacenada durante su procesamiento y cuando se encuentra en tránsito. (Areitio Bertolín, J. 2008)

1.2.2.4.Integridad

La integridad es la encargada de garantizar que la información del sistema no haya sido alterada por usuarios no autorizados, evitando la perdida de consistencia. Cuando se trata de integridad de datos el objetivo principal es velar que la información no haya sido alterada, mientras se almacena, procesa o transmite, en cambio cuando se menciona la integridad del sistema es la cualidad que posee un sistema cuando desempeña sus funciones de manera, limpia no deteriorada y sobretodo libre de manipulación no autorizada. (Areitio Bertolín, J. 2008)

1.2.2.5.Disponibilidad.

Cuando se habla de disponibilidad se hace referencia a que la información del sistema debe permanecer accesible a elementos autorizados. El objetivo principal de la disponibilidad es prevenir interrupciones no autorizadas de todos los recursos informáticos. En términos de seguridad informática “un sistema está disponible cuando su diseño e implementación permite deliberadamente negar el acceso a datos o servicio determinados”. Es decir, un sistema es disponible si permite no estar disponible. (Mifsud E. 2012)

1.2.2.6.No Repudio.

“Este objetivo garantiza la participación de las partes en una comunicación. En toda comunicación, existe un emisor y un receptor, por lo que puede distinguir dos tipos de no

repudio: a) No repudio en origen: garantiza que la persona que envía el mensaje no puede negar que es el emisor del mismo, ya que el receptor tendrá pruebas del envío. b) No repudio en destino: El receptor no puede negar que recibió el mensaje, porque el emisor tiene pruebas de la recepción del mismo.” (infosegur. 2013)

CAPÍTULO II

MÉTODO

2.1. Análisis

2.1.1. Estudio Preliminar

Como ya se ha mencionado en el capítulo anterior, la información es el recurso más importante que una empresa puede tener y ese es el motivo por el cual se la debe proteger a como dé lugar para evitar daños irreparables que afectarían a las empresas. Existen varias formas para proteger la información, en esta ocasión se usará el cifrado.

El cifrado de datos es una técnica que apareció hace unos 4000 años atrás, donde los jeroglíficos que ahora se conoce, son considerados como una técnica de encriptación donde según hace referencia la historia, para descifrar estos mensajes se usó la llamada Piedra Rosetta. Así el cifrado ha ido formando parte de las comunicaciones de las sociedades más antiguas, como la Antigua Grecia, la Antigua Roma con el cifrado César, pasando por la Edad Media donde la criptografía sufre algunos cambios y da paso a la creación del cifrado Alberti que es el más conocido de la época. Con el pasar del tiempo la técnica del cifrado fue una herramienta imprescindible para uso militar en todo el mundo, un claro ejemplo y el que más

destaca es la creación de la máquina Enigma que fue pieza clave en la Segunda Guerra Mundial, porque con el uso de esta máquina prácticamente hacia que las comunicaciones sean indescifrables y permitiera que los Alemanes pudieran controlar el Atlántico Norte con sus submarinos. Esto dio origen no solo al conflicto armado sino también a la lucha para encontrar el código o clave para descifrar sus mensajes, en la cual estaban inmersos prestigiosos matemáticos, ingenieros, criptógrafos, entre ellos Alan Turing que se encontraban concentrados en Bletchley Park; el resultado de esto fue el descifrado de los mensajes que codificaba la máquina Enigma acelerando el fin de la Segunda Guerra Mundial y evitando la muerte de millones de personas. De ese modo y de otros ya creados en la Primera Guerra Mundial, como el uso del lenguaje nativo de los americanos, fue que el cifrado se convirtió en una herramienta importante para las comunicaciones hace mucho tiempo.

En la actualidad existen diversos algoritmos y técnicas para cifrar información y comunicaciones, pero en algunas empresas esta medida de prevención casi no es utilizada. Con el aumento del flujo de información y sobretodo de documentos confidenciales se han vuelto más comunes los delitos de robo de información, por lo que esto genera una gran preocupación en las empresas ya que su información se encuentra cada vez más vulnerable ante las diferentes amenazas que se encuentran en la red, así lo indica una encuesta que se realizó en el Security Report Latinoamérica 2016, que revela que una de las principales preocupaciones que tienen los encargados de la seguridad de la información es el acceso indebido a su información. Esta revelación no es nueva ya que hace tres años atrás las declaraciones que hizo Edward Snowden sobre la violación de la privacidad de la información avivó la preocupación sobre la confidencialidad, una de estas declaraciones del ex trabajador de la CIA y NSA fue publicada por “The Washington Post” que afirmaba que la NSA recolectó más de 250 millones de buzones

de diferentes proveedores de servicio de correo electrónico, poniendo al descubierto la necesidad de implementar medidas para proteger la confidencialidad e integridad de toda información.

Figura #18. Estadísticas sobre las preocupaciones en materia de seguridad de la información en las empresas de Latinoamérica.

Fuente: ESET Security Day 2016



Después de las declaraciones que hiciera Snowden, en los últimos años ha surgido un nuevo delito conocido como “haxposición”, el cual se caracteriza por el robo de la información y la exposición de la misma, pero no solo es eso sino que la estrategia de este ataque es la exposición de muchos “secretos peligrosos” que significa serios daños a la imagen de la empresa y a sus clientes. De acuerdo al investigador Stephen Cobb la motivación para que los atacantes realicen estas actividades son el descontento con los modelos de negocios de las empresas que serían las víctimas. Como referencia a este tipo de delito se puede citar varios casos empezando por Ashley Madison página muy conocida que realizaba citas extramatrimoniales, ocurrido en Julio del 2015 que fue atribuido a un grupo de hackers informáticos autodenominado “Impact Team” que amenazaron con filtrar información de los

usuarios que hacían uso del servicio de esta página si no cumplían sus demandas, las cuales eran cumplir con el servicio de borrar los datos de los clientes después de haber cancelado una suma de dinero lo cual Ashley Madison nunca había cumplido; teniendo como resultado la filtración de 10GB de datos personales entre ellos números de tarjetas de crédito y correos electrónicos de aproximadamente 37 millones de usuarios.

Otro caso muy conocido que causó conmoción a nivel mundial fue el ataque que sufrió la empresa de seguridad de la información italiana “Hacking Team”, la cual perdió en una sola noche 400GB de información acerca de sus actividades. El ataque tuvo éxito debido a que la empresa hacía uso de “contraseñas débiles”, entre las que se incluyen la de su cuenta oficial de twitter, donde los atacantes dejaron una publicación con un link del repositorio para acceder a la información robada. En estos dos casos y en otros que se han suscitado en estos tiempos y que se ha visto comprometida su información las empresas en ese momento no contaban con alguna solución de cifrado que protegiera dicha información de los atacantes.

Así como el cifrado puede ser una herramienta para ayudar a proteger que la información llegue a manos equivocadas, esta técnica puede servir para ocultar la información que ya fue sustraída y empezar a distribuirla al público, tal como sucedió con el caso de los “Panamá Papers” donde la fuente que reveló estos documentos, que hacían público el uso de empresas ficticias (offshore) para que los clientes puedan ocultar sus activos, tomó contacto en primera ocasión y por medio de un servicio de mensajería encriptado (Jabber, Telegram, Wickr) con un periodista Alemán para darle instrucciones de cómo le llegarían dichos documentos; más tarde luego de que el “hacker” había dejado claro algunos puntos los documentos empezaron a llegar hasta que se recabó toda la información con un total de 2.6TB, archivos que fueron distribuidos

en algunos discos encriptados usando el software libre denominado VeraCrypt, según declaraciones de Mar Cabra que es jefa de Unidad de Datos e Investigación del ICIJ (Consejo Internacional de Periodistas de Investigación).

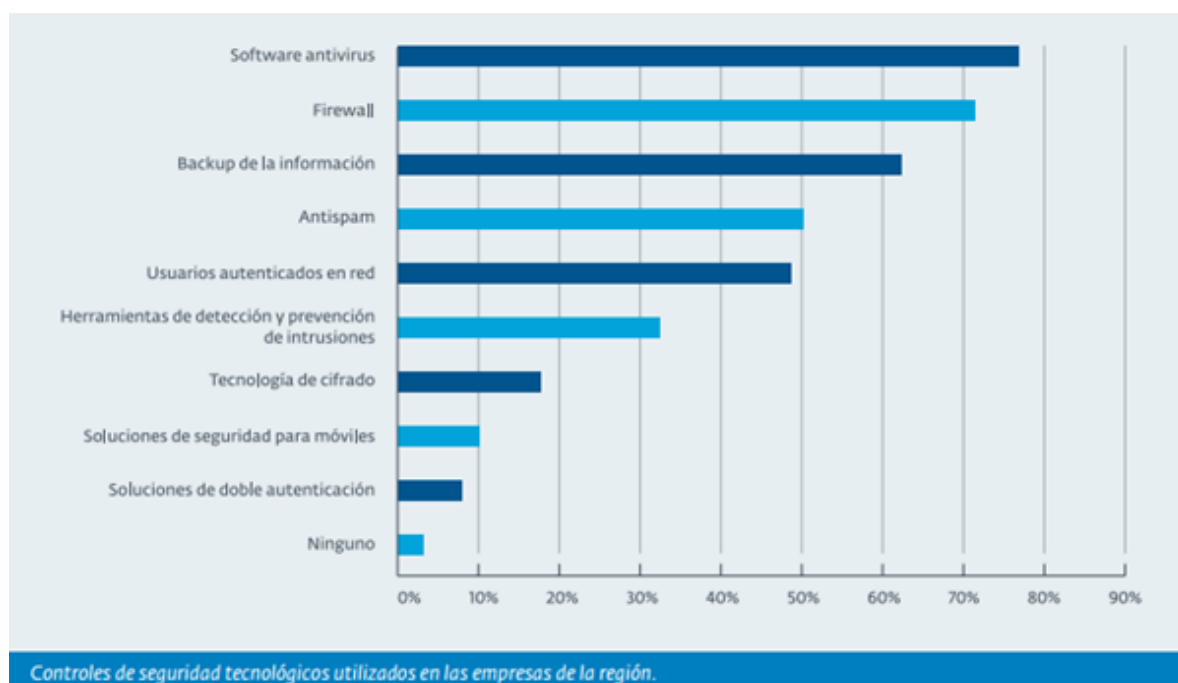
Según Mounir Idrassi, quien fue el principal desarrollador de VeraCrypt, explicó a Forbes que esta aplicación arreglo muchas vulnerabilidades de su antecesor (TrueCrypt), usando algoritmos más sólidos que prácticamente serían imposibles descifrar. Al finalizar, estos documentos llegaron al buscador Amazon donde fueron compartidos a más de 400 periodistas que ingresarían mediante un link y una contraseña que se generaría previamente de manera aleatoria, esto para empezar a buscar cualquier archivo que al periodista le interesara. Nuevamente el cifrado hace aparición en este sonado caso y es que cualquier persona que ingresara al sitio lo haría a través de líneas protegidas usando el protocolo de encriptación SSL.

Después de tantos casos, las empresas deberían aplicar controles más efectivos para poner a buen recaudo su información, no solo la que se encuentra almacenada en las terminales de sus usuarios o las que se encuentran en sus servidores, sino también las que se encuentran en tránsito por diferentes vías; así como lo hizo la ICIJ, quienes usaron el cifrado para publicar esos polémicos documentos.

Es la época donde la innovación genera ventajas y estas deben ser aprovechadas por las empresas, complementando sus soluciones de seguridad de la información con técnicas y herramientas de cifrado. A pesar de ello, la realidad de las empresas demuestra totalmente lo

contrario donde el cifrado casi no es tomado en cuenta como herramienta para proteger la información.

Figura #19. Estadísticas sobre los controles de seguridad utilizados en las empresas de Latinoamérica.
Fuente: ESET Security Day 2016



El Security Eset Report (2016), indica que en Latinoamérica el uso del cifrado no es una solución que los encargados del área de tecnología apliquen para proteger su información, por tal motivo este proyecto da apertura a la implementación de técnicas de cifrado, así como a herramientas con las que cuentan los sistemas que se usan en la mayoría de empresas; tal es el caso del servicio de RMS (Rights management Services) que brinda Microsoft en su sistema operativo Windows Server 2008, a esto se suma la ejecución de buenas prácticas en cuanto a políticas de cifrado, políticas de gestión de claves, las cuales pueden disminuir considerablemente el robo de información, ahorrando tiempo y dinero pero sobretudo brindando más confianza a la empresa.

2.1.2. Estudio de Factibilidad

Para determinar la factibilidad de este proyecto se utilizó tres variables que nos ayudarán a concluir si el proyecto es factible.

Tabla #4. Tipos de factibilidad.

Elaborado por: Danilo Ninabanda.

Tipo de Factibilidad	Concepto
Operativa	Determina si los recursos de servicios y de personal son adecuados para la implementación de Rights Management Services.
Tecnológica	Determina si los equipos y la infraestructura son los adecuados para la implementación de Rights Management Services
Económica	Esta variable es la más importante ya que de acuerdo a un análisis de costos indica el capital que necesita la empresa para aplicar este servicio.

2.1.2.1. Factibilidad Operativa

Después de la implementación del modelo de comunicaciones seguras la colaboración del personal de tecnologías de la información de la empresa es indispensable y debe estar totalmente capacitado para brindar soporte sobre cualquier incidencia que ocurra sobre el servicio de RMS; con esto se asegura que el personal de tecnologías será completamente autónomo en la creación de nuevas políticas para el uso de documentos electrónicos de la empresa.

Las personas a cargo deberán tener conocimientos y aptitudes de acuerdo a lo que se detalla a continuación.

Tabla #5. Perfil de competencias necesarias para la operación del proyecto.

Elaborado por: Danilo Ninabanda.

Cargo	Funciones del cargo
Gerente de infraestructura	Los Gerentes de Infraestructura de TI desarrollan estándares técnicos, implementan tecnología y supervisan a los trabajadores que se ocupan de los temas de tecnología de información en las organizaciones. Si una herramienta nueva y útil de TI es identificada, el CTO (Chief Technology Officer) determina una o más estrategias para su posible aplicación, considerando el análisis del costo-beneficio y el retorno de la inversión. (Referencia: Departamento del Trabajo USA)
Administrador de redes	Los Administradores de Redes diseñan, instalan y brindan soporte a los sistemas de información de las organizaciones. Los Administradores de Redes son responsables de las redes LAN, WAN, segmentos de red, Internet e intranet. Ellos instalan y proporcionan soporte al hardware y software de la red. Los Administradores de Redes se encargan de que el sistema de información de la organización, las computadoras, el software y la red propiamente dicha funcionen correctamente en forma conjunta. (Referencia: Departamento del Trabajo USA)
Analista seguridad de la información	El Analista de Seguridad planifica, coordina y mantiene la seguridad de la información de una organización. Estos profesionales educan a los usuarios sobre la seguridad de la información, instalan software de seguridad, supervisan las redes para detectar los puntos vulnerables de seguridad, responden a los ataques cibernéticos, y en algunos casos, reúnen datos y pruebas que se utilizarán en la persecución de la delincuencia cibernética. (Referencia: Departamento del Trabajo USA)
Analista de riesgos de TI	El Analista de Riesgos de las Tecnologías de la Información se encarga del proceso de identificación, cuantificación y priorización de los riesgos comparándolos con el criterio para su aceptación dentro del marco de los objetivos relevantes para la organización. Los resultados de este proceso permitirán determinar la acción apropiada de gestión; así como, las prioridades para manejar la información de los riesgos de seguridad y poder implementar controles y medidas de protección contra estos riesgos. (Referencia: ISACA)
Arquitecto de sistemas de información	El Arquitecto de Sistemas de Información utiliza las herramientas de TI para ayudar a que las empresas funcionen eficientemente y puedan alcanzar sus objetivos estratégicos. La mayoría de los analistas de sistemas de información trabajan con sistemas de información específicos; por ejemplo, de negocios, contabilidad, financieros, científicos y de ingeniería de sistemas, que varían con el tipo de organización. (Referencia: OnetCenter - Departamento del Trabajo USA)

2.1.2.2.Factibilidad Tecnológica

Para la implementación del modelo de comunicaciones seguras se requiere:

Tabla #6. Requisitos de hardware para aplicar RMS de Microsoft

Elaborado por: Danilo Ninabanda.

REQUISITO	RECOMENDACIÓN
Un procesador Pentium 4 a 3 GHz o superior	Dos procesadores Pentium 4 a 3 GHz o superior
512 MB de memoria RAM	1024 MB de memoria RAM
40 GB de espacio libre en el disco duro	80 GB de espacio libre en el disco duro

Tabla #7. Requisitos de software para aplicar RMS de Microsoft

Elaborado por: Danilo Ninabanda.

SOFTWARE	REQUISITOS
Sistema Operativo	Windows Server 2008 R2
Sistema de archivos	Sistema de archivos NTFS recomendado
Mensajes	Message Queue Server
Servicios web	Internet Information Services (IIS) ASP.NET debe estar habilitado
Active Directory o AD DS	AD RMS debe estar instalado en un dominio de Active Directory en el que los controladores de dominio ejecuten Windows Server 2003, Windows Server 2008 o Windows Server 2008 R2. Todos los usuarios y grupos que usen AD RMS para adquirir licencias y publicar contenido deberán tener una dirección de correo electrónico configurada en Active Directory.
Servidor de base de datos	AD RMS necesita un servidor de base de datos (como Microsoft SQL Server 2005) y procedimientos almacenados para llevar a cabo operaciones.

2.1.2.3.Factibilidad Económica

En cuanto al costo para implementar el modelo de comunicaciones se deberá tomar en cuenta la tabla que se encuentra a continuación de este apartado, donde se detalla cada uno de los rubros necesarios, además en el ANEXO 2 se pone a consideración una cotización de las licencias de uso del servicio de RMS de Microsoft.

Tabla #8. Cuadro de costos para la implementación de RMS en una infraestructura Microsoft

Elaborado por: Danilo Ninabanda.

TAREA O ACTIVIDAD	TIEMPO DURACIÓN (d)	R E C U R S O S H U M A N O S						O T R O S R E C U R S O S						COSTO POR TAREA O ACTIVIDAD
		CONSULTOR MASTER			CONSULTOR JUNIOR			EQUIPOS			MATERIALES			
		% partici- pación	Valor / hora	Valor parcial	% partici- pación	Valor / hora	Valor parcial	% partici- pación	Valor / hora	Valor parcial	Cantidad	Valor unitario	Valor parcial	
Elaboración del plan detallado de trabajo	1	1,0	\$ 20,00	\$ 160,00	0	\$ -	\$ -			0			0	\$ 160,00
Especificación de requerimientos	1	1,0	\$ 10,00	\$ 80,00		\$ -	\$ -			0			0	\$ 80,00
Reclutamiento	1	1,0	\$ 5,00	\$ 40,00	1	\$ 10,00	\$ 80,00			0			0	\$ 120,00
Investigación documental	2	1,0	\$ 10,00	\$ 160,00	0,5	\$ 10,00	\$ 80,00			0			0	\$ 240,00
Levantamiento de procesos	2	1,0	\$ 20,00	\$ 320,00		\$ -	\$ -			0			0	\$ 320,00
Elaboración de la Norma de procedimiento	2	1,0	\$ 20,00	\$ 320,00	0,5	\$ 10,00	\$ 80,00			0			0	\$ 400,00
Validación de la NP.	1	1,0	\$ 20,00	\$ 160,00	0,2	\$ 10,00	\$ 16,00			0			0	\$ 176,00
Aprobación de la NP.	1	1,0	\$ 20,00	\$ 160,00		\$ -	\$ -			0			0	\$ 160,00
Elaboración del plan de implantación de procesos	1	1,0	\$ 20,00	\$ 160,00	0,5	\$ 10,00	\$ 40,00			0			0	\$ 200,00
Capacitación	2	1,0	\$ 20,00	\$ 320,00	0,5	\$ 10,00	\$ 80,00			0			0	\$ 400,00
Implantación de procesos	5	1,0	\$ 20,00	\$ 800,00	0,5	\$ 10,00	\$ 200,00			0	5	\$ 55,62	\$ 278,10	\$ 1.278,10
Evaluación de la implantación	5	0,5	\$ 20,00	\$ 400,00	0,6	\$ 10,00	\$ 240,00			0			0	\$ 640,00
Auditoría 1 de precertificación	1	1,0	\$ 20,00	\$ 160,00	0	\$ -	\$ -			0			0	\$ 160,00
Acompañamiento en correcciones	2	0,5	\$ 20,00	\$ 160,00	1	\$ 10,00	\$ 160,00			0			0	\$ 320,00
Auditoría 2 de precertificación	1	1,0	\$ 20,00	\$ 160,00	0	\$ -	\$ -			0			0	\$ 160,00
Acompañamiento en correcciones	2	0,5	\$ 20,00	\$ 160,00	1	\$ 10,00	\$ 160,00			0			0	\$ 320,00
Certificación	1	1,0	\$ 20,00	\$ 160,00	0,5	\$ 10,00	\$ 40,00			0			0	\$ 200,00
COSTO POR RECURSO	31			\$ 3.880,00			\$ 1.176,00			0			\$ 278,10	\$ 5.334,10

2.2. Diseño

2.2.1. Esquema General de la Solución

Figura #20. Diseño general del modelo de comunicaciones seguras
Elaborado por: Danilo Ninabanda

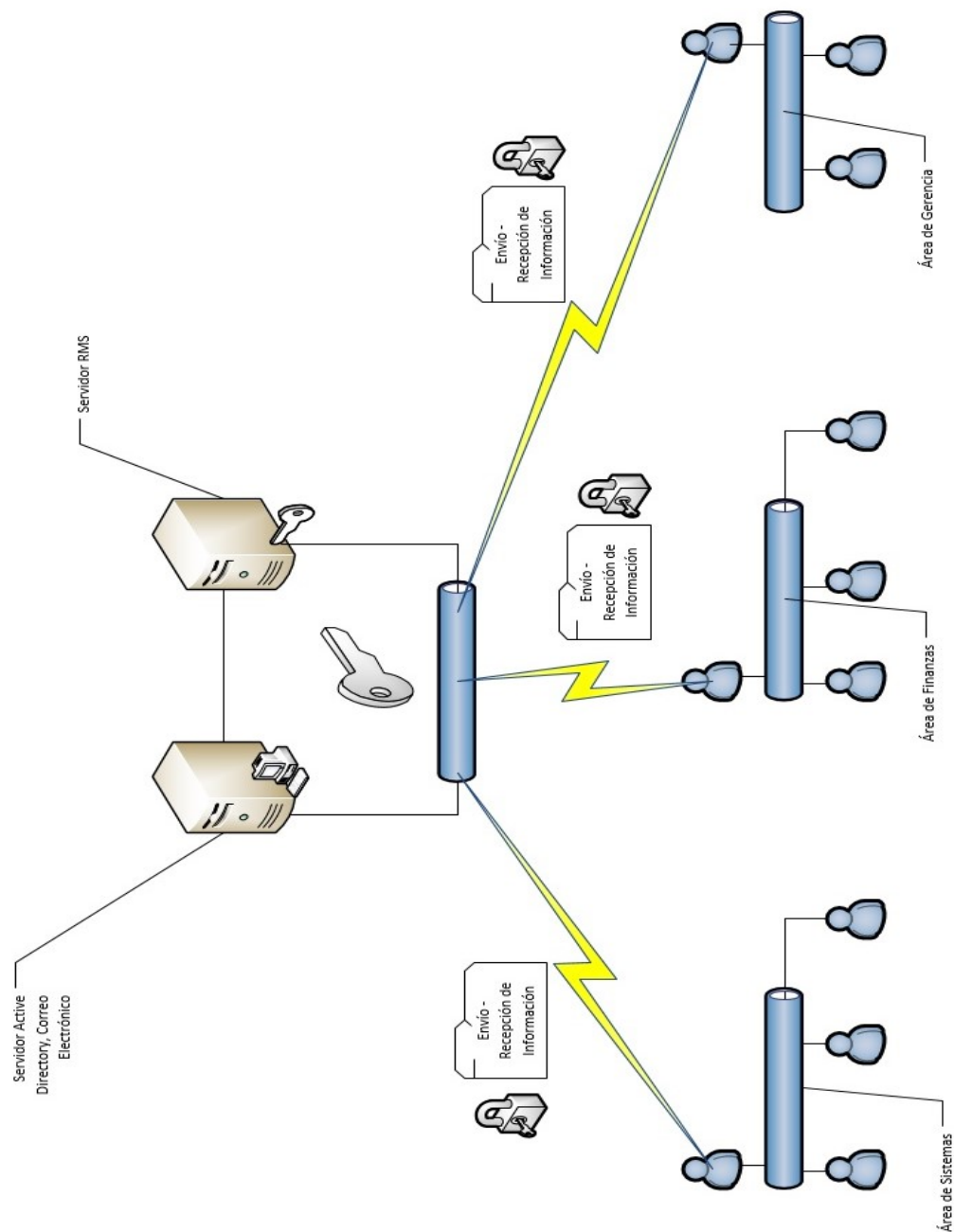


Figura #21. Diagrama de secuencias del modelo de comunicaciones seguras
Elaborado por: Danilo Ninabanda

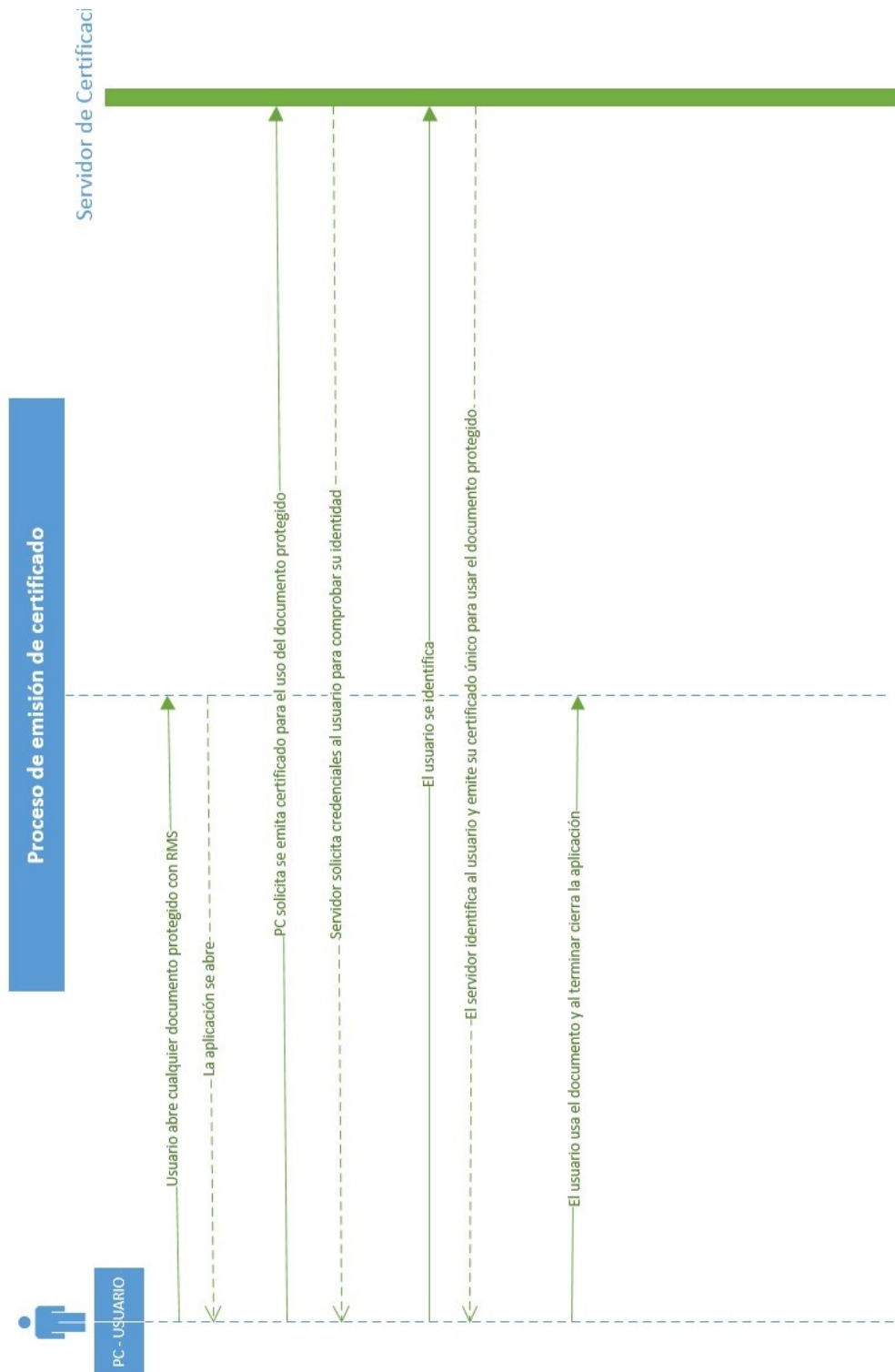


Figura #22. Diagrama de actividades del modelo de comunicaciones seguras
Elaborado por: Danilo Ninabanda

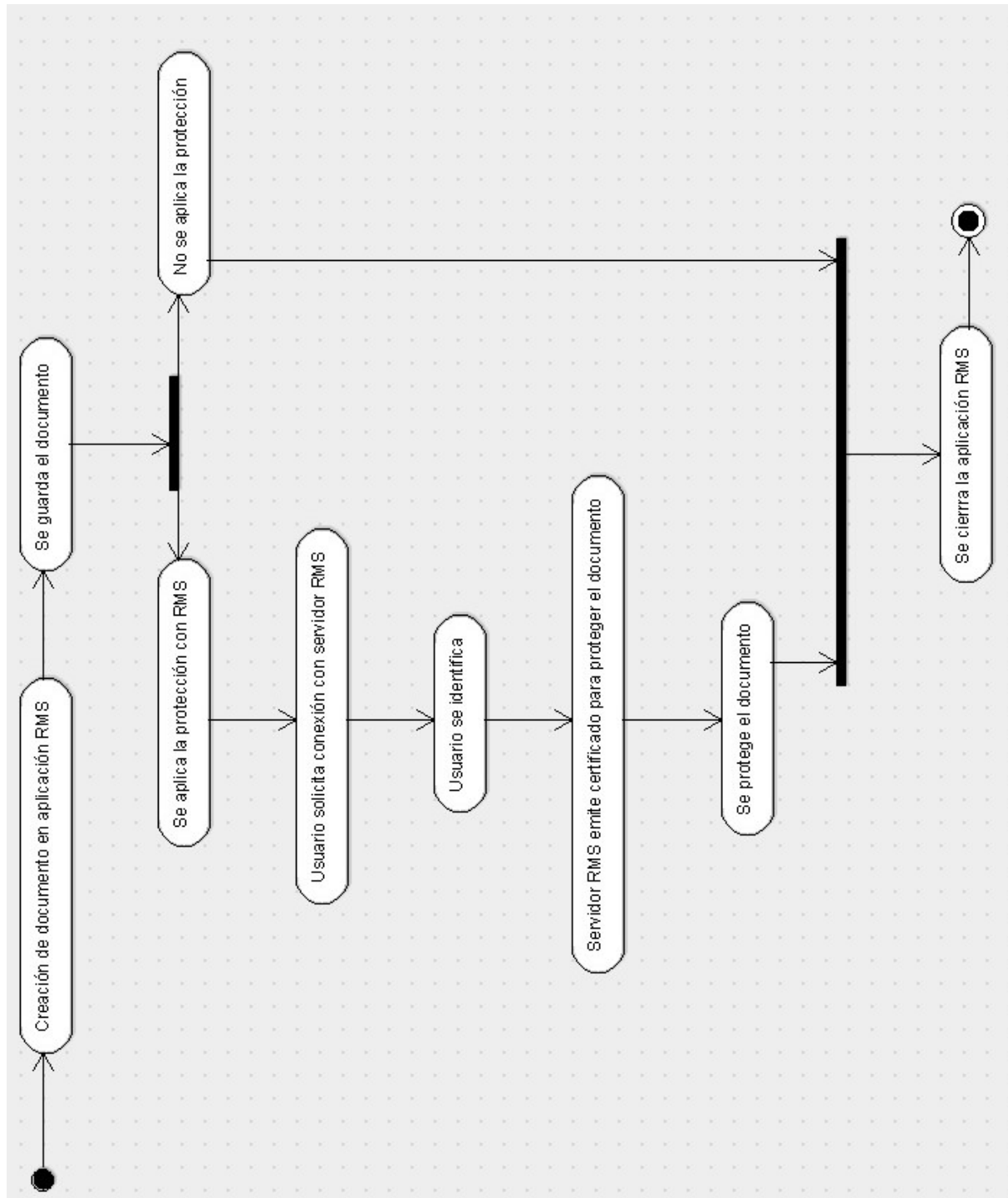
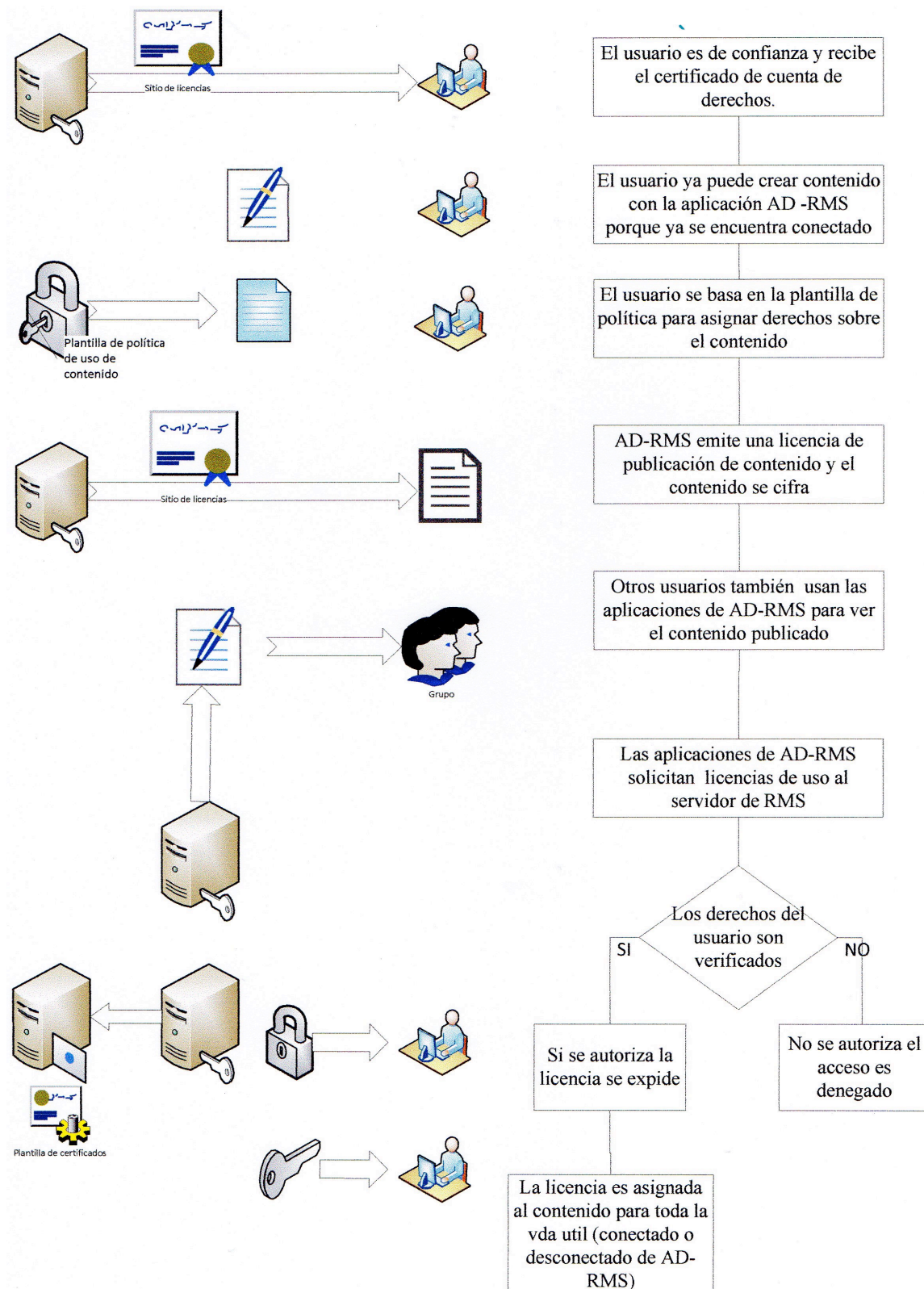


Figura #23. Creación de un documento protegido por RMS
Elaborado por: Danilo Ninabanda



CAPÍTULO III

RESULTADOS

3.1. Construcción

3.1.1. Generalidades

El modelo de comunicaciones seguras basado en el servicio RMS de Microsoft trabajará junto con otros servicios como son: Active Directory (AD DS), Sistema de nombre de Dominio (DNS), Internet Information Services (IIS), World Wide Web Publishing Services, Message Queuing; Microsoft Exchange 2010, Microsoft Office 2010.

Las empresas que decidan hacer uso del modelo de comunicaciones seguras de RMS detallado en este proyecto, contarán con que todo su contenido siempre estará cifrado. El tipo de cifrado que utiliza este servicio es de 1024 bits usando el algoritmo RSA para la clave, el método de protección de los documentos es de tipo AES de longitud variable entre 128 y 256 bits, además RMS usa el algoritmo de encriptación SHA-256 para los certificados digitales.

En este capítulo también se realizó la documentación de cada uno de los pasos para la implementación del sistema de comunicaciones seguras, desde el levantamiento de máquinas

virtuales, prerequisites, configuración servidor RMS, hasta la configuración del cliente RMS, brindando así a cualquier persona la posibilidad de una mejor comprensión y sobretodo incentivando el uso del servicio de RMS de Microsoft.

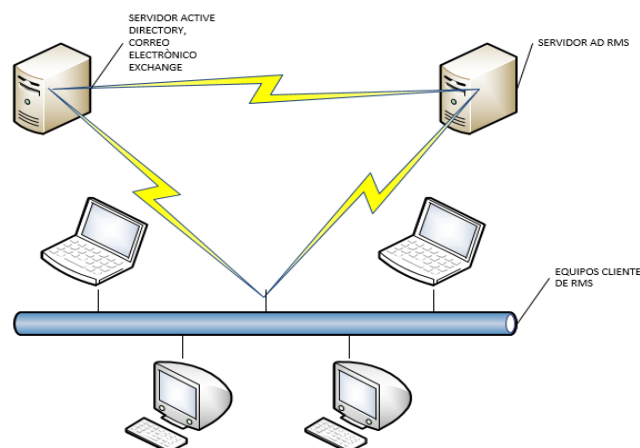
3.1.2. Descripción de Componentes

Para la demostración de la funcionalidad de RMS se realizó la simulación de implementación en una pequeña empresa la cual cuenta con:

- Servidor de Active Directory con servicios de DNS y Exchange instalados y funcionando, donde previo al uso de RMS se crearon usuarios y grupos de trabajo con sus respectivos roles.
- Servidor Rights Management Services, aquí se configurarán las políticas de seguridad para la documentación electrónica según las necesidades.
- Cliente con Windows 8.1 Pro y Office 2010, aquí se hará uso del servicio que brinda el servidor de RMS.

Figura #24. Modelo de Implementación.

Elaborado por: Danilo Ninabanda.



3.1.3. Levantamiento Máquinas Virtuales.

Como primer requisito para la demostración del modelo de comunicaciones seguras de RMS, es necesario realizar el levantamiento de un entorno de pruebas con máquinas virtuales usando el programa VMware edición Workstation versión 12, aquí se alojarán los sistemas operativos de servidor (Windows Server 2008 R2 Standard) y de cliente (Windows 8.1 Pro); tomando en cuenta que se debe tener preparado los DVD o imágenes en formato .ISO para su instalación.

La instalación de las máquinas virtuales con sus sistemas operativos se realizó de la siguiente manera:

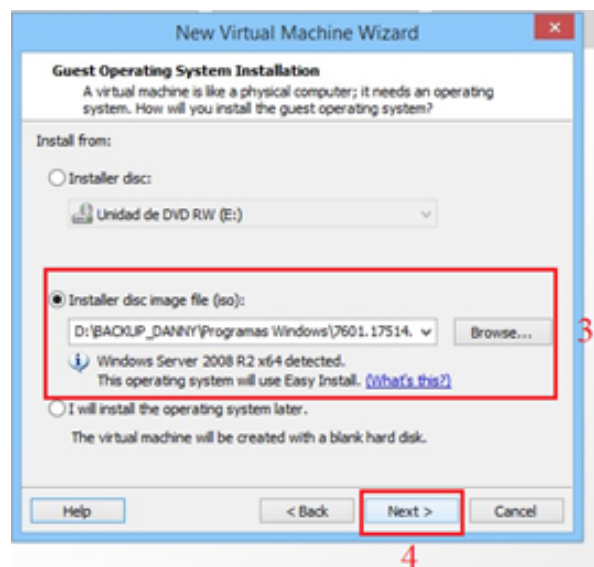
Con los instaladores de los sistemas operativos listos, se procede a abrir el programa VMware Workstation, en la pantalla principal del programa se despliegan opciones, la que se debe usar es la que indica la creación de una nueva máquina virtual (+) señalada como 1 en la figura 21, al escoger la opción mencionada el programa mostrará una pequeña ventana con el asistente de creación de nuevas máquinas virtuales, en el que se selecciona la instalación típica y a continuación se da clic en siguiente.

Figura #25. Asistente de instalación de nueva máquina virtual.
Elaborado por: Danilo Ninabanda.



A continuación el asistente preguntará si la instalación será por Disco (DVD) o imagen (.ISO), en este caso se usó imágenes, en el botón “Browser” se selecciona la ubicación donde se encuentra la imagen del instalador y el asistente lo detecta de inmediato; hecho esto continuamos dando clic en siguiente.

Figura #26. Medio de instalación.
Elaborado por: Danilo Ninabanda.



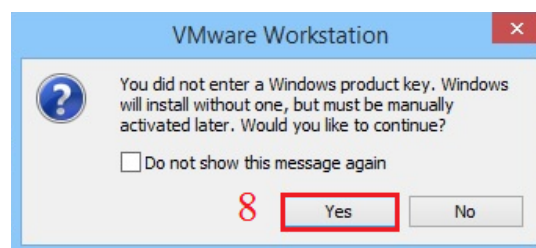
La siguiente ventana el asistente preguntará que versión del sistema operativo se quiere instalar, para esta demostración se eligió Windows Server 2008 R2 Standard, aquí también se debe escoger un nombre para el usuario del sistema operativo, no es obligatorio el uso de clave ya que más adelante haremos algunos cambios en los usuarios de todas las máquinas virtuales. En caso de tener el serial de activación del sistema operativo se lo puede ingresar también en esta ventana.

Figura #27. Usuario del sistema operativo
Elaborado por: Danilo Ninabanda



En caso de no ingresar el serial de activación del sistema operativo en el paso anterior, VMware indicará que lo podemos hacer manualmente después, por lo que damos clic en “SI” para continuar.

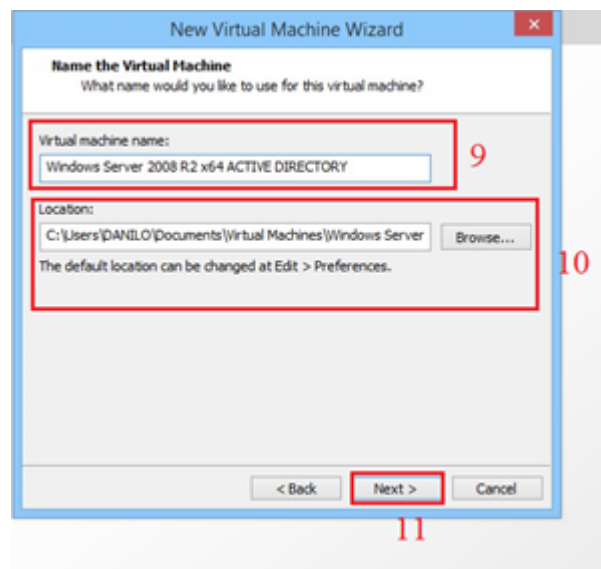
Figura #28. Alerta de serial de activación
Elaborado por: Danilo Ninabanda



El asistente de VMware indicará el nombre y la ubicación donde de la máquina virtual se creará, esto se puede cambiar según la necesidad de la empresa o persona que implementará el diseño de comunicaciones seguras. Para continuar con la creación de la máquina virtual, realice clic en siguiente.

Figura #29. Nombre y ubicación de la máquina virtual

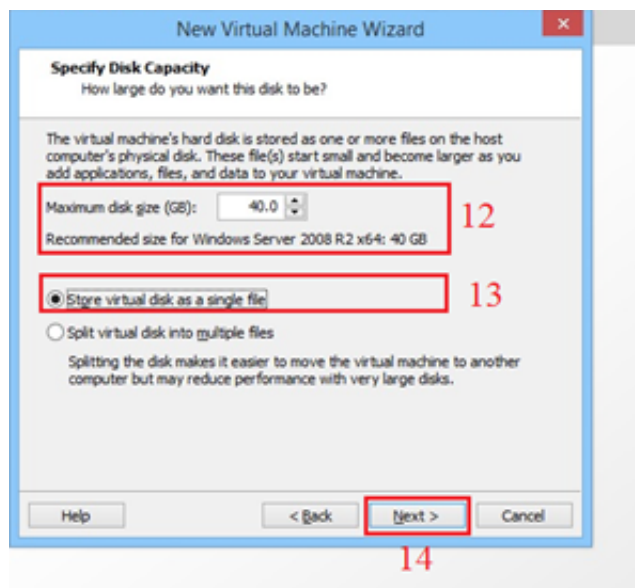
Elaborado por: Danilo Ninabanda



Antes de finalizar la creación de la máquina virtual se debe escoger el espacio de disco que usará la misma, para la demostración de este proyecto se dejó el espacio predeterminado, además se debe marcar la opción que indica que se creará un disco simple así como se indica a continuación.

Figura #30. Espacio de disco de máquina virtual

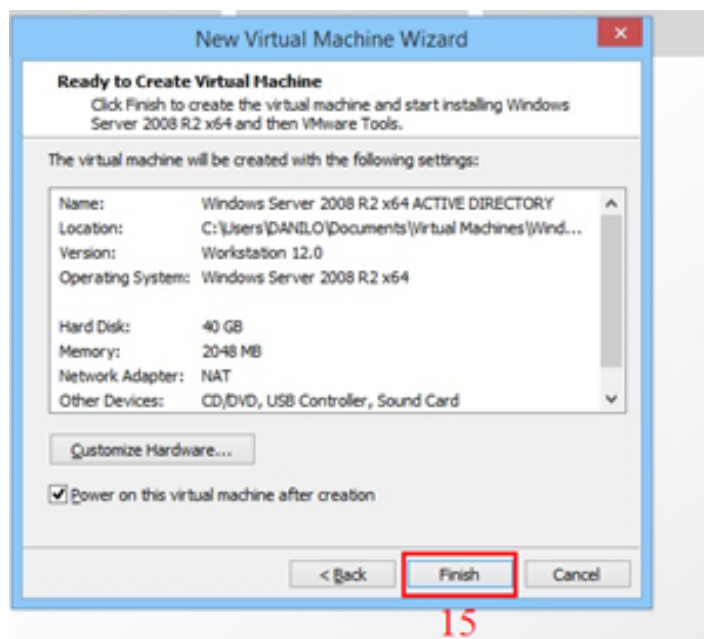
Elaborado por: Danilo Ninabanda



Antes de finalizar el asistente de creación de máquinas virtuales nos indica la configuración establecida, para dar paso a la creación de la máquina virtual realizar clic en finalizar.

Figura #31. Finalización del asistente de creación de máquinas virtuales

Elaborado por: Danilo Ninabanda.



Así el programa VMware empezará la creación e instalación del sistema operativo de manera automática, se debe esperar hasta que finalice y el sistema operativo arranque por sí solo.

Figura #32. Instalación de Windows Server 2008 R2

Elaborado por: Danilo Ninabanda.

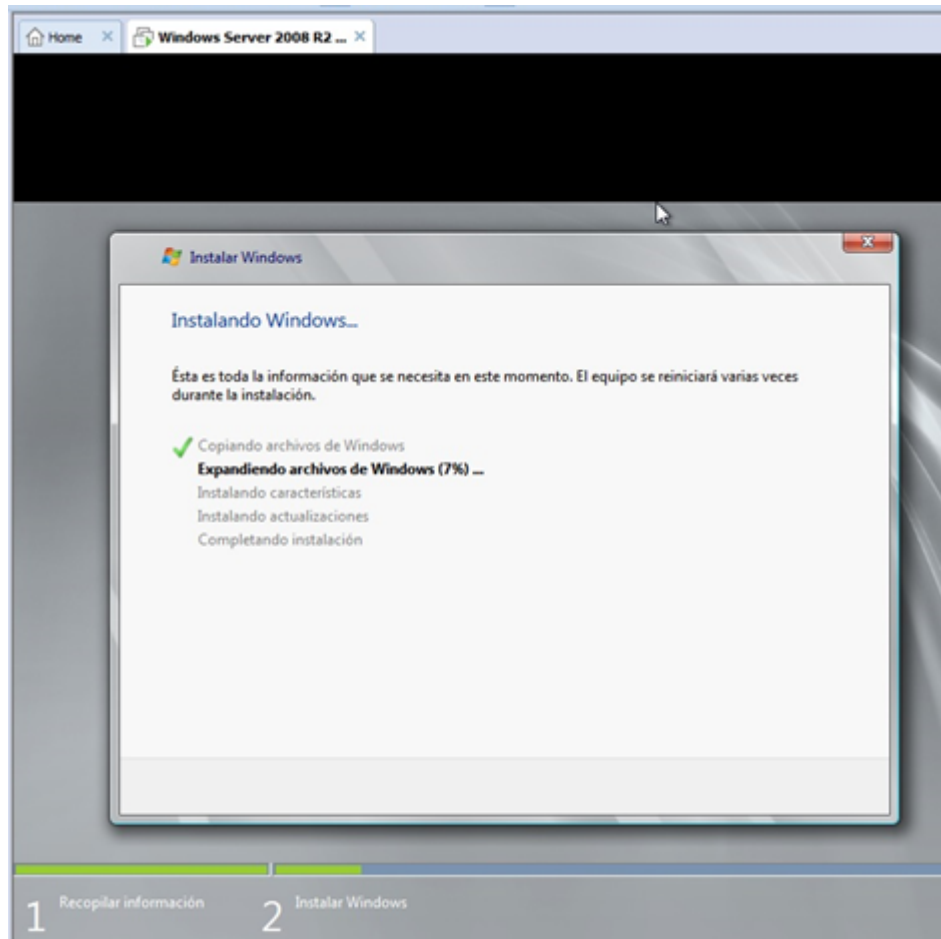
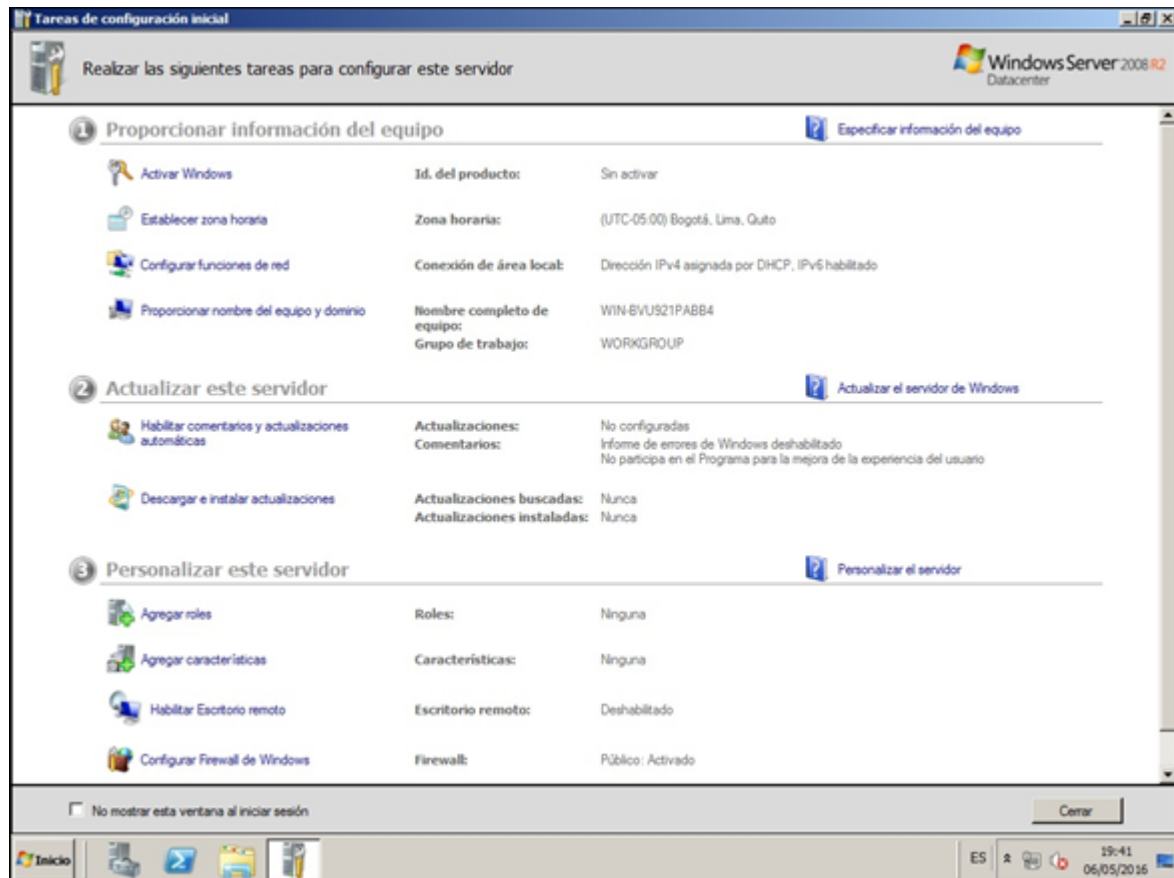


Figura #33. Windows Server 2008 R2 Standard instalado e iniciado
Elaborado por: Danilo Ninabanda.



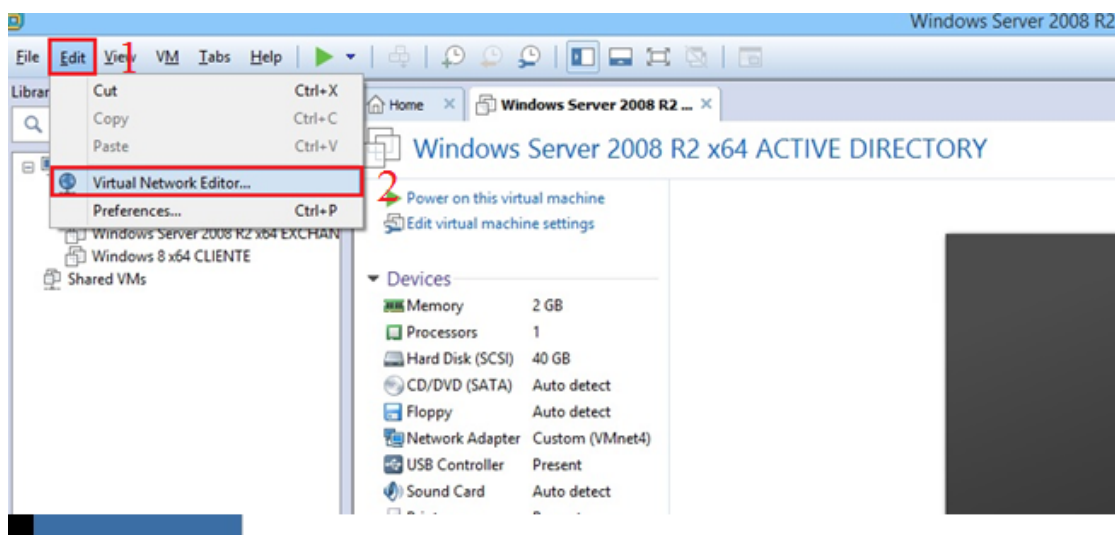
Con estos procedimientos se ha creado correctamente la primera máquina virtual, para continuar se debe repetir el proceso de creación de nueva máquina virtual para el sistema de servidor que albergará el servicio RMS y otra en donde estará alojado el sistema operativo de los clientes RMS (Windows 8.1 Pro).

3.1.4. Configuración red virtual en VMware Workstation 12.

Es necesario la configuración de la red virtual ya que debe haber una comunicación entre los servidores y máquinas clientes, para tener dicha conexión se realizaron los siguientes procedimientos.

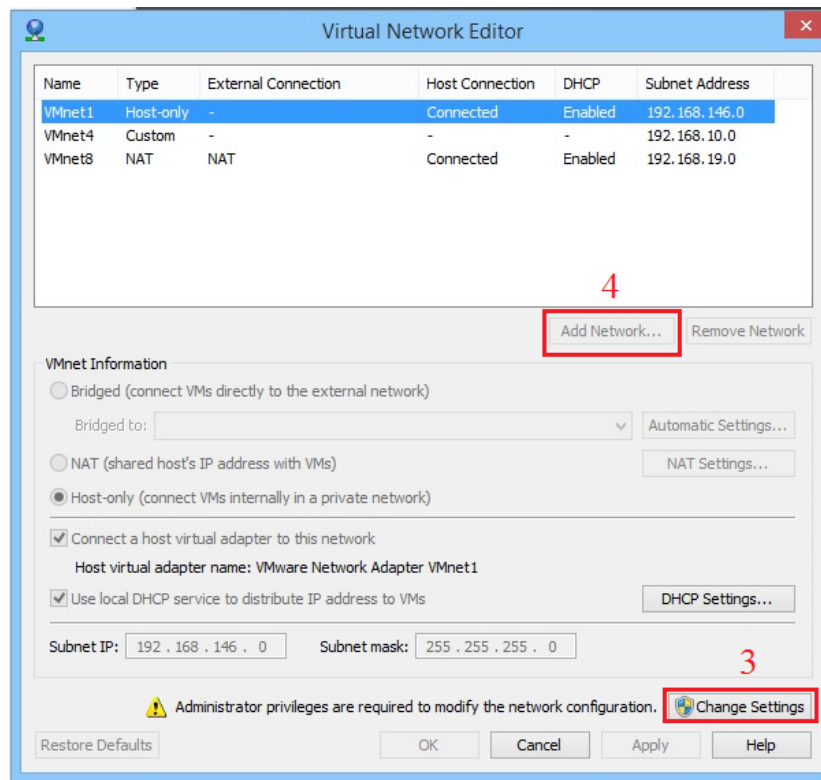
Con todas las máquinas virtuales apagadas, en la barra de menús del programa VMware Workstation se debe dar clic en la opción “Edit” o Editar, según el idioma en el que este configurado el programa. A continuación con un clic se debe abrir la opción “Virtual Network Editor” o Editor de redes virtuales.

Figura #34. Menú editar de VMware Workstation
Elaborado por: Danilo Ninabanda.



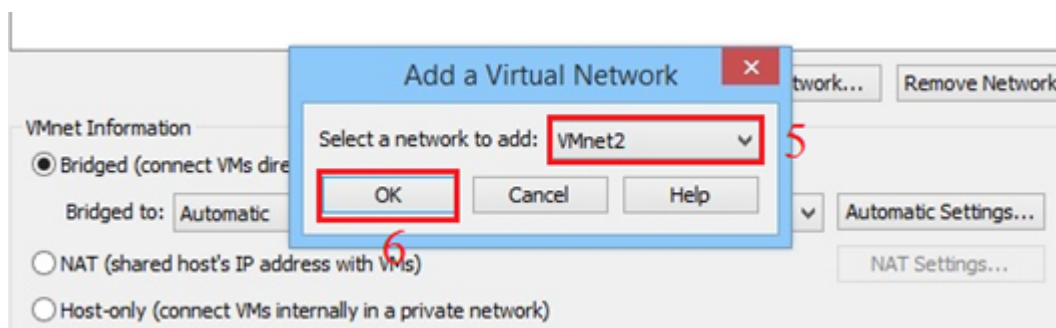
Una ventana se desplegará al realizar la acción anterior, en esta se visualizarán las redes que existen al momento en el programa VMware. Ahora con el fin que el programa y Windows autoricen la creación de la nueva red virtual dar clic en “Change Settings”, acto seguido saldrá una alerta la cual se debe aceptar, y para continuar dar clic en el botón “Add Network”.

Figura #35. Creación de la nueva red virtual
Elaborado por: Danilo Ninabanda.



Para agregar la nueva red virtual debe tomar en cuenta que la que se crea no exista en la lista de redes, para este caso se escogió la red “VMnet4”, y para continuar clic en “OK”.

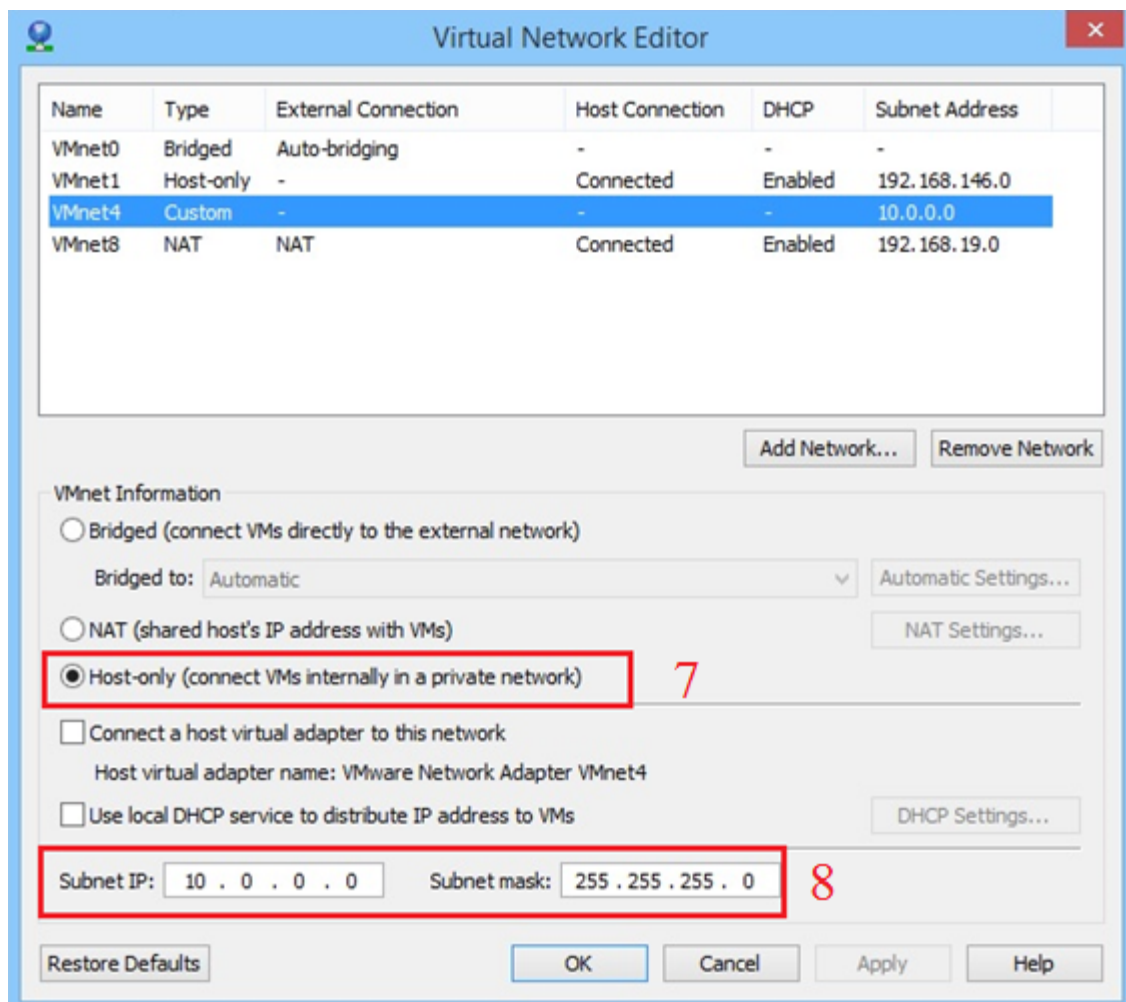
Figura #36. Nueva red virtual
Elaborado por: Danilo Ninabanda



Creada la nueva red virtual se configura para dejarla como una red privada “Host only”, además se debe escoger el rango de IP que la infraestructura cubrirá; con esto se termina la configuración de la red virtual.

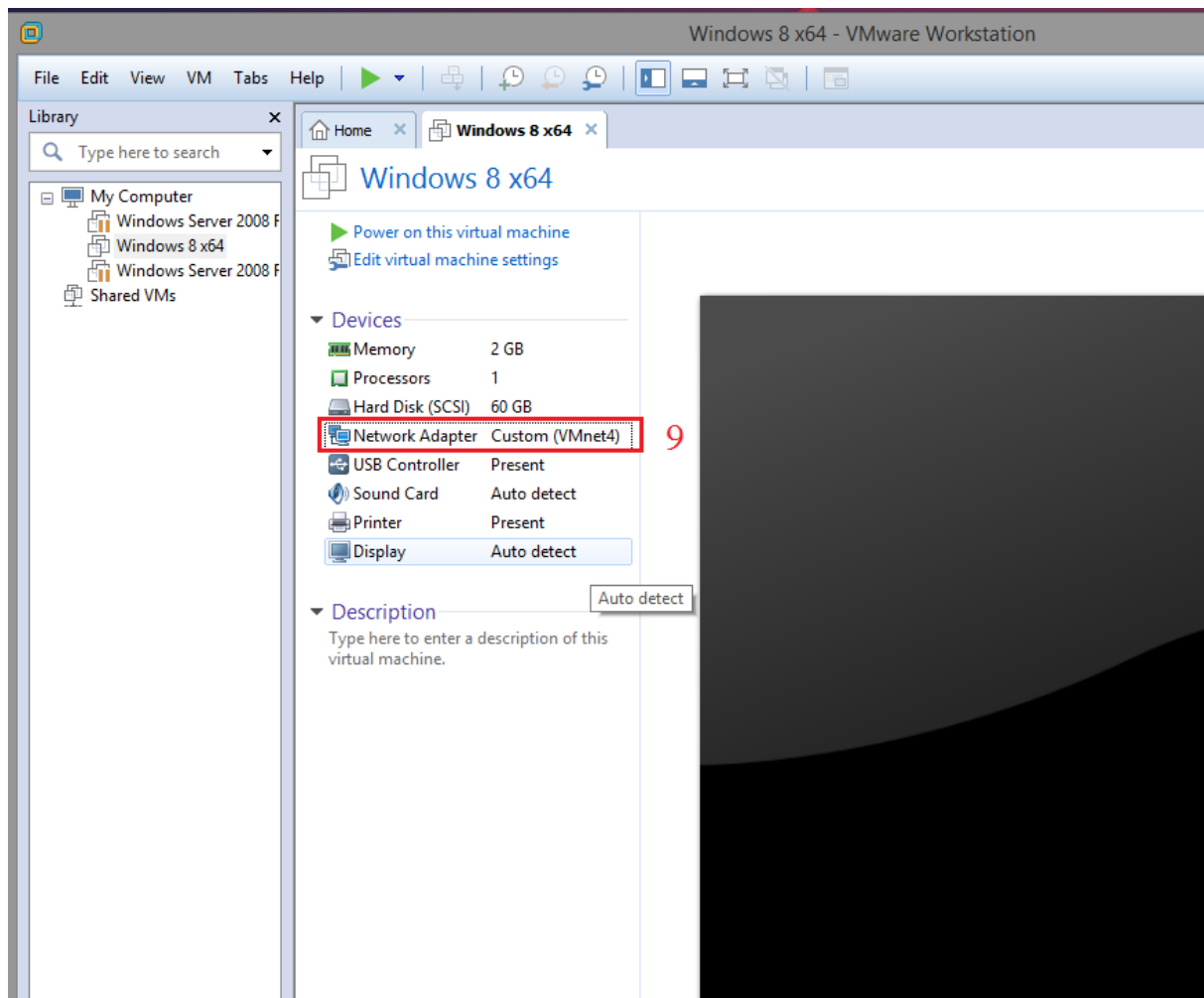
Figura #37. Configuración de red virtual

Elaborado por: Danilo Ninabanda



Para concluir se configura los adaptadores de red de cada una de las máquinas virtuales; se deberá seleccionar la máquina virtual y en “Network Adapter” dar clic para empezar hacer los cambios necesarios.

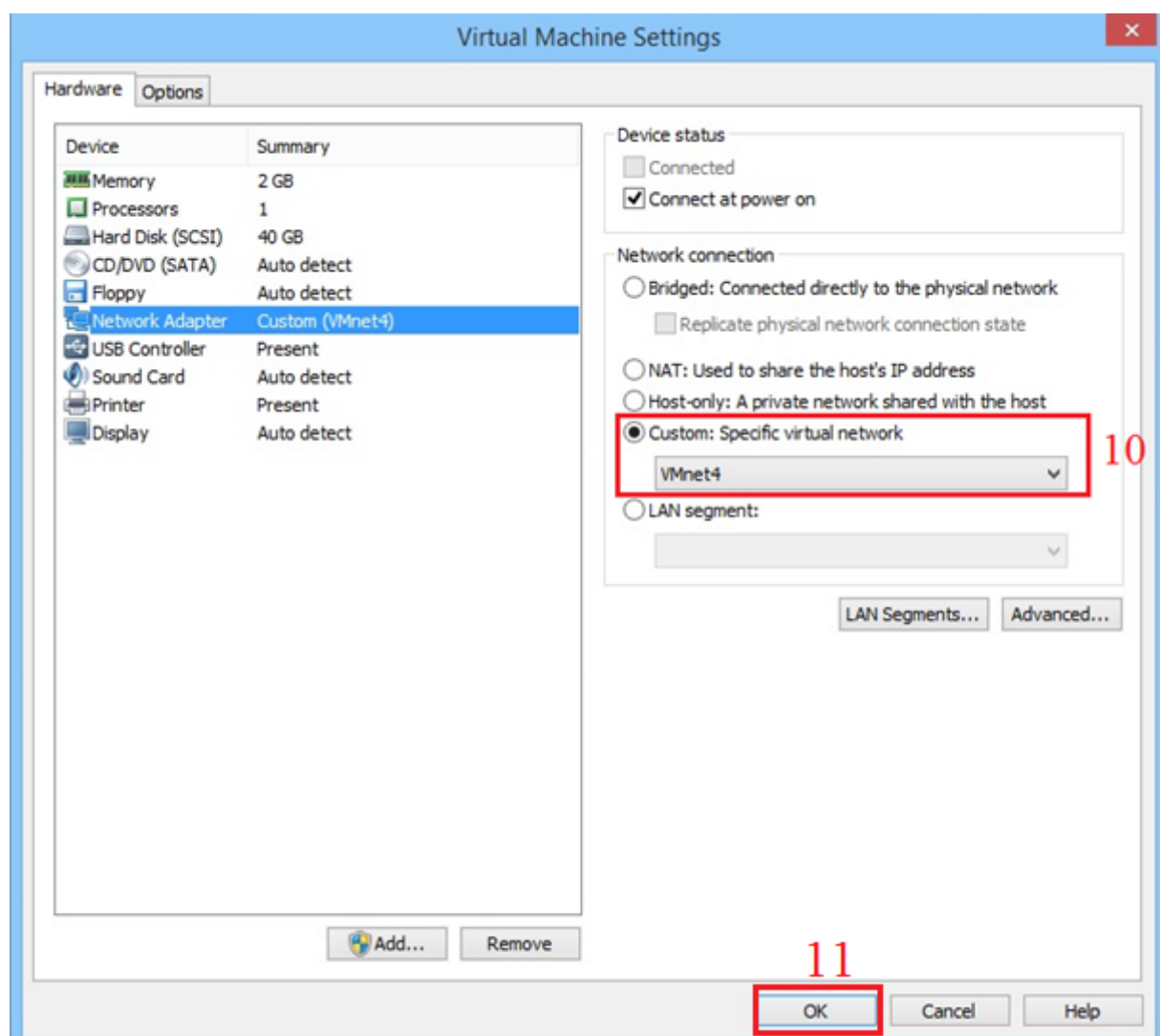
Figura #38. Selección adaptador de red de máquina virtual
Elaborado por: Danilo Ninabanda



Hecho lo anterior se desplegará otra pantalla en la que se debe escoger la opción personalizada, además se tendrá que elegir la que se creó anteriormente “VMnet4”, para finalizar se dará clic en el botón “OK”.

Este proceso se lo debe realizar en todas la máquinas virtuales que contemplen la infraestructura del modelo de comunicaciones seguras.

Figura #39. Selección de adaptador de red para máquinas virtuales
Elaborado por: Danilo Ninabanda.



Finalizado el proceso anterior, iniciar las máquinas virtuales y en configurar en cada una de ellas sus direcciones IP. En este proyecto el direccionamiento IP se encuentra en la siguiente tabla.

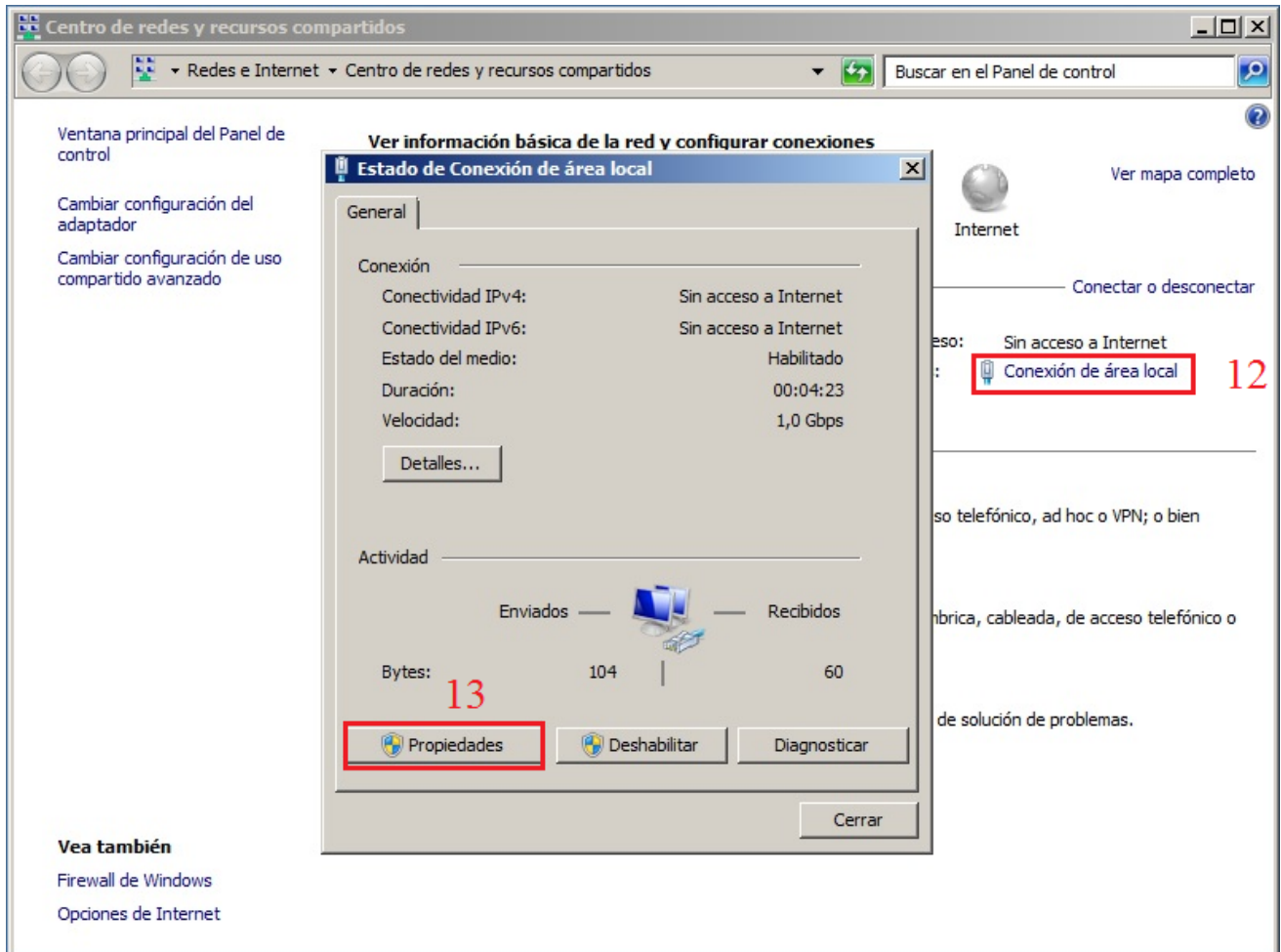
Tabla #9. Direccionamiento IP del proyecto
Elaborado por: Danilo Ninabanda.

Nombre de PC	Sistema Operativo	Configuración IP	Configuración DNS
SRV-AD	Windows Server 2008 R2	Dirección IP: 10.0.0.1 Máscara de subred: 255.255.255.0	Configurado con el rol de servidor DNS
SRV-RMS	Windows Server 2008 R2	Dirección IP: 10.0.0.2 Máscara de subred: 255.255.255.0	Preferido: 10.0.0.1
PC-USER	Windows 8.1 Pro	Dirección IP: 10.0.0.5 Máscara de subred: 255.255.255.0	Preferido: 10.0.0.1

La asignación de las IP en las máquinas virtuales, se debe realizar en cada una de ellas. Previamente es importante que al momento de realizar este proceso se desactive el Firewall de Windows, caso contrario no se tendrá comunicación entre los componentes de la infraestructura.

Abrir el “Centro de redes y recursos compartidos” que se encuentra en Panel de control > Redes e Internet, y abrir con un clic la Conexión de Área Local; en ese momento se desplegará una ventana en la cual se da clic en “Propiedades”.

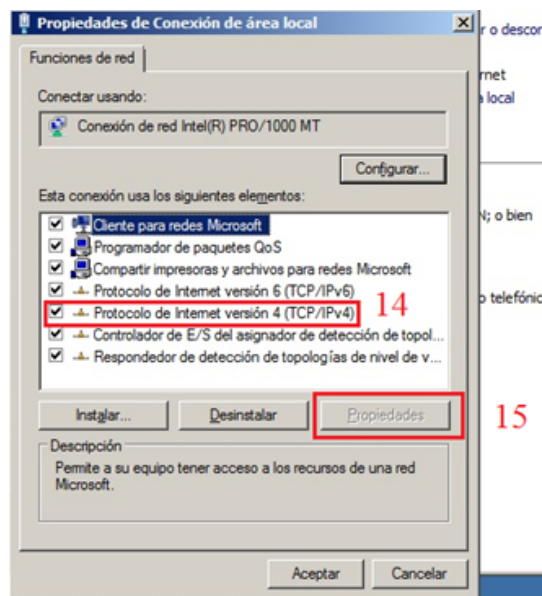
Figura #40. Estado de conexión de área local
Elaborado por: Danilo Ninabanda



Al realizar acción anterior se tendrá como resultado otra ventana en la que se escogerá la opción “Protocolo de Internet Versión 4(TCP/IP)”, activando la opción propiedades que se deberá abrir dando clic y así poder empezar con la configuración del direccionamiento IP.

Figura #41. Funciones de red

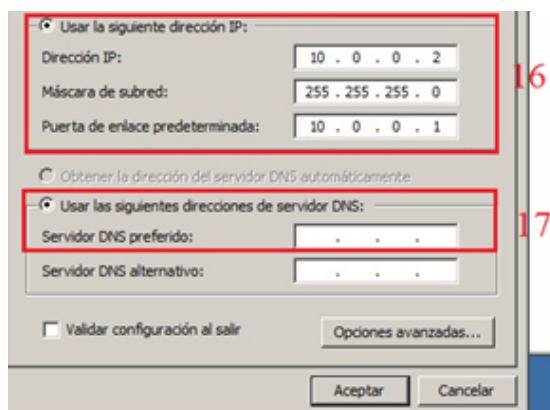
Elaborado por: Danilo Ninabanda.



En la nueva ventana que se abrió al realizar la acción anterior se debe llenar los campos: Dirección IP, Máscara de subred, Puerta de enlace predeterminada y Servidor DNS preferido, según el direccionamiento que se haya establecido para la estructura; en el caso de este proyecto se toma en cuenta el direccionamiento planteado en la Tabla 9.

Figura #42. Direccionamiento IP

Elaborado por: Danilo Ninabanda

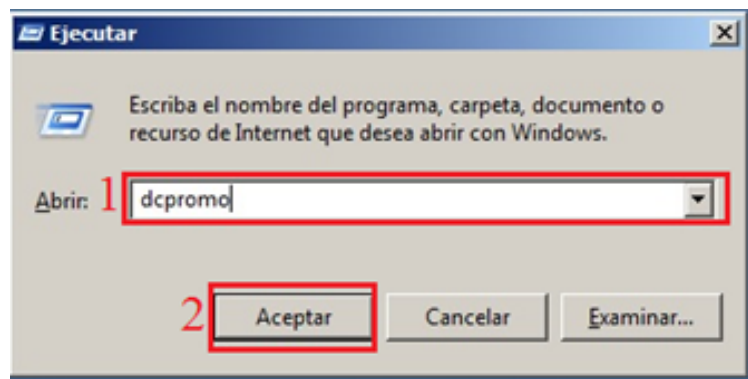


La configuración se guardará dando clic en “Aceptar”. Este procedimiento se debe completar en todas las máquinas que formen parte de la red, del servicio de Active Directory así como también en todas las máquinas clientes tomadas en cuenta para que usen RMS.

3.1.5. Instalación Active Directory.

En la máquina virtual destinada para la configuración de Active Directory, iniciamos el sistema operativo como Administrador. Una vez que el sistema carga completamente, se procede a ingresar por teclado la combinación de teclas “Windows + R”, esto abrirá la ventana Ejecutar y en el campo de texto ingresar “dcpromo” y esperar que cargue el asistente de configuración de Active Directory.

Figura #43. Asistente de configuración de Active Directory
Elaborado por: Danilo Ninabanda.



Cuando el asistente haya iniciado se necesita verificar que la casilla de instalación en modo avanzado este desactivada de ese modo se podrá avanzar con el botón siguiente.

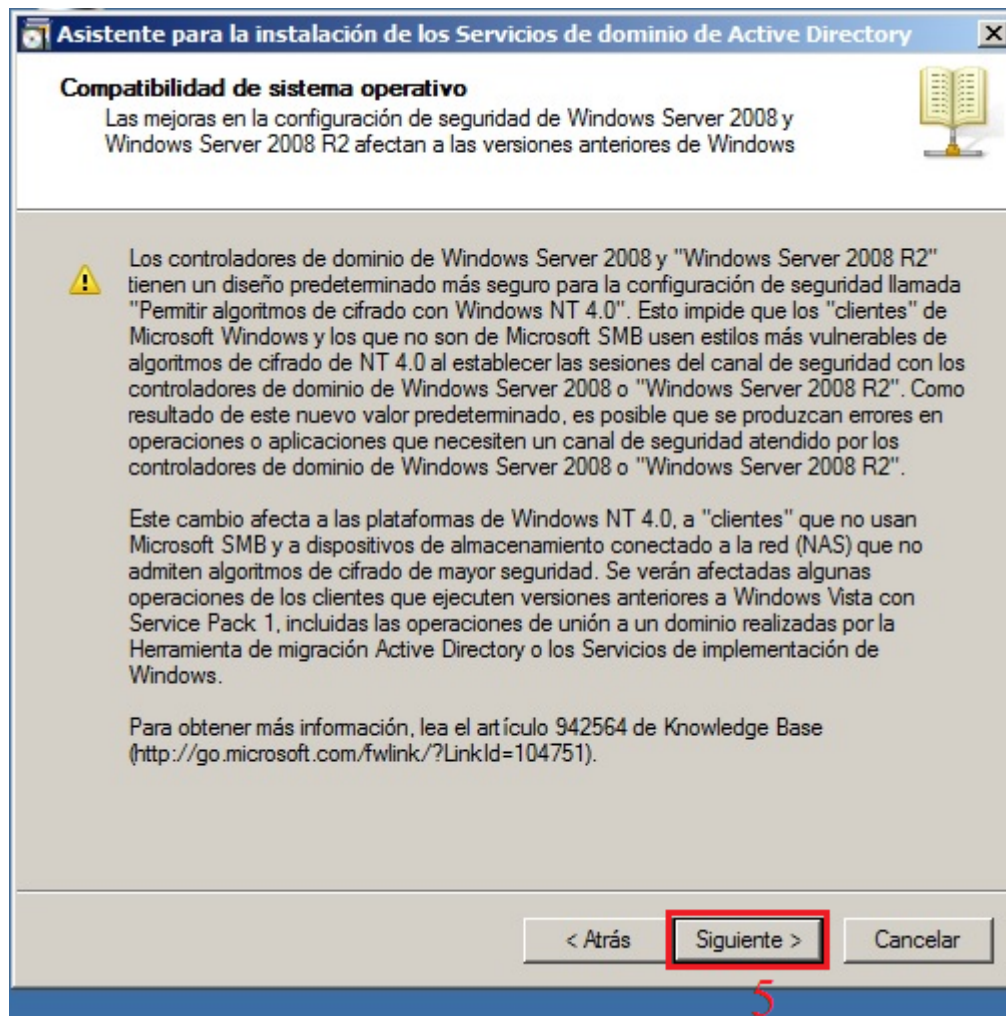
Figura #44. Inicio del asistente de instalación de Active Directory

Elaborado por: Danilo Ninabanda



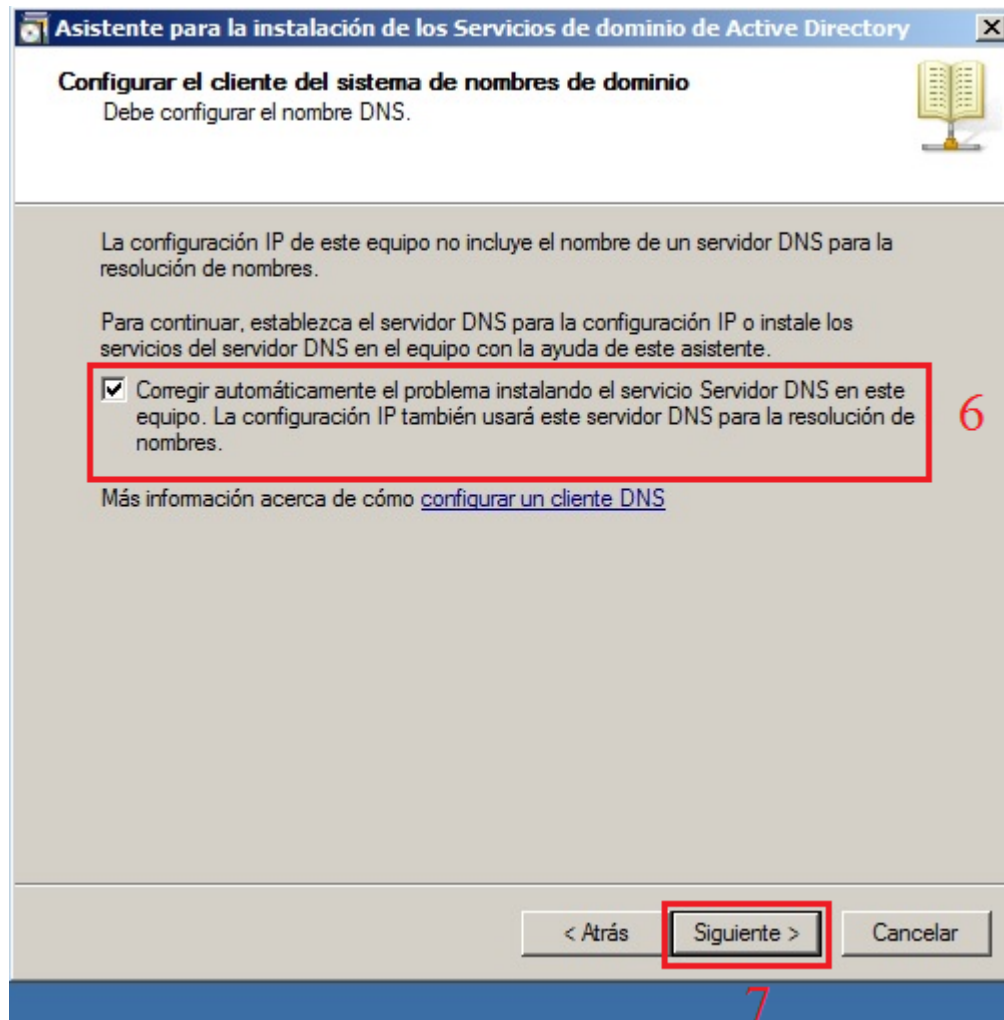
A continuación el asistente indicará si el sistema operativo de servidor es compatible con Active Directory. Comprendida la alerta que indica el asistente continuamos con el botón Siguiente.

Figura #45. Compatibilidad de sistema operativo
Elaborado por: Danilo Ninabanda



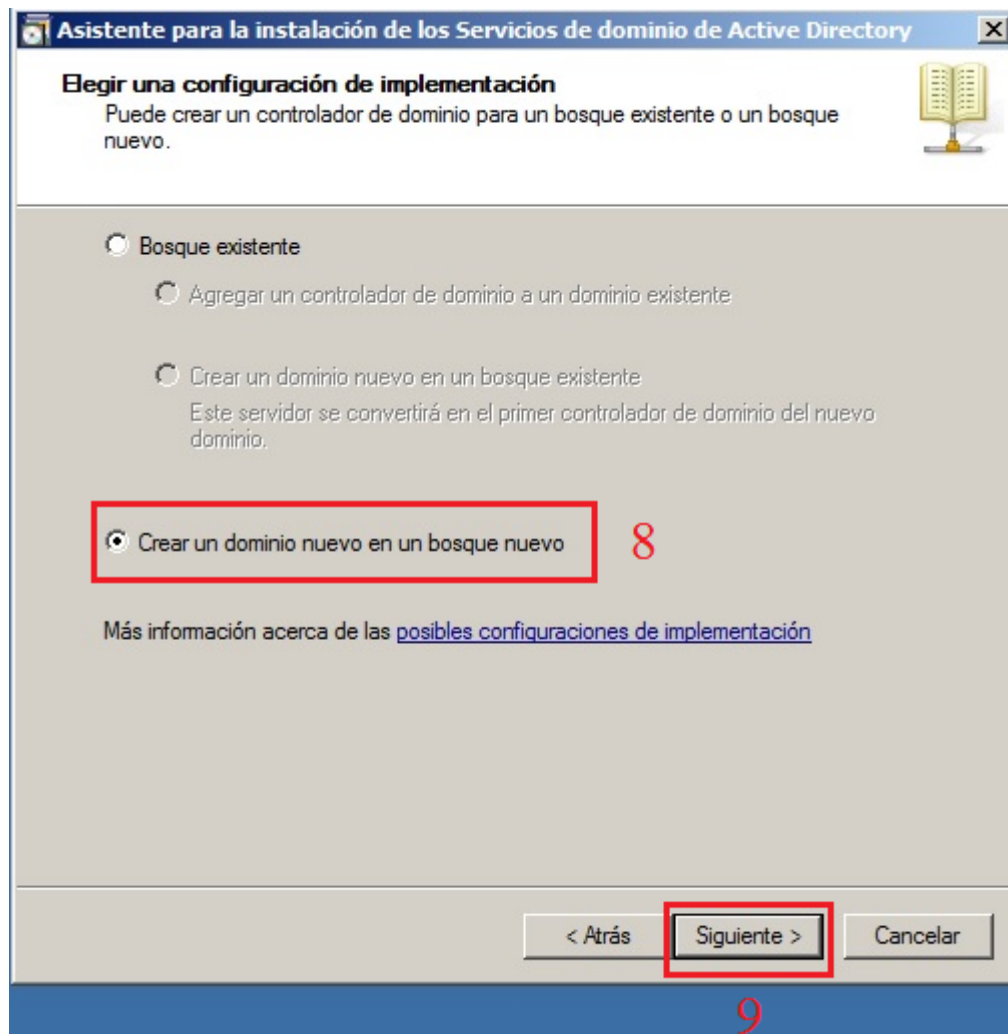
Como este servidor será el que resuelva los servicios de DNS, se debe marcar la casilla de instalación del servicio. Corregido esto, avanzar con el asistente con el botón Siguiente.

Figura #46. Configuración de DNS
Elaborado por: Danilo Ninabanda



En esta parte el asistente de instalación de Active Directory nos pide que se escoja el tipo de configuración del dominio, a la que seleccionamos la creación de un dominio nuevo en un bosque nuevo.

Figura #47. Configuración de implementación
Elaborado por: Danilo Ninabanda.



En la siguiente pantalla del asistente se debe escoger el nombre del dominio, el nombre debe incluir el apartado “.com”. Cuando el nombre ha sido escogido podremos avanzar con el botón “siguiente”.

Figura #48. Nombre al dominio raíz del bosque

Elaborado por: Danilo Ninabanda.

Asistente para la instalación de los Servicios de dominio de Active Directory

Asigne un nombre al dominio raíz del bosque

El primer dominio del bosque es el dominio raíz del bosque. Su nombre también es el nombre del bosque.

Escriba el nombre de dominio completo (FQDN) del nuevo dominio raíz del bosque.

FQDN del dominio raíz del bosque:

empresa.com

Ejemplo: corp.contoso.com

< Atrás **Siguiete >** Cancelar

A continuación se establecerá el nivel funcional del bosque y el nivel funcional del dominio, para asegurar la compatibilidad con todos los sistemas operativos de servidor se elegirá Windows Server 2003.

Figura #49. Nivel funcional del bosque

Elaborado por: Danilo Ninabanda

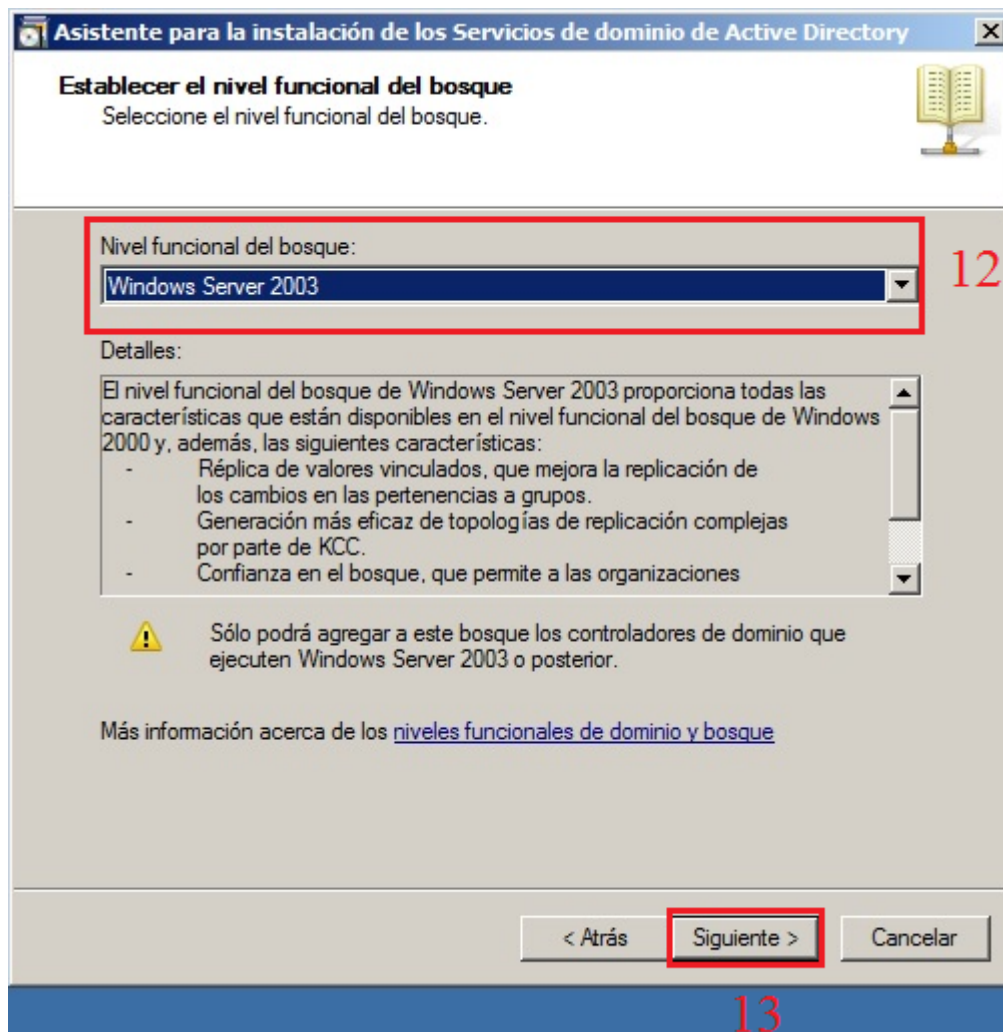
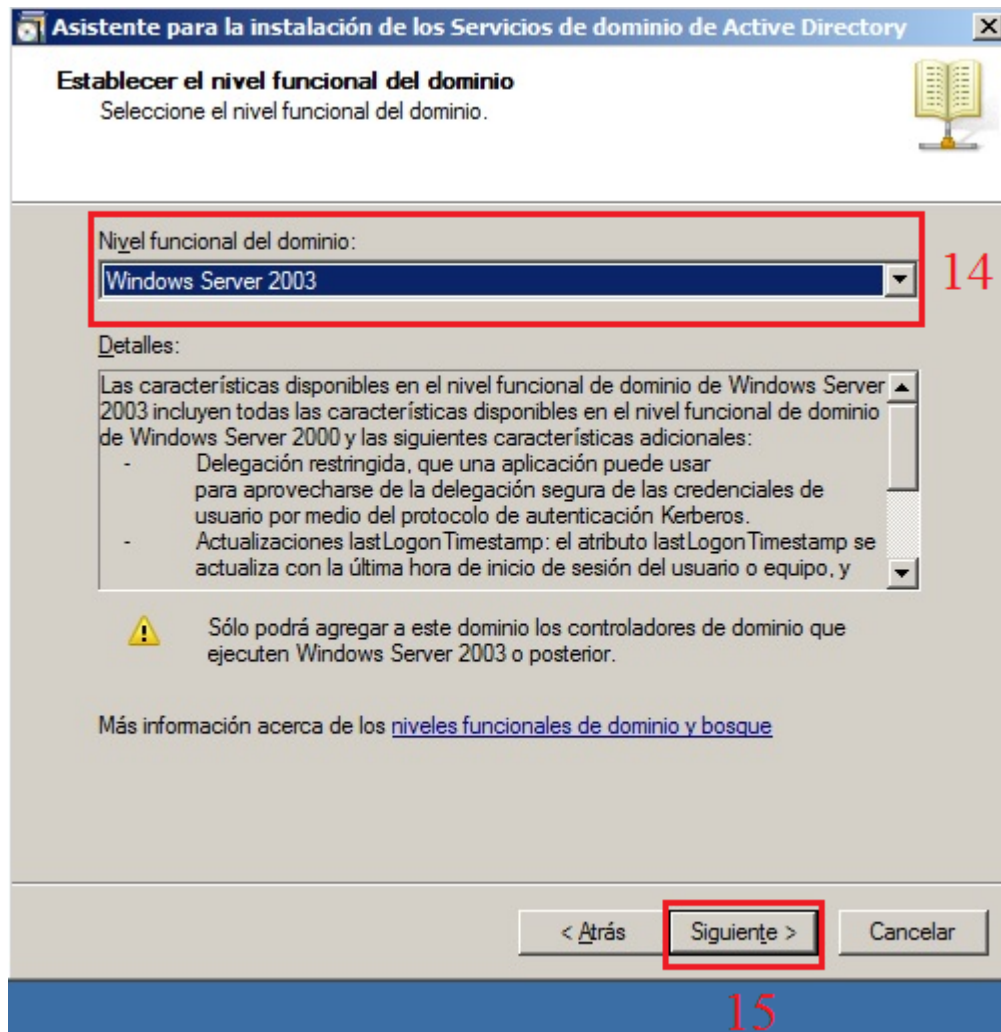


Figura #50. Nivel funcional del dominio

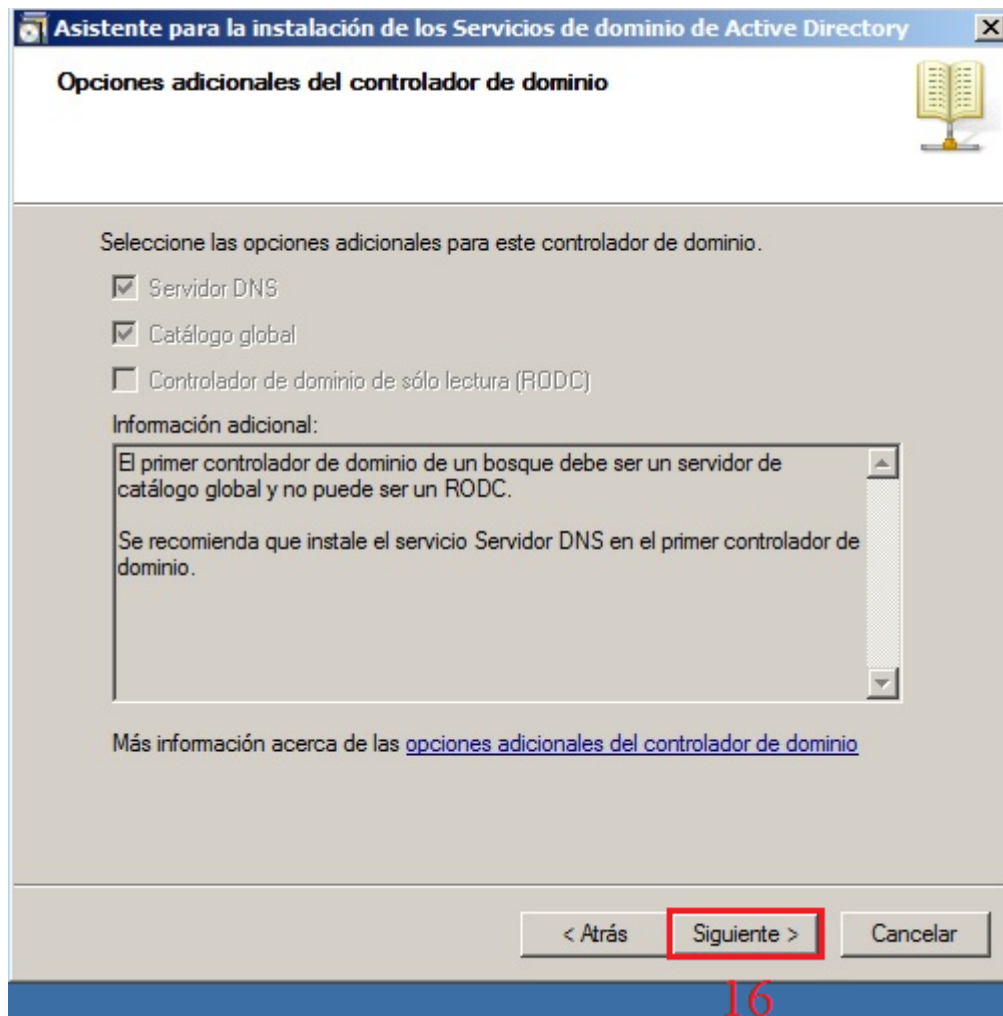
Elaborado por: Danilo Ninabanda



Luego de configurar el nivel funcional el asistente mostrará algunas opciones adicionales que se instalarán, sin realizar ningún cambio se debe avanzar con el botón “Siguiente”.

Figura #51. Opciones adicionales del controlador de dominio

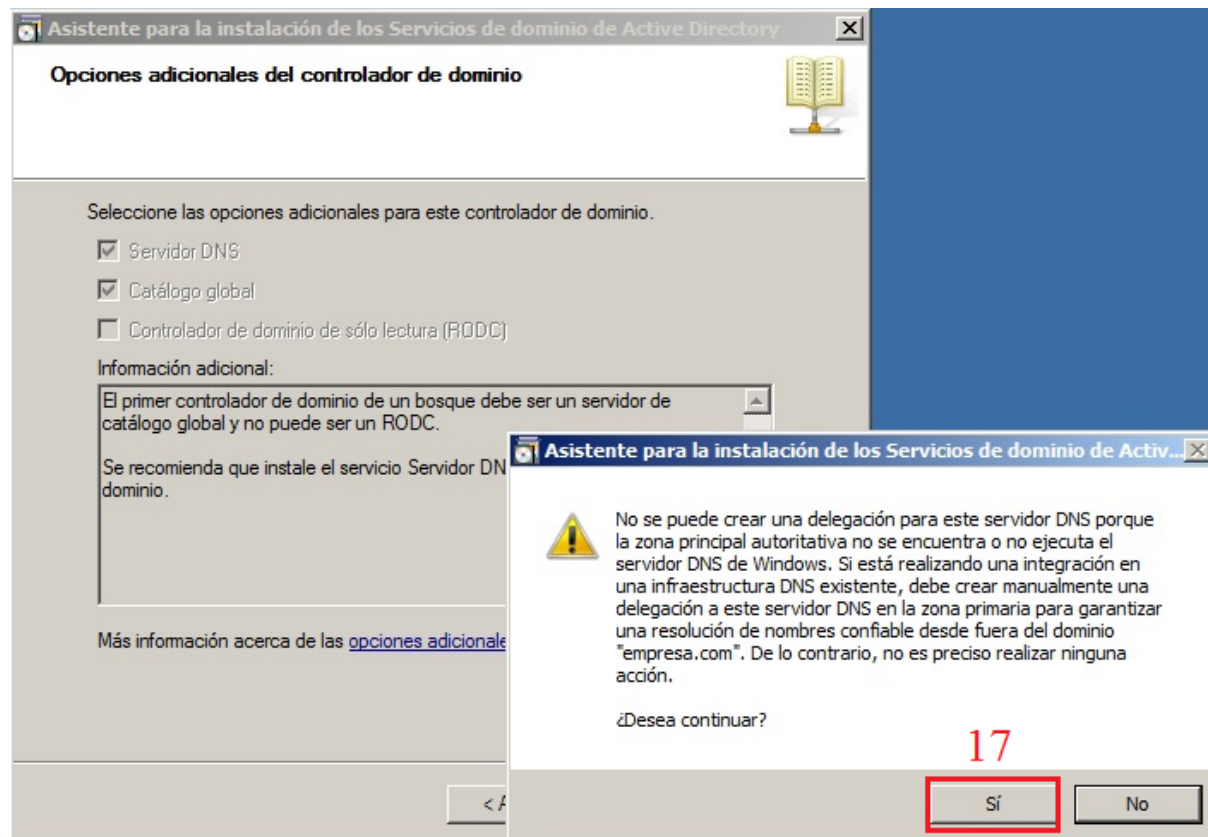
Elaborado por: Danilo Ninabanda



En esta parte de la instalación de active directory, el asistente muestra una alerta sobre la configuración del servicio DNS y para continuar se debe dar clic en el botón “SI”.

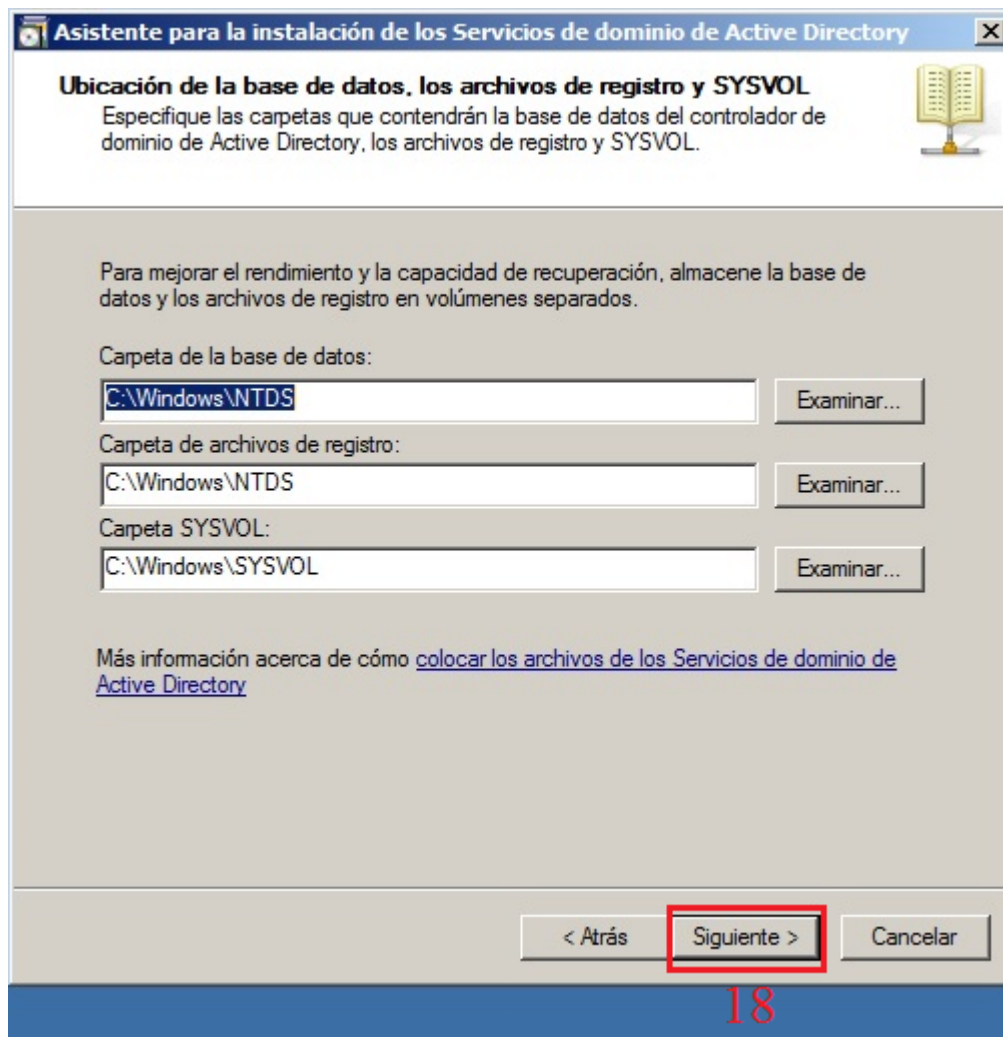
Figura #52. Alerta sobre servicio DNS

Elaborado por: Danilo Ninabanda.



En este punto se debe mantener la configuración predeterminada que nos da el asistente, y continuar con el botón “Siguiente”.

Figura #53. Ubicación de la base de datos, los archivos de registro y SYSVOL
Elaborado por: Danilo Ninabanda.



Active Directory maneja una contraseña para restablecer los servicios de directorio, en esta parte el asistente permite configurar una contraseña para la cuenta de administrador.

Figura #54. Contraseña de administrador para restauración de servicios de directorio
Elaborado por: Danilo Ninabanda.

Asistente para la instalación de los Servicios de dominio de Active Directory

Contraseña de admin. del modo de restauración de servicios de directorio

La cuenta de Administrador del modo de restauración de servicios de directorio es diferente de la cuenta de Administrador del dominio.

Asigne una contraseña para la cuenta de administrador que se usará cuando el controlador de dominio se inicie en el modo de restauración de servicios de directorio. Se recomienda elegir una contraseña segura.

Contraseña:

Confirmar contraseña:

Más información acerca de la [contraseña del modo de restauración de servicios de directorio](#)

< Atrás **Siguiete >** Cancelar

19

20

Para finalizar el asistente mostrará en un resumen las configuraciones elegidas anteriormente, se revisa cada punto y si todo está bien se debe continuar con el botón “Siguiente” y la instalación comenzará.

Figura #55. Resumen

Elaborado por: Danilo Ninabanda

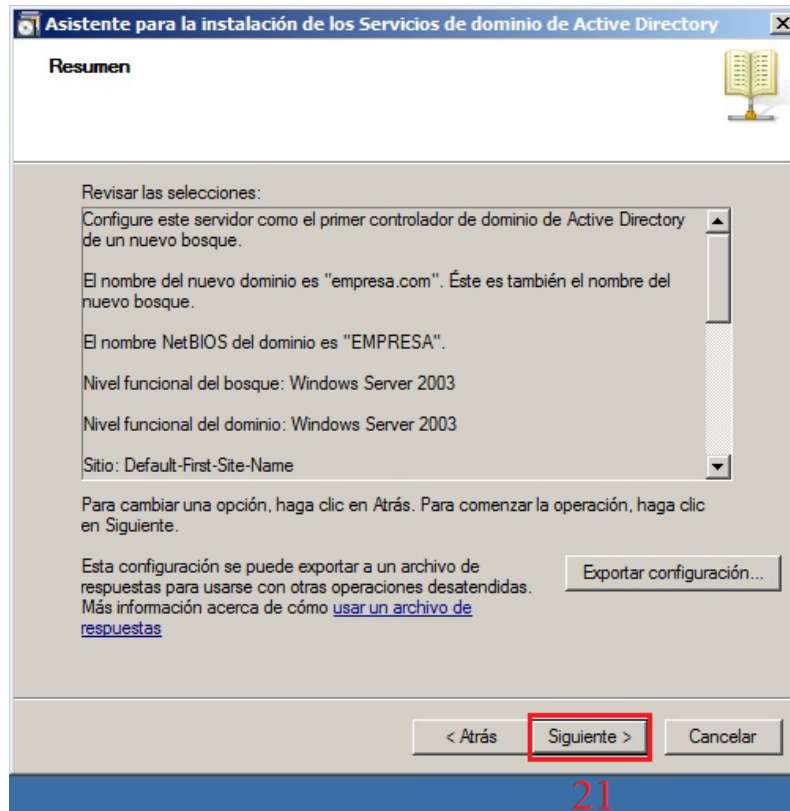
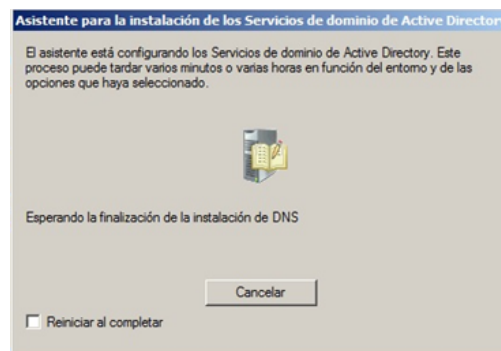


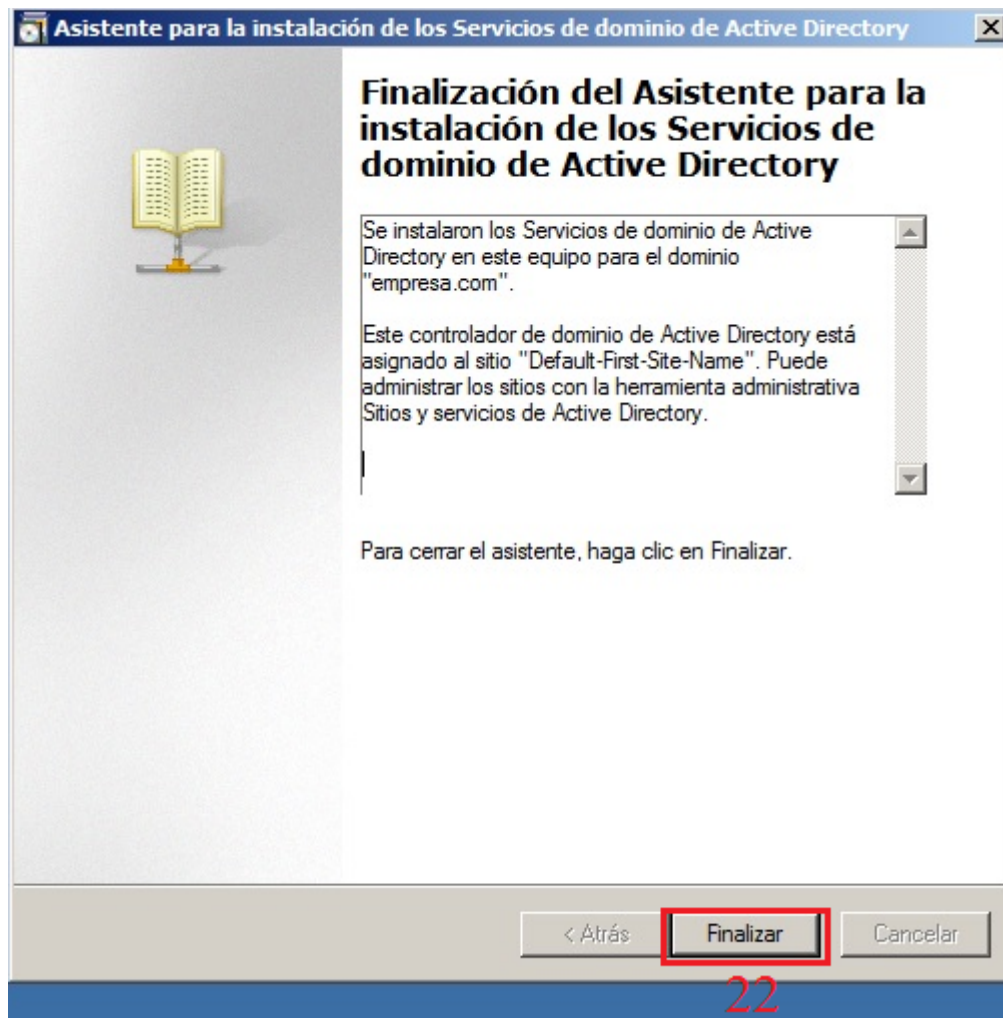
Figura #56. Proceso de instalación de Active Directory

Elaborado por: Danilo Ninabanda



El asistente concluirá la instalación y a continuación mostrará un resultado parecido al de la imagen, sino existe ningún problema no se obtendrá errores en esta parte y la instalación será todo un éxito.

Figura #57. Finalización del asistente de instalación de Active Directory
Elaborado por: Danilo Ninabanda.



3.1.6. Instalación Microsoft Exchange.

Para empezar con la instalación de Microsoft Exchange 2010 se deben realizar ciertas instalaciones de pre – requisitos que son necesarios para el correcto funcionamiento del servidor de correo electrónico Exchange. Empezando con la descarga y posterior instalación de 2007 Office System Converter: Microsoft Filter Pack, el cual se puede encontrar en el siguiente link:

<https://www.microsoft.com/es-es/download/details.aspx?id=20109>

La instalación de este complemento se la realizará en el servidor donde se configuró el servicio de Active Directory. El asistente de instalación guiará todo el proceso.

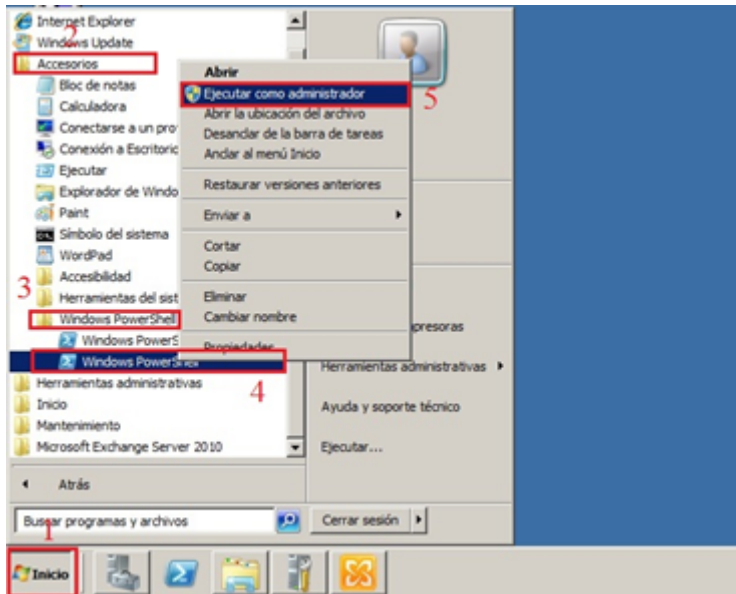
Figura #58. Asistente de instalación de Filter Pack 1.0

Elaborado por: Danilo Ninabanda.



Concluida la instalación de Filter Pack, abrir “Windows Power Shell”, esta herramienta se la encuentra en Inicio > Accesorios > Windows PowerShell. Abrirla como Administrador para poder realizar la instalación de algunos complementos más.

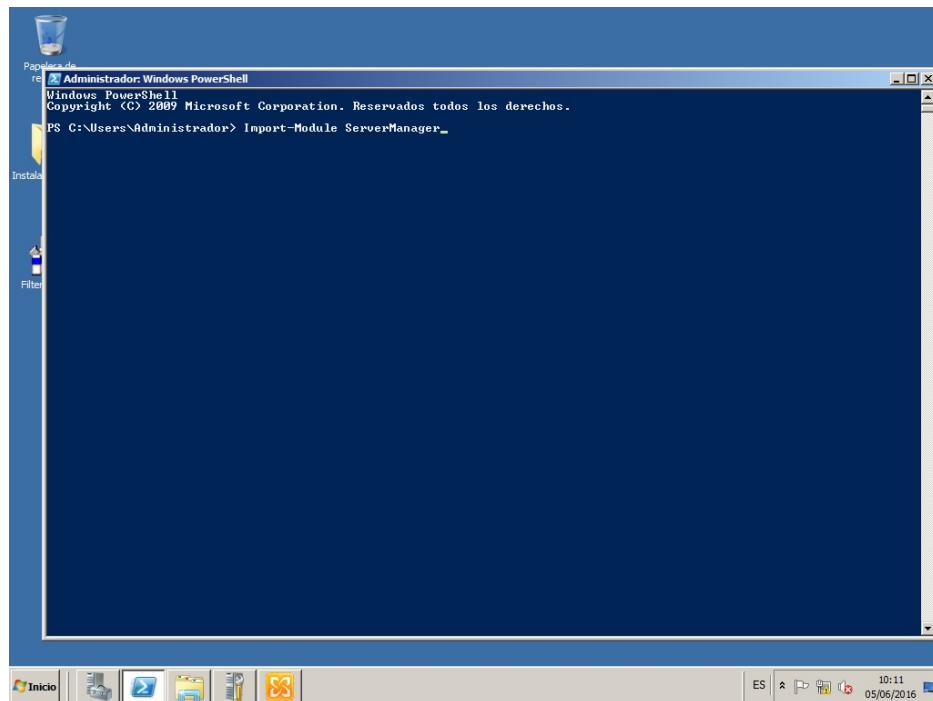
Figura #59. Windows PowerShell
Elaborado por: Danilo Ninabanda.



En la interfaz de PowerShell se debe ejecutar las 2 líneas de comandos que se encuentran a continuación, estas instalar algunos complementos necesarios para el funcionamiento de Exchange, al finalizar esta instalación el servidor se reiniciará automáticamente, se debe esperar hasta que este proceso termine y el servidor inicie nuevamente.

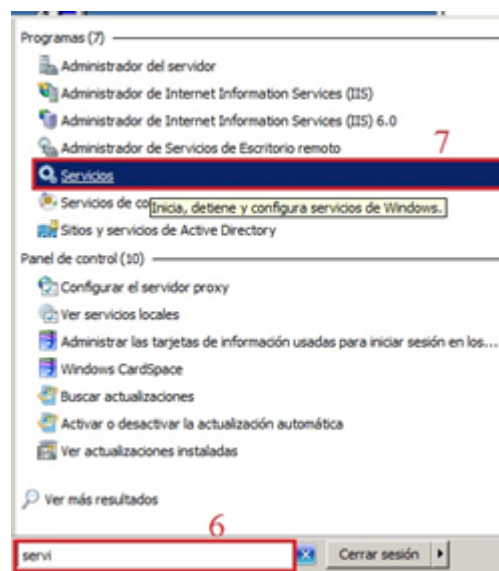
- `Import-Module ServerManager`
- `Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Basic-Auth,Web-Windows-Auth,Web-Metabase,Web-Net-Ext,Web-Lgcy-Mgmt-Console,WAS-Process-Model,RSAT-Web-Server,Web-ISAPI-Ext,Web-Digest-Auth,Web-Dyn-Compression,NET-HTTP-Activation,RPC-Over-HTTP-Proxy -Restart`

Figura #60. Ejecutando comandos en PowerShell
Elaborado por: Danilo Ninabanda.



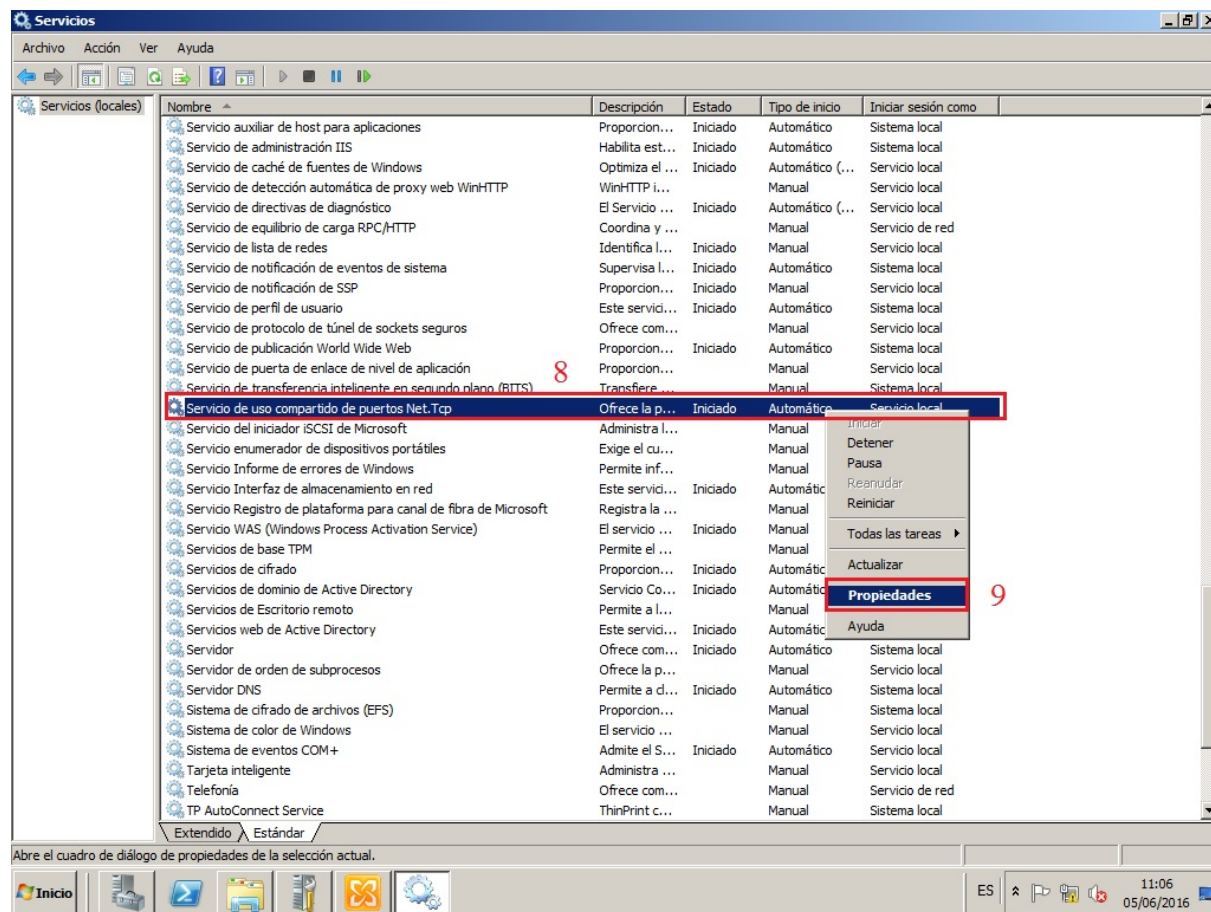
Cuando el servidor haya iniciado y si no nos ha dado algún error, abrir los Servicios de Windows.

Figura #61. Servicios de Windows
Elaborado por: Danilo Ninabanda.



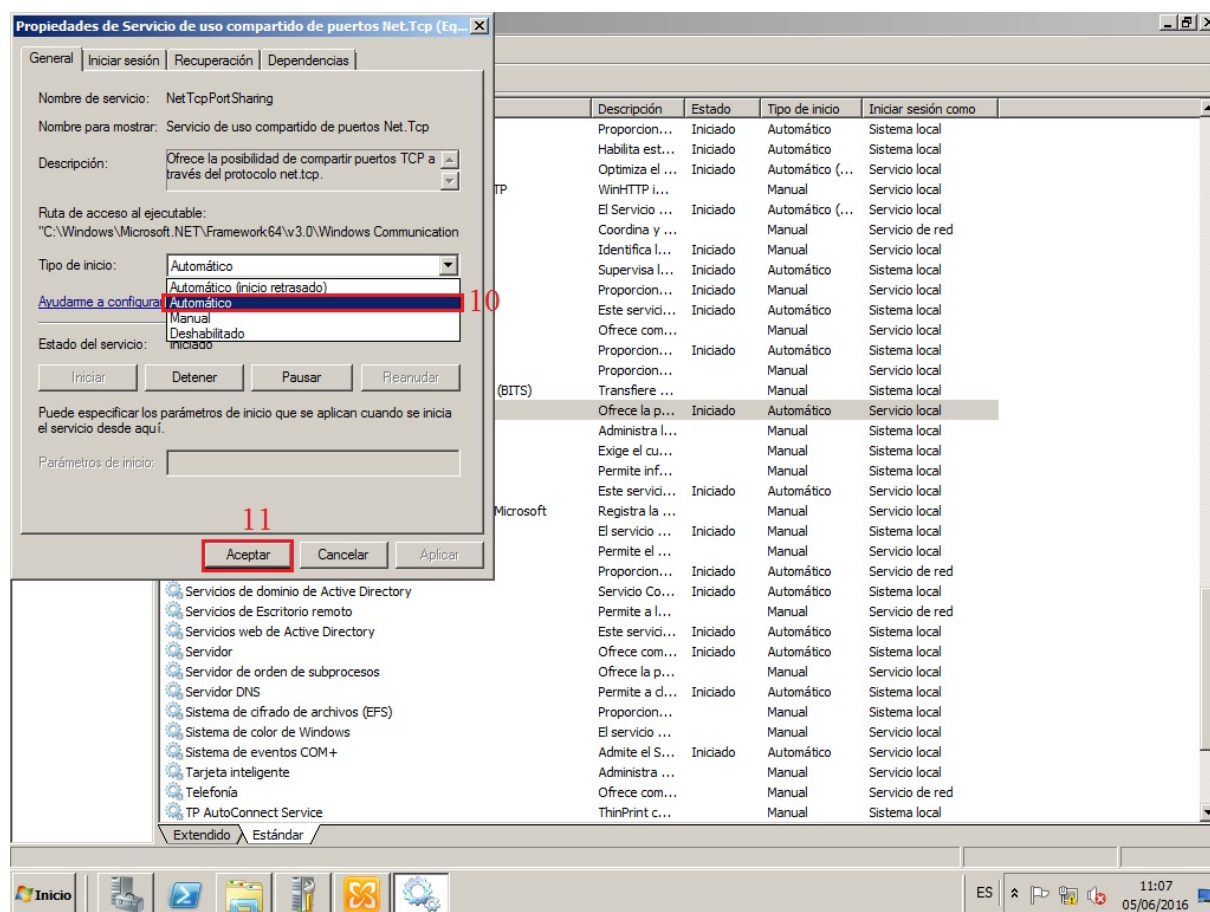
En los servicios de Windows se debe buscar “Servicio de uso compartido de puertos Net.Tcp” y verificar si esta iniciado.

Figura #62. Servicios de Windows
Elaborado por: Danilo Ninabanda.



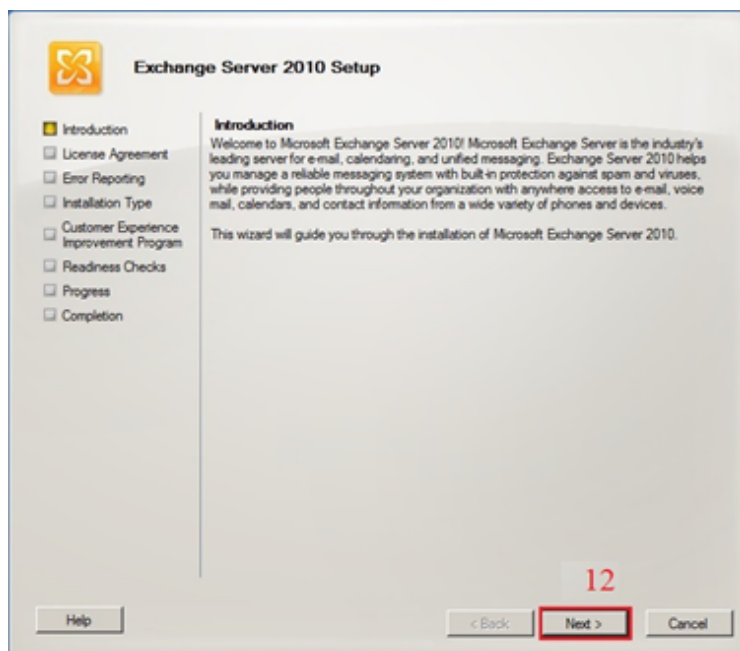
Ahora como este servicio está configurado para que se inicie de manera manual, se debe cambiarlo a automático. Esto se lo realiza dando clic derecho en el servicio y cambiar su tipo de inicio.

Figura #63. Inicio del servicio
Elaborado por: Danilo Ninabanda.



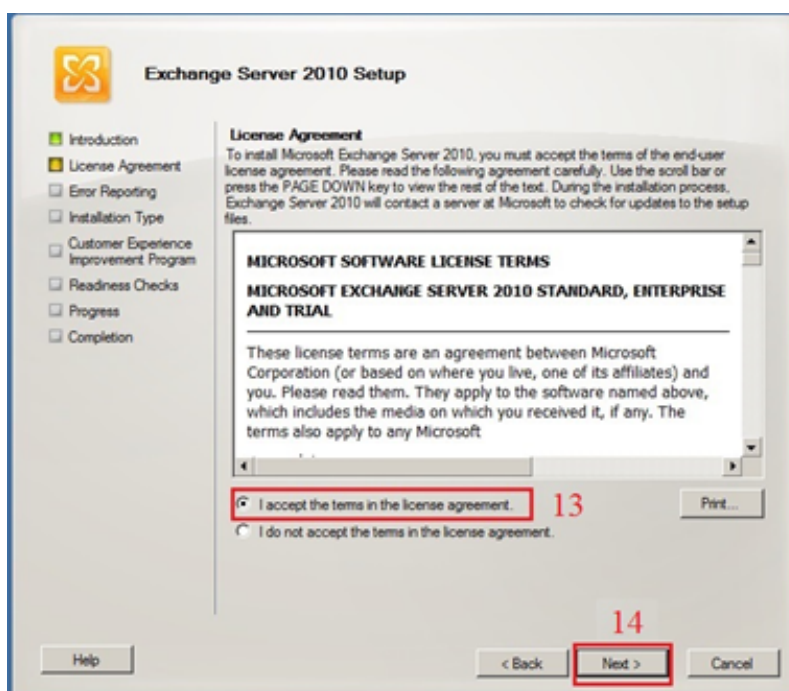
Para iniciar la instalación de Exchange, es necesario iniciar el asistente de instalación; como punto de partida se observa la introducción del asistente y para continuar se da clic en “Siguiente”.

Figura #64. Inicio del asistente de instalación de Exchange
Elaborado por: Danilo Ninabanda.



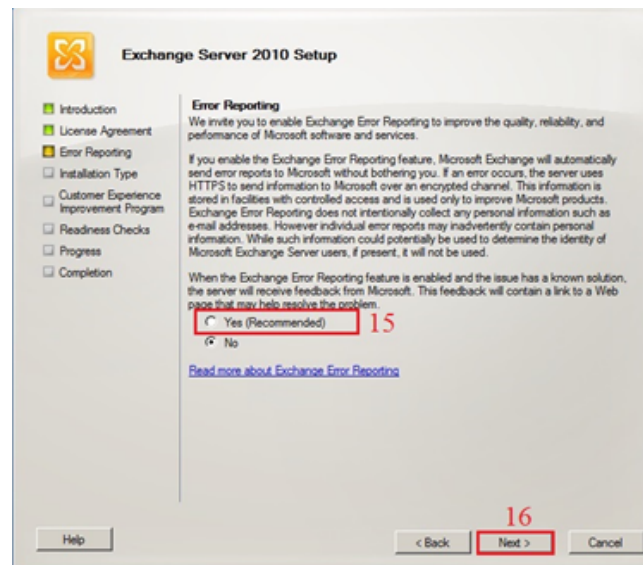
A continuación se debe aceptar los términos y condiciones de la licencia de Exchange y continuar en el botón “Siguiente”.

Figura #65. Acuerdo de licencia de Microsoft Exchange
Elaborado por: Danilo Ninabanda.



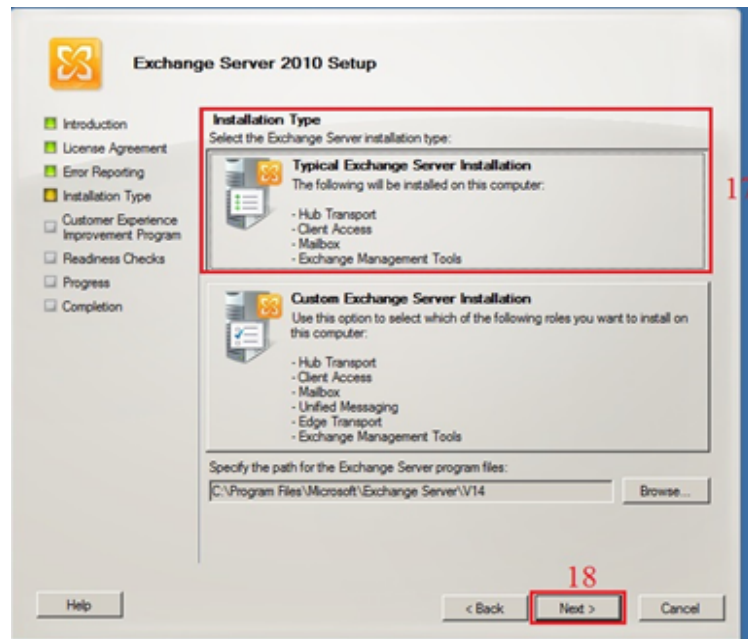
En la opción de reporte de errores de Microsoft Exchange, indica que si se desea saber la solución de cualquier error que ocurra durante la instalación, se debe seleccionar “Sí” y continuar en el botón “Siguiente”.

Figura #66. Reporte de errores
Elaborado por: Danilo Ninabanda.



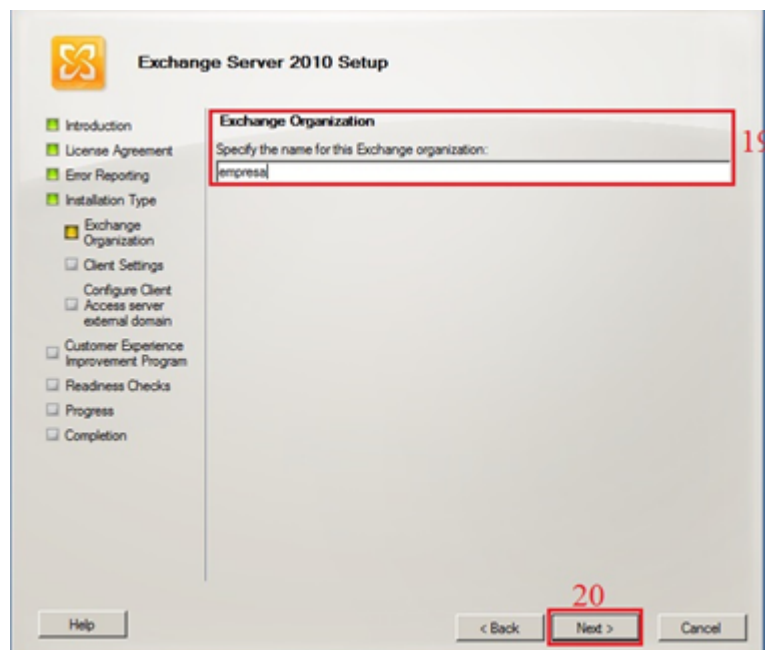
El tipo de instalación de Microsoft Exchange será típica porque se instalarán los complementos básicos de funcionamiento del servicio de correo electrónico para una red interna, se debe seleccionar este tipo y continuar dando clic en el botón “Siguiente”.

Figura #67. Tipo de instalación Microsoft Exchange
Elaborado por: Danilo Ninabanda.



En esta parte de la instalación se debe escoger el nombre de la organización para Exchange, se recomienda usar el mismo nombre con el que se configuró el dominio.

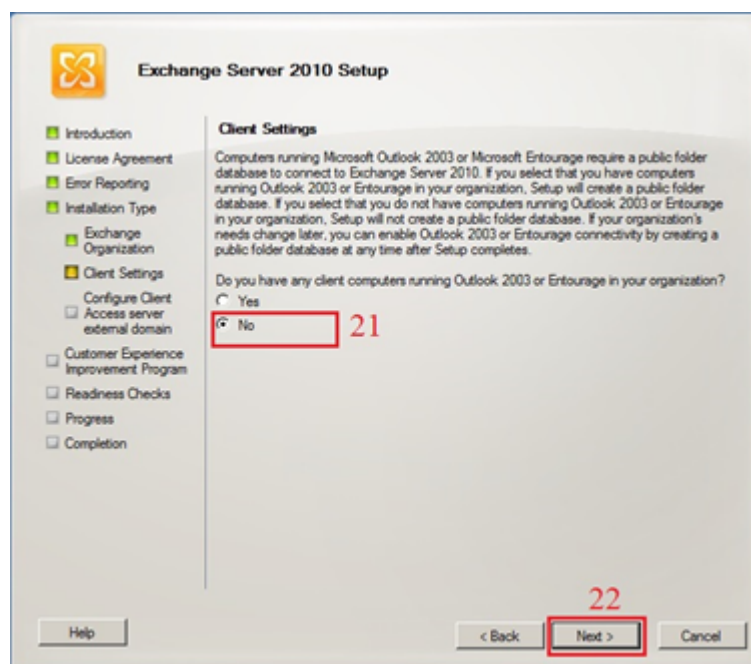
Figura #68. Organización Exchange
Elaborado por: Danilo Ninabanda.



En esta parte el asistente de instalación de Microsoft Exchange, pregunta si en la organización alguna maquina cliente usa Outlook 2003 para instalar los respectivos complementos para que funcione con esta versión. Como en esta demostración no se tiene ningún cliente con Outlook 2003 se escoge la opción “No” y se continúa en el botón “Siguiente”.

Figura #69. Configuración clientes Outlook 2003

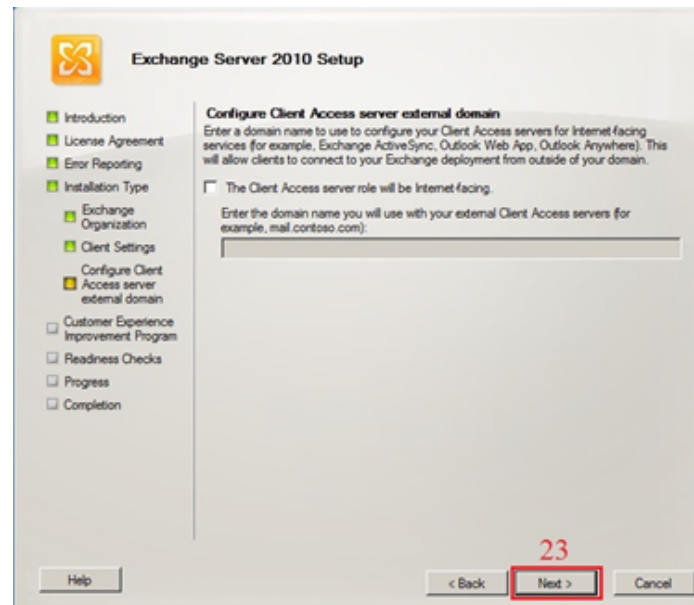
Elaborado por: Danilo Ninabanda.



Como en esta ocasión Exchange se usará internamente en la demostración de empresa no se configura el servicio de dominio externo. Únicamente se debe avanzar en el botón “Siguiente”.

Figura #70. Configuración de acceso a clientes mediante servidores de dominio externos

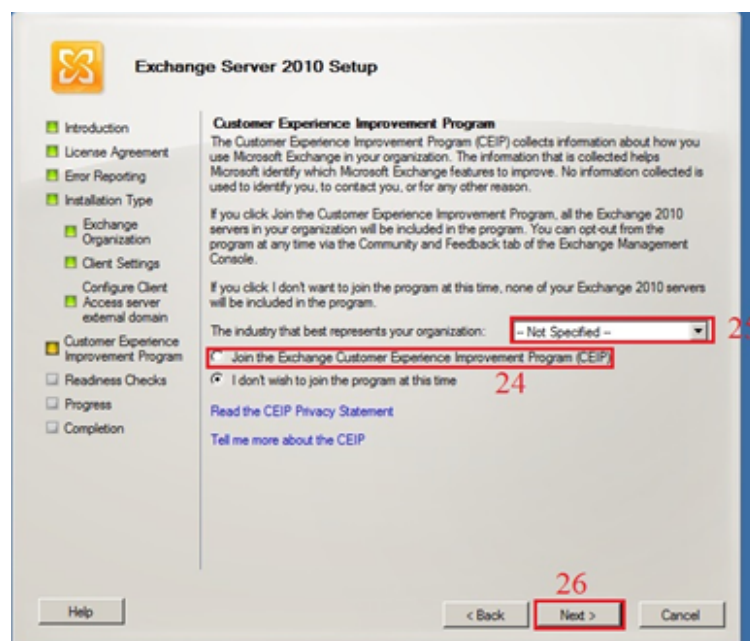
Elaborado por: Danilo Ninabanda.



Para continuar con la instalación de Exchange se debe formar parte del programa de mejora del cliente, especificando a que se dedica la organización y después continuar en el botón “Siguiente”.

Figura #71. Programa de mejora de la experiencia del cliente

Elaborado por: Danilo Ninabanda.



Al continuar el asistente verificará si todo lo necesario para la instalación está funcionando, si es así el botón “Instalar” estará disponible para que se pueda dar clic y empezar la instalación. Se debe tomar en cuenta que para instalar Microsoft Exchange se lo debe realizar como administrador.

Figura #72. Comprobación de disponibilidad

Elaborado por: Danilo Ninabanda.



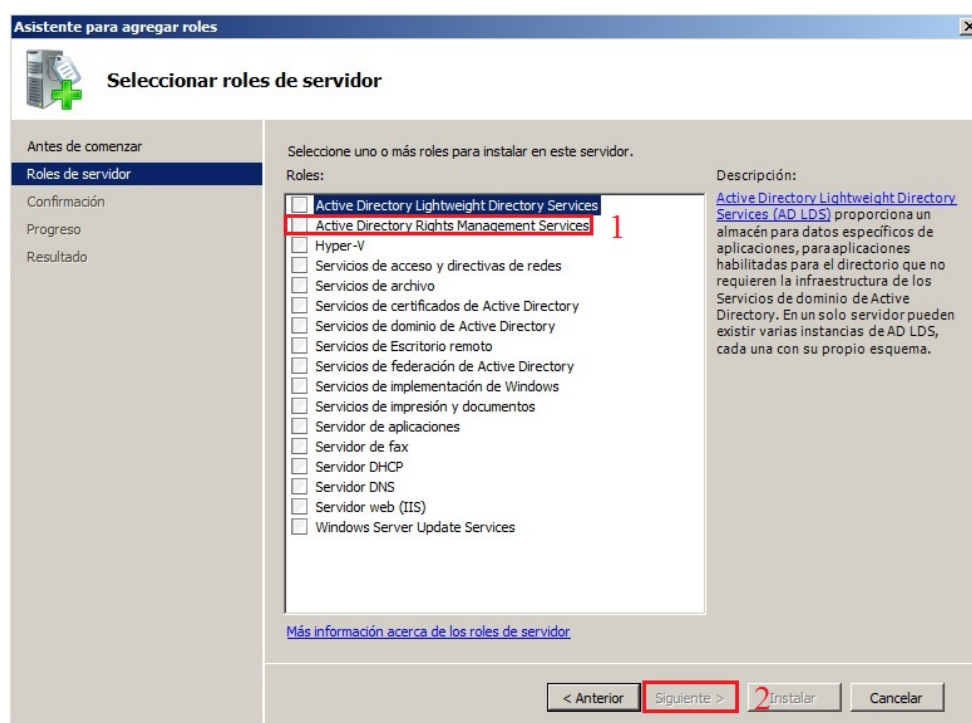
Así concluye la preparación de instalación para Exchange, a continuación se iniciará de forma automática el administrador de correo electrónico Exchange, dando a conocer que la instalación fue un éxito.

3.2. Implementación

3.2.1. Implementación de RMS

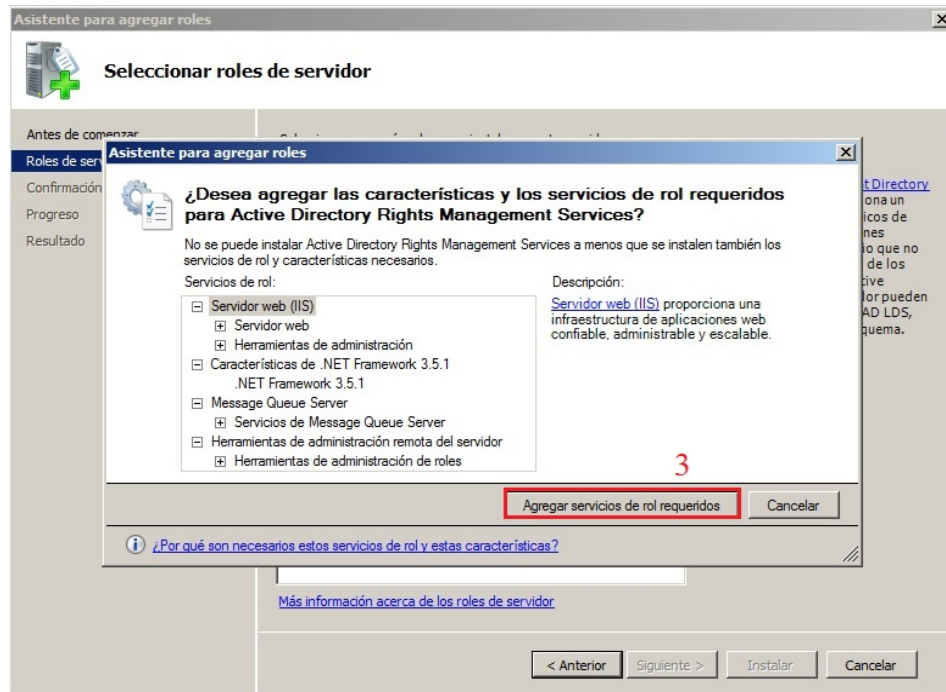
Para la implementación de RMS de Microsoft se debe agregar el rol Active Directory Rights Management Services; esta opción la encontramos en el Administrador del Servidor > Roles > Agregar Roles.

Figura #73. Asistente para agregar roles
Elaborado por: Danilo Ninabanda.



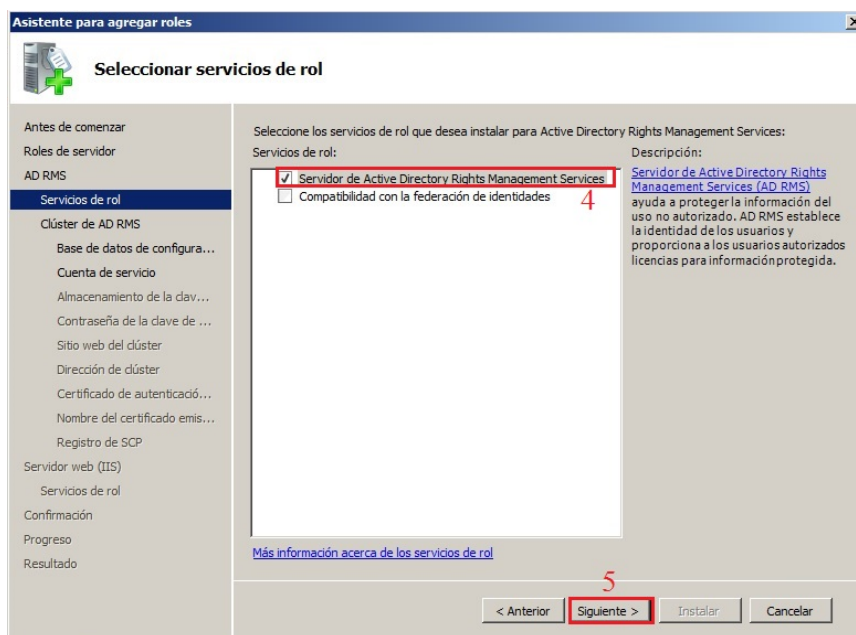
El administrador para agregar roles indicará que se necesitan algunos servicios para que RMS funcione, en ese recuadro se deberá dar clic únicamente en “Agregar servicios de rol requeridos”, para continuar.

Figura #74. Servicios de rol requeridos para RMS
Elaborado por: Danilo Ninabanda.



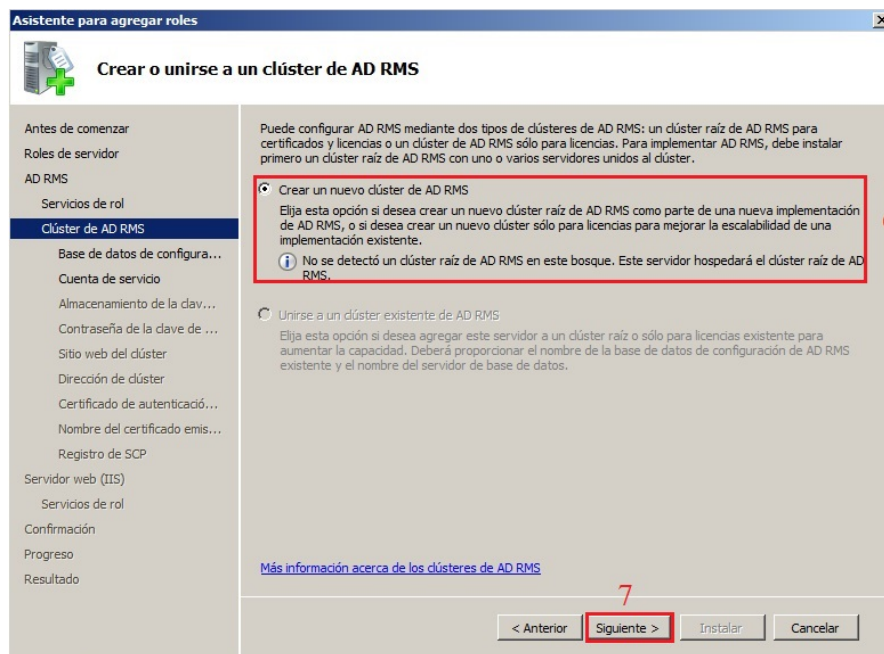
RMS posee dos servicios, el primero es de servidor de active directory rights management services y el segundo es la compatibilidad con la federación de identidades, para este proyecto se instalará únicamente el primero; ya que la segunda opción es para cuando se desea ampliar el control hacia otros dominios.

Figura #75. Servicios de rol
Elaborado por: Danilo Ninabanda.



En esta parte del asistente de instalación del rol se seleccionará el apartado que indica que se creará un nuevo clúster de AD RMS, ya que este clúster será el que emita las licencias y certificados de uso de aplicaciones compatibles con RMS.

Figura #76. Crear un clúster de AD RMS
Elaborado por: Danilo Ninabanda.



RMS puede usar dos tipos de bases de datos las cuales albergarán las configuraciones y políticas creadas, en el presente proyecto se usará una base de datos interna en el mismo servidor donde se está instalando RMS.

Figura #77. Base de datos de configuración de políticas de RMS
Elaborado por: Danilo Ninabanda.

Asistente para agregar roles

Seleccionar base de datos de configuración

Los clústeres de AD RMS usan una base de datos para almacenar información de configuración y de directivas. Esta base de datos puede estar hospedada en Windows Internal Database o en otro servidor de base de datos.

☒ Usar Windows Internal Database en este servidor

El uso de Windows Internal Database limita este clúster de AD RMS a ser de un solo servidor. Si pretende unir más servidores a este clúster de AD RMS, no use esta opción.

☐ Usar un servidor de base de datos distinto

Seleccione el servidor SQL Server o escriba el nombre del servidor o su alias CNAME (preferido) y, a continuación, haga clic en Obtener instancias de base de datos.

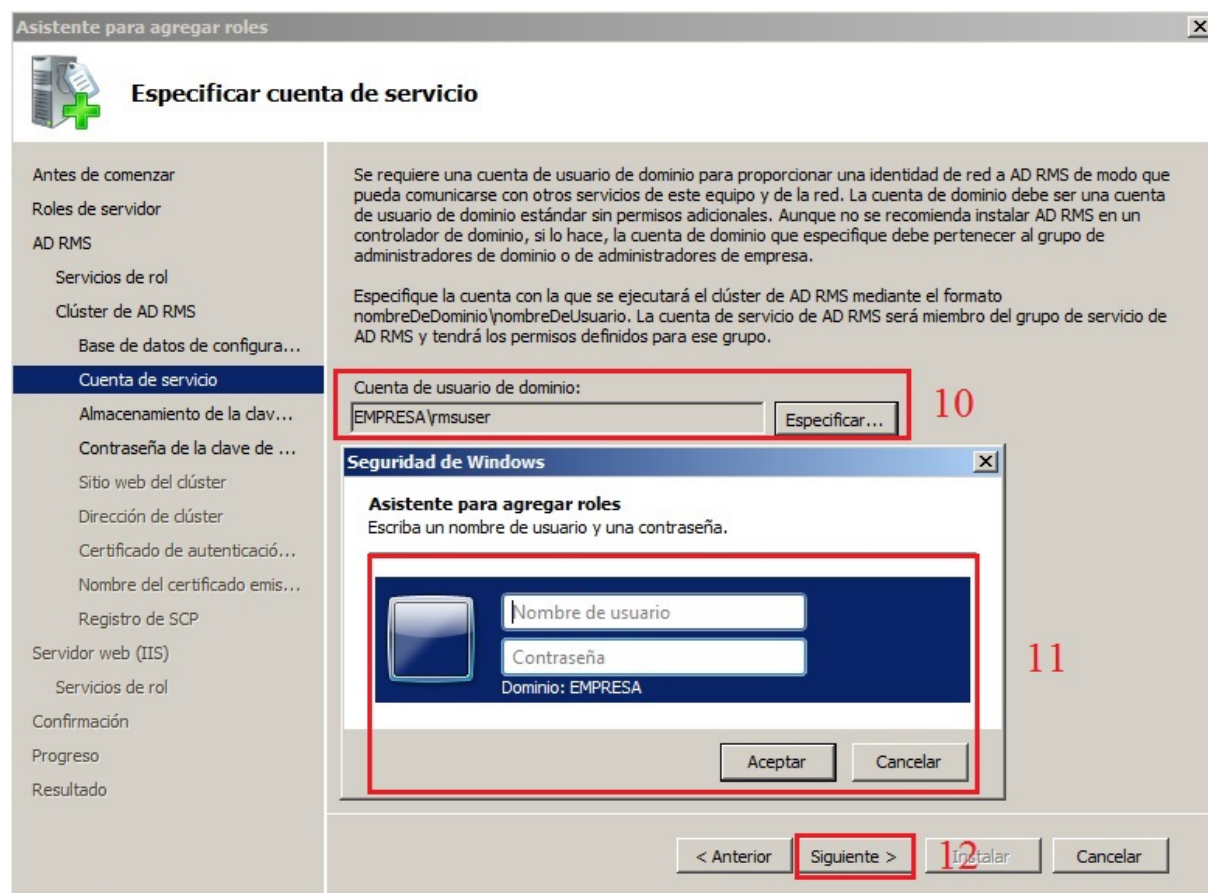
Servidor:

Instancia de base de datos:

[Más información acerca de las bases de datos de AD RMS](#)

Previamente se debe crear un usuario con el rol de administrador en active directory, este se usará en esta parte de la instalación de RMS con el fin de que este servidor sea identificado y pueda comunicarse con otros servicios del equipo y de la red.

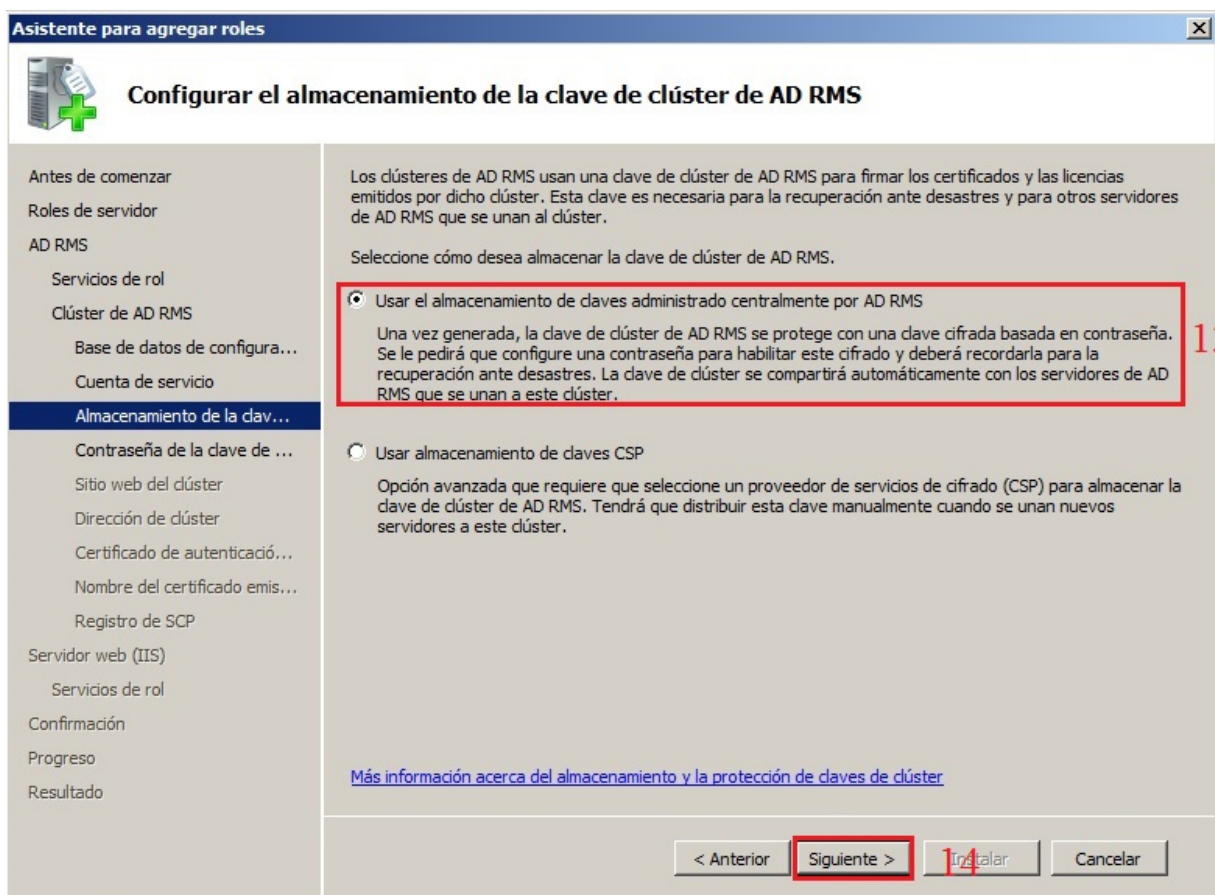
Figura #78. Cuenta de servicio de RMS
Elaborado por: Danilo Ninabanda.



El clúster de AD RMS se encarga de firmar y emitir las licencias de uso para las aplicaciones compatibles con el servicio para esto necesita una clave, en esta parte de la instalación se elegirá la opción de usar el almacenamiento de claves administrado centralmente por AD RMS.

Figura #79. Almacenamiento de la clave de clúster de AD RMS

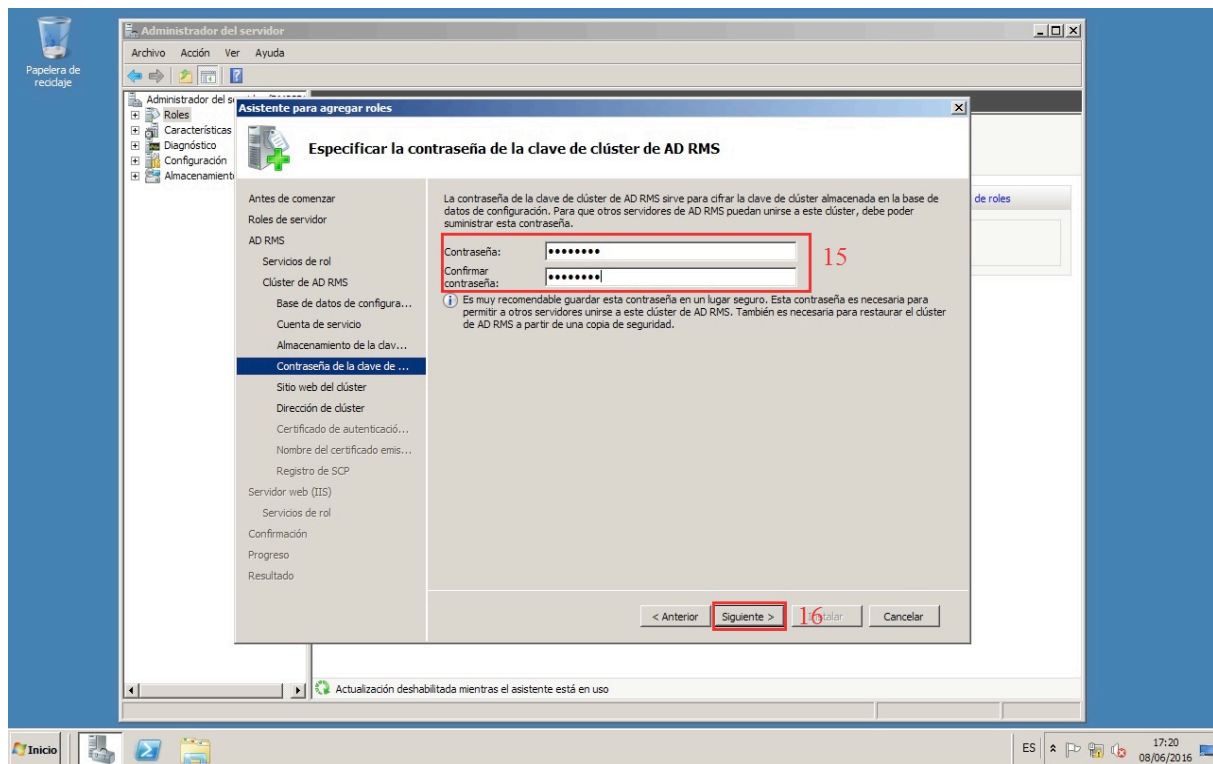
Elaborado por: Danilo Ninabanda.



A continuación se debe ingresar la clave de clúster de Ad RMS que servirá para cifrar la clave almacenada en la base de datos de configuración. Posteriormente cuando se vincule otro servidor de RMS se debe proporcionar esta clave.

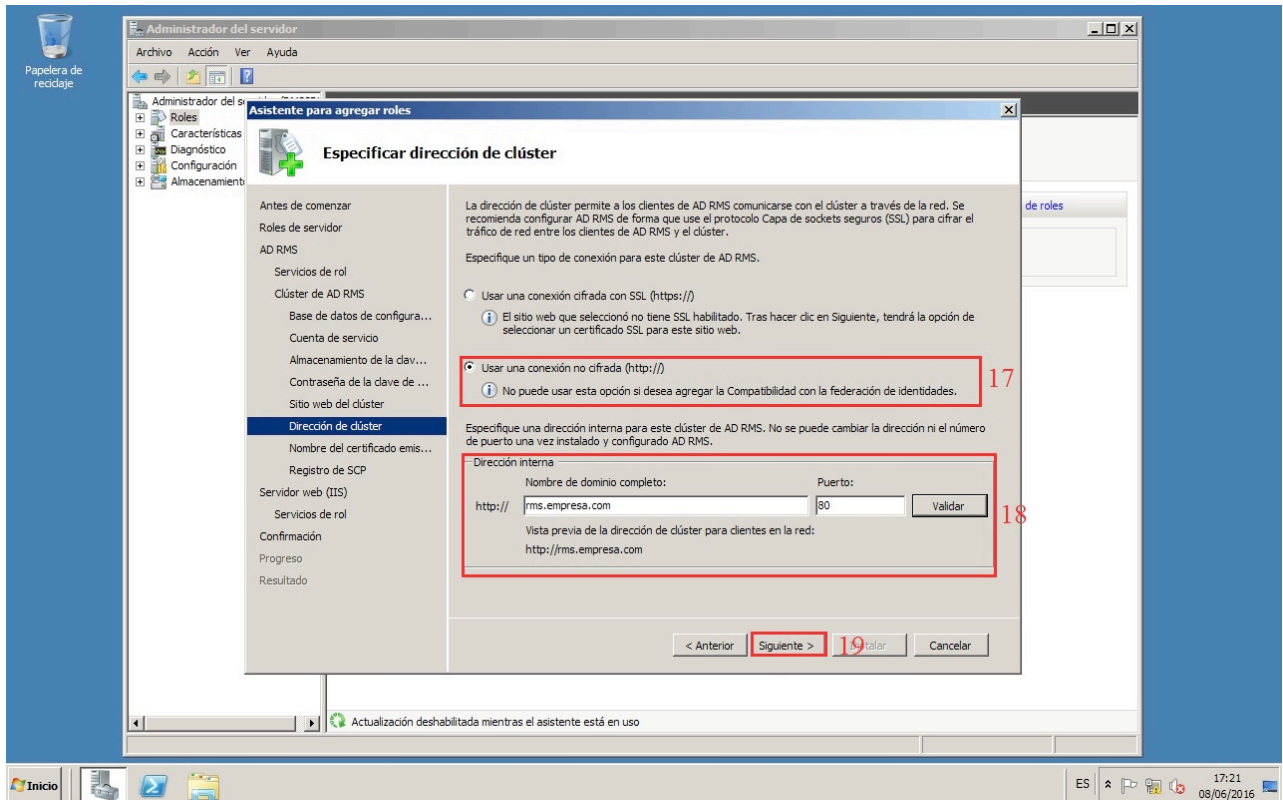
Figura #80. Contraseña de la clave de clúster de AD RMS

Elaborado por: Danilo Ninabanda.



Para la comunicación entre el servidor de RMS y los usuarios se debe configurar una dirección interna de red. Esta puede estar basada en SSL que significa que la comunicación de la red está cifrada o una conexión no cifrada.

Figura #81. Dirección de clúster
Elaborado por: Danilo Ninabanda.



Como RMS crea un certificado que se emite para la autorización del uso de contenido a los clientes, este certificado debe tener un nombre para ser identificado.

Figura #82. Nombre Para el Certificado Emisor de Licencias de Servidor
Elaborado por: Danilo Ninabanda.

Asistente para agregar roles

Especificar un nombre para el Certificado emisor de licencias de servidor

Antes de comenzar
Roles de servidor
AD RMS
Servicios de rol
Clúster de AD RMS
Base de datos de configura...
Cuenta de servicio
Almacenamiento de la clav...
Contraseña de la clave de ...
Sitio web del clúster
Dirección de clúster
Nombre del certificado emis...
Registro de SCP
Servidor web (IIS)
Servicios de rol
Confirmación
Progreso
Resultado

AD RMS crea un Certificado emisor de licencias de servidor que establece la identidad de este clúster de AD RMS para los clientes.
Escriba un nombre que le ayude a identificar fácilmente este certificado.

Nombre:
Empresa RMS

20

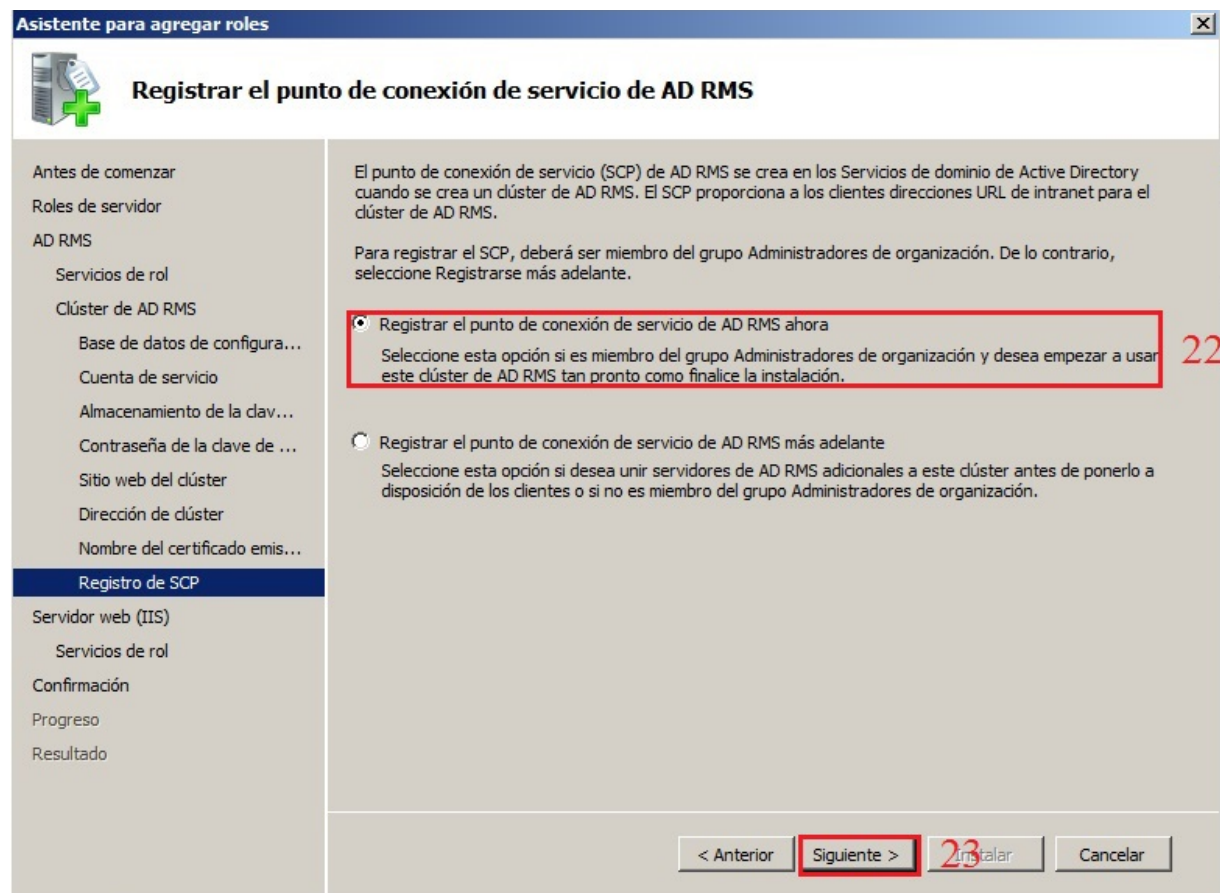
< Anterior **Siguiete >** Instalar Cancelar

21

En esta parte de la instalación de RMS se debe seleccionar la opción “Registrar el punto de conexión de servicio de AD RMS ahora”, esto para que el servicio empiece a funcionar y emitir las licencias a los equipos de los usuarios registrados.

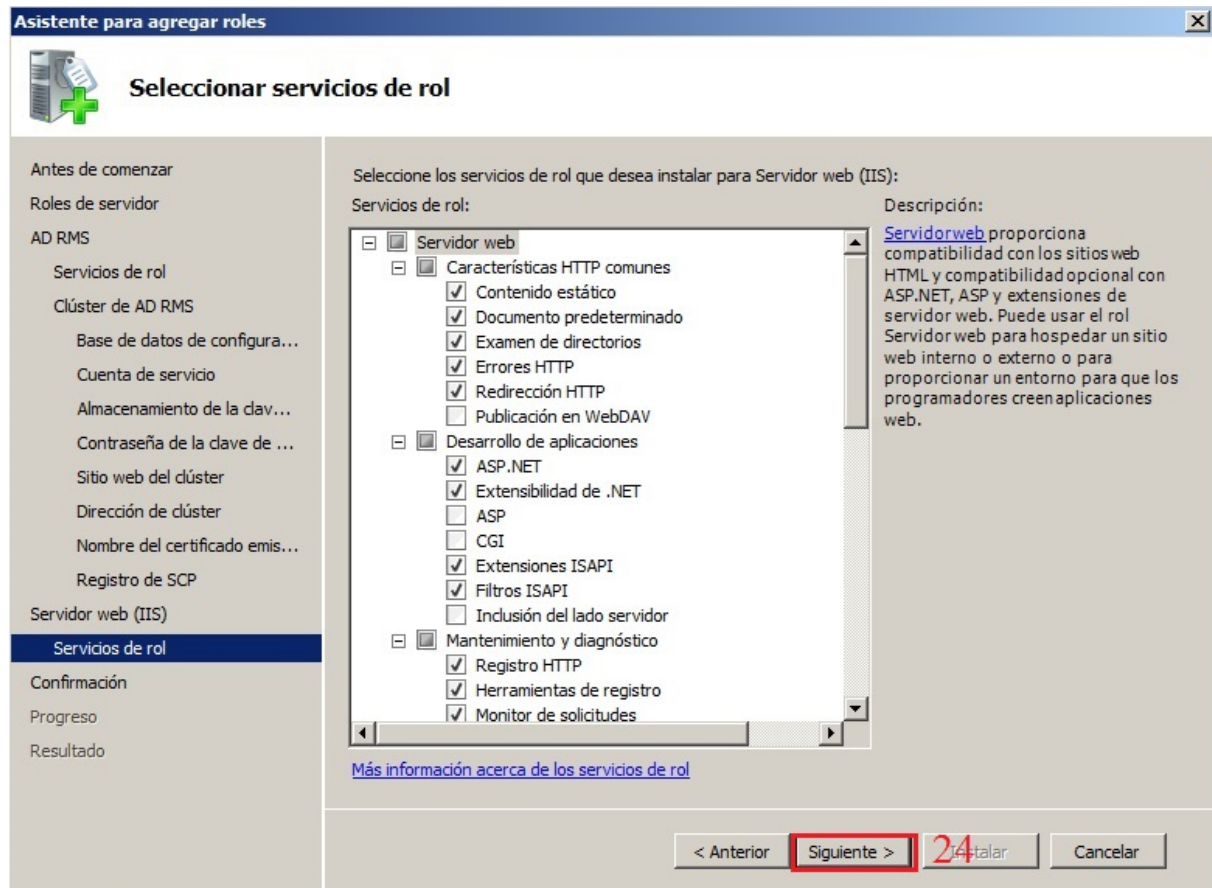
Figura #83. Punto de conexión de servicio de AD RMS

Elaborado por: Danilo Ninabanda.



A continuación si gusta se puede instalar algún otro servicio adicional al que RMS necesita, para continuar con la instalación se da clic en “Siguiete”.

Figura #84. Seleccionar servicios de rol
Elaborado por: Danilo Ninabanda



Antes de empezar la instalación el asistente muestra los parámetros seleccionados anteriormente los cuales se debe comprobar que este correctamente configurados. Para empezar la instalación se da clic en “Instalar”.

Figura #85. Lista de selecciones para instalación
Elaborado por: Danilo Ninabanda.

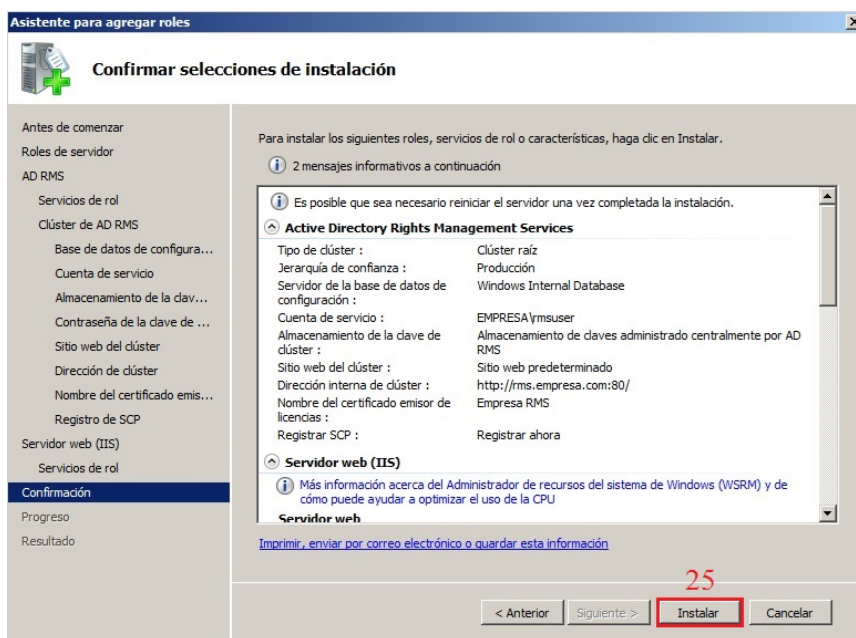
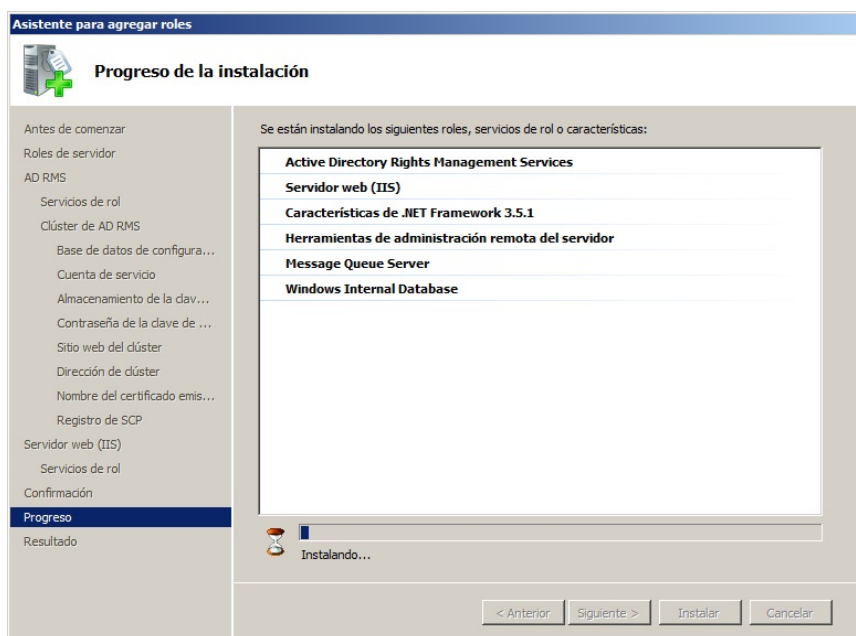
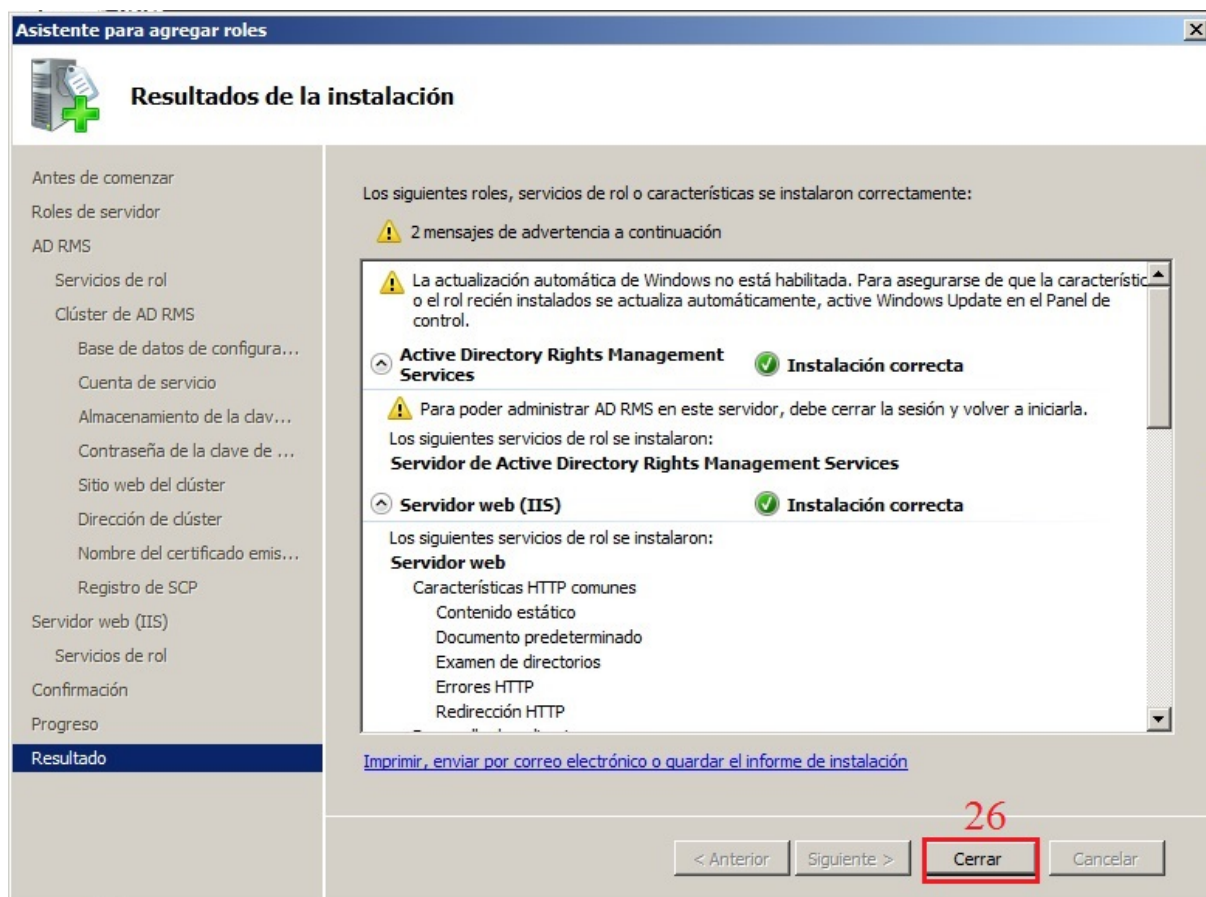


Figura #86. Proceso de instalación
Elaborado por: Danilo Ninabanda.



Si la instalación es un éxito se obtendrá un resultado como el de la siguiente figura, caso contrario el asistente indicará el error y la posible razón por la que no se pudo completar la instalación.

Figura #87. Resultados de la instalación
Elaborado por: Danilo Ninabanda.



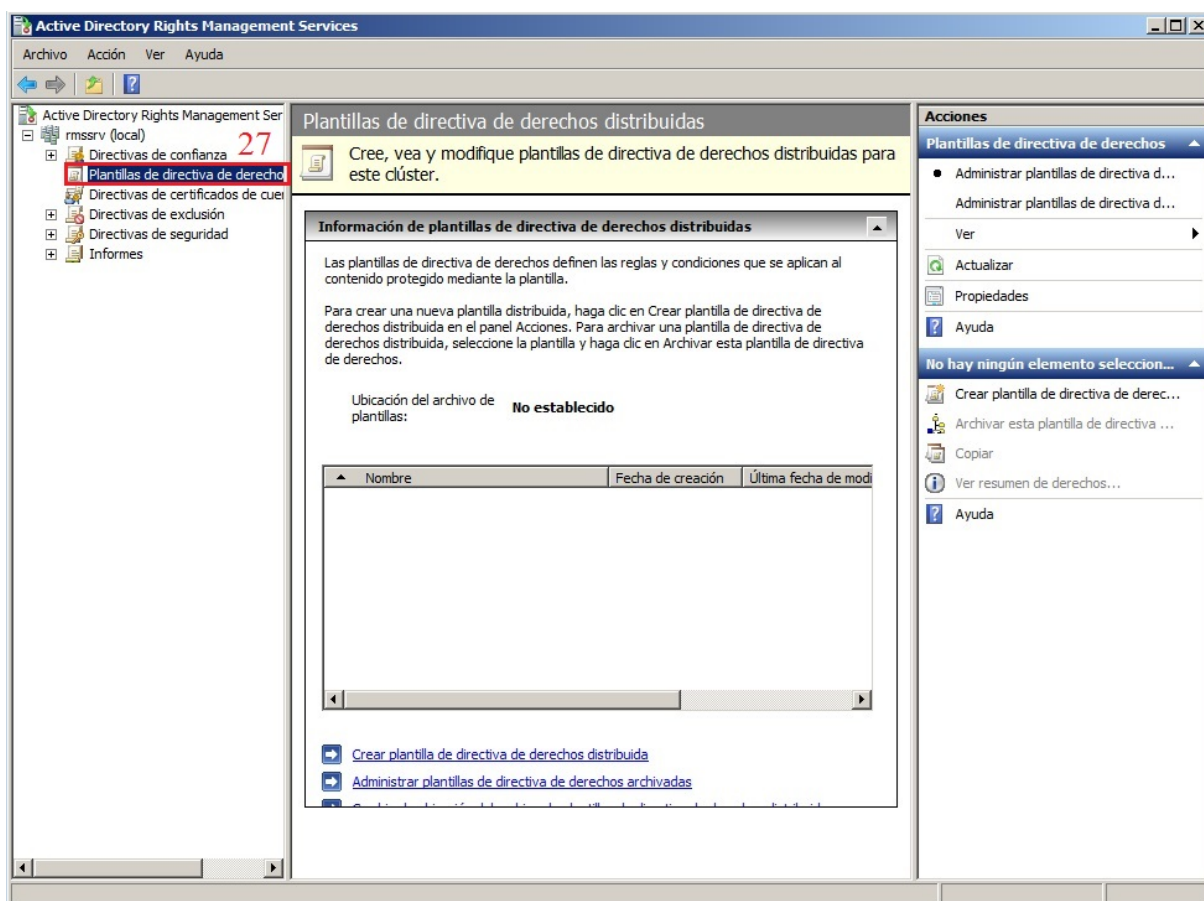
3.2.2. Creación de plantillas de directivas de derechos distribuidos.

Una vez concluida la instalación del ron de RMS, se debe obligatoriamente reiniciar el servidor, para a continuación empezar con la creación de las políticas de uso de contenido.

Realizado lo anterior se debe abrir el panel de “Active Directory Rights Management Services”, en la opción de plantillas de directivas de derechos distribuidos.

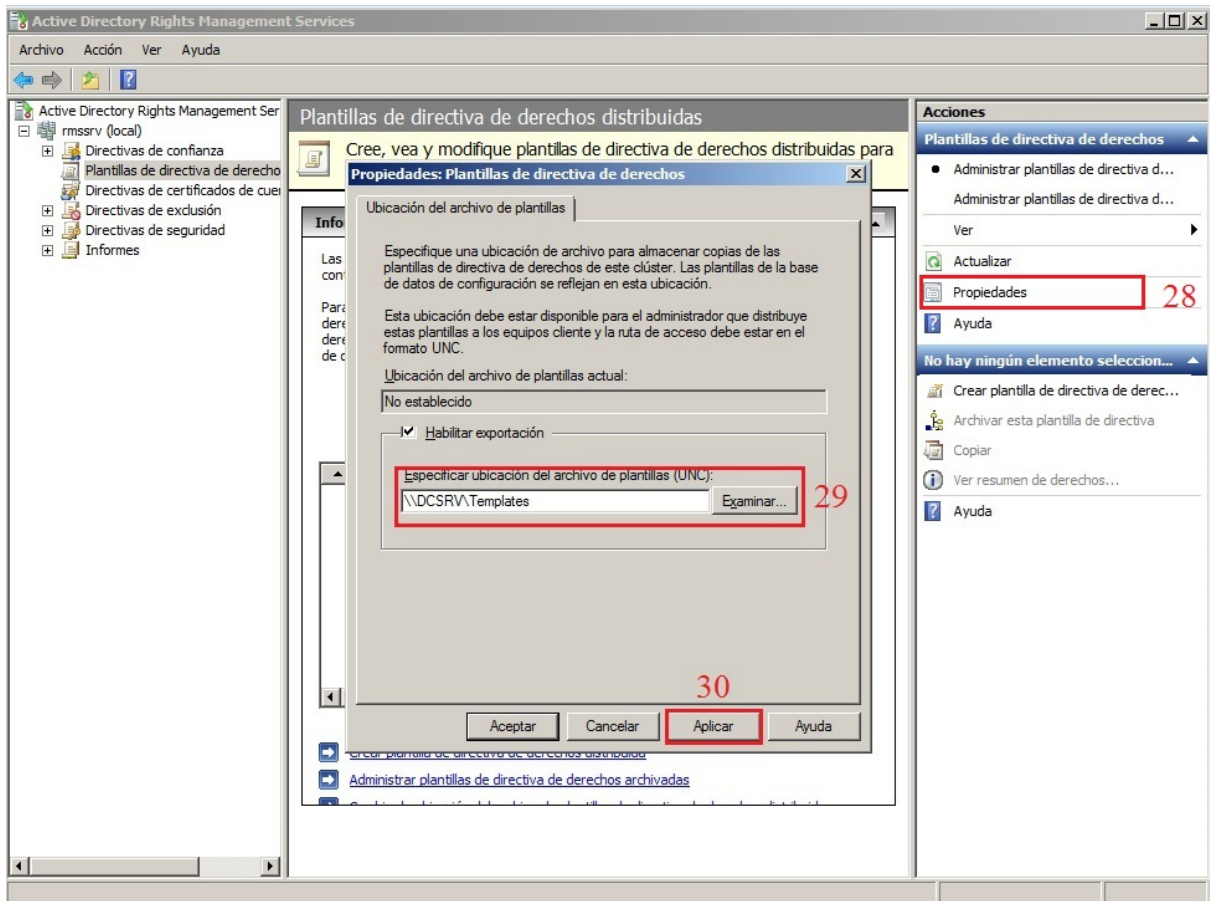
Figura #88. Plantillas de directivas de derechos distribuidos

Elaborado por: Danilo Ninabanda.



Lo primero en configurar es la ubicación donde se guardarán las plantillas, para esto se debe abrir las propiedades de las plantillas de directivas de derechos, y se deberá colocar la dirección de la carpeta que contendrá las plantillas.

Figura #89. Direccionamiento de plantillas de directivas de derechos
Elaborado por: Danilo Ninabanda.



En la ventana que se desplegará el listado de todas las directivas creadas, para añadir una nueva directiva clic en “Agregar” para continuar.

Figura #90. Crear plantilla de directiva de derechos distribuidos

Elaborado por: Danilo Ninabanda.

Crear plantilla de directiva de derechos distribuida

Agregar información de identificación de plantilla

1. Agregar información de ...
2. Agregar derechos de u...
3. Especificar directiva de...
4. Especificar directiva ext...
5. Especificar directiva de...

Las plantillas de directiva de derechos pueden admitir clientes con idiomas distintos. Configure la información de identificación de esta plantilla para cada idioma admitido en los equipos cliente.

Identificación de la plantilla

Idioma	Nombre	Descripción

32 **Agregar** Editar Quitar

33 < Anterior **Siguiete >** Finalizar Cancelar

En la ventana que continúa se debe llenar los campos que indica, y a continuación para avanzar con la creación de la plantilla se realiza clic en “Agregar”.

Figura #91. Agregar nueva información de identificación de la plantilla
Elaborado por: Danilo Ninabanda.

The screenshot shows a Windows-style window titled "Crear plantilla de directiva de derechos distribuida". Inside, there's a section titled "Agregar información de identificación de plantilla" with a list of steps on the left: "1. Agregar información de ...", "2. Agregar derechos de u...", "3. Especificar directiva de...", "4. Especificar directiva ext...", and "5. Especificar directiva de...". The main area contains instructions: "Las plantillas de directiva de derechos pueden admitir clientes con idiomas distintos. Configure la información de identificación de esta plantilla para cada idioma admitido en los equipos cliente." A modal dialog box titled "Agregar nueva información de identificación de la plantilla" is open, containing fields for "Idioma:" (set to "Español (España, internacional)"), "Nombre:" (set to "Informes Confidenciales"), and "Descripción:" (set to "Empresa Documentos"). Below these fields are "Agregar" and "Cancelar" buttons. At the bottom of the main window, there are "< Anterior", "Siguiete >", and "Cancelar" buttons. Red handwritten numbers 34, 35, and 36 are placed next to the dialog box, the "Agregar" button, and the "Siguiete >" button respectively.

Crear plantilla de directiva de derechos distribuida

Agregar información de identificación de plantilla

1. Agregar información de ...
2. Agregar derechos de u...
3. Especificar directiva de...
4. Especificar directiva ext...
5. Especificar directiva de...

Las plantillas de directiva de derechos pueden admitir clientes con idiomas distintos. Configure la información de identificación de esta plantilla para cada idioma admitido en los equipos cliente.

Agregar nueva información de identificación de la plantilla

Seleccione el idioma de la plantilla y, a continuación, escriba un nombre y una descripción de la plantilla para mostrar a los usuarios del idioma seleccionado.

Idioma: Español (España, internacional)
Nombre: Informes Confidenciales
Descripción: Empresa Documentos

Agregar Cancelar

< Anterior Siguiete > Cancelar

Esta parte de la creación de la directiva es muy importante ya que aquí se vincularán las personas o grupos de trabajo a las cuales se les desea especificar derechos sobre contenido protegido. Así concluiría la implementación de RMS en el servidor, a continuación se debe realizar algunos pasos más en las máquinas de los usuarios de RMS.

Figura #92. Agregar usuario o grupo

Elaborado por: Danilo Ninabanda.

Crear plantilla de directiva de derechos distribuida

Agregar derechos de usuario

1. Agregar información de ...
2. Agregar derechos de u...
3. Especificar directiva de...
4. Especificar directiva ext...
5. Especificar directiva de...

Especifique los usuarios y grupos que tienen derechos para trabajar con contenido protegido con esta plantilla. Algunos derechos no se usan en aplicaciones habilitadas para RMS comunes.

Usuarios y derechos

finanzas@empresa.com
secretarias@empresa.com

Agregar...
Quitar...

Derechos de finanzas@empresa.com:

Control total	☐
Ver	☒
Editar	☒
Guardar	☒
Exportar (Guardar como)	☒

Crear derecho personalizado... Eliminar derecho personalizado...

☒ Conceder al propietario (autor) derecho de control total sin expiración

URL de solicitud de derechos:

< Anterior Siguiente > **Finalizar** Cancelar

40

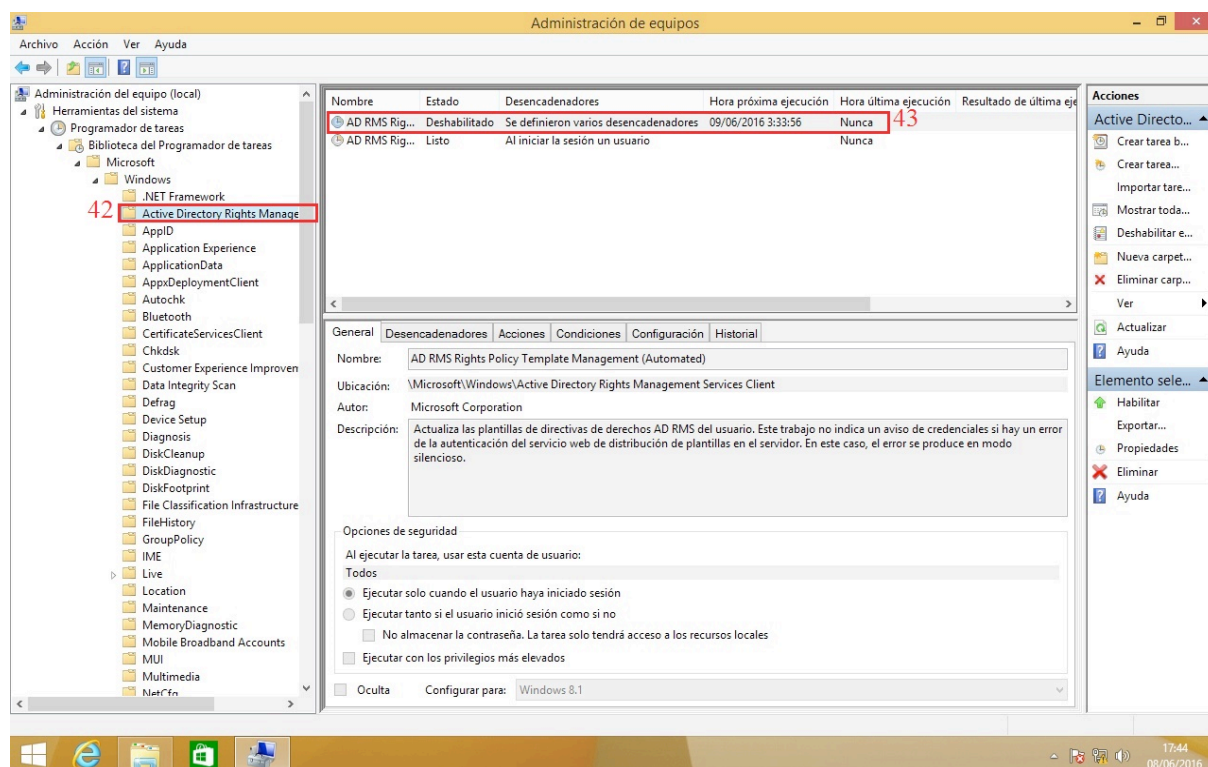
41

3.2.3. Configuración de Terminal de Usuarios de RMS.

Para que RMS funcione correctamente se debe realizar lo siguiente, ingresar al Administrador de Equipos y dirigirse a: Biblioteca del programador de tareas > Microsoft > Windows > Active Directory Rights Management. En esta parte en las opciones, todas se deben encontrar habilitadas si no lo están debe hacerlo para que el servicio en la terminal inicie.

Figura #93. Servicios de RMS en terminales de usuarios

Elaborado por: Danilo Ninabanda.



A continuación para finalizar la configuración en la terminal cliente se necesita ingresar al Editor de Registro y dirigirse a la siguiente ruta: HKEY_CURRENT_USER\Software\Microsoft\Office\Common, aquí se deberá crear una nueva clave con el nombre “DRM”; en esta nueva clave se agregará un valor de cadena expandible con la dirección donde se guardarán las plantillas de directivas.

Figura #94. Creación de nueva clave
Elaborado por: Danilo Ninabanda.

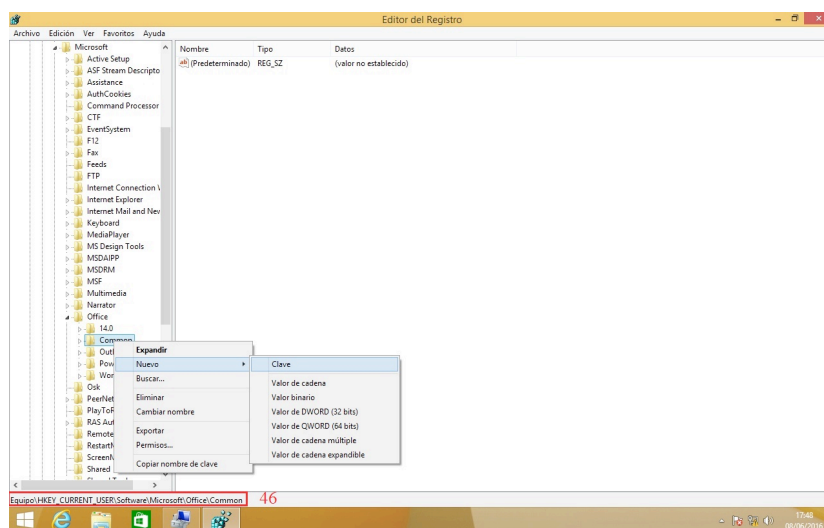
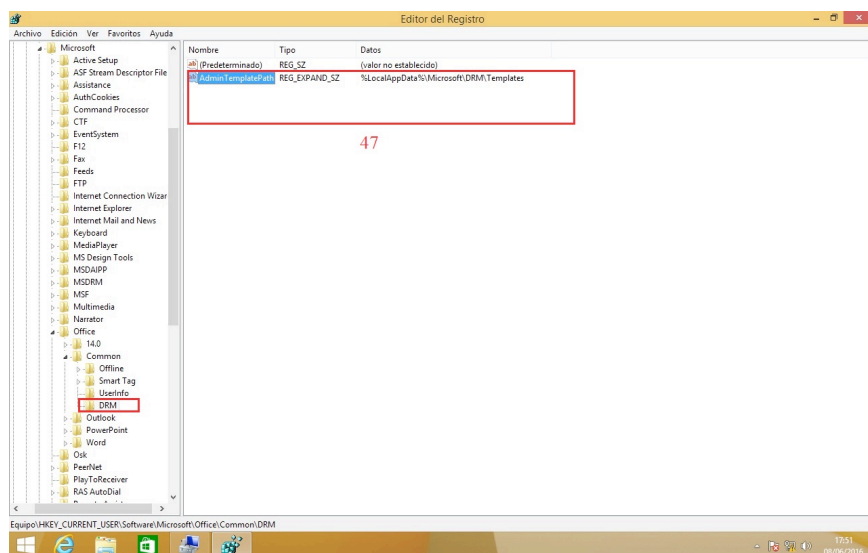


Figura #95. Creación de valor de cadena expandible
Elaborado por: Danilo Ninabanda



CAPÍTULO IV

DISCUSIÓN

4.1. Conclusiones

- Se puede concluir que con el estudio de los diferentes algoritmos criptográficos queda abierto un amplio panorama para que en la actualidad se pueda usar estas técnicas valiosas para preservar la confidencialidad de toda la información no solo que se maneja en las redes de las empresas, sino también en la información que maneja cada persona en sus diversos entornos.
- El modelo de comunicaciones seguras diseñado en base al dominio 10 de la norma ISO/IEC 27002:2013, además de brindar la confidencialidad por medio de algoritmos criptográficos en las comunicaciones que se generen con el servicio de correo electrónico Microsoft Exchange, garantiza la integridad de todos los documentos electrónicos que se encuentren en las empresas por medio de la función Hash que forma parte de los algoritmos criptográficos aplicados junto al servicio de RMS.
- En la implementación sobre el ambiente de pruebas de este proyecto se pudo llegar a la conclusión que algunos de los pre-requisitos para el funcionamiento de RMS, como

Active Directory mejoran la gestión de usuarios y todos los recursos como por ejemplo: archivos electrónicos, que una empresa posee y se encuentran vinculadas al dominio de la misma. Además este servicio presta una importante ayuda en cuanto a la gestión de claves, que es muy indispensable para cumplir con protección de la información.

- El diseño del modelo de comunicaciones seguras realizado con RMS de Microsoft y que usa los servicios de Microsoft Exchange, ha demostrado ser una solución que impide la pérdida de información para cualquier empresa que lo implemente ya que todo el contenido que se crea, almacena e intercambia en la empresa se encuentra cifrado; así los documentos que salgan de manera ilegal de la empresa no podrán ser visualizados por los intrusos.
- En este proyecto se ha mencionado sobre la importancia de la información y el valor que tiene para el funcionamiento de las empresas; así que se pudo llegar a la conclusión que la implementación de RMS y el uso de la criptografía darán la pauta para que las empresas empiecen a utilizar alternativas de seguridad poco comunes que complementarían a sus sistemas de seguridad ya implantados disminuyendo considerablemente el riesgo de perder documentos electrónicos importantes y conservar la integridad de los mismos.
- Se puede concluir que con el uso de este modelo de comunicaciones seguras basadas en RMS se puede evitar la fuga de información o documentos electrónicos de las empresas los cuales pueden registren pérdidas económicas, daños al nombre de la marca, incluso la interrupción en la continuidad del negocio.

4.2.Recomendaciones

- En base al estudio del dominio 10 de ISO/IEC 27002:2013, para la implementación de este modelo de comunicaciones seguras, se recomienda que para tener un mejor resultado en cuanto a la protección de los documentos electrónicos, se implementen algunos dominios más con sus respectivos controles con el fin de aumentar la protección en dichos documentos.
- Se recomienda a todas las personas encargadas del área de tecnologías de la información de las empresas que deseen aplicar las herramientas y servicios expuestos en este trabajo, que deberán realizarlo primero en un ambiente de pruebas con el modelo de su infraestructura, para así evitar cualquier error al momento de realizar la implementación.
- Para complementar la implementación de RMS, se recomienda también la creación de políticas de gestión de claves que es muy importante para que el modelo de comunicaciones seguras no quede expuesto ante el uso de técnicas de criptoanálisis.
- Se recomienda la creación de suficientes políticas de gestión de documentos electrónicos mediante RMS con el fin de proteger la mayor cantidad de información de personal no autorizado.

BIBLIOGRAFÍA

Areitio Bertolín, J. (2008). Seguridad de la Información. Madrid: Paraninfo.

Disponible en

<https://books.google.com.ec/books?id=z2GcBD3deYC&printsec=frontcover&hl=es#v=onepage&q&f=false>

Carreño Castelló, M., & Valenzuela Ramírez, J. E. (2015). Software para Cifrado y

Descifrado de Archivos de Texto. Disponible en

<http://tesis.bnct.ipn.mx/bitstream/handle/123456789/14365/Software%20para%20cifrado%20y%20descifrado%20de%20archivos%20de%20texto.pdf?sequence=1>

Infosegur. (2013). Objetivos de la seguridad de la información. Recuperado el 13 de mayo de 2016. Disponible en

<https://infosegur.wordpress.com/tag/no-repudio/>

ISO. (2016). ISO FOREWORD. Recuperado el 20 de abril de 2016. Disponible en

<https://www.iso.org/obp/ui/#iso:std:54533:en>

ISO27000. (2016). Controles ISO 27002:2103. Recuperado el 20 de abril de 2016.

Disponible en

<http://www.iso27000.es/download/ControlesISO27002-2013.pdf>

ISO27002. (2016). Documento de política de seguridad de la información. Disponible en

<https://iso27002.wiki.zoho.com/5-1-1-Documento-de-pol%C3%ADtica-de-seguridad-de-la-informaci%C3%B3n.html>

Lucena Manuel. (2015). Criptografía y Seguridad en Computadores. Disponible en

<http://criptografiayseguridad.blogspot.com.es/p/criptografia-y-seguridad-en.html>

Mendoza, T., & César, J. (2008). Demostración de cifrado simétrico y asimétrico. Disponible

<http://www.dspace.ups.edu.ec/bitstream/123456789/8185/1/Demostraci%C3%B3n%20de%20cifrado%20sim%C3%A9trico%20y%20asim%C3%A9trico.pdf>

Microsoft. (2016). Introducción a Active Directory.

Fecha de recuperación 21 de abril de 2016. Disponible en

<https://www.citethisforme.com/es/cite/website/autocite>

Microsoft. (2016). Como funciona RMS.

Fecha de recuperación 21 de abril de 2016. Disponible en

[https://technet.microsoft.com/es-es/library/cc747763\(v=ws.10\).aspx](https://technet.microsoft.com/es-es/library/cc747763(v=ws.10).aspx)

Microsoft. (2016). Windows Server 2008 y Windows Server 2008 R2.

Recuperado el 20 de abril de 2016. Disponible en

[https://technet.microsoft.com/es-es/library/dd349801\(v=ws.10\).aspx](https://technet.microsoft.com/es-es/library/dd349801(v=ws.10).aspx)

Mifsud E. (2012). Introducción a la seguridad informática - seguridad de la información

Disponible en

<http://recursostic.educacion.es/observatorio/web/ca/software/softwaregeneral/1040introduccion-a-la-seguridad-informatica?start=1>

Morales Lara, Alberto. (2012). Análisis de los algoritmos de cifrado de llave secreta y su uso

dentro de una organización pública (Doctoral dissertation). Disponible en

<http://tesis.bnct.ipn.mx/bitstream/handle/123456789/8870/ANALGOR.pdf?sequence=1>

Navarro, M. Á. E. (2001). Los archivos de documentos electrónicos. El profesional de la información, 10(12), 41-45. Disponible en

<http://www.elprofesionaldelainformacion.com/contenidos/2001/diciembre/9.pdf>

Pacheco Federico. (2014). Criptografía. Disponible en

<http://www.redusers.com/noticias/publicaciones/criptografia>

Paguay Cuvi, M. H. (2015). Análisis de Algoritmos Matemáticos de Criptografía Pública para

Mejorar el aprendizaje de la materia de Criptografía en la Carrera de Ingeniería en

Sistemas de la ESPOCH. Disponible en

<http://dspace.esPOCH.edu.ec/handle/123456789/4431#sthash.Jl1pnL3L.dpuf>

Paredes, G. G. (2006). Introducción a la Criptografía. Revista Digital Universitaria, 7.

Disponible en

http://www.revista.unam.mx/vol.7/num7/art55/jul_art55.pdf

Pérez Martínez, C. A. (2008). Estudio y desarrollo de una máquina enigma-software.

Disponible en

<http://repositorio.upct.es/bitstream/handle/10317/110/pfc1724.pdf?sequence=1&isAllowed=y>

SANS Consensus Policy Resource Community. (2014). End User Encryption Key Protection Policy.

<https://www.sans.org/security-resources/policies/general/pdf/end-user-encryption-key-protection-policy>

Seguinfo. (2007). Qué es RSA? Disponible en.

<https://seguinfo.wordpress.com/2007/09/14/%C2%BFque-es-rsa/>

Tanenbaum, A. S. (2009). Sistemas operativos modernos. Tercera Edición. Disponible en

<http://www.itsi.edu.ec/wp-content/uploads/2016/02/sistemas-operativos-modernos.pdf>

Universidad Autónoma de México – Facultad de Ingeniería. (2016). Fundamentos de Criptografía. Disponible en

<http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/3-gestion-de-claves/31-politicas-de-gestion-de-claves>

Velasco, R. D. V. (2006) Criptografía, una necesidad moderna. Disponible en

http://www.revista.unam.mx/vol.7/num7/art56/jul_art56.pdf

Vela, D. C. (2006). El correo electrónico: El nacimiento de un nuevo género. Disponible en

<http://pendientedemigracion.ucm.es/BUCM/tesis/fl1/ucm-t29391.pdf>

ANEXOS

ANEXO #1. ESTRUCTURA DE UNA POLITICA DE PROTECCION DE CLAVES ENCRYPTADAS PARA USUARIOS FINALES ELABORADO POR SANS

End User Encryption Key Protection Policy

Free Use Disclaimer: *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.*

Things to Consider: *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.*

Last Update Status: *Updated June 2014*

1. Overview

Encryption Key Management, if not done properly, can lead to compromise and disclosure of private keys use to secure sensitive data and hence, compromise of the data. While users may understand it's important to encryption certain documents and electronic communications, they may not be familiar with minimum standards for protection encryption keys.

2. Purpose

This policy outlines the requirements for protecting encryption keys that are under the control of end users. These requirements are designed to prevent unauthorized disclosure and subsequent fraudulent use. The protection methods outlined will include operational and technical controls, such as key backup procedures, encryption under a separate key and use of tamper-resistant hardware.

3. Scope

This policy applies to any encryption keys listed below and to the person responsible for any encryption key listed below. The encryption keys covered by this policy are:

- encryption keys issued by <Company Name>
- encryption keys used for <Company Name> business
- encryption keys used to protect data owned by <Company Name>

The public keys contained in digital certificates are specifically exempted from this policy.

4. Policy

All encryption keys covered by this policy must be protected to prevent their unauthorized disclosure and subsequent fraudulent use.

4.1 Secret Key Encryption Keys

Keys used for secret key encryption, also called symmetric cryptography, must be protected as they are distributed to all parties that will use them. During distribution, the symmetric encryption keys must be encrypted using a stronger algorithm with a key of the longest key length for that algorithm authorized in <Company Name>'s *Acceptable Encryption Policy*. If the

keys are for the strongest algorithm, then the key must be split, each portion of the key encrypted with a different key that is the longest key length authorized and the each encrypted portion is transmitted using different transmission mechanisms. The goal is to provide more stringent protection to the key than the data that is encrypted with that encryption key.

Symmetric encryption keys, when at rest, must be protected with security measures at least as stringent as the measures used for distribution of that key.

4.2 Public Key Encryption Keys

Public key cryptography, or asymmetric cryptography, uses public-private key pairs. The public key is passed to the certificate authority to be included in the digital certificate issued to the end user. The digital certificate is available to everyone once it issued. The private key should only be available to the end user to whom the corresponding digital certificate is issued.

4.2.1 <Company Name>'s Public Key Infrastructure (PKI) Keys

The public-private key pairs used by the <Company Name>'s public key infrastructure (PKI) are generated on the tamper-resistant smart card issued to an individual end user. The private key associated with an end user's identity certificate, which are only used for digital signatures, will never leave the smart card. This prevents the Infosec Team from escrowing any private keys associated with identity certificates. The private key associated with any encryption certificates, which are used to encrypt email and other documents, must be escrowed in compliance with

<Company Name> policies.

Access to the private keys stored on a <Company Name>issued smart card will be protected by a personal identification number (PIN) known only to the individual to whom the smart card is issued. The smart card software will be configured to require entering the PIN prior to any private key contained on the smart card being accessed.

4.2.2 Other Public Key Encryption Keys

Other types of keys may be generated in software on the end user's computer and can be stored as files on the hard drive or on a hardware token. If the public-private key pair is generated on smartcard, the requirements for protecting the private keys are the same as those for private keys associated with <Company Name>'s PKI. If the keys are generated in software, the end user is required to create at least one backup of these keys and store any backup copies securely. The user is also required to create an escrow copy of any private keys used for encrypting data and deliver the escrow copy to the local Information Security representative for secure storage.

The Infosec Team shall not escrow any private keys associated with identity certificates. All backups, including escrow copies, shall be protected with a password or passphrase that is compliant with <Company Name> *Password Policy*. Infosec representatives will store and protect the escrowed keys as described in the <Company Name> *Certificate Practice Statement Policy*.

4.2.2.1 Commercial or Outside Organization Public Key Infrastructure (PKI) Keys

In working with business partners, the relationship may require the end users to use public-private key pairs that are generated in software on the end user's computer. In these cases, the public-private key pairs are stored in files on the hard drive of the end user. The private keys are only protected by the strength of the password or passphrase chosen by the end user. For example, when an end user requests a digital certificate from a commercial PKI, such as VeriSign or Thawte, the end user's web browser will generate the key pair and submit the public key as part of the certificate request to the CA. The private key remains

in the browser's certificate store where the only protection is the password on the browser's certificate store. A web browser storing private keys will be configured to require the user to enter the certificate store password anytime a private key is accessed.

4.2.2.2 PGP Key Pairs

If the business partner requires the use of PGP, the public-private key pairs can be stored in the user's key ring files on the computer hard drive or on a hardware token, for example, a USB drive or a smart card. Since the protection of the private keys is the passphrase on the secret keying, it is preferable that the public-private keys are stored on a hardware token. PGP will be configured to require entering the passphrase for every use of the private keys in the secret key ring.

4.3 Hardware Token Storage

Hardware tokens storing encryption keys will be treated as sensitive company equipment, as described in <Company Name>'s *Physical Security policy*, when outside company offices. In addition, all hardware tokens, smartcards, USB tokens, etc., will not be stored or left connected to any end user's computer when not in use. For end users traveling with hardware tokens, they will not be stored or carried in the same container or bag as any computer.

4.4 Personal Identification Numbers (PINs), Passwords and Passphrases

All PINs, passwords or passphrases used to protect encryption keys must meet complexity and length requirements described in <Company Name>'s *Password Policy*.

4.5 Loss and Theft

The loss, theft, or potential unauthorized disclosure of any encryption key covered by this policy must be reported immediately to The Infosec Team. Infosec personnel will direct the end user in any actions that will be required regarding revocation of certificates or public-private key pairs.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

- Acceptable Encryption Policy
- Certificate Practice Statement Policy
- Password Policy
- Physical Security policy

7. Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:

<https://www.sans.org/security-resources/glossary-of-terms/>

- Certificate authority (CA)
- Digital certificate
- Digital signature
- Key escrow
- Plaintext
- Public key cryptography
- Public key pairs
- Symmetric cryptography

8. Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format

ANEXO #2. COTIZACIÓN DE LICENCIAS PARA EL USO DEL SERVICIO RMS DE MICROSOFT



Quito, 07 de enero de 2016

Ing.
Danilo Ninabanda
ASEO TOTAL SA
Presente.-

Estimado Danilo:

Es muy grato para ASICECUADOR presentar esta propuesta de Licencias Microsoft Right Management Services, la misma que cumple con los requerimientos solicitados por su empresa.

En las siguientes páginas podrá encontrar en forma detallada toda la información correspondiente a nuestra oferta.

Estamos atentos a solventar cualquier inquietud que pueda surgir de la presente propuesta.

Atentamente,

Carlos Aráuz G
Software Sales Specialist
ASIC Ecuador S.A





Objetivo

El objetivo del presente documento es detallar las licencias Microsoft, requeridas con el mejor valor y costo beneficio para la empresa.

Propuesta Comercial

Num. Part.	Descripción	Cant.	Precio Unit.	Precio Tot.
T98-02646	WinRightsMgmtSrvcsCAL 2012 SNGLOLP NL UsrCAL	5	\$ 55,62	\$ 278,10
			SUBTOTAL	\$ 278,10
			IVA	\$ 33,37
			TOTAL	\$ 311,47

Forma de Pago

El pago por la entrega de estas licencias deberá ser realizado de la siguiente manera:

- 100% a la entrega de las licencias

Tiempo de Entrega

El tiempo de entrega de los documentos de titularidad respectivos, será de 3 días calendario.