



UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

**CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES
DE COMUNICACIÓN**

**DISEÑO Y SIMULACIÓN DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA
BASADA EN EL ESTÁNDAR DE CERTIFICADOS DIGITALES X.509 A TRAVÉS
DE SOFTWARE LIBRE PARA UTILIZARLOS EN LA SEGURIDAD DEL CORREO
ELECTRÓNICO EN LA RED DE DATOS INTERNA DEL CUERPO DE
INGENIEROS DEL EJÉRCITO EN LA MATRIZ QUITO**

**PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA EN
ELECTRÓNICA Y REDES DE COMUNICACIÓN**

AUTOR: DAVID RICARDO VALENCIA DE LA TORRE

DIRECTOR: ING. CARLOS VÁSQUEZ

Ibarra, 2014



UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

**AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD
TÉCNICA DEL NORTE**

1. IDENTIFICACIÓN DE LA OBRA

La UNIVERSIDAD TÉCNICA DEL NORTE dentro del proyecto Repositorio Digital Institucional determina la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información:

DATOS DEL CONTACTO	
CÉDULA DE IDENTIDAD	1002849824
APELLIDOS Y NOMBRES	Valencia de la Torre David Ricardo
DIRECCIÓN	Calle 5 de Junio y 10 de Agosto - Ibarra
EMAIL	david_300587@hotmail.com
TELÉFONO FIJO	062631582
TELÉFONO MÓVIL	0997102289

DATOS DE LA OBRA	
TÍTULO	DISEÑO Y SIMULACIÓN DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA BASADA EN EL ESTÁNDAR DE CERTIFICADOS DIGITALES X.509 A TRAVÉS DE SOFTWARE LIBRE PARA UTILIZARLOS EN LA SEGURIDAD DEL CORREO ELECTRÓNICO EN LA RED DE DATOS INTERNA DEL CUERPO DE INGENIEROS DEL EJÉRCITO EN LA MATRIZ QUITO
AUTOR	Valencia de la Torre David Ricardo
FECHA	14 de Noviembre del 2014
PROGRAMA	Pregrado
TÍTULO POR EL QUE SE ASPIRA	Ingeniería en Electrónica y Redes de Comunicación
DIRECTOR	Ing. Carlos Vásquez

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, David Ricardo Valencia de la Torre, con cédula de identidad Nro. 1002849824, en calidad de autor y titular de los derechos patrimoniales del trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y el uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad de material y como apoyo a la educación, investigación y extensión, en concordancia con la ley de Educación Superior Artículo 143.

.....

Firma

Nombre: David Ricardo Valencia de la Torre

Cédula: 1002849824

Ibarra a los 14 días del mes de noviembre del 2014



UNIVERSIDAD TÉCNICA DEL NORTE

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, DAVID RICARDO VALENCIA DE LA TORRE, con cédula de identidad Nro. 1002849824, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor del trabajo de grado denominado: **“DISEÑO Y SIMULACIÓN DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA BASADA EN EL ESTÁNDAR DE CERTIFICADOS DIGITALES X.509 A TRAVÉS DE SOFTWARE LIBRE PARA UTILIZARLOS EN LA SEGURIDAD DEL CORREO ELECTRÓNICO EN LA RED DE DATOS INTERNA DEL CUERPO DE INGENIEROS DEL EJÉRCITO EN LA MATRIZ QUITO”**, que ha sido desarrollado para optar por el título de: **Ingeniero en Electrónica y Redes de Comunicación**, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En mi condición de autor me reservo los derechos morales de la obra antes mencionada, aclarando que el trabajo aquí descrito es de mi autoría y que no ha sido previamente presentado para ningún grado o calificación profesional.

En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.

.....

Firma

Nombre: David Ricardo Valencia de la Torre

Cédula: 1002849824

Ibarra a los 14 días del mes de noviembre del 2014

DECLARACIÓN

Yo **DAVID RICARDO VALENCIA DE LA TORRE** declaro bajo juramento que el trabajo aquí descrito es de mi autoría, y que éste no ha sido previamente presentado para ningún grado o calificación personal.

A través de la presente declaración cedo los derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Técnica del Norte, según lo establecido por las leyes de propiedad intelectual, reglamentos y normatividad vigente.

.....

David Ricardo Valencia de la Torre

Cédula: 1002849824

Ibarra a los 14 días del mes de noviembre del 2014

CERTIFICACIÓN

Certifico, que el presente trabajo de titulación **“DISEÑO Y SIMULACIÓN DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA BASADA EN EL ESTÁNDAR DE CERTIFICADOS DIGITALES X.509 A TRAVÉS DE SOFTWARE LIBRE PARA UTILIZARLOS EN LA SEGURIDAD DEL CORREO ELECTRÓNICO EN LA RED DE DATOS INTERNA DEL CUERPO DE INGENIEROS DEL EJÉRCITO EN LA MATRIZ QUITO”** ha sido desarrollado en su totalidad por el señor David Ricardo Valencia de la Torre portador de la cédula de identidad 1002849824, bajo mi supervisión.

.....

Ing. Carlos Vásquez

DIRECTOR DEL PROYECTO

CERTIFICACIÓN

Quito, 19 de noviembre de 2014

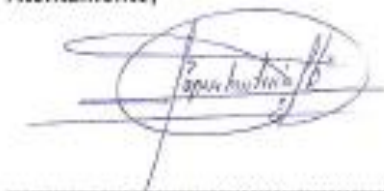
Señores
UNIVERSIDAD TÉCNICA DEL NORTE
Presente

De mis consideraciones.-

Siendo auspiciantes del proyecto de tesis del egresado DAVID RICARDO VALENCIA DE LA TORRE con CI:1002849824 quien desarrollo su trabajo con el tema **DISEÑO Y SIMULACIÓN DE UN INFRAESTRUCTURA DE CLAVE PÚBLICA BASADA EN EL ESTÁNDAR DE CERTIFICADOS DIGITALES X.509 A TRAVÉS DE SOFTWARE LIBRE PARA UTILIZARLOS EN LA SEGURIDAD DEL CORREO ELECTRÓNICO EN LA RED DE DATOS INTERNA DEL CUERPO DE INGENIEROS DEL EJÉRCITO EN LA MATRIZ QUITO**, me es grato informar que se han superado con *satisfacción las pruebas técnicas y la revisión de cumplimiento de los requerimientos funcionales*, por lo que se recibe el proyecto como culminado y realizado por parte del egresado DAVID RICARDO VALENCIA DE LA TORRE. Una vez que hemos recibido la capacitación y documentación respectiva nos comprometemos a continuar utilizando el mencionado aplicativo en beneficio de nuestra institución.

El egresado DAVID RICARDO VALENCIA DE LA TORRE puede hacer uso de este documento para los fines pertinentes en la Universidad Técnica del Norte.

Atentamente;



TNTE. ESP. LÓPEZ B. MARCELO S.
JEFE DE TECNOLOGÍAS DE LA INFORMACIÓN
CUERPO DE INGENIEROS DEL EJÉRCITO - C.I.E.

DEDICATORIA

Este proyecto de titulación se lo dedico a mis padres Nelson y Mariana en gratitud a su enorme esfuerzo y apoyo brindado durante toda esta etapa de preparación, siendo los principales mentores en inculcar valores y ética ante cualquier instancia de la vida, convirtiéndose en un verdadero ejemplo de lucha y perseverancia.

David R. Valencia

AGRADECIMIENTOS

En especial a mis padres y hermanos por su inestimable apoyo durante todas las etapas de mi vida, mis agradecimientos y gratitud hacia ellos.

Al Ing. Carlos Vásquez, en calidad de director de este proyecto, por su buena voluntad, asesoría y comprensión prestadas, en beneficio de su desarrollo.

A la Universidad Técnica del Norte y a todos los docentes de la carrera por los conocimientos impartidos durante todo este proceso de formación personal y académica.

Al Departamento de Sistemas del Cuerpo de Ingenieros del Ejército, por su apertura y apoyo incondicional, principalmente al Ing. Freddy Chuquimarca, Ing. Karina Pérez, y al Capitán Braulio Moreno, por su confianza y ayuda oportuna.

A mi familia y amigos quienes indirectamente contribuyeron al desarrollo de este trabajo, con su amistad, confianza y ánimo inquebrantable.

David R. Valencia

CONTENIDO

ÍNDICE GENERAL

RESUMEN	XIX
ABSTRACT	XX
CAPÍTULO 1. ESTUDIO DEL ESTÁNDAR X.509 REFERENTE A LA INFRAESTRUCTURA DE CLAVE PÚBLICA	1
1.1. ASPECTOS DE SEGURIDAD EN REDES Y CRIPTOGRAFÍA	1
1.1.1. ANTECEDENTES	1
1.1.1.1. Arquitectura de la Seguridad.....	2
1.1.1.1.1. Capas de Seguridad	3
a. Capa Seguridad de Infraestructura.....	4
b. Capa Seguridad de Servicios.....	4
c. Capa Seguridad de Aplicaciones.....	4
1.1.1.1.2. Planos de Seguridad	5
a. Plano de Gestión	5
b. Plano de Control.....	5
c. Plano de Usuario de Extremo.....	5
1.1.1.1.3. Dimensiones o Servicios de la Seguridad	6
a. Privacidad y Confidencialidad de Datos	6
b. Integridad de Datos.....	6
c. Disponibilidad.....	7
d. Autenticación	7
e. No Repudio.....	8
f. Control de Acceso.....	8
g. Seguridad de la Comunicación	8
1.1.1.2. Modelos de Seguridad.....	9
1.1.1.2.1. Seguridad por Obscuridad.....	9

1.1.1.2.2.	Seguridad del perímetro.....	9
1.1.1.2.3.	Seguridad en Profundidad.....	10
1.1.2.	CRIPTOGRAFÍA.....	11
1.1.2.1.	Criptosistema.....	11
1.1.2.1.1.	El tipo de operaciones empleadas para cifrar el texto plano.....	12
1.1.2.1.2.	La cantidad de datos que son procesados	12
1.1.2.1.3.	Las claves empleadas.....	12
1.1.2.2.	Simétricos o de Clave Privada	13
1.1.2.2.1.	Algoritmos de Cifrado Simétricos.....	14
a.	Data Encryption Standard (DES).....	14
b.	Advanced Encryption Standard (AES).....	14
c.	International Data Encryption Algorithm (IDEA).....	15
d.	RC4.....	16
e.	Variantes de DES	16
1.1.2.3.	Asimétricos o de Clave Pública.....	17
1.1.2.3.1.	Algoritmos de Cifrado Asimétricos.....	18
a.	RSA.....	18
b.	Diffie Hellman.....	20
c.	ElGamal.....	22
d.	DSA (Digital Signature Algorithm)	24
1.1.2.4.	Criptoanálisis	26
1.1.3.	FIRMA DIGITAL	26
1.1.3.1.	Funciones Resumen.....	27
1.1.3.1.1.	MD5 (Message Digest 5).....	30
1.1.3.1.2.	SHA-1 (Secure Hash Algorithm – version 1)	31
1.1.4.	DISTRIBUCIÓN Y ADMINISTRACIÓN DE CLAVES.....	33
1.2.	INFRAESTRUCTURA DE CLAVES PÚBLICAS (PKI)	35
1.2.1.	COMPONENTES DE LA PKI	35

1.2.1.1.	Autoridad de Certificación (Certification Authority - CA).....	35
1.2.1.2.	Autoridad de Registro (Registration Authority - RA).....	37
1.2.1.3.	Autoridad de Sellado de Tiempo (Time Stampig Authority - TSA)	39
1.2.1.4.	Certificado Digital	41
1.2.1.4.1.	Tipos de Certificados	43
1.2.1.5.	Directorio de Publicación de Certificados	43
1.2.1.5.1.	Lista de Revocación de Certificados (CRL).....	44
1.2.1.6.	Usuario Suscriptor	46
1.2.2.	FUNCIONAMIENTO DE UNA PKI	46
1.2.3.	APLICACIONES DE LA PKI	49
1.2.4.	ASPECTOS LEGALES DE LA PKI	49
1.3.	CORREO ELECTRÓNICO	53
1.3.1.	ESTRUCTURA DE UNA DIRECCIÓN DE CORREO ELECTRÓNICO	53
1.3.2.	COMPONENTES Y FUNCIONAMIENTO	55
1.3.2.1.	SMTP (Simple Mail Transport Protocol)	58
1.3.2.2.	POP3 (Post Office Protocol v3).....	60
1.3.2.3.	IMAP (Internet Message Access Protocol)	62
1.3.3.	SEGURIDAD EN CORREO ELECTRÓNICO	64
1.3.3.1.	S/MIME (SECURE / MULTIPURPOSE INTERNET MAIL EXTENSIONS)	65
1.3.3.1.1.	Data	66
1.3.3.1.2.	SignedData.....	66
1.3.3.1.3.	EnvelopedData	66
1.3.3.2.	PGP (PRETTY GOOD PRIVACY)	70
	CAPÍTULO 2. ANÁLISIS SITUACIONAL DE LA RED INTERNA DE DATOS DE LA INSTITUCIÓN	72
2.1.	CUERPO DE INGENIEROS DEL EJÉRCITO (CEE).....	72
2.1.1.	MISIÓN INSTITUCIONAL	72
2.1.2.	VISIÓN AL 2021.....	72
2.2.	DESCRIPCIÓN FÍSICA.....	73

2.2.1.	DISTRIBUCIÓN DE ÁREAS.....	74
2.3.	DESCRIPCIÓN DE LA RED.....	76
2.3.1.	BACKBONE Y CABLEADO HORIZONTAL	80
2.4.	DESCRIPCIÓN DE SERVICIOS.....	83
2.4.1.	CORREO ELECTRÓNICO.....	83
2.4.2.	DNS Y DIRECTORIO	85
2.4.3.	WEB	85
2.4.4.	TELEFONÍA IP	86
2.4.5.	ANTIVIRUS	86
2.5.	ENLACES WAN.....	87
2.6.	MECANISMOS DE SEGURIDAD	87
CAPÍTULO 3.	DISEÑO DE LA INFRAESTRUCTURA PKI Y DE LA PLATAFORMA DE CORREO ELECTRÓNICO.....	91
3.1.	CRITERIOS DE DISEÑO.....	91
3.2.	INFAESTRUCTURA DE CLAVE PÚBLICA PKI	101
3.2.1.	ARQUITECTURA DE LA PKI	101
3.2.2.	SOFTWARE PARA EL DISEÑO DE LA PKI.....	105
3.2.2.1.	EJBCA	107
3.2.2.1.1.	Arquitectura	108
3.2.2.2.	Herramientas de Software Complementario	110
3.2.3.	DESPLIEGE DE LA PKI	111
3.2.3.1.	Servidor de Dominio – DNS	111
3.2.3.1.1.	Virtualización.....	112
3.2.3.2.	Jerarquía PKI.....	113
3.2.3.2.1.	Diseño del Certificado Digital	114
3.2.3.3.	Iniciar la Operación de la Entidad Certificadora.....	116
3.2.4.	DIMENSIONAMIENTO DE HARDWARE	117
3.2.4.1.	Dimensionamiento del Procesador	118

3.2.4.2.	Dimensionamiento del Disco Duro.....	121
3.2.4.3.	Dimensionamiento de la Memoria RAM.....	122
3.3.	SISTEMA DE CORREO ELECTRÓNICO.....	122
3.3.1.	SOFTWARE PARA EL SISTEMA DE CORREO	123
3.3.1.1.	El Proyecto Zimbra - Zimbra Collaboration Suite	127
3.3.1.1.1.	Arquitectura	127
a.	MTA	128
b.	Core	128
c.	LDAP (OpenLDAP).....	128
d.	Store	128
e.	SNMP y Logger.....	128
3.3.2.	DESPLIEGUE DEL SISTEMA DE CORREO	129
3.3.2.1.	Interfaces de Administración y Webmail de Zimbra.....	130
3.3.2.2.	Clase de Servicio (COS).....	131
3.3.2.3.	Certificación del servidor Zimbra	132
3.3.2.4.	Migración de las Cuentas de Correo del Servidor Exchange hacia Zimbra	135
3.3.3.	DIMENSIONAMIENTO DE HARDWARE	137
3.3.3.1.	Dimensionamiento del Procesador.....	138
3.3.3.2.	Dimensionamiento del Disco Duro.....	140
3.3.3.3.	Dimensionamiento de la Memoria RAM.....	142
CAPÍTULO 4.	PRUEBAS DE FUNCIONAMIENTO	143
4.1.	PROCESO DE CERTIFICACIÓN	143
4.1.1.	REGISTRO.....	144
4.1.2.	CONFIAR EN LA CA RAÍZ DE LA PKI	144
4.1.2.1.	Instalación del Certificado.....	145
4.1.3.	EMISIÓN E INSTALACIÓN.....	146
4.2.	EJECUCIÓN DEL SISTEMA DE CORREO ELECTRÓNICO	149
4.2.1.	CREACIÓN DE UNA CUENTA DE USUARIO.....	149

4.2.2.	CONFIGURACIÓN DE LA CUENTA	149
4.2.3.	CONFIGURAR EL CLIENTE DE CORREO PARA ACTIVAR LOS MECANISMOS DE CIFRADO Y FIRMA DIGITAL	152
4.2.4.	OBTENER LOS CERTIFICADOS DE LOS USUARIOS DE LA PKI.....	153
4.3.	ESCENARIOS DE PRUEBA.....	159
4.3.1.	CAPTURA DE PAQUETES Y ANÁLISIS DEL PROTOCOLO SMTP	160
4.3.2.	COMPORTAMIENTO ANTE CERTIFICADOS CADUCADOS.....	164
4.3.3.	COMPORTAMIENTO ANTE CERTIFICADOS REVOCADOS.....	166
CAPÍTULO 5. PRESUPUESTO REFERENCIAL.....		169
5.1.	ANÁLISIS DE COSTOS	169
5.1.1.	COSTOS DEL EQUIPAMIENTO	169
5.1.1.1.	Análisis del costo referencial de hardware de los servidores	169
5.1.1.2.	Análisis del costo referencial del software de los servicios	171
5.1.2.	COSTOS DE IMPLEMENTACIÓN	171
5.1.3.	COSTOS DE ADMINISTRACIÓN	172
5.1.4.	PRESUPUESTO REFERENCIAL DEL PROYECTO	172
CAPÍTULO 6. CONCLUSIONES Y RECOMENDACIONES		174
6.1.	CONCLUSIONES	174
6.2.	RECOMENDACIONES	177
REFERENCIAS BIBLIOGRÁFICAS		179
ANEXO A. GENERACIÓN DE CONTRASEÑAS ROBUSTAS		185
ANEXO B. AC Y AR LEGALIZADOS EN ECUADOR.....		189
ANEXO C. INSTALACIÓN DE EJBCA VERSIÓN 4.0.10		192
ANEXO D. INSTALACIÓN Y CONFIGURACIÓN DE BIND9		222
ANEXO E. CONFIGURACIÓN DE EJBCA VERSIÓN 4.0.10.....		229
ANEXO F. INSTALACIÓN DE ZIMBRA VERSIÓN 8.0.5 GA.....		257
ANEXO G. MIGRACIÓN DE LAS CUENTAS DE CORREO ACTUAL EXCHANGE A ZIMBRA SERVER.....		284
ANEXO H. MANUAL DE ADMINISTRADOR.....		347

ANEXO I. MANUAL DE USUARIO348

ÍNDICE DE FIGURAS

CAPÍTULO I

Figura 1. Elementos de la Arquitectura de Seguridad según UIT-T X.805.....	3
Figura 2. Esquema de Cifrado Simétrico	13
Figura 3. Cifrado de Información empleando Algoritmos Asimétricos.....	17
Figura 4. Generación de Claves, Cifrado y Descifrado de un mensaje mediante el algoritmo RSA.....	19
Figura 5. Intercambio de claves mediante el algoritmo Diffie-Hellman	21
Figura 6. Generación de Claves, Cifrado, Descifrado y Firma Digital de un mensaje mediante el algoritmo ElGamal.....	23
Figura 7. Proceso de DSA para generar el par clave y Firmar Digitalmente un mensaje.....	25
Figura 8. Esquema de la Firma Digital empleando Algoritmos Asimétricos y Funciones Resumen.....	28
Figura 9. Diagrama de Funcionamiento de las Funciones Hash.....	29
Figura 10. Conformación de la longitud del mensaje m	30
Figura 11. Arquitectura Jerárquica de Certificación.....	36
Figura 12. Registro Presencial	38
Figura 13. Registro Remoto.....	39
Figura 14. Esquema del Sellado de Tiempo.....	40
Figura 15. Tipos de Certificados Digitales	43
Figura 16. Funcionamiento de los componentes de un entorno PKI.....	47
Figura 17. Funcionamiento del Protocolo OSCP	48
Figura 18. Estructura de una dirección electrónica.....	54
Figura 19. Estructura y Funcionamiento del Correo Electrónico	56
Figura 20. Proceso de envío y recepción de un mensaje de datos a través de correo electrónico.....	57
Figura 21. Conexión SMTP.....	61
Figura 22. Funcionamiento de IMAP.....	63

CAPÍTULO II

Figura 23. Diagrama de la Topología Lógica de la Red de Datos del CEE - Quito.....	78
Figura 24. Diagrama de Backbone de la Red de Datos del CEE - Quito.....	81

CAPÍTULO III

Figura 25. Proceso de certificación en el entorno PKI del CEE - Quito.....	93
Figura 26. Interacción del Usuario, la PKI y el Sistema de Correo en el entorno del CEE – Mensaje Firmado	98

Figura 27. Interacción del Usuario, la PKI y el Sistema de Correo en el entorno del CEE – Mensaje Cifrado (Sobre Digital)	99
Figura 28. Repositorio de Certificados Digitales de Windows 7 Ultimate - Navegador Google Chrome	102
Figura 29. Arquitectura de EJBCA.....	109
Figura 30. Virtualización de Servidores	112
Figura 31. Visualización de la interfaz de administración	130
Figura 32. Visualización de la interfaz webmail – Creación de un correo.....	131
Figura 33. Alternativas para sustituir el certificado digital predeterminado de zimbra	132
Figura 34. Parámetros que identifican y personalizan al certificado SSL de zimbra	133

CAPÍTULO IV

Figura 35. Generar una solicitud de firma de certificado - CSR	134
Figura 36. Proceso de registro del usuario solicitante	144
Figura 37. Descargar el certificado de la CA Raíz	145
Figura 38. Administrador de Certificados de Google Chrome	146
Figura 39. Usuario y contraseña del solicitante	146
Figura 40. Establecer la longitud del par clave.....	147
Figura 41. Descifrar la clave criptográfica privada	147
Figura 42. Contraseña de protección de la clave privada	148
Figura 43. Certificado Personal instalado en el repositorio Windows visualizado empleando Google Chrome	148
Figura 44. Supervisar la ejecución de los servicios de zimbra.....	149
Figura 45. Creación de una cuenta de correo	150
Figura 46. Buzones administrados por el servidor Zimbra.....	150
Figura 47. Parámetros de configuración de la cuenta	151
Figura 48. Configuración de puertos	151
Figura 49. Habilitar las técnicas S/MIME de cifrado y firma digital	152
Figura 50. Certificado de firma digital	153
Figura 51. Enviar un mensaje firmado digitalmente	154
Figura 52. Contraseña de protección de la clave privada - emisor	154
Figura 53. Comprobación de la firma del mensaje	155
Figura 54. Agregar un contacto incluyendo su certificado.....	156
Figura 55. Envío de un mensaje cifrado	156
Figura 56. Contraseña para utilizar la clave privada	157
Figura 57. Visualizar el mensaje cifrado	157

Figura 58. Mensaje cifrado que contiene documentos adjuntos.....	158
Figura 59. Visualizar un mensaje cifrado con documentos adjuntos.....	158
Figura 60. Visualizar un mensaje firmado y cifrado	159
Figura 61. Mensaje sin ningún tipo de protección.....	160
Figura 62. Captura SMTP con Wireshark de un mensaje en texto plano.....	161
Figura 63. Mensaje Cifrado	161
Figura 64. Captura SMTP con Wireshark de un mensaje cifrado	162
Figura 65. Mensaje cifrado transferido por un canal protegido por TLS	163
Figura 66. Captura SMTP con Wireshark de un mensaje cifrado - TLS activado.....	163
Figura 67. Firma Digital invalidada	165
Figura 68. Certificado Digital caducado.....	165
Figura 69. Intentar firmar un mensaje con un certificado revocado	166
Figura 70. Vigencia y Número de Serie del Certificado	167
Figura 71. CRL actualizada publicada por la CA.....	167

ÍNDICE DE TABLAS

CAPÍTULO I

Tabla 1. Descripción de características importantes de los algoritmos simétricos más usuales.....	14
Tabla 2. Valores predefinidos para los registros de MD5	31
Tabla 3. Valores predefinidos para los registros de SHA-1	32
Tabla 4. Valores predefinidos para las constantes de cada función de SHA-1	33
Tabla 5. Formato de Certificados Digitales según la recomendación UIT-T X.509.....	42
Tabla 6. Formato de CRL según la recomendación UIT-T X.509.....	45
Tabla 7. Descripción del campo código de razón según UIT-T X.509.....	46
Tabla 8. Algunos Servicios y Protocolos que emplean Certificados Digitales	50
Tabla 9. Ejemplos de dominios de nivel superior.....	55
Tabla 10. Comandos usuales que emplea SMTP	59
Tabla 11. Códigos de Respuesta del Servidor SMTP	60
Tabla 12. Estructura PKCS#7 de un mensaje S/MIME firmado digitalmente.....	67
Tabla 13. Estructura PKCS#7 de un mensaje S/MIME contenido en un sobre digital.....	69

CAPÍTULO II

Tabla 14. Distribución Departamental y Terminales de Red – Edificio	74
Tabla 15. Distribución Departamental y Terminales de Red – Campamento	75
Tabla 16. Switch Capa 3 – Especificaciones Técnicas.....	76
Tabla 17. Firewall - Características de Hardware y Software.....	79
Tabla 18. UPS – Especificaciones Técnicas	79
Tabla 19. Características de Hardware.....	84
Tabla 20. Grupos de Trabajo del CEE - Quito	88

CAPÍTULO III

Tabla 21. Componentes Estructurales necesarios para desplegar la PKI del CEE	92
Tabla 22. Descripción de las Soluciones Open Source en entornos PKI.....	106
Tabla 23. Software complementario para la compilación e instalación de EJBCA	110
Tabla 24. Nombre Distintivo que contendrán los certificados del CEE.....	115
Tabla 25. Usos para los que serán emitidos los certificados del CEE.....	116
Tabla 26. Soluciones Linux que permiten implementar un sistema de correo electrónico.....	125
Tabla 27. Componentes de la Arquitectura Zimbra Server	128
Tabla 28. Requerimientos de Hardware - Zimbra Server	138
Tabla 29. Tamaño de los buzones de usuario - Exchange	140

Tabla 30. Cálculo de la Capacidad de Almacenamiento.....	141
--	-----

CAPÍTULO V

Tabla 31. Características de Hardware del Servidor PKI	170
--	-----

Tabla 32. Presupuesto Referencial del Proyecto.....	173
---	-----

RESUMEN

El presente proyecto consiste en el diseño de una Infraestructura de Clave Pública que emita y gestione Certificados Digitales basados en el estándar X.509, para utilizarlos en la seguridad de la información transferida por el correo electrónico institucional, en el entorno de la red de datos interna del “Cuerpo de Ingenieros del Ejército” localizado en la ciudad de Quito.

El primer capítulo expone los fundamentos teóricos referente a los principales mecanismos de seguridad de la información, para comprender el funcionamiento de la Infraestructura de Clave Pública (PKI), y las técnicas de aplicación de los certificados digitales durante el proceso de transferencia del correo electrónico.

En el segundo capítulo se analizará la situación actual de la red de datos interna del “Cuerpo de Ingenieros del Ejército”, para establecer los requerimientos actuales y futuros a ser considerados en el diseño de la Infraestructura PKI, y en la plataforma de correo electrónico.

En el tercer capítulo se diseñará la Infraestructura de Clave Pública, y la plataforma de correo electrónico que provea los servicios actuales y soporte mecanismos de protección en capa transporte (SSL/TLS); esto implica la simulación de cada uno de estos servicios para efectuar las pruebas de funcionamiento.

En el cuarto capítulo se efectuarán las pruebas de funcionamiento de la PKI, conjuntamente con la plataforma de correo electrónico, para verificar su operatividad y mediante el análisis de resultados determinar si se ha podido garantizar la transferencia fiable de mensajes de correo electrónico institucional, que es el principal propósito de este proyecto.

El quinto capítulo expone un presupuesto referencial de las herramientas de hardware y software utilizadas en el desarrollo de este proyecto, de tal manera que sirva como base para una futura implementación.

Finalmente, el sexto capítulo contiene las conclusiones y recomendaciones establecidas durante el desarrollo de este proyecto.

ABSTRACT

This project involves the design of a Public Key Infrastructure that issue and manage Digital Certificates based on the X.509 Standard. Such certificates will be used in the information security that is transferred via institutional e-mail in the internal data network environment of the “Cuerpo de Ingenieros del Ejército” located in the city of Quito.

The first chapter presents the theoretical foundations concerning the main information security mechanisms. In order to understand the operation of the Public Key Infrastructure (PKI) and the digital certificates’ application techniques during the email’s transferring process.

In the second chapter the actual internal data network current status pertaining to the “Cuerpo de Ingenieros del Ejército” will be analyzed; so that the current and future requirements to be considered in designing the PKI Infrastructure and email’s platform are fully established.

In the third chapter the Public Key Infrastructure will be designed, as well the email platform that provides the current services and support protection mechanisms in transport layer (SSL/TLS). This stage involves the simulation of each of these services which allow running of performance tests.

In the fourth chapter, the performance tests of the PKI shall be made, together with the email platform, to verify its functionality. Consequently through results analysis, determine if a reliable institutional email messaging transference has been reached, being this project’s main purpose.

Chapter fifth presents a referential hardware and software tools budget employed in developing this project, such that it acts as the basis for future implementation.

Finally, the sixth chapter contains the conclusions and recommendations made during the development of this project.

CAPÍTULO 1. ESTUDIO DEL ESTÁNDAR X.509

REFERENTE A LA INFRAESTRUCTURA DE CLAVE

PÚBLICA

1.1.ASPECTOS DE SEGURIDAD EN REDES Y CRIPTOGRAFÍA

1.1.1. ANTECEDENTES

Desde tiempos remotos ha existido la necesidad de proteger la información para evitar que ésta experimente cualquier tipo de modificación imprevista o para mantener la privacidad de datos personales, considerando que el valor de los mismos depende de la importancia que tengan para cada persona u organización.

Antes del uso de sistemas informáticos y redes de comunicación, la seguridad de la información fue implantada utilizando medios físicos con acceso restringido, pero con el desarrollo tecnológico experimentado se generaron diversas tendencias de comunicación, que renovaron los recursos limitados bajo los cuales se desarrollaban las actividades laborales en las organizaciones.

El internet es uno de los factores importantes que han influido en este desarrollo, permitiendo compartir cualquier tipo de información, efectuar transacciones bancarias o pago de impuestos remotamente, o establecer negocios y comunicación con personas de cualquier parte del mundo haciendo uso del correo electrónico y las redes sociales.

Esto ha mejorado notablemente las condiciones de vida de las personas, descartando en ocasiones la necesidad de movilizarse físicamente hasta ciertos lugares para realizar sus trámites personales.

Sin embargo, para aprovechar favorablemente este aporte tecnológico, es necesario determinar que las personas que intervienen en una comunicación, en realidad sean quienes dicen ser, o que la información en trayecto sea manipulada únicamente por personas hacia quienes fue destinada. Lamentablemente de manera simultánea al desarrollo tecnológico, también evolucionan técnicas delictivas para tratar de robar o manipular información y producir daños o pérdidas de cualquier tipo.

Debido a esto y a diversos riesgos a los cuales están expuestos en la actualidad los sistemas informáticos y las redes de comunicación, la seguridad de la información es cada día más trascendental.

1.1.1.1. Arquitectura de la Seguridad

La seguridad de la información es un conjunto de técnicas que garantizan “protección a los sistemas informáticos con el propósito de preservar objetivos de integridad, disponibilidad y confidencialidad de los recursos de dichos sistemas (incluye hardware, software, firmware, información / datos y telecomunicaciones)” (Stallings, 2006, p.9, traducido).

Para ello se ha establecido una arquitectura cuya aplicación sea posible en cualquier tipo de redes de comunicación (de voz o de datos), sin importar la tecnología que éstas utilicen (inalámbrica, cable u óptica), con la intención de proteger los datos que están o van a ser

almacenados en dispositivos y sistemas de red, como también a aquellos en tránsito a través de la misma.

Esta arquitectura de seguridad está integrada por segmentos, mediante los cuales se identifican los riesgos, la infraestructura y las aplicaciones de red que se deben proteger, para garantizar seguridad en las comunicaciones extremo a extremo. Los segmentos que conforman esta arquitectura son las capas, los planos y las dimensiones de seguridad (véase Figura 1).

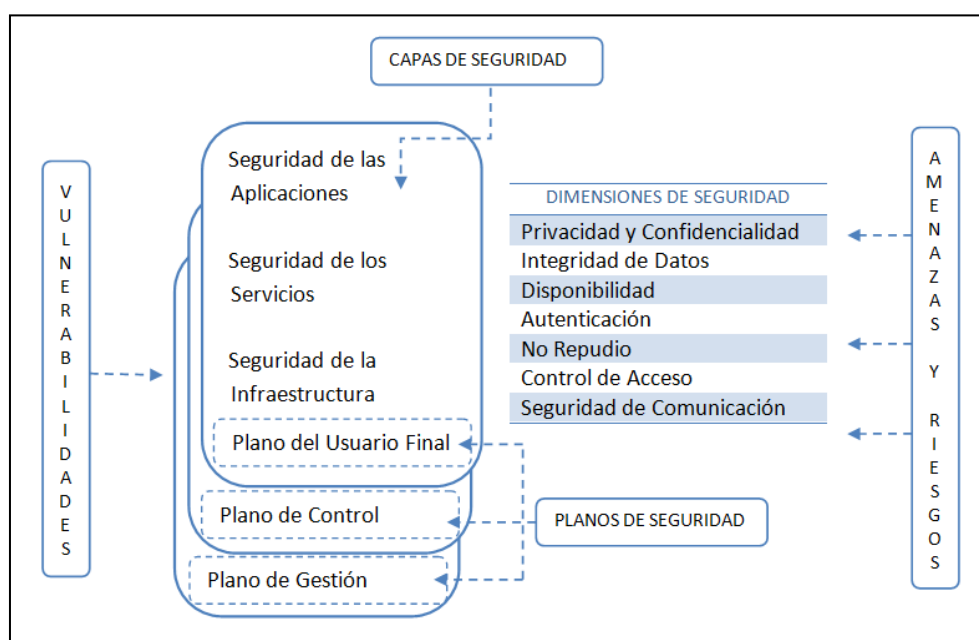


Figura 1. Elementos de la Arquitectura de Seguridad según UIT-T X.805

Fuente: Adaptado de UIT-T. (2003). La Seguridad de las Telecomunicaciones y las Tecnologías de la Información. Recuperado de <http://www.itu.int/itudoc/itu-t/85097-es.pdf>

1.1.1.1.1. Capas de Seguridad

Las capas son consideraciones sobre los dispositivos de red y sistemas, que permiten enfocar desde distintos puntos de vista sus vulnerabilidades, y definir medidas de seguridad que las compensen.

a. Capa Seguridad de Infraestructura

Esta capa es la encargada de la seguridad en los dispositivos de transmisión como routers y switches, en sistemas que conforman la red como servidores, y enlaces de comunicación (Wireless).

b. Capa Seguridad de Servicios

Enfocada en proteger los servicios de red proporcionados a los usuarios, como por ejemplo servicios de nombre de dominio, servicios de alojamiento web, servicios de autenticación AAA¹, servicios de telefonía IP (VoIP²), calidad de servicio (QoS), servicios de correo electrónico, entre otros; considerando técnicas delictivas como la denegación de servicios (DoS – Denial of Service) que intentan paralizarlos total o parcialmente.

c. Capa Seguridad de Aplicaciones

Las aplicaciones son aquellas actividades originadas por los servicios de red, y esta capa proporciona seguridad a toda esta gama de aplicaciones a las que los usuarios tienen acceso a través de la red, como navegación web, manejo de correo electrónico, transferencia de archivos FTP³, etc.

¹ **Authentication, Authorization and Accounting** - Autenticación, Autorización y Contabilidad

² Voz sobre IP

³ **File Transfer Protocol** - Protocolo de Transferencia de Archivos

1.1.1.1.2. Planos de Seguridad

Este segmento se refiere a la seguridad de las actividades que se ejecutan en una red, estableciéndose para ello tres planos que representan a dichas actividades: de gestión de red, de control de red, y de usuario extremo.

a. Plano de Gestión

Este plano se refiere a las funciones de operación, administración y mantenimiento de todos los elementos que integran una red de telecomunicaciones, y el aprovisionamiento de sus servicios dentro de infraestructuras multifabricantes; es decir, las funciones OAM&P (Operation, Administration, Maintenance and Provisioning).

b. Plano de Control

El plano control protege la información de señalización generada en dispositivos como routers o switches, para enrutar o conmutar de forma eficiente el tráfico de la red, manteniendo una alta disponibilidad y evitando al máximo los cuellos de botella debido a la sobreutilización de rutas de circulación de tráfico.

c. Plano de Usuario de Extremo

Este plano de seguridad protege las actividades del usuario sobre la red, considerando el acceso a la misma y la utilización de los servicios de red a través de las aplicaciones.

1.1.1.1.3. Dimensiones o Servicios de la Seguridad

Las dimensiones de seguridad son medidas de protección contra las principales amenazas que ponen en riesgo la seguridad de la red.

a. Privacidad y Confidencialidad de Datos

La confidencialidad se refiere a proteger los datos de publicaciones no autorizadas, asegurando que únicamente los usuarios legítimos tengan acceso a ellos. Este principio se debe garantizar durante cada etapa de su procesamiento, tanto los que están almacenados en dispositivos y sistemas, como también aquellos que están en tránsito a través de la red. La implementación de la confidencialidad se lleva a cabo mediante técnicas de cifrado de datos, o el manejo de archivos protegidos por contraseñas.

La recomendación UIT-T X.805 refiere a la privacidad como el principio que protege información que se podría obtener analizando las actividades de los usuarios en la red, como los sitios web visitados, las direcciones IP, los DNS o la posición geográfica.

b. Integridad de Datos

Es la característica que garantiza la exactitud de los datos, protegiéndolos de modificaciones imprevistas o intentos de destrucción.

Algunas de las amenazas que pueden poner en riesgo la integridad de la información son los virus informáticos, fallos de hardware, de software o ataques informáticos. El mecanismo

de protección más habitual para salvaguardar este servicio de seguridad, es la aplicación de funciones resumen o hash⁴.

c. Disponibilidad

Se refiere a la característica de los sistemas y las redes para recuperarse ante cualquier interrupción o eventualidad de la manera más rápida, garantizando con ello el acceso oportuno y confiable a la información, servicios y aplicaciones.

Tanto la confidencialidad, integridad y disponibilidad se relacionan directamente, debido a que no tendría sentido que la información se encuentre almacenada intacta en el sistema, si los usuarios no pueden acceder a ella. Un ataque de denegación de servicio vulnera la disponibilidad de la información.

d. Autenticación

Son procesos que permiten demostrar que la identidad de una persona, aplicación, servicio, mecanismo o cualquier entidad que puede intervenir en una comunicación, es la deseada; evitando que fuentes de dudosa procedencia la suplanten.

⁴ Son funciones que generan a partir del mensaje original, secuencias de bits (resúmenes) que contienen menor información, y falsearlas resulta muy complicado.

e. No Repudio

Son estrategias que impiden la negación de eventos cuando en realidad fueron llevados a cabo, por ejemplo la transmisión, recepción, el acceso o la modificación de información, datos o archivos.

f. Control de Acceso

Esta dimensión de seguridad protege los recursos de la red ante accesos no autorizados, a través de controles que determinan que persona o entidad legítima, previamente identificada, tiene autorización para acceder a los recursos de red, y que actividades puede realizar sobre cierto recurso.

Esta protección es llevada a cabo mediante métodos de autenticación que se basan generalmente en algo que se puede tener, como una tarjeta con chip (chipcard o smartcard), alguna característica biológica de las personas, como la huella dactilar o la retina del ojo (biometría), o algo que se conoce, como una contraseña.

g. Seguridad de la Comunicación

Esta dimensión asegura el flujo de tráfico de la red, para que circule únicamente a través de la ruta establecida entre el emisor y el receptor, garantizando que en todo su trayecto no existan desviaciones o interceptación por parte de fuentes ilegítimas.

1.1.1.2. Modelos de Seguridad

Los modelos de seguridad son métodos y técnicas que defienden los recursos de las redes y sistemas, compensando sus vulnerabilidades y reduciendo el riesgo de que un ataque sea efectuado. Existen tres tipos de modelos:

1.1.1.2.1. Seguridad por Obscuridad

El principio de este modelo de seguridad es mantener en secreto el diseño o implementación de la red o sistema, pues de esta forma si nadie conoce su existencia, es poco probable que identifiquen sus vulnerabilidades o sea objeto de algún ataque.

La debilidad de este modelo radica en el número de personas que conozcan el secreto y la forma de mantener su privacidad, pues si fuese revelado el sistema o la red quedarán expuestos al análisis de debilidades y correr el riesgo de sufrir algún ataque.

1.1.1.2.2. Seguridad del perímetro

La seguridad perimetral está enfocada en defender los puntos de acceso que interconectan las redes internas con las externas, a través del uso de sistemas de seguridad. Para ello es primordial determinar los accesos (puertos de red) que son necesarios para habilitar las actividades cotidianas de los usuarios de la red interna, y mediante firewalls o proxys deshabilitar el resto de accesos disminuyendo el riesgo de potenciales ataques.

Además es posible utilizar sistemas de detección de intrusos conjuntamente con sistemas de monitoreo, para alertar al administrador de las invasiones que se pueden suscitar, y se tomen las medidas de seguridad pertinentes.

El problema de este modelo son los ataques realizados desde la red interna, o que algún sistema de seguridad falle, dejando totalmente vulnerable a la red. La seguridad no puede ser considerada como un absoluto, sino más bien como conjunto de sistemas y políticas que constantemente deben ser evaluados, mejorados y actualizados, para garantizar un nivel de protección de la red.

1.1.1.2.3. Seguridad en Profundidad

La defensa en profundidad supone que las medidas de seguridad implantadas para proteger ciertos recursos no son del todo fiables, y que en ocasiones van ser eludidas por algún atacante; es por ello que, el fundamento de este modelo es implantar un sistema de seguridad formado por varias capas, de esta forma se asegura que si una capa o nivel de protección es eludido, debe existir otro que pueda neutralizar el ataque, pues es poco probable que un ataque sea efectuado eludiendo cada nivel de protección sin que antes sea detectado.

Este modelo es el más sólido ya que al establecer varios niveles de protección, es posible independizar a las redes o sistemas dotándolos de recursos para protegerse por sí solos, considerando a cada uno como una isla que se protege a sí misma.

1.1.2. CRIPTOGRAFÍA

Es la ciencia que trata sobre técnicas de cifrado que permiten ocultar información para preservar su confidencialidad. Estas técnicas modifican (cifran) los mensajes de datos utilizando un algoritmo de cifrado y una clave o llave, de manera que puedan descifrarlos e interpretarlos únicamente quienes dispongan de la clave apropiada.

Mediante el uso de la criptografía es posible garantizar ciertos servicios de seguridad de la información, como la confidencialidad (transformándolos en datos ilegibles), la integridad (utilizando funciones hash, el destinatario identifica si los mensajes sufrieron alguna modificación) y el no repudio (la única manera de descifrar el mensaje es con la llave apropiada, con ello se autentica el origen de dónde provino el mensaje, e implícitamente impide que niegue haberlo enviado).

1.1.2.1. Criptosistema

Un sistema criptográfico está integrado por un conjunto de mensajes que mediante algoritmos de cifrado y el uso de claves, pueden ser protegidos ante revelaciones fraudulentas. Todo criptosistema debe cumplir la condición, de que independientemente del algoritmo utilizado para cifrar un mensaje o la clave empleada, debe ser posible obtener nuevamente el mensaje original a través del uso de técnicas de descifrado y empleando las claves apropiadas.

Según (Stallings, 2006) los sistemas criptográficos se caracterizan de acuerdo a: las operaciones utilizadas para cifrar el texto plano⁵, las claves utilizadas y la cantidad de datos que pueden procesar.

1.1.2.1.1. El tipo de operaciones empleadas para cifrar el texto plano

Los algoritmos de cifrado basan su funcionamiento en dos principios: el primero consiste en reemplazar cada elemento del texto plano por otro (sustitución), en el otro en cambio no se reemplazan, sino más bien todos los elementos del texto plano son reordenados (transposición). Algunos algoritmos de cifrado para garantizar mayor protección, combinan estos dos principios y los aplican varias veces, la condición es que todas las operaciones que se apliquen deben ser reversibles para obtener nuevamente el mensaje original.

1.1.2.1.2. La cantidad de datos que son procesados

Existen algoritmos que dividen los mensajes originales en bloques de tamaño definidos, para luego cifrarlos (cifrado por bloques), otros algoritmos en lugar de dividirlos, los cifran continuamente bit a bit (cifrado de flujo).

1.1.2.1.3. Las claves empleadas

Si el emisor y el receptor usan la misma clave para cifrar y descifrar los mensajes, se llama cifrado simétrico o de clave privada; pero si usan claves distintas, se llama cifrado asimétrico o de clave pública.

⁵ Es el mensaje en su forma original

1.1.2.2. Simétricos o de Clave Privada

Un esquema de este tipo de sistemas criptográficos se muestra la Figura 2, en la que el usuario A genera un mensaje m que necesita enviar a B , cifra este mensaje utilizando la clave privada⁶ K_p y se lo envía $E_{K_p}(m)$ (los algoritmos simétricos combinan y reordenan los datos del mensaje, con los de la clave, para formar una secuencia ilegible); finalmente B descifra este mensaje utilizando la misma clave y obtiene el mensaje original.

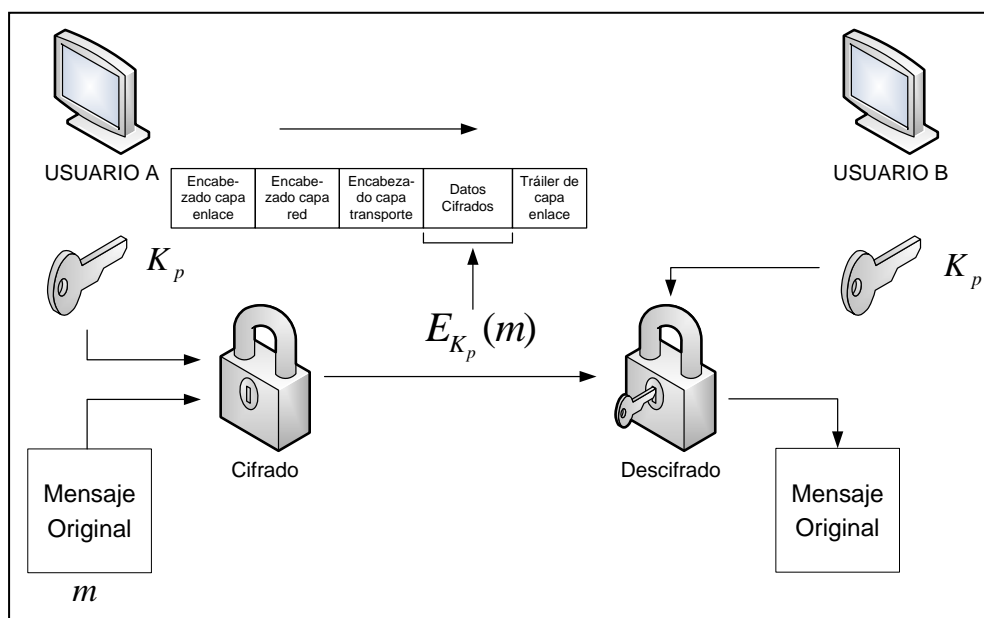


Figura 2. Esquema de Cifrado Simétrico

Fuente: Adaptado de Stallings, W. (2006). *Cryptography and Network Security Principles and Practice*. Recuperado de [http://evilzone.org/ebooks/cryptography-and-network-security-principles-\(5th-edition\)/](http://evilzone.org/ebooks/cryptography-and-network-security-principles-(5th-edition)/)

La fortaleza de estos criptosistemas radica en la privacidad de la clave, pero curiosamente, esta es una de sus principales vulnerabilidades, debido a la complejidad que involucra su distribución a través de canales inseguros, para que emisor y receptor puedan obtenerla. La Tabla 1 describe los algoritmos simétricos más usuales.

⁶ Clave de conocimiento personal.

1.1.2.2.1. Algoritmos de Cifrado Simétricos

Tabla 1. Descripción de características importantes de los algoritmos simétricos más usuales

ALGORITMO	DESARROLLO	CARACTERÍSTICAS	PROCESO DE CIFRADO	GENERACIÓN DE SUBCLAVES
a. Data Encryption Standard (DES)	Desarrollado con fundamento en el algoritmo LUCIFER creado por IBM.	Es un algoritmo de cifrado por bloques de 64 bits de longitud.	Se aplica una transposición para reorganizar los bits del mensaje.	Las subclaves se generan aplicando una transposición a la clave de 56 bits
	Implementado mediante hardware.	Utiliza una clave de 64 bits, pero son restados 8 usados como paridad.	Luego una ronda de operaciones que los transpone y sustituye con subclaves generadas, esta ronda se repite 16 veces.	Luego para cada ronda una operación de desplazamiento circular hacia la izquierda.
	En 1998 miembros de la EFF fabricaron una máquina que descifró un mensaje de datos cifrado con DES.		Finalmente se aplica una transposición que es inversa a la inicial y genera el texto cifrado de 64 bits.	Finalmente una transposición final, da como resultado una subclave de 48 bits. Se repite 16 veces.
b. Advanced Encryption Standard (AES)	Se llama Rijndael por sus creadores Joan Daemen y Vincent Rijmen, pero fue desarrollado con apoyo público.	Es un algoritmo de cifrado por bloques de longitud variable entre 128 a 256 bits (128 bits es el estándar)	Se realizan cuatro operaciones por cada ronda, el número de rondas depende de la longitud del mensaje: Una sustitución no lineal a cada byte de la matriz estado.	AES transporta los bytes del mensaje, uno a uno hacia una matriz estado de cuatro filas y variable número de columnas.

ALGORITMO	DESARROLLO	CARACTERÍSTICAS	PROCESO DE CIFRADO	GENERACIÓN DE SUBCLAVES
	A finales del 2000 sustituyó a DES declarándolo como estándar de cifrado.	Una clave variable de 128, 192 o 256 bits	<p>Un desplazamiento circular a la izquierda, de los bytes de cada fila de la matriz.</p> <p>Una operación mezclar columnas de la matriz.</p> <p>Finalmente una operación XOR ente ésta matriz, con la matriz de subclaves generada para cada ronda.</p>	<p>De forma similar la clave también es trasportada hacia otra matriz de clave.</p> <p>Para generar las subclaves se aplican operaciones de expansión y selección sobre la matriz de clave.</p> <p>Se genera una subclave para cada ronda.</p>
c. International Data Encryption Algorithm (IDEA)	<p>Desarrollado por Xuejia Lai y James Massey en los años 90.</p> <p>Es considerado un algoritmo bastante robusto, al resistir a diferentes técnicas de criptoanálisis.</p> <p>Además utiliza una longitud de clave adecuada, para dotarlo de seguridad frente a ataques de fuerza bruta.</p>	<p>Es un algoritmo que utiliza bloques de 64 bits de longitud.</p> <p>Cada bloque es dividido en cuatro segmentos iguales de 16 bits.</p> <p>Emplea una clave de 128 bits.</p> <p>Se generan 52 subclaves de 16 bits utilizadas durante todo el proceso (Z_1, Z_2, \dots, Z_{52}).</p>	<p>Cada ronda consta de operaciones como: Multiplicación, suma y función XOR, entre los cuatro segmentos del bloque de datos, y las seis primeras subclaves.</p> <p>Esta ronda se repite 8 veces y utiliza 48 subclaves, dando como resultado 4 sub-bloques. Finalmente:</p> <p>Multiplica el primer sub-bloque por Z_{49} Suma el segundo con Z_{50} Suma el tercero con Z_{51} Multiplica el cuarto por Z_{52}</p>	<p>La generación de las primeras 8 subclaves se realiza dividiendo la clave inicial en bloques iguales de 16 bits.</p> <p>Para las siguientes 8 se realiza un desplazamiento de 25 bits a la izquierda sobre la clave inicial, y se divide nuevamente.</p> <p>Mediante este proceso se obtienen las 52 subclaves.</p>

ALGORITMO	DESARROLLO	CARACTERÍSTICAS	APLICACIONES
d. RC4	<p>Fue desarrollado por Ron Rivest para la compañía de seguridad de datos RSA.</p> <p>Es de carácter privado, por lo que es necesario pagar por su utilización, en especial para usos comerciales.</p>	<p>Es un algoritmo de cifrado de flujo.</p> <p>Es usado para generar secuencias.</p> <p>Emplea una longitud de clave variable entre 1 a 256 bytes.</p>	<p>El código de funcionamiento de este algoritmo no se ha expuesto, pero se realizaron publicaciones anónimas que lo describen, debido al análisis de las secuencias generadas por este algoritmo.</p> <p>Es usado en aplicaciones como: seguridad en servidores y navegadores web mediante SSL/TLS, acceso seguro a redes inalámbricas mediante el protocolo WEP, o el más difundido WPA.</p>
e. Variantes de DES	<p>La debilidad de DES es que utiliza una clave de longitud muy corta, por ello se han desarrollado variantes para compensar esta vulnerabilidad.</p>	<p>Una de estas variantes es emplear varias veces el algoritmo DES, pero usando claves distintas, por ejemplo 3DES. En otra variante las subclaves que eran generadas a partir de la original, son sustituidas por claves independientes para cada ronda.</p>	

Fuente: Creado a partir de Lucena, L. M. J. (2009). Criptografía y Seguridad en Computadores. Recuperado de <http://es.scribd.com/doc/39400098/Criptografia#download>
 Stallings, W. (2006). Cryptography and Network Security Principles and Practice. Recuperado de [http://evilzone.org/ebooks/cryptography-and-network-security-principles-\(5th-edition\)/](http://evilzone.org/ebooks/cryptography-and-network-security-principles-(5th-edition)/)

1.1.2.3. Asimétricos o de Clave Pública

Estos criptosistemas resuelven el problema de distribución de la clave privada, de los sistemas simétricos, debido a que utilizan dos claves diferentes para cifrar mensajes de datos, una pública⁷ y una privada, pero que tienen una relación matemática (par clave).

La clave pública k_{pu} puede ser compartida abiertamente (sin cifrarse), con las personas con quienes se va a establecer comunicación, como lo hace el usuario B en la Figura 3; de forma que, cuando A necesite enviarle un mensaje que contenga cualquier tipo de información (texto, voz, video, etc.), pueda hacerlo, cifrándolo con la clave obtenida $E_{k_{pu}}(m)$. Por su parte B descifrará este mensaje utilizando únicamente su clave privada k_p , logrando con ello confidencialidad de la información.

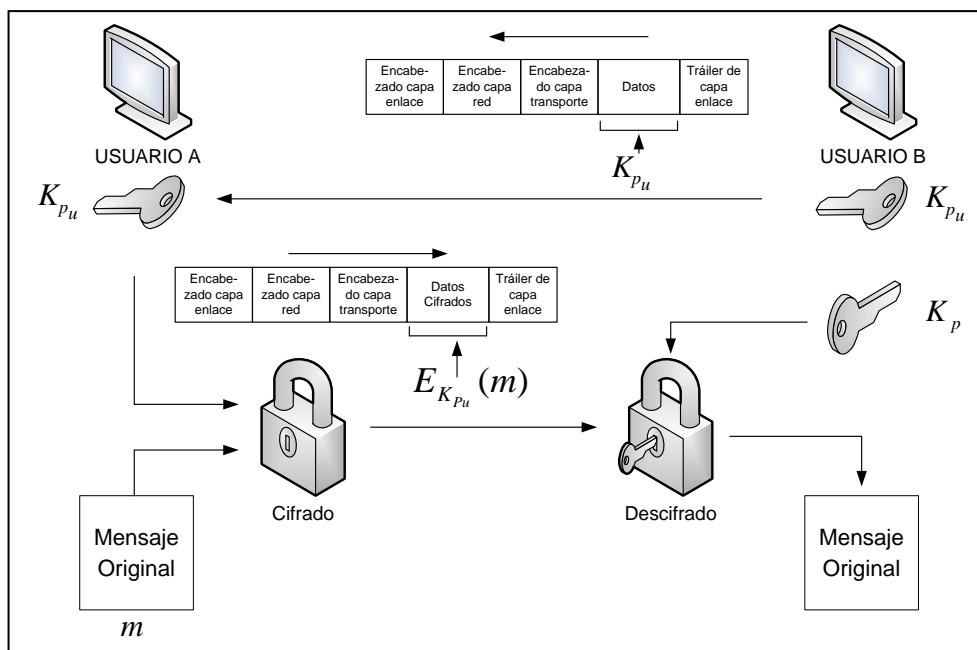


Figura 3. Cifrado de Información empleando Algoritmos Asimétricos

Fuente: Adaptado de Lucena, L. M. J. (2009). Criptografía y Seguridad en Computadores. Recuperado de <http://es.scribd.com/doc/39400098/Criptografia#download>

⁷ Clave que puede conocer cualquier entidad.

La utilización de este tipo de cifrado implica que emisor y receptor obtengan un par clave, la pública debe registrarse en un repositorio público o en un archivo de fácil acceso, para que el resto de usuarios puedan obtenerla y formar en conjunto un anillo de claves públicas; mientras que la privada es confidencial para cada propietario.

El requerimiento principal en estos sistemas es que el conocimiento de la clave pública no permita calcular su par, la privada, y la desventaja es que son necesarios muchos recursos computacionales para implementarlos, lo que significa que puede volver lentos a algunos sistemas o aplicaciones.

1.1.2.3.1. Algoritmos de Cifrado Asimétricos

Algunos de los algoritmos asimétricos más conocidos son los siguientes:

a. RSA

Es un algoritmo desarrollado para satisfacer el nuevo desafío de utilizar sistemas de clave pública, que impusieron los estudios de Diffie-Hellman, empleados para el intercambio de claves simétricas. Fue creado por Ronald Rivest, Adi Shamir y Leonard Adleman en 1977, y se mantuvo en evaluación y perfeccionamiento constante, hasta finales del 2000, año en el que fue publicado para usos comerciales; las primeras versiones de seguridad en correo electrónico PGP⁸, lo adoptaron como técnica de cifrado y firma digital, debido a su fiabilidad.

⁸ **Pretty Good Privacy** - Privacidad Bastante Buena

Para generar el par clave, se eligen aleatoriamente dos números primos diferentes p y q , cuyo producto n (módulo) es uno de los parámetros que conforman la clave pública; además, para proteger los mensajes cifrados con este algoritmo, p y q deben ser conservados en secreto, o de preferencia destruidos (véase Figura 4).

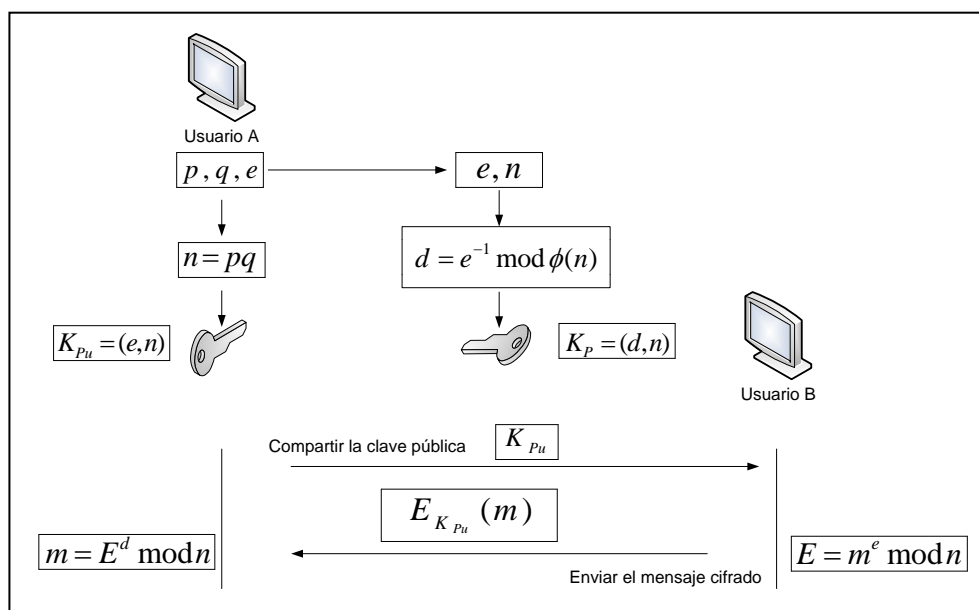


Figura 4. Generación de Claves, Cifrado y Descifrado de un mensaje mediante el algoritmo RSA

Fuente: Creado a partir de Lucena, L. M. J. (2009). Criptografía y Seguridad en Computadores. Recuperado de <http://es.scribd.com/doc/39400098/Criptografia#download>

También se debe establecer otro número primo e , el cual es combinado con n , para generar el valor de la clave pública K_{pu} , que desde este punto puede ser compartida abiertamente con quienes se desee establecer comunicación. El par clave RSA está integrado complementariamente por la clave privada K_p , para generarla, este algoritmo calcula d , y con el fin de evitar exponerla directamente, la combina con n . Este valor debe ser conservado en privado por su propietario, para garantizar la funcionalidad de este algoritmo.

El proceso para cifrar y descifrar un mensaje m con algoritmos asimétricos, se ilustra en la Figura 3, pero las operaciones que realiza RSA tanto para obtener un mensaje cifrado E en el extremo del emisor, como para descifrarlo y obtener el mensaje original m en el receptor, son las que se muestran en la Figura 4.

Las condiciones bajo las cuales se deben establecer p , q y e son:

- p y q deben ser números primos de gran longitud, como 512 o 1024 bits, con el propósito de fortalecer al algoritmo, ante ataques provenientes de cualquier técnica delictiva que intente vulnerarlo.
- $1 < e < \phi(n)$, también debe ser primo, siendo $\phi(n) = \phi(pq) = (p - 1)(q - 1)$, esta expresión representa la función de Euler.

Entonces, la única manera de descifrar un mensaje de datos RSA, es utilizando la clave privada, por ello los hackers orientan todos sus esfuerzos para lograr determinarla, aunque otra manera sería conociendo el valor de p y q , pero al tratarse de valores de gran longitud que son conservados en secreto, es computacionalmente imposible encontrarlos aleatoriamente; por tal motivo, es recomendable utilizar longitudes de 512 o 1024 bits para p y q , garantizando longitudes de 1024 o 2048 bits respectivamente, para las claves RSA.

b. Diffie Hellman

Este algoritmo surgió de estudios de matemática modular, realizados por Whitfield Diffie y Martin Hellman, en busca del desarrollo de una técnica que permita el intercambio de claves

secretas a través de canales de comunicación inseguros. Esta técnica tomó el nombre de algoritmo de Diffie-Hellman, y fue el origen de la criptografía de clave pública.

El fundamento de este algoritmo es utilizar la función modular $\alpha^x \pmod{p}$, por lo que se debe elegir inicialmente los valores de la base α , y de la variable del módulo p ; estos valores pueden generarlos emisor o receptor, y darlos a conocer abiertamente al otro (véase Figura 5).

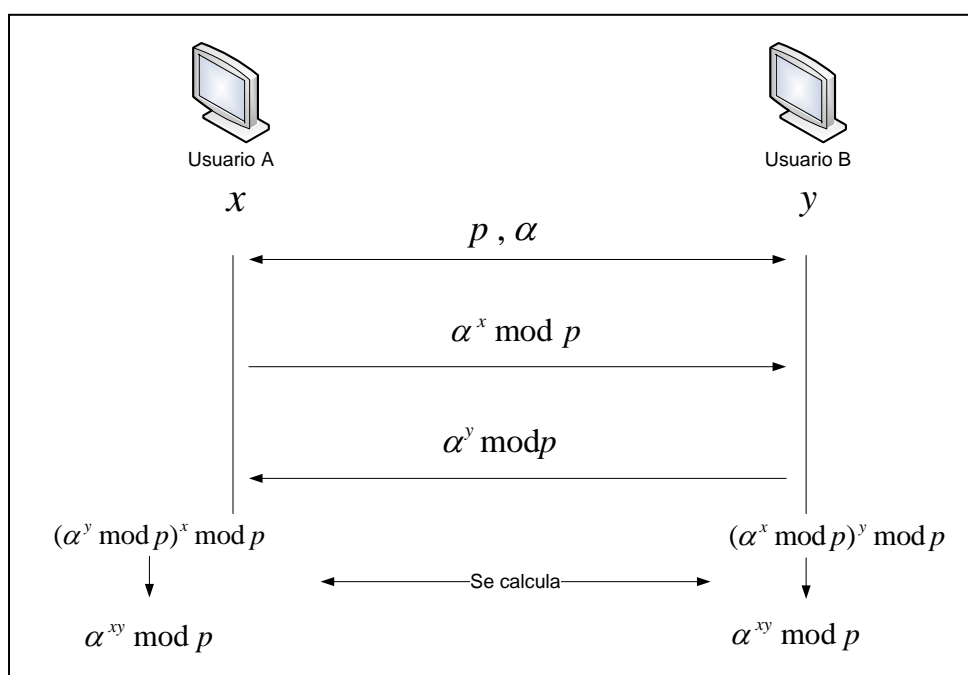


Figura 5. Intercambio de claves mediante el algoritmo Diffie-Hellman

Fuente: Adaptado de Fernández, G. A. (2007). Seguridad en Redes – Intercambio de Claves DIFFIE-HELLMAN. Recuperado de <http://fernandezg.wordpress.com/2007/08/11/intercambio-de-claves-de-diffie-hellman/>

El exponente de la función modular deben elegirlo independientemente emisor y receptor y conservarlos en secreto (es decir x y y), y emplear las funciones modulares $\alpha^x \pmod{p}$ y $\alpha^y \pmod{p}$, para intercambiarlos sin correr el riesgo de exponerlos directamente; conservando de esta forma su privacidad, ya que de ello depende la robustez de operación de este algoritmo.

Finalmente cuando se han intercambiado estos valores, emisor y receptor los emplean conjuntamente con su número privado, para calcular una clave que resulta ser la misma en ambos extremos, debido a las operaciones realizadas; intercambiando así, una clave compartida, sin correr el riesgo de que ningún intruso pueda calcularla de la misma forma.

Las condiciones bajo las cuales se deben seleccionar α , p , x y y son:

- La variable modular p debe ser un número primo de gran longitud (512 o 1024 bits), además, el resultado de la operación $(p - 1)/2$ también debe ser un número primo.
- La base α debe ser la raíz primitiva en el módulo p , y también $2 \leq \alpha \leq (p - 2)$.
- Los números secretos x y y de forma similar, deben ser de gran longitud para prevalecer ante técnicas de criptoanálisis, sus valores deben ser $1 \leq x$ o $y \leq (p - 2)$.

Cualquier intruso podrá conocer los valores de la base, la variable modular, o los resultados de las funciones modulares, pero no conoce x y y , que al ser aleatorios y de gran longitud, resulta demasiado complicado deducirlos; de esta forma, emisor y receptor han acordado una clave simétrica, garantizando que ningún intruso que intercepte cualquier mensaje cifrado con ella, pueda realizar el mismo cálculo para descifrarlo.

c. ElGamal

Este algoritmo fue desarrollado en 1984, inicialmente con propósitos de utilizarlo para generar firmas digitales, aunque tiempo después fue adaptado para cifrar datos. Su desarrollo al igual que RSA fue en base al algoritmo Diffie-Hellman, es decir, la complejidad de cálculo

que imponen los logaritmos discretos; por ello, fue empleado en aplicaciones como creación de firmas digitales (DSS⁹), o la seguridad en el correo electrónico S/MIME¹⁰.

Análogamente a RSA, es necesario generar el par clave, para ello, este algoritmo establece un número primo p y dos números menores a éste elegidos al azar q y e , con los cuales se calcula y , para formar el par clave, la pública K_{Pu} , y la privada K_p (véase Figura 6).

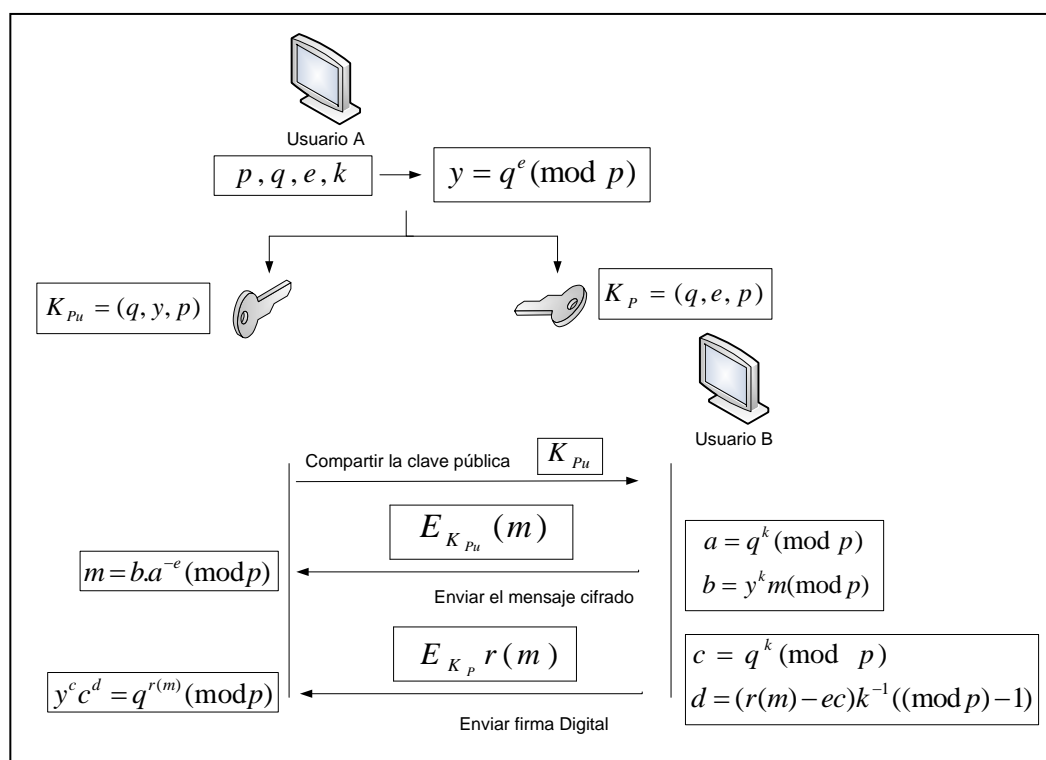


Figura 6. Generación de Claves, Cifrado, Descifrado y Firma Digital de un mensaje mediante el algoritmo ElGamal

Fuente: Creado y adaptado a partir de Lucena, L. M. J. (2009). Criptografía y Seguridad en Computadores. Recuperado de <http://es.scribd.com/doc/39400098/Criptografia#download>

Estas claves se generan mediante la combinación de tres números de gran longitud, con el propósito de evitar exponerlos de forma independiente, aumentando con ello la complejidad para deducirlos aleatoriamente, mediante alguna técnica de criptoanálisis.

⁹ DSS – Estándar de Firmas Digitales

¹⁰ S/MIME – Extensiones de Correo de Internet de Propósitos Múltiples / Seguridad

ElGamal establece un número aleatorio k , que debe ser distinto cada vez, fortaleciendo de esta manera, sus operaciones y funcionamiento. En la Figura 3 se explica el proceso para cifrar un mensaje mediante algoritmos asimétricos, pero las operaciones que realiza ElGamal para ello, son calcular a y b , y combinarlos para formar el mensaje cifrado (a, b) , por lo que se obtiene un mensaje cifrado del doble de longitud que el original; el receptor en el otro extremo, debe calcular m para obtener el mensaje en texto plano (véase Figura 6).

El proceso para firmar digitalmente un mensaje y verificarlo, se ilustra en la Figura 8, pero las operaciones que realiza ElGamal para ello, son el cálculo de c y d en el emisor, para generar la firma digital (c, d) ; por su parte el receptor debe comprobar que $y^c c^d = q^{r(m)} \pmod{p}$, para verificar la firma y determinar la autenticidad del mensaje (véase Figura 6).

Los requerimientos bajo los cuales deben ser seleccionados p , q , e y k son:

- p , q y e deben ser números primos de gran longitud, la ventaja es que mientras más grandes sean, más complejo será deducirlos aleatoriamente.
- $1 < k < (p - 1)$ y también ser relativo con $(p - 1)$, es decir $\text{mcd}(k, p - 1) = 1$, además debe ser diferente cada vez para reducir el riesgo del criptoanálisis sobre el algoritmo.

a. DSA (Digital Signature Algorithm)

Este algoritmo está orientado para generar firmas digitales, su desarrollo fue en base a la generación de firmas de ElGamal, empleando operaciones con logaritmos discretos para

garantizar robustez y fiabilidad de operación; por tal motivo, es utilizado en el Estándar de Firmas Digitales DSS.

El cálculo del par clave depende de cuatro números primos de gran longitud (p, q, e, x) , a los cuales DSA los combina, para generar la clave privada K_p ; para la pública K_{pu} calcula y , y la combina con (p, q, e) (véase Figura 7).

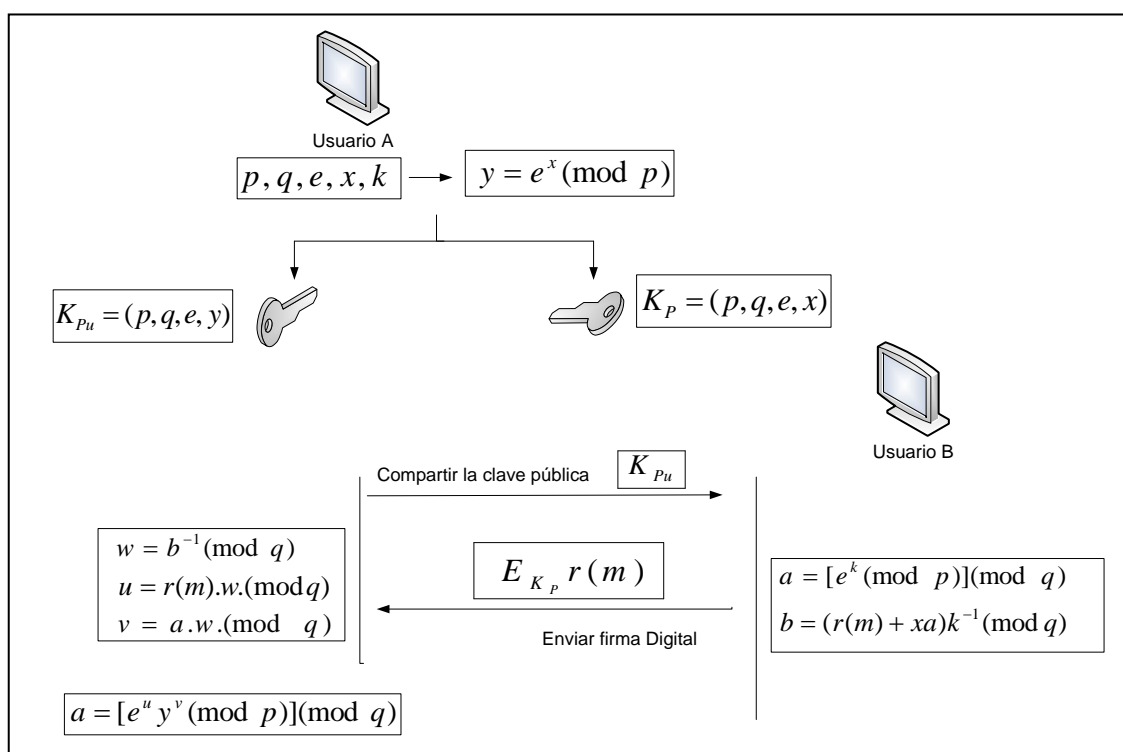


Figura 7. Proceso de DSA para generar el par clave y Firmar Digitalmente un mensaje

Fuente: Creado y adaptado a partir de Tema 4: Firmas Digitales. Recuperado de http://personales.upv.es/~fjmartin/cdii_web/traspas/Firmas_sin_fondo_2x.pdf

El proceso para generar una firma digital de un mensaje m , se lo explica en la Figura 8, pero las operaciones que DSA realiza para ello, es calcular a y b , obteniendo el valor de la firma digital (a, b) en el extremo del emisor. Para verificar esta firma, el receptor calcula w, u, v , y comprueba si se cumple la condición $a = [e^u y^v \pmod{p}] \pmod{q}$, en cuyo caso se acepta la legitimidad de la firma, y la autenticidad del mensaje.

Los requerimientos para elegir p , q , e , x y k son:

- p debe ser un número primo con una longitud entre 512 y 1024 bits, pero también ser múltiplo de 64.
- q primo de 160 bits, que sea divisor de $p - 1$.
- Un número $g \in Z_p^*$ y calcular $e = g^{(p-1)/q} \pmod{q}$.
- x es un número entero $1 \leq x \leq (q - 1)$.
- k es un número aleatorio $0 < k < q$.

1.1.2.4. Criptoanálisis

Es el estudio de los métodos de cifrado con el propósito de determinar vulnerabilidades que comprometan la seguridad de un criptosistema; la mayoría de estos estudios, están enfocados en la revelación de la clave o claves utilizadas para cifrar cierto mensaje.

Para ello, emplean cualquier técnica o habilidad, como el análisis de mensajes cifrados que circulan por la red, o aplicar claves aleatorias al algoritmo, hasta obtener un mensaje con sentido como resultado; en el caso de algoritmos asimétricos estas técnicas se enfocan en deducir a partir de la clave pública, su par, la clave privada.

1.1.3. FIRMA DIGITAL

Es una secuencia binaria que viaja por la red adjunta a un mensaje de datos o documento, para garantizar su integridad, y verificar la identidad de quien provino; proporcionando de esta manera, un mecanismo de seguridad en las comunicaciones.

La Ley 67¹¹ en su artículo 14 establece que: “La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba en juicio”, esto admite su utilización en cualquier aplicación telemática, obviamente de acuerdo a los requisitos y obligaciones estipulados en la Ley.

Técnicamente la Firma Digital (signatura) es la combinación de dos mecanismos de seguridad, el cifrado asimétrico y las funciones hash, debido a que aplicarla directamente sobre documentos completos, demandaría de muchos recursos computacionales, es más eficiente emplear un resumen de menor tamaño para ello.

El proceso de firma digital se muestra en la Figura 8, e inicia cuando B aplicando una función hash (MDC) al mensaje original, obtiene un resumen $r(m)$, lo cifra con su clave privada k_p y lo envía conjuntamente con el mensaje original m . A utilizando m , genera un resumen $r'(m)$ de igual forma como lo hizo B , descifra con la clave pública de B el resumen cifrado que recibió, y los compara para verificar la autenticidad del mensaje m .

1.1.3.1. Funciones Resumen

Las funciones resumen o hash se utilizan para crear la huella (firma) digital de un documento, comprimiéndolo hasta transformarlo en una secuencia de bits infalsificable (véase Figura 9); a diferencia de las funciones de compresión usuales como ZIP, deben ser irreversibles, con el propósito de salvaguardar la integridad del documento.

¹¹ Ley de comercio electrónico, firmas electrónicas y mensajes de datos vigente en Ecuador

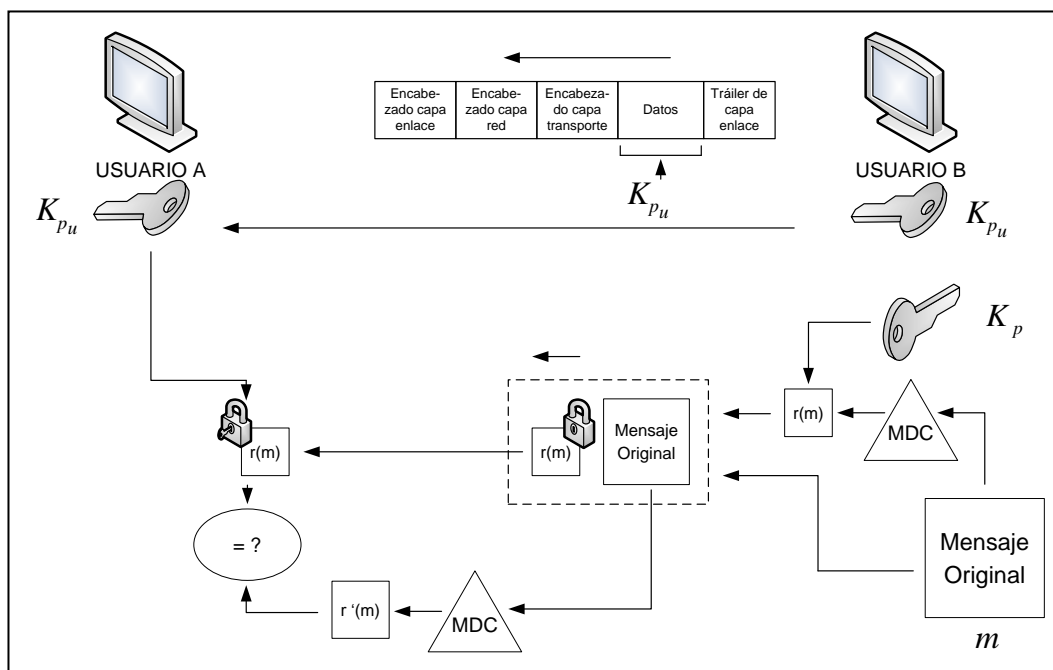


Figura 8. Esquema de la Firma Digital empleando Algoritmos Asimétricos y Funciones Resumen

Fuente: Adaptado de Lucena, L. M. J. (2009). Criptografía y Seguridad en Computadores. Recuperado de <http://es.scribd.com/doc/39400098/Criptografia#download>

Para generar un resumen se realizan distintas operaciones, dependiendo del algoritmo empleado (MD5, SHA1, entre otros), pero se distinguen dos tipos de funciones hash: las que operan directamente sobre el contenido de los mensajes de datos a ser transmitidos llamadas MDC¹², y las que utilizan una llave complementaria en sus operaciones, para autenticar a usuarios o dispositivos, ante algún sistema informático o recurso de red, denominadas MAC¹³.

¹² **Modification Detection Codes** – Códigos de Detección de Modificación

¹³ **Message Authentication Code** – Códigos de Autenticación de Mensajes

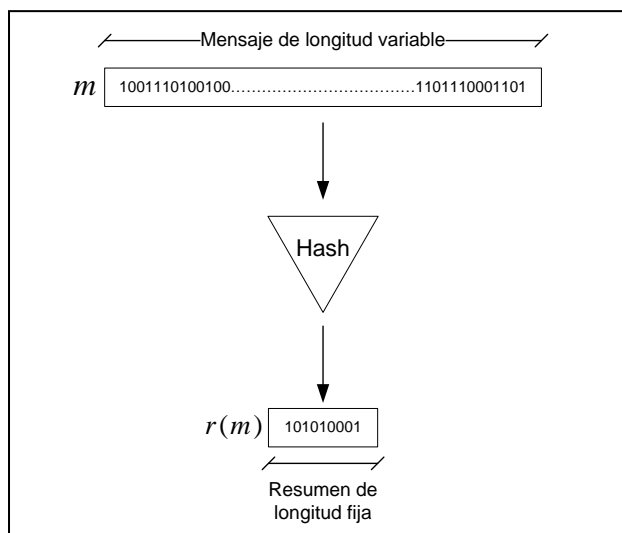


Figura 9. Diagrama de Funcionamiento de las Funciones Hash

Fuente: Adaptado de Stallings, W. (2006). *Cryptography and Network Security Principles and Practice*. Recuperado de [http://evilzone.org/ebooks/cryptography-and-network-security-principles-\(5th-edition\)/](http://evilzone.org/ebooks/cryptography-and-network-security-principles-(5th-edition)/)

Al ser técnicas que fortalecen a los criptosistemas de clave pública, deben garantizar seguridad, para ello, es necesario cumplir ciertas propiedades:

- Deben ser irreversibles, de forma que el conocimiento del código resumen, no permita el cálculo computacional inverso que revele el mensaje original.
- Partiendo de bloques de datos de longitud arbitraria, generan bloques de longitud fija de menor tamaño.
- Simplicidad de cálculo
- Para garantizar integridad de datos, cualquier modificación en el mensaje original, por más intrascendente que parezca (como alterar un solo bit), debe generar una función hash totalmente diferente.
- No deben existir colisiones, es decir, que cada mensaje conlleva a un resumen único, esto implica la imposibilidad computacional para deducir un resumen, que permita encontrar el mensaje original, o viceversa.

Los algoritmos más conocidos para crear funciones resumen son MD5 y SHA-1.

1.1.3.1.1. MD5 (Message Digest 5)

Es uno de los algoritmos MDC de generación de resúmenes, empleado en aplicaciones de seguridad de información para crear firmas digitales; fue desarrollado por Ronald Rivest, en base a ciertas modificaciones sobre MD4, para lograr mayor fiabilidad. PGP fue una de las aplicaciones de seguridad de correo electrónico que lo aplicaron en sus primeras versiones.

MD5 opera con bloques de 512 bits, formados a partir de la segmentación y relleno de los mensajes a transferirse, hasta que sean 64 bits inferiores a 512 (o a uno de sus múltiplos); para ello, inserta una secuencia de bits con el primero en 1, acompañado de tantos 0's como sea necesario.

Los 64 bits restantes para completar estos bloques son añadidos de los mensajes iniciando por el byte menos significativo (véase Figura 10). Cada bloque es dividido en 16 segmentos de 32 bits, para realizar operaciones.

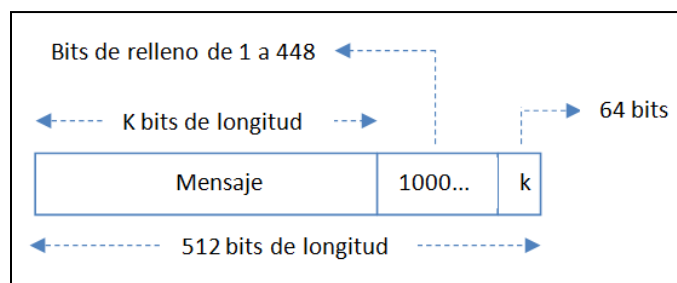


Figura 10. Conformación de la longitud del mensaje m

Fuente: Ramió, A. J. (2006). Funciones Hash en Criptografía (Tema 6). Recuperado de http://criptosec.unizar.es/doc/tema_c7_criptosec.pdf

El funcionamiento del algoritmo, comienza al establecer cuatro registros de 32 bits (A, B, C, D), inicializados con valores predefinidos (véase Tabla 2); estos valores se copian a las variables (a, b, c, d) para operarlas con los segmentos.

Tabla 2. Valores predefinidos para los registros de MD5

Registros	Valores Hexadecimales
A	01234567
B	89ABCDEF
C	FEDCBA98
D	76543210

Fuente: Ramió, A. J. (2006). Funciones Hash en Criptografía (Tema 6). Recuperado de http://criptosec.unizar.es/doc/tema_c7_criptosec.pdf

Para completar, se emplean cuatro funciones, en las cuales realizan operaciones lógicas (16 para cada función) entre las variables y los segmentos de cada bloque; al finalizar se obtienen nuevos valores para las variables (a, b, c, d), que son sumadas con los registros (A, B, C, D), formando los nuevos registros para operar con el siguiente bloque.

Este proceso se repite para cada bloque, obteniendo al finalizar cuatro registros de 32 bits, que forman el resumen de 128 bits.

1.1.3.1.2. SHA-1 (Secure Hash Algorithm – version 1)

SHA es una familia de algoritmos desarrollados por la NSA¹⁴ con el fin de establecer un algoritmo estándar de cálculo de funciones resumen, para emplearlo en el Estándar de Firmas Digitales (DSS). La primera versión llamada SHA-0 se publicó en 1993, tiempo después tras una serie de mejoras aparece SHA-1 (actual estándar de DSS), que se erigió como el principal

¹⁴ **National Security Agency** – Agencia de Seguridad Nacional de los Estados Unidos

de esta familia. Las siguientes versiones mantienen este esquema, pero difieren en la longitud de bits de los resúmenes que generan, así se tiene SHA-224, SHA-256, SHA-384 y SHA-512, conocidos en conjunto como SHA-2.

SHA-1 fue desarrollado en base a MD5, por lo que opera de forma parecida, segmentando y alargando los mensajes originales en bloques de 512 bits, y subdividiendo a cada uno en 16 segmentos de 32 bits, para calcular la función resumen (véase Figura 10).

La razón principal que convierten a SHA-1 en más fiable que MD5, es que utiliza en lugar de cuatro, cinco registros de 32 bits, para realizar operaciones lógicas en cada función. Los valores con los que deben ser inicializados estos registros, son los que muestra la Tabla 3.

Tabla 3. Valores predefinidos para los registros de SHA-1

Registros	Valores Hexadecimales
A	67452301
B	EFCDAB89
C	98BADCFE
D	10325476
E	C3D2E1F0

Fuente: Creado a partir de Lucena, L. M. J. (2009). Criptografía y Seguridad en Computadores. Recuperado de <http://es.scribd.com/doc/39400098/Criptografia#download>

Análogamente a MD5, se inicializan cinco variables (a, b, c, d, e) empleadas en cuatro funciones que las operan lógicamente con los segmentos de 32 bits, cada función realiza 20 operaciones lógicas. Algo adicional que utiliza SHA-1, es una constante en cada función, para fortalecer el funcionamiento del algoritmo, la Tabla 4 muestra sus valores.

Tabla 4. Valores predefinidos para las constantes de cada función de SHA-1

Registros	Valores Hexadecimales
K_0	5A827999
K_1	6ED9EBA1
K_2	8F1BBCDC
K_3	CA62C1D6

Fuente: Creado a partir de Lucena, L. M. J. (2009). Criptografía y Seguridad en Computadores. Recuperado de <http://es.scribd.com/doc/39400098/Criptografia#download>

Al finalizar las operaciones de las cuatro funciones, se han calculado nuevos valores para las variables (a, b, c, d, e) , que son sumadas con cada registro (A, B, C, D, E) para generar los nuevos registros del siguiente bloque de datos. Este procedimiento se repite hasta terminar con todos los bloques del mensaje, obteniendo un resumen de 160 bits.

1.1.4. DISTRIBUCIÓN Y ADMINISTRACIÓN DE CLAVES

La fortaleza de los criptosistemas radica en la privacidad de las claves criptográficas, por ello, su administración y distribución depende de protocolos y técnicas de cifrado, para garantizar el establecimiento de comunicaciones con entidades remotas fiables.

En criptosistemas de clave privada los métodos de generación de las claves son sencillos, pero su distribución a través de canales inseguros involucra métodos complejos para protegerlas.

Generar una clave simétrica y compartirla personalmente con otra entidad asegura su privacidad, pero en ambientes reales en los que las relaciones laborales se desarrollan entre una gran variedad de empresas y agrupaciones de personas, que interactúan de manera conjunta desde cualquier parte del mundo, este proceso resulta impráctico.

El algoritmo de Diffie-Hellman permite el intercambio de claves simétricas entre usuarios remotos, pero al no proveer autenticación, queda expuesto a un potencial ataque que podría interceptar las variables transferidas al establecer la clave y conocer los valores privados, de allí en adelante la conexión cifrada ya no es segura.

El método más eficaz es emplear KDC¹⁵, como entidades que emiten y administran claves simétricas, en quien los usuarios pueden confiar (un tercero de confianza). En la práctica algunos de estos sistemas de seguridad son: TACACS (Terminal Access Controller Access Control System), RADIUS (Remote Authentication Dial In User), y el protocolo de autenticación Kerberos.

Los criptosistemas asimétricos notoriamente solventaron el problema de difusión de la clave simétrica, utilizando un par clave; la pública debe ser difundida abiertamente para que todos la conozcan, en bases de datos o directorios de acceso público, de esta forma, la identidad de un usuario remoto está ligada a esta clave.

La desventaja es que una clave pública contiene únicamente una secuencia de bits, que puede ser autogenerada por cualquier persona, utilizando medios informáticos; esto produce una gran vulnerabilidad, al no existir la posibilidad de comprobar que dicha clave es realmente de quien se espera. En base a esto, se ha desarrollado un método denominado Certificado Digital, que al ser emitido por una entidad imparcial (Autoridad de Certificación), vincula legítimamente la identidad de una persona con su clave pública.

¹⁵ **Key Distribution Center** – Centro de Distribución de Claves

1.2.INFRAESTRUCTURA DE CLAVES PÚBLICAS (PKI)

La PKI es un sistema de seguridad formado por hardware, software, personas y políticas, que aseguran la emisión y gestión de certificados digitales basados en claves criptográficas, avalando la relación usuario – clave pública, para implantar mecanismos de cifrado y firma digital sobre un conjunto diverso de aplicaciones telemáticas.

1.2.1. COMPONENTES DE LA PKI

El funcionamiento de la PKI depende primordialmente de entidades denominadas autoridades de certificación, apoyadas en autoridades de registro y directorios, que operan bajo ciertos procedimientos de control establecidos por las políticas de seguridad, para gestionar los certificados digitales y enfocar su uso en la protección de información sensible.

1.2.1.1. Autoridad de Certificación (Certification Authority - CA)

La Autoridad Certificadora es una entidad imparcial en quien emisor y receptor confían mutuamente, aunque ellos no se conozcan con anterioridad (tercero de confianza), podría ser considerada como un notario electrónico que avala la comunicación entre entidades legítimas.

La CA es la encargada de verificar y acreditar la identidad de un usuario o dispositivo, a través de la emisión de un certificado digital que lo vincula con una clave pública, como también de su publicación en directorios, su renovación, y la revocación o suspensión en caso de que haya expirado, se compruebe falsedad en los datos del registro, o se vea comprometida su par clave privada.

Para evitar que un certificado emitido sea suplantado, la CA antes de entregarlo lo firma digitalmente, transformándolo en un documento auto-prottegido, y admitiendo que cualquier entidad esté en capacidad de verificar la legitimidad de la información en él contenida.

En esta autoridad de certificación radica la confianza de toda una comunidad de personas de un entorno local, pero globalmente puede formar parte de un conjunto jerárquico de autoridades certificadoras que extienden la cadena confianza (véase Figura 11).

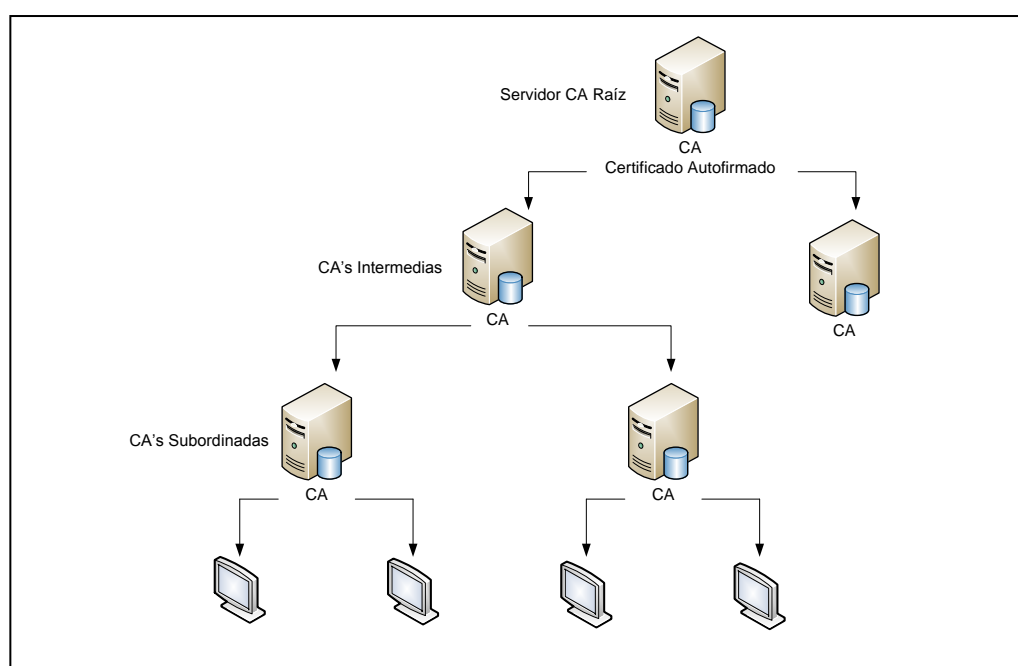


Figura 11. Arquitectura Jerárquica de Certificación

Fuente: Cuesta, R. J., & Puñales, C. M. (2002). Seguridad en Redes Telemáticas-Infraestructura de Clave Pública (PKI). Recuperado de <http://es.scribd.com/doc/116154580/Infraestructura-de-clave-publica-PKI>

Una arquitectura jerárquica de CAs centraliza la fiabilidad en la autoridad raíz, que genera su propio certificado avalado por su firma digital (se auto-certifica), convirtiéndose en el respaldo en el que todos los usuarios de un entorno local, ciudad o país confían. Esta CA emite certificados firmados digitalmente a autoridades intermedias, habilitándolas para certificar a autoridades subordinadas, de menor jerarquía en la arquitectura; finalmente éstas

últimas son las que certifican a usuarios y dispositivos finales tras un proceso de registro y verificación.

De esta forma un usuario al interactuar sobre ciertas aplicaciones telemáticas percibirá certificados emitidos por autoridades desconocidas, poniendo en duda su legitimidad, sin embargo, esta organización jerárquica de la arquitectura, permite verificar las autoridades de nivel superior que emitieron los certificados, extendiendo de esta forma los niveles de confianza y certeza. Al establecer comunicación con autoridades que no forman parte de la jerarquía, la certificación cruzada entre CAs es la que permite que se asocien y confíen mutuamente, obviamente luego de un sondeo que determine su legitimidad.

Existen instituciones o empresas cuyo requerimiento es que los certificados sean destinados únicamente para uso interno, en estos casos una arquitectura aislada de CAs satisface estos requerimientos de certificación, al no existir la necesidad de establecer enlaces de confianza con CAs que no pertenezcan a la jerarquía. Esta arquitectura puede integrarse por una CA raíz que emita certificados directamente a usuarios finales, o complementarse por autoridades intermedias, subordinadas y de registro.

1.2.1.2. Autoridad de Registro (Registration Authority - RA)

Las CAs desempeñan diversas funciones para certificar a autoridades finales o intermedias, pero cuando la PKI cubre entornos con gran demanda de usuarios, o con dependencias geográficamente distantes, resulta complicado dar atención eficiente a todas las peticiones de certificación, incluso la CA podría colapsar por la sobrecarga de actividades.

Por tal motivo, existen ocasiones en las que la CA delega a una Autoridad de Registro el proceso de gestión de registro y autenticación de usuarios que soliciten certificación. La ventaja de utilizar esta autoridad adicional es garantizar escalabilidad en el servicio, al implementarse tantas como sean necesarias para dar atención a la mayoría de peticiones de certificación en distintos lugares, limitando a la CA a certificar únicamente a usuarios y dispositivos finales que han sido autenticados y autorizados por la RA.

La RA es el vínculo entre el usuario final y la CA atendiendo solicitudes de registro, certificación, recuperación de claves o certificados, asociación entre la clave pública y el titular del certificado, y gestión del ciclo de vida de los certificados resaltando la revocación, expiración, renovación, reemisión del par clave criptográfico o actualización de información del certificado.

El registro en entornos locales puede ser llevado a cabo de manera presencial, el solicitante se acerca personalmente a la RA para presentar toda la documentación requerida, previa verificación y aprobación la RA envía una solicitud a la CA para que emita el certificado solicitado, una vez emitido la RA lo descarga y distribuye al usuario (véase Figura 12).

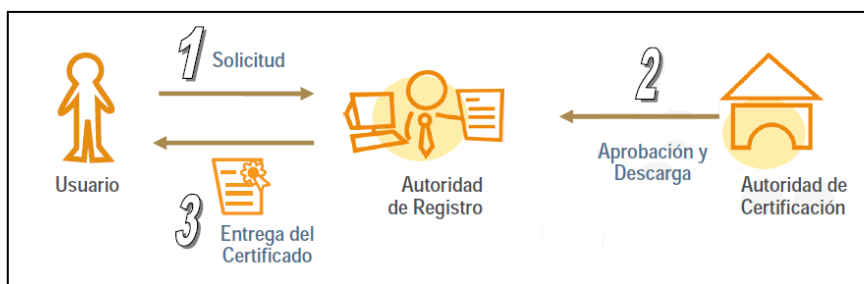


Figura 12. Registro Presencial

Fuente: INDRA Sistemas, S.A. (2005). Infraestructura de Clave Pública (PKI). Recuperado de http://www.inteco.es/extfrontinteco/es/pdf/Formacion_PKI.pdf

Para brindar mayor flexibilidad en el proceso de certificación es posible extender este servicio para que los solicitantes lo obtengan remotamente, configurando las autoridades CA y RA para permitir al usuario establecer un pre-registro remoto en la CA, luego remotamente este usuario presentará toda la documentación pertinente ante la RA, si ésta lo aprueba envía una solicitud de petición a la CA para que emita el certificado solicitado que será distribuido por la RA o la CA a la entidad solicitante (véase Figura 13).

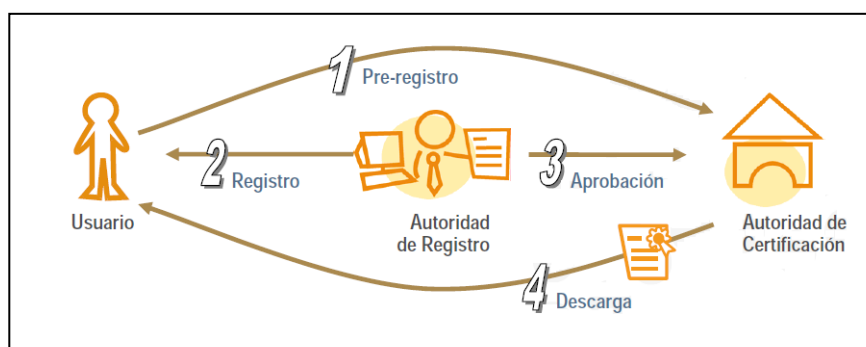


Figura 13. Registro Remoto

Fuente: INDRA Sistemas, S.A. (2005). Infraestructura de Clave Pública (PKI). Recuperado de http://www.inteco.es/extfrontinteco/es/pdf/Formacion_PKI.pdf

1.2.1.3. Autoridad de Sellado de Tiempo (Time Stampig Authority - TSA)

El sellado de tiempo es un servicio ofrecido por una entidad de confianza, mediante el cual es posible determinar que cierta información ha existido en un período de tiempo y que no ha sido modificada desde ese momento. Este es un componente importante dentro del conjunto de servicios ofrecidos por la PKI, llevado a cabo por la TSA para avalar que en realidad un conjunto de datos existieron en cierto tiempo, sin posibilidad de que ni siquiera el emisor pueda modificarlos luego de ser sellados.

La importancia de este servicio puede ser notoria al verificar por ejemplo que una firma digital fue aplicada a un mensaje antes de que el certificado haya expirado, que un documento

fue terminado a tiempo cuando existen plazos críticos para hacerlo, para registrar y evidenciar el momento en el que se realizó una transacción telemática, la existencia de contratos, investigaciones científicas o registros médicos.

Para aplicar un sello de tiempo a un documento digital o mensaje, el solicitante debe calcular el hash de los datos y enviar una solicitud “Timestamp Request” definida en el RFC 3161, a la autoridad de certificación de sellado de tiempo; ésta verifica y aprueba la solicitud, concatena un sello de tiempo al hash recibido y calcula un nuevo valor hash, al cual lo firma digitalmente con su clave privada; finalmente retorna al usuario los valores firmados en conjunto con el sello de tiempo (véase Figura 14).

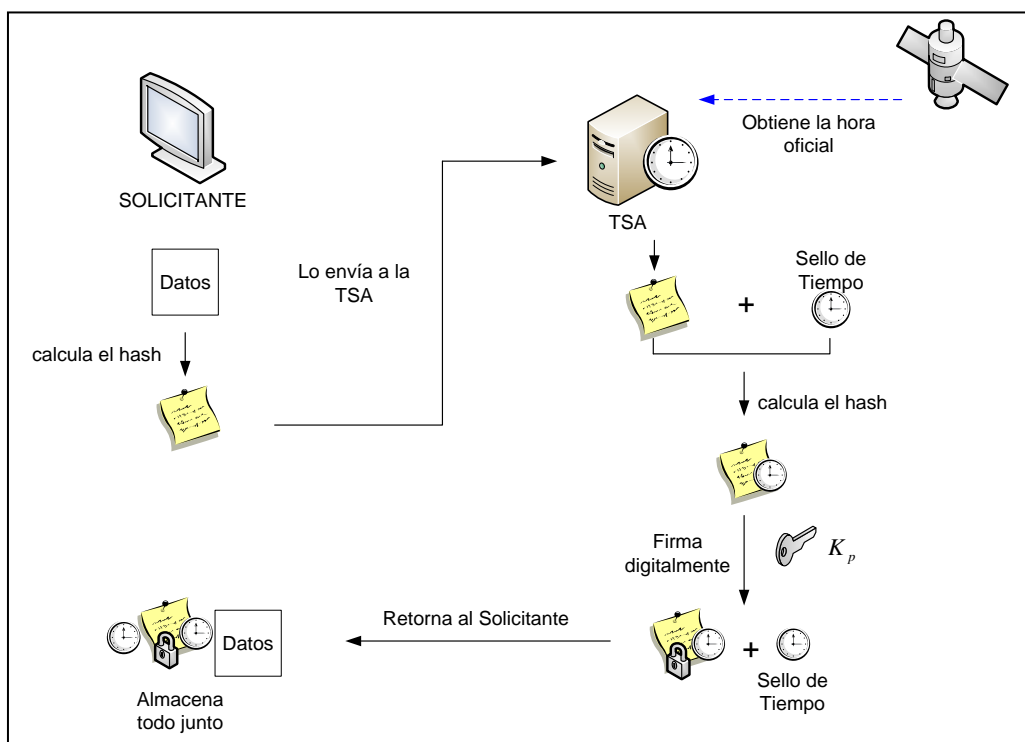


Figura 14. Esquema del Sellado de Tiempo

Fuente: Adaptado de Ministerio de Ciencia y Tecnología – Dirección de Certificadores de Firma Digital. Política de Sellado de tiempo del Sistema Nacional de Certificación Digital. Recuperado de <http://www.firmadigital.go.cr/Documentos/PoliticadeSelladodetiempover100.pdf>

Desde este momento el usuario puede hacer uso de este documento sellado para demostrar legalidad sobre ciertas aplicaciones, o ante determinadas entidades.

El proceso que ejecutan los ordenadores para que cualquier entidad verifique la legitimidad de este documento sellado, es generar un valor hash del documento original, concatenarlo con el sello proporcionado por la TSA y calcular su valor hash. Comprueba la firma digital del sello empleando la clave pública de la entidad certificadora, obtiene el valor hash generado por esta entidad, y lo compara con el valor hash que calculó inicialmente, cerciorándose de que los valores coincidan.

1.2.1.4. Certificado Digital

Es un documento que asocia la identidad de una persona o dispositivo informático, con una clave pública, para demostrar ante los demás que es fiable, evitando potenciales suplantaciones sobre aplicaciones telemáticas de carácter confidencial.

Los certificados Digitales para evidenciar la pertenencia a una entidad, persona o dispositivo informático, pueden contener diversa información, como datos personales de su titular, su clave pública, datos de la entidad que lo emitió, su firma digital, y otras consideraciones adicionales; por ello, se ha desarrollado un estándar que especifica el formato de información que debe contener un certificado, la recomendación UIT-T X.509.

Esta recomendación ha sido desarrollada en 1988 con el propósito de estandarizar el formato de información de los certificados digitales, listas de revocación de certificados CRLs, algoritmos de validación entre jerarquías de certificación, entre otras cosas.

UIT-T X.509 es parte de la serie X.500 que refieren al servicio de directorio, la versión que se desarrolló inicialmente fue mejorada para implementar el servicio de control de acceso a los directorios, consecuentemente esta versión 2 del estándar se complementó con mejoras que permiten establecer comunicaciones seguras (como el correo electrónico), esta es la versión 3 de uso actual. Los campos de este formato los describe la Tabla 5.

Tabla 5. Formato de Certificados Digitales según la recomendación UIT-T X.509

CAMPO	DESCRIPCIÓN
Versión	Identifica la versión del certificado 1, 2 o 3.
Número de Serie	Es un identificador único para cada certificado.
Identificador del algoritmo de firma digital	Este campo indica el algoritmo aplicado para generar la firma, por ejemplo RSA o DSA.
Nombre del Certificador	Contiene el nombre de la autoridad certificadora que emitió y firmó el certificado.
Periodo de validez	Es el rango de tiempo en el que el certificado es válido, contiene la fecha de inicio de vigencia y la de caducidad.
Nombre del sujeto	Es el nombre del sujeto o dispositivo que ha solicitado certificación, quien posee el par clave privada correspondiente.
Clave pública del sujeto	Describe esta clave y algunos parámetros adicionales, como el algoritmo con el que se la puede emplear.
Identificador único del certificador (v2)	Estos campos fueron los que se agregaron para soportar control de acceso a directorios en la versión 2 del estándar. Se utilizan para identificar a un sujeto y una CA respectivamente, ante diferentes eventos.
Extensiones (v3)	Forman parte de las mejoras implantadas con la versión 3, existen diferentes tipos de extensiones como indicadores de importancia, limitaciones, políticas de certificación, uso de la clave, etc. En general son parámetros para aplicaciones que trabajan en modo seguro.
Firma digital	Es la firma generada en base a toda la información anterior, llevada a cabo por la entidad certificadora.

Fuente: Creado a partir de Talens-Oliag, S. Introducción a los certificados digitales. Recuperado de http://www.uv.es/~sto/articulos/BEI-2003-11/certificados_digitales.pdf

1.2.1.4.1. Tipos de Certificados

Los certificados digitales posibilitan la interacción sobre diversas aplicaciones telemáticas como acceso seguro a servidores web, intranets o redes privadas virtuales, correo electrónico seguro, etc.; por tal motivo, su emisión varía dependiendo de su propósito y hacia quién o que está destinado (véase Figura 15).

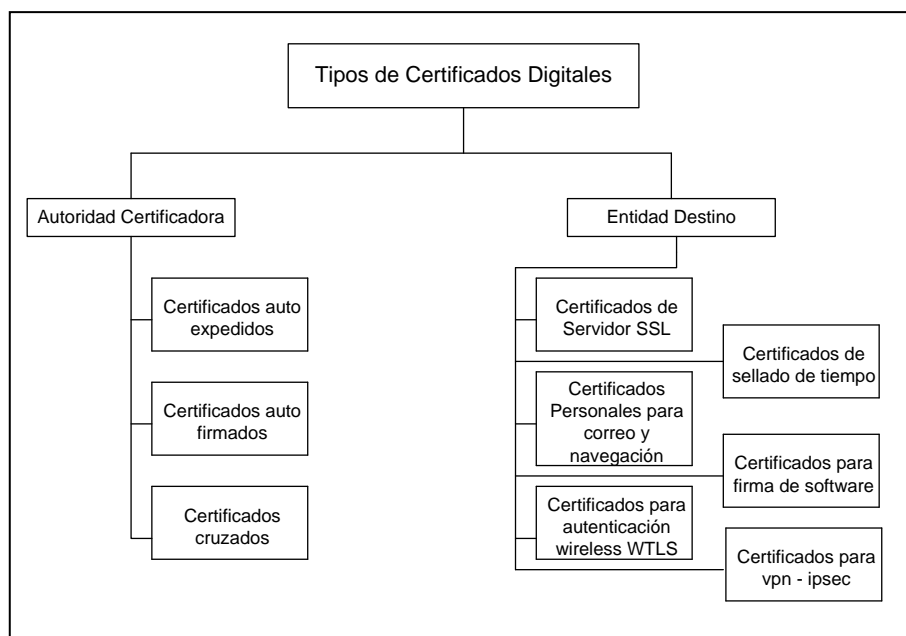


Figura 15. Tipos de Certificados Digitales

Fuente: Creado a partir de Salazar, J. E. Desarrollo de una guía práctica para la implantación y manejo de la Infraestructura de Clave Pública (PKI) en la WEB. Recuperado de <http://ftp.puce.edu.ec/handle/22000/1368>

1.2.1.5. Directorio de Publicación de Certificados

Los directorios son servicios empleados en entornos PKI, para almacenar los certificados emitidos por la CA, manteniéndolos disponibles ante el acceso de usuarios que necesiten recuperarlos, para el establecimiento de comunicaciones seguras.

Su implementación contribuye a la administración de los certificados, debido a que posibilita su distribución y control de su estado de vigencia, mediante listas de revocación. Estos servicios mantienen una arquitectura cliente-servidor, en la que el cliente puede ser una aplicación dedicada, enlaces de acceso hacia un servidor Web, o aplicaciones de correo electrónico, y el servidor es la base de datos en la que se almacenan los certificados digitales.

Los protocolos de acceso complementan esta arquitectura, siendo el vínculo entre el cliente y el servidor, que permite la obtención y búsqueda de información; DAP¹⁶ es un protocolo de acceso desarrollado para trabajar con directorios X.500, pero el protocolo más difundido es LDAP¹⁷, debido a su compatibilidad con redes TCP/IP.

LDAP es un protocolo ligero que forma parte de X.500, aunque puede ser empleado para trabajar con diversas plataformas de servicios de directorio como OpenLDAP que es de software libre, o Active Directory bajo licencia de Windows. Este protocolo ejecuta funciones de transporte y enrutamiento de forma sencilla, en comparación a los convencionales, a fin de agilizar los procesos de directorio y evitar flujo de tráfico adicional innecesario que puede saturar la red.

1.2.1.5.1. Lista de Revocación de Certificados (CRL)

Los certificados digitales son emitidos para ser válidos durante un periodo de tiempo, pero existen diversas razones que pueden invalidarlos sin necesidad de haber expirado, por ejemplo si la clave privada del usuario se ve comprometida, o si sus datos en el certificado ya no corresponden a los actuales.

¹⁶ **Directory Access Protocol** - Protocolo de Acceso a Directorio

¹⁷ **Lightweight Directory Access Protocol** - Protocolo Ligero de Acceso a Directorio

Por ello la necesidad de que la CA publique una lista en la que consten aquellos certificados que por determinadas circunstancias han sido invalidados, de manera que cualquier entidad esté en capacidad de verificar su estado de vigencia; este directorio se denomina lista de revocación de certificados (Certificate Revocation List - CRL).

La CRL es actualizada permanentemente, y su legitimidad radica en la firma digital generada por la CA, que avala la veracidad de la información en ella publicada; de forma que una entidad final pueda descargarla y verificar si cierto certificado consta en la lista, para determinar su validez.

Esta lista es de gran importancia en aplicaciones telemáticas, debido a que ninguna de ellas autenticará a una persona o dispositivo, o aceptará una firma digital, en la que se haya empleado un certificado que ya expiró, pero es muy probable que uno revocado siga siendo utilizado. Análogamente a los certificados digitales la recomendación UIT-T X.509 estandariza el formato de la CRL, los campos de este formato los muestran la Tabla 6.

Tabla 6. Formato de CRL según la recomendación UIT-T X.509

CAMPO	DESCRIPCIÓN
Versión	Identifica la versión 2 de este formato.
Firma	Es un identificador del algoritmo empleado para firmar la CRL.
Nombre del generador	Contiene el nombre de la entidad certificadora que emitió y firmó la CRL.
Actualización	Contiene la hora y fecha en que fue publicada la CRL.
Próxima actualización	Este campo es importante al indicar cuándo se publicará la siguiente actualización.
Certificado del usuario	Los certificados invalidados son identificados por su número de serie.
Fecha de anulación	Indica cuándo se invalidó un certificado

Fuente: Creado a partir de Salazar, J. E. Desarrollo de una guía práctica para la implantación y manejo de la Infraestructura de Clave Pública (PKI) en la WEB. Recuperado de <http://ftp.puce.edu.ec/handle/22000/1368>

También puede existir un campo adicional (código de razón), en el que se describen los motivos por los cuales el certificado fue revocado (véase Tabla7).

Tabla 7. Descripción del campo código de razón según UIT-T X.509

MOTIVO	DESCRIPCIÓN
Compromiso de la clave	Si la clave privada del usuario fue divulgada, destruida o robada.
Compromiso de la autoridad certificadora	Si la clave privada de la CA está comprometida.
Superado	Si este certificado fuere reemplazado.
Cese de operación	Si el certificado ya no es útil con el propósito para el que fue destinado.
Certificado en espera	Cuando fue suspendido temporalmente.
Sin especificar	Por motivos diferentes a los descritos.

Fuente: Creado a partir de Salazar, J. E. Desarrollo de una guía práctica para la implantación y manejo de la Infraestructura de Clave Pública (PKI) en la WEB. Recuperado de <http://ftp.puce.edu.ec/handle/22000/1368>

1.2.1.6. Usuario Suscriptor

Este usuario complementa el ciclo de operación de la PKI, al confiar y utilizar sus servicios de forma voluntaria sobre aplicaciones telemáticas, generando o validando firmas digitales, o cifrando documentos para protegerlos, y fundamentalmente por poseer la clave privada correspondiente a la pública contenida en el certificado.

1.2.2. FUNCIONAMIENTO DE UNA PKI

La integración de todos los componentes de la PKI y las operaciones que realiza cada uno para gestionar los certificados digitales, son las que se muestran en la Figura 16.

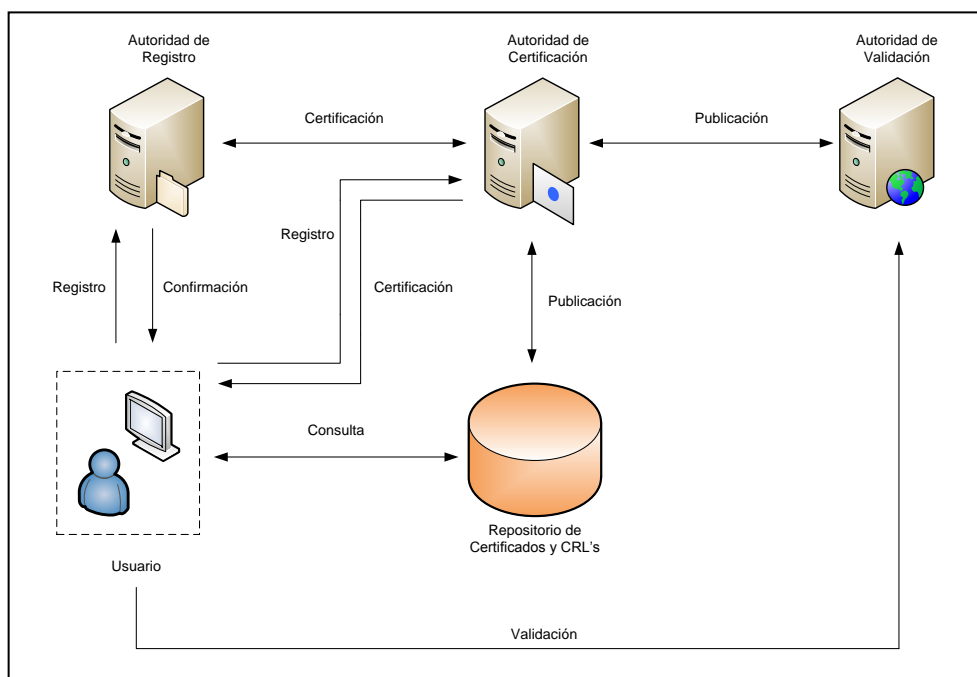


Figura 16. Funcionamiento de los componentes de un entorno PKI

Fuente: INDRA Sistemas, S.A. (2005). Infraestructura de Clave Pública (PKI). Recuperado de http://www.inteco.es/extfrontinteco/es/pdf/Formacion_PKI.pdf

Vale la pena destacar que la solicitud de certificación y su respuesta, pueden ser establecidas directamente entre el solicitante y la CA, o si se ha implementado, empleando a la RA como entidad intermedia.

La validación de certificados digitales es un proceso de vital importancia en entornos PKI, para garantizar comunicación con usuarios y entidades legítimas, por tal motivo, los usuarios suscriptores deben en primera instancia consultar la existencia de determinado certificado en el directorio de publicación de la CA, para confirmar su vinculación.

Para definir el estado de este certificado, deben descargar la CRL y revisar si se encuentra registrado en la lista como suspendido, revocado o expirado, de lo contrario se entenderá que está activo. Pero existe otra forma mucho más eficiente de realizar esta operación, esto es

implementando una Autoridad de Validación (VA) en la PKI, que posibilite la consulta en línea del estado del certificado, a través del protocolo OCSP¹⁸.

La ventaja de este método es que la CA actualiza de manera inmediata la información de la VA luego de realizar cualquier modificación sobre el estado de los certificados, a diferencia de las CRLs en las que cada cierto periodo de tiempo establecido se publican en conjunto todas las modificaciones realizadas.

El protocolo OCSP posibilita que determinadas aplicaciones proporcionen información referente al estado de un certificado digital X.509, de manera más oportuna que las CRLs. Su interacción inicia cuando el solicitante envía una petición de consulta OCSP, hacia un servicio alojado en la Autoridad de Validación, denominado OCSP responder, que revela el estado del certificado (véase Figura 17).

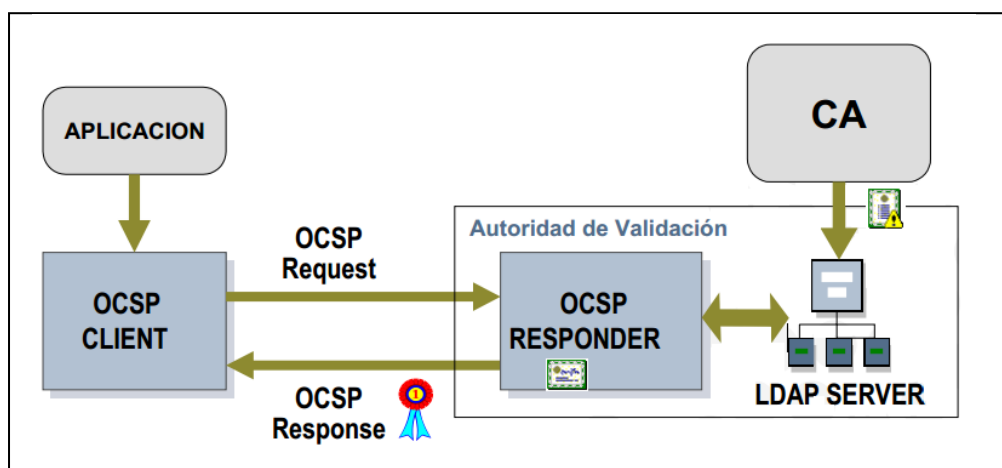


Figura 17. Funcionamiento del Protocolo OCSP

Fuente: INDRA Sistemas, S.A. (2005). Infraestructura de Clave Pública (PKI). Recuperado de http://www.inteco.es/extfrontinteco/es/pdf/Formacion_PKI.pdf

¹⁸ **Online Certificate Status Protocol** – Protocolo en línea de Estado de Certificado

Una solicitud de consulta está formada básicamente por la versión del protocolo y un identificador en el que se almacenan parámetros como el número de serie del certificado, o el hash de la clave pública de la entidad emisora. Una respuesta a esta solicitud será firmada digitalmente, indicando el estado activo, revocado o en ocasiones desconocido cuando existen ambigüedades en el certificado.

Estos mensajes OCSP se transmiten mediante el protocolo HTTP, su descripción está definida en la RFC 2560, en la que se detalla su sintaxis, requerimientos, y otras consideraciones adicionales.

1.2.3. APLICACIONES DE LA PKI

Algunos servicios y protocolos que emplean certificados digitales para proporcionar cierto nivel de seguridad sobre determinadas aplicaciones, pueden ser considerados como los campos de aplicación de la PKI (véase Tabla 8).

1.2.4. ASPECTOS LEGALES DE LA PKI

El avance tecnológico y las nuevas tendencias de comercio electrónico han dado lugar a la elaboración de un marco regulatorio, que permita impulsar y masificar el uso de los sistemas informáticos y las redes de comunicación en territorio ecuatoriano, para aportar a su desarrollo en distintos ámbitos: tecnológico, comercial, productivo, de trabajo, educativo y cultural; esta es la Ley 67: Ley de comercio electrónico, firmas electrónicas y mensajes de datos, publicada en el 2002, y el Reglamento correspondiente a esta ley.

Tabla 8. Algunos Servicios y Protocolos que emplean Certificados Digitales

	Descripción
Servicios	Firma Digital Al interactuar sobre ciertas aplicaciones telemáticas, como transacciones bancarias, pagos con tarjeta de crédito o el envío y recepción de correo electrónico, la firma digital es la evidencia que comprueba el acuerdo entre las partes para realizar determinada actividad. Para usarla como una prueba, es necesario verificar que el certificado digital contenga la clave pública legítima, y que su entidad emisora es fiable.
	Cifrado Generalmente complementa a la firma digital, ocultando aquella información sensible que circula por la red, o es almacenada en sistemas informáticos.
	Registro de Hora Este servicio demuestra que ciertos documentos digitales han existido en un período de tiempo, con ello se puede comprobar por ejemplo que ciertas acciones en realidad se llevaron a cabo, en el caso de un juicio, o que una propuesta fue terminada a tiempo, aunque al interesado le haya llegado tiempo después por cualquier eventualidad.
Protocolos	SSL ¹⁹ Es un protocolo de capa transporte, cuyo uso se ha difundido en aplicaciones de comercio electrónico, que necesitan establecer comunicaciones seguras con servidores WEB. Emplea el cifrado simétrico y las funciones hash (MAC) para garantizar confidencialidad e integridad de los datos en tránsito, y los certificados digitales para autenticarse ante el cliente, y en ocasiones el cliente ante el servidor.
	TLS ²⁰ Este protocolo es equivalente a SSL en su versión 3 de uso actual, su funcionamiento es bastante similar, difieren en ciertos aspectos.
	WTLS ²¹ Es un protocolo de transporte que garantiza un alto grado de protección para dispositivos móviles, primordialmente en cuanto su acceso a la red. Es una adaptación de TLS y forma parte de la familia de protocolos de aplicaciones inalámbricas (WAP).
	S/MIME ²² Son técnicas que permiten la transferencia de mensajes de correo electrónico, auto-protegidos por mecanismos como el cifrado y la firma digital.
	TSP ²³ Es un protocolo que a través de los servicios de la TSA, garantiza que ciertos datos existieron en un momento determinado.

Fuente: Creado a partir de Salazar, J. E. Desarrollo de una guía práctica para la implantación y manejo de la Infraestructura de Clave Pública (PKI) en la WEB. Recuperado de <http://ftp.puce.edu.ec/handle/22000/1368>

¹⁹ **Secure Sockets Layer** - Capa de Sockets Segura

²⁰ **Transport Layer Security** - Capa de Transporte Seguro

²¹ **Wireless Transport Layer Security** - Capa de Transporte Inalámbrico Seguro

²² **Secure / Multipurpose Internet Mail Extensions** - Extensiones Multipropósito Seguras de Correo de Internet

²³ **Time Stamp Protocol** - Protocolo de Sellado de Tiempo

El propósito es regular aspectos referentes a la validez y uso de los mensajes de datos, la validez de la firma electrónica y el control sobre entidades que ofrecen servicios de certificación para implantarla, la prestación de servicios electrónicos y la adecuada protección para los usuarios que los utilizan, entre otros aspectos.

De acuerdo con esta ley los mensajes de datos pueden ser utilizados con los mismos propósitos con los que se utilizan los documentos escritos, tienen la misma validez jurídica, e inclusive se pueden utilizar como evidencia en casos judiciales si la situación lo amerita, por tal motivo, el emisor de un mensaje deberá responsabilizarse por su contenido.

También contempla que la firma electrónica es un conjunto de datos adjuntos electrónicamente a un mensaje, que tiene la misma validez y efectos jurídicos que la firma manuscrita. El propósito de emplearla es identificar al titular de la firma y responsabilizarlo por el contenido del mensaje de datos firmado; de esta forma, se posibilita su uso legal sobre cualquier tipo de aplicación telemática, como también para efectos jurídicos si la situación lo amerita. Para que sea válida debe cumplir con ciertos requisitos, y el firmante con determinadas obligaciones estipuladas en la ley.

Además, la ley 67 define la validez de los certificados de firma electrónica (certificados digitales) emitidos por entidades acreditadas en el país, como también aquellos que provienen de entidades de certificación extranjeras. Su revocación o suspensión temporal, serán efectuadas por razones dispuestas en la misma, y en ocasiones es el CONATEL²⁴ como ente regulador, quien interviene directamente con las entidades certificadoras para solicitar cualquiera de estas acciones.

²⁴ Consejo Nacional de Telecomunicaciones

El acuerdo 181 determina que los sistemas informáticos independientemente de su plataforma, deben implementar la utilización de certificados digitales para estandarizar este tipo de aplicativos, y además, señala los tipos de certificados que deben ser emitidos y los campos obligatorios en cada tipo, para que sean considerados como válidos.

En cuanto a las entidades de certificación, señala que para ejercer legítimamente sus actividades en territorio ecuatoriano deben estar legalmente autorizadas por el CONATEL, que es el organismo de regulación, autorización y registro; como también, cumplir con las obligaciones y responsabilidades definidas en la ley, en beneficio de la gestión eficiente de los certificados digitales que han emitido, y la protección de datos confidenciales adquiridos en sus labores cotidianas.

El organismo que controla las entidades de certificación acreditadas por el CONATEL, es la SUPERTEL²⁵, cuyas funciones están determinadas en esta ley; y el organismo de difusión de información acerca del comercio electrónico, la utilización de la firma electrónica y demás servicios electrónicos, es el COMEXI²⁶.

Todos estos documentos que forman parte de la regulación de la Firma Electrónica vigente en Ecuador, y que se han referenciado en esta parte del proyecto, están publicados en <http://www.regulaciontelecomunicaciones.gob.ec/firma-electronica-regulacion-vigente/>.

²⁵ Superintendencia de Telecomunicaciones

²⁶ Consejo de Comercio Exterior e Inversiones

1.3.CORREO ELECTRÓNICO

El correo electrónico (electronic mail o e-mail) es un servicio que permite la transferencia y recepción de mensajes a través de redes de comunicación, al emplear sistemas informáticos configurados como servidores de correo, que posibilitan su intercambio independientemente del tipo de redes intermedias para llegar a los destinatarios.

Esto ha renovado las formas convencionales de comunicación, dotándonos de un sistema cuya simplicidad y efectividad facilita la comunicación desde y hacia cualquier lugar del mundo.

1.3.1. ESTRUCTURA DE UNA DIRECCIÓN DE CORREO ELECTRÓNICO

Para utilizar este servicio, los usuarios deben registrarse y obtener una cuenta de un servidor de correo electrónico, administrado por un proveedor, o la institución a la que pertenecen, el cual les asignará una dirección que los identifique de manera única ante los demás; esta dirección es creada generalmente de acuerdo al nombre del usuario solicitante, y a ciertos parámetros con los que fue configurado el servidor de correo, como el nombre del host y el dominio al que pertenece; su estructura es la que se muestra en la Figura 18.

Si se trata de correo institucional, el formato adoptado mayoritariamente para establecer el nombre de usuario es colocar la inicial del primer nombre, seguido del apellido, aunque no hay un estándar establecido referente a esto, de hecho, al crear una cuenta de correo gratuita como hotmail, yahoo, gmail, el nombre de usuario lo elige el solicitante, de acuerdo a ciertas recomendaciones o sugerencias de los proveedores; éste parámetro de la dirección electrónica

es el único que difiere, en comparación con el resto de direcciones gestionadas bajo el mismo dominio del servidor.

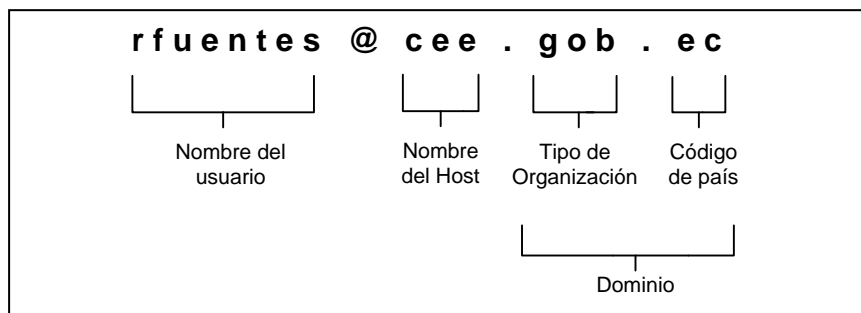


Figura 18. Estructura de una dirección electrónica

Fuente: Modificado de Valzacchi. Capítulo 4: Correo Electrónico. Recuperado de <http://www.educoas.org/portal/bdigital/contenido/valzacchi/ValzacchiCapitulo-4New.pdf>

El signo @ al no tener ninguna similitud con cualquier letra o número, es empleado como un delimitante para identificar que parte de la dirección pertenece al usuario, y que parte al dominio al que está vinculada.

El nombre del host identifica al proveedor o institución que administra este servicio, pueden ser proveedores que ofrecen el servicio gratuita y abiertamente como yahoo, hotmail o gmail, y aquellos que son pagados, por ejemplo aquel correo que un proveedor de internet ofrece como servicio adicional por contratar y mantener un enlace. Algunas entidades por razones de seguridad prefieren implementar un servidor de correo electrónico institucional administrado internamente, esto les garantiza mayor confiabilidad al intercambiar información a través de este medio.

El dominio está integrado por una parte que identifica al tipo de organización, y otra al país de origen del servidor. Algunos ejemplos de estos parámetros son los que muestra la Tabla 9.

Tabla 9. Ejemplos de dominios de nivel superior

Tipo de Organización		País	
Identificador	Significado	Identificador	Significado
.com	Empresas o entidades comerciales	.ec	Ecuador
.org	Organismos no gubernamentales sin fines de lucro	.ar	Argentina
.edu	Instituciones educativas	.au	Australia
.gov	Organismos gubernamentales	.jp	Japón
.net	Servicios de internet	.co	Colombia
.int	Organismos internacionales	.es	España
.mil	Organismos militares	.us	Estados Unidos

Fuente: Creado a partir de Valzacchi. Capítulo 4: Correo Electrónico. Recuperado de <http://www.educoas.org/portal/bdigital/contenido/valzacchi/ValzacchiCapitulo-4New.pdf>
Cisco Networking Academy. Malla Curricular CCNA 1 versión 4.0

1.3.2. COMPONENTES Y FUNCIONAMIENTO

El correo electrónico está estructurado de acuerdo a un modelo cliente - servidor, que se comunican entre sí a través de protocolos para posibilitar la transferencia de mensajes. El proceso inicia y termina en el extremo del cliente, cuando éste envía o recibe un mensaje empleando una aplicación cliente de correo denominada MUA²⁷, como Microsoft Outlook, Eudora o Mozilla Thunderbird.

Los servidores de correo están configurados para desempeñar dos procesos diferentes: de agente de transferencia de correo (MTA²⁸), que reenvía los mensajes hacia el MTA que administra el buzón del destinatario; y de agente de entrega de correo (MDA²⁹), que almacena los mensajes en los buzones correspondientes a cada destinatario para su posterior entrega (véase Figura 19).

²⁷ **Mail User Agent** – Agente de Usuario de Correo

²⁸ **Mail Transport Agent**

²⁹ **Mail Delivery Agent**

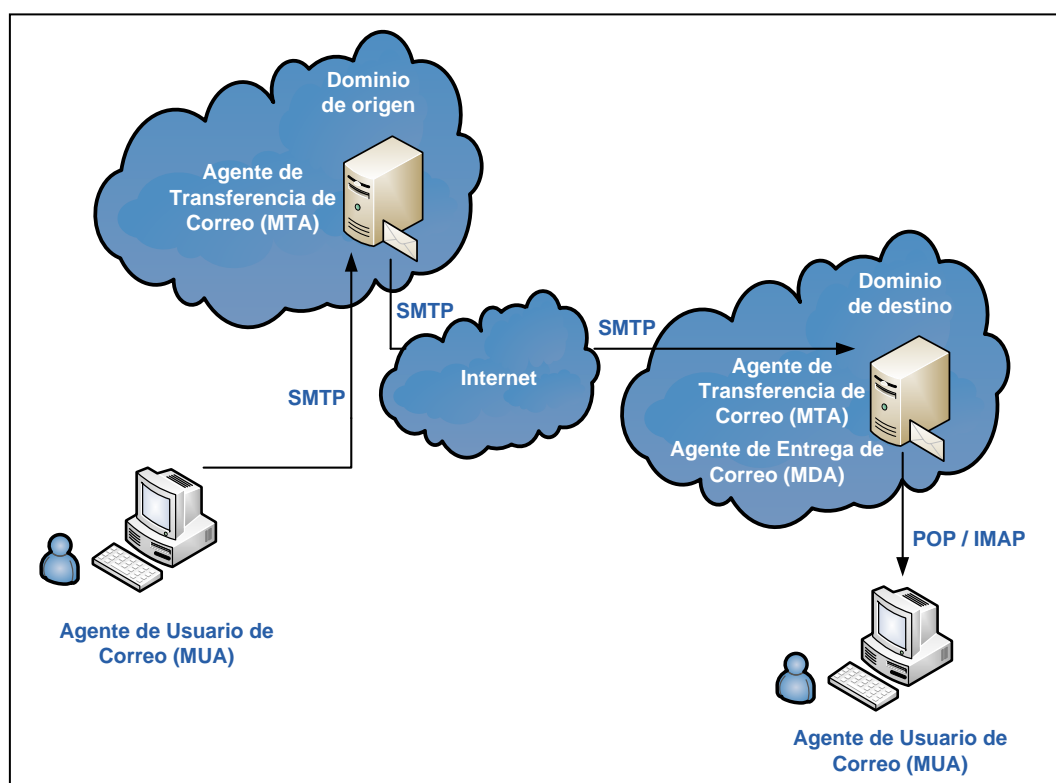


Figura 19. Estructura y Funcionamiento del Correo Electrónico

Fuente: Modificado de Veiga, M. (2008). Redes y Servicios Telemáticos - Aplicaciones. Recuperado de <http://www-gris.det.uvigo.es/wiki/pub/Main/PaginaRst/Tema3.pdf>
Cisco Networking Academy. Malla Curricular CCNA 1 versión 4.0

El cliente de correo (MUA) por parámetros de su configuración identifica a su servidor de correo MTA saliente, entonces para enviar un mensaje, se lo transfiere mediante el protocolo SMTP³⁰ (véase Figura 20). Luego el MTA saliente utiliza el dominio de la dirección del destinatario, e inicia una comunicación con el DNS³¹ al que está vinculado, para identificar al MTA que administra este dominio. Con ello, el MTA de origen establece una conexión TCP con puerto destino 25 (estándar de SMTP), hacia el servidor MTA destino, y le transfiere el mensaje original. Finalmente este servidor de destino verifica si tiene alojada la dirección del receptor, y opera como agente MDA para almacenar el mensaje en el buzón del destinatario correspondiente, para su próxima descarga o visualización.

³⁰ **Simple Mail Transfer Protocol** – Protocolo para la Transferencia Simple de Correo

³¹ **Domain Name System** – Sistema de Nombre de Dominio

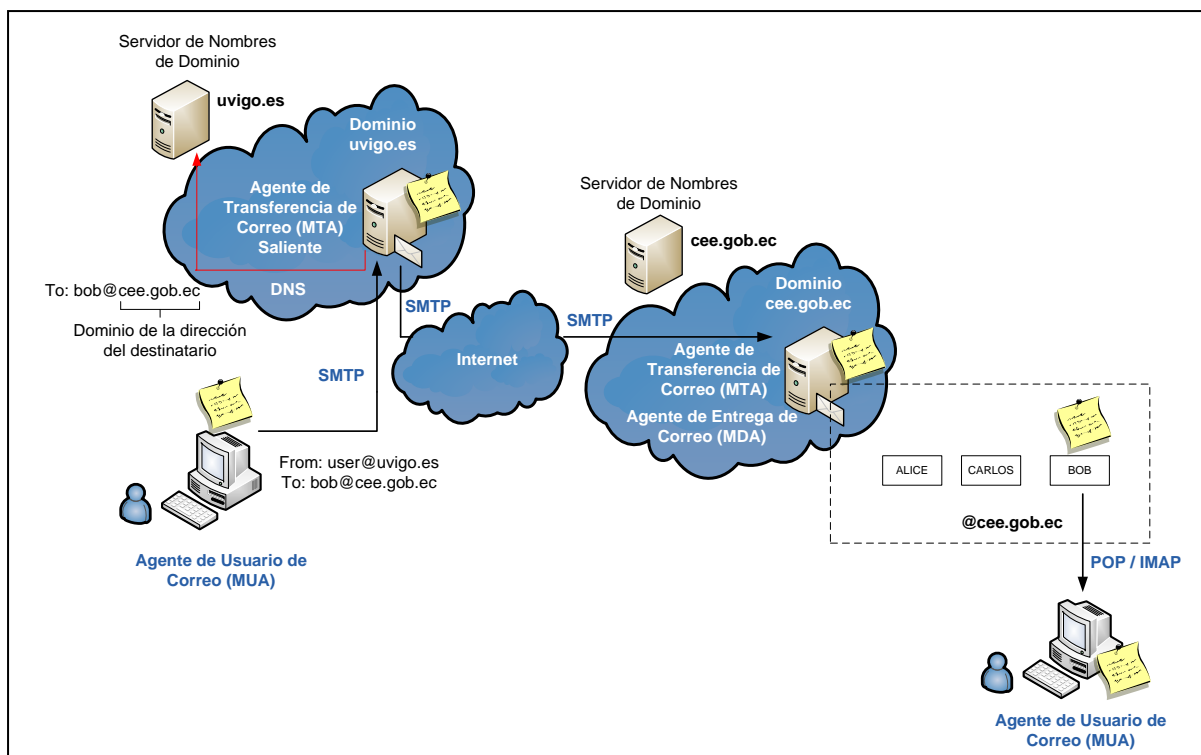


Figura 20. Proceso de envío y recepción de un mensaje de datos a través de correo electrónico

Fuente: Modificado de Veiga, M. (2008). Redes y Servicios Telemáticos - Aplicaciones. Recuperado de <http://www-gris.det.uvigo.es/wiki/pub/Main/PaginaRst/Tema3.pdf>
Cisco Networking Academy. Malla Curricular CCNA 1 versión 4.0

Si existen circunstancias en las que el MTA origen no puede establecer conexión directa con el MTA destino, el protocolo SMTP activa mecanismos que posibilitan la transferencia de mensajes empleando MTAs intermedios hasta llegar al destino.

El MDA cumple con algunas funciones de entrega, como análisis de virus o correo no deseado, y se mantiene en espera constante de que el MUA se conecte al servidor para entregar los mensajes almacenados en los buzones. Esta entrega se realiza a través de dos diferentes protocolos, POP3³² en el caso de que el MUA descargue los correos del MDA para almacenar una copia de ellos en el ordenador del cliente, e IMAP³³ para revisión remota de los buzones.

³² Post Office Protocol v3 – Protocolo de Oficina de Correos versión 3

³³ Internet Message Access Protocol – Protocolo de Acceso a Mensajes de Internet

Esta es la estructura bajo la cual operan la mayoría de las comunicaciones de correo electrónico, aunque existen otras alternativas propietarias como Lotus Notes de IBM o Exchange de Microsoft, en las cuales puede variar de cierto modo esta estructura, en especial por la utilización de protocolos propietarios.

El servicio de correo web es otra alternativa, que integra en los servidores aplicaciones que le permiten al usuario acceder a su buzón, a través del protocolo HTTP³⁴, descartando la necesidad de instalar programas de cliente MUA en los equipos finales; algunos ejemplos de este tipo de servidores son hotmail, yahoo o gmail.

1.3.2.1. SMTP (Simple Mail Transport Protocol)

Es un protocolo que debido a sus constantes modificaciones para perfeccionar su funcionamiento, se ha establecido como un estándar para las comunicaciones de correo electrónico en internet. Su primera versión fue definida en la RFC 821, la siguiente que implantaba varios cambios lo define la RFC 1123, finalmente en la actualidad este protocolo es de uso masivo y se denomina SMTP Extendido (ESMTP), definido en la RFC 2821.

Su funcionamiento se basa en la interacción entre agentes (MUA-MTA o MTA-MTA), al intercambiar instrucciones y respuestas formadas por caracteres ASCII, que representan las operaciones a ejecutarse, como por ejemplo: iniciar sesión, identificar al emisor, al receptor o finalizar sesión.

³⁴ **Hypertext Transfer Protocol** – Protocolo de Transferencia de Hipertexto

Estas instrucciones o comandos se encuentran definidas en la RFC 1651, en la que consta un registro de las extensiones del protocolo SMTP, nuevos comandos SMTP, y parámetros adicionales de los comandos MAIL FROM y RCPT TO; algunas de las instrucciones más comunes se muestran en la Tabla 10.

Tabla 10. Comandos usuales que emplea SMTP

Comando	Descripción
HELO	Comando para abrir una sesión con el servidor.
EHLO	Permite que el servidor envíe un listado de extensiones o comandos nuevos que soporta SMTP, para determinar su compatibilidad con los comandos de SMTP Extendido (ESMTP).
HELP	Devuelve una lista de comandos compatibles con SMTP. Si se especifica un parámetro proporciona información referente al comando escrito.
EXPN	Solicita al servidor listas de correo.
DATA	Indica que a partir de la siguiente línea es el inicio del mensaje (cabecera y contenido). Para indicar el final del mensaje se escribe una línea solamente con un punto (".").
MAIL FROM	Identifica al remitente del mensaje
RCPT TO	Identifica el o los destinatarios del mensaje.
VRFY	Comprueba que un buzón está disponible para la entrega de mensajes.
AUTH	Sirve para autenticarse ante el servidor, empleando el método indicado, para cifrar el usuario y la contraseña.
NOOP	Se utiliza para comprobar que la conexión con el servidor sigue activa, y que el servicio está disponible. Si es el caso, el servidor responde un OK.
TURN	El emisor cede el turno al receptor para que actúe como emisor, sin necesidad de establecer una nueva conexión.
RSET	Aborta el envío actual y reinicia la comunicación desde que se creó la conexión.
QUIT	Finaliza la conexión con el servidor.

Fuente: Modificado a partir de Lara, E. 10º Unidad Didáctica: Correo Electrónico. Recuperado de <http://personals.ac.upc.edu/elara/documentacion/INTERNET%20-%20UD10%20-20Correo%20Electronico.pdf>

Los códigos de respuesta del servidor MTA a diferencia de los comandos del cliente, se caracterizan por mantener un formato de tres dígitos más una descripción, la parte numérica significa un proceso como respuesta a una solicitud, y obviamente el propósito de la descripción es para interpretación de las personas. Las respuestas se clasifican en categorías dependiendo del primer dígito del código (véase Tabla 11).

Tabla 11. Códigos de Respuesta del Servidor SMTP

Código	Descripción
2??	La acción solicitada mediante el comando se ejecutó correctamente.
3??	Se aceptó la orden del comando pero se esperan más datos.
4??	El comando ha sido rechazado de forma temporal.
5??	Falló permanentemente debido a que no hay permisos o a que el comando está mal escrito.

Fuente: Modificado a partir de Lara, E. 10^o Unidad Didáctica: Correo Electrónico. Recuperado de <http://personals.ac.upc.edu/elara/documentacion/INTERNET%20-%20UD10%20-%20Correo%20Electronico.pdf>

El formato de un mensaje lo integran la cabecera, en la que se escriben parámetros como subject (asunto), from (de), o to (para), y el cuerpo del mensaje que es el texto en cuestión. La Figura 21 muestra un ejemplo de una conexión SMTP, en la cual C es el cliente y S el servidor.

1.3.2.2. POP3 (Post Office Protocol v3)

Es un protocolo estándar de capa aplicación del modelo OSI diseñado únicamente para recibir correos, por tal motivo, es utilizado por clientes de correo MUA para descargar mensajes desde servidores de correo local o remoto. Originalmente en su primera etapa de desarrollo fue denominado POP, la versión 2 de este protocolo fue estandarizada con el

puerto 109, finalmente a la versión 3 que fue la más difundida y de uso actual, se le asignó el puerto 110.

```

S: 220 Servidor ESMTP
C: HELO
S: 250 Hello, please meet you
C: MAIL FROM: yo@midominio.com
S: 250 Ok
C: RCPT TO: destinatario@sudominio.com
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: Subject: Campo de asunto
C: From: yo@midominio.com
C: To: destinatario@sudominio.com
C:
C: Hola,
C: Esto es una prueba.
C: Adios.
C: .
S: 250 Ok: queued as 12345
C: quit
S: 221 Bye

```

Figura 21. Conexión SMTP

Fuente: Obtenido de Wol, A. Telemática. Recuperado de <http://es.scribd.com/doc/49816497/Telematica>

La comunicación POP cliente-servidor se ejecuta en base a ciertos estados, inicialmente los clientes POP (MUA) inician la conexión TCP con el servidor empleando el puerto 110, este es el estado de autorización, en el que el servidor espera el nombre de la cuenta de usuario y la contraseña respectiva. Al verificar que son los correctos bloquea temporalmente el buzón para que ningún otro usuario pueda acceder a éste, mientras dure la conexión, y cambia al estado de transacción, atendiendo las solicitudes como la descarga de mensajería del buzón. Al finalizar, el cliente mediante el comando QUIT origina que el servidor cambie al estado de actualización, para eliminar los mensajes descargados y dar por terminada la sesión.

Toda esta comunicación análogamente a SMTP, se basa en el intercambio de instrucciones (comandos) en base a ciertas palabras clave para solicitar alguna acción, y respuestas a estas

instrucciones, formadas por un campo numérico y un texto descriptivo. La RFC 1939 describe los comandos, respuestas y funcionamiento de POP3.

La particularidad de este protocolo es que establece una conexión temporal con el servidor, mientras dure la descarga de la mensajería pendiente en el equipo del usuario, esto le permite revisarla más adelante; esta conexión puede establecerse localmente, o a través de internet, dependiendo de la ubicación del servidor.

La versión 3 de este protocolo incorpora una serie de comandos adicionales con respecto a las anteriores, enfocados principalmente en mejorar la seguridad; actualmente cuenta con métodos de autenticación seguros como APOP que utiliza funciones hash MD5 para proteger de ataques a las contraseñas de usuario, de hecho algunos MUA como Eudora, Mozilla Thunderbird o Novell Evolution ya la implementan.

1.3.2.3. IMAP (Internet Message Access Protocol)

Este protocolo fue desarrollado por Mark Crispin en 1986 como una alternativa a POP3, diseñado para posibilitar la administración remota de buzones de mensajería. Opera en función de un modelo cliente-servidor definido en la RFC 1730, pero a diferencia de POP3 permite al usuario manipular su mensajería directamente sobre el servidor, manteniendo con este una conexión TCP permanente mediante el puerto 143 (estándar IMAP), que puede ser local, o remota a través de internet, dependiendo de la ubicación del servidor.

Esta característica puede ser relevante en ambientes en los cuales los usuarios comparten sus ordenadores, permitiéndoles utilizar diferentes ordenadores cada vez para revisar su mensajería, sin el riesgo de que posteriormente alguien más lo haga (véase Figura 22).

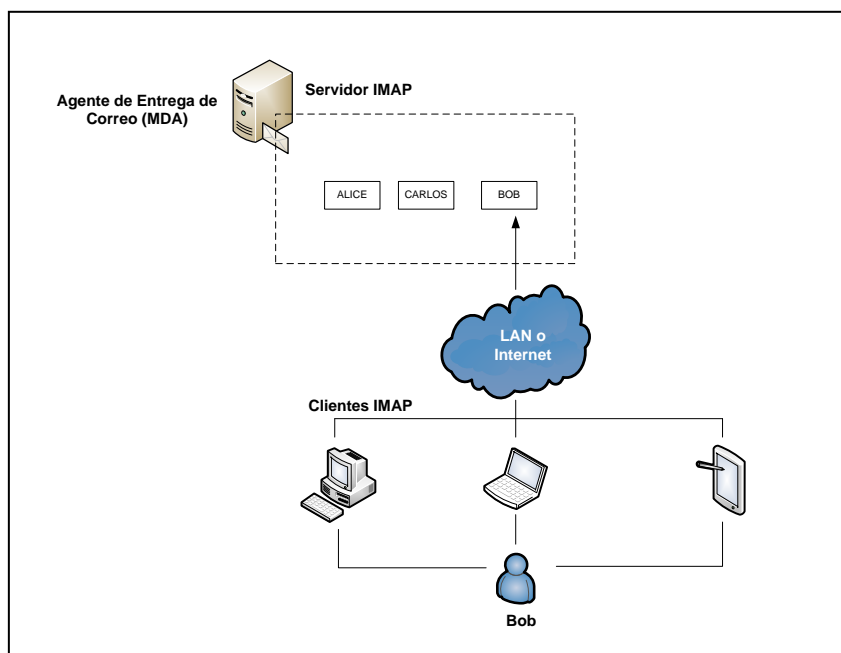


Figura 22. Funcionamiento de IMAP

Fuente: Modificado a partir de Jara, F. A. (2012). Sistema Selectivo de Correos Electrónicos Orientado a Dispositivos Móviles NMM: No More Mails (Tesis de Pregrado). Recuperado de <http://cybertesis.uach.cl/tesis/uach/2012/bmfcij.37s/doc/bmfcij.37s.pdf>

Complementariamente IMAP a diferencia de POP3 permite el acceso simultáneo de diversos usuarios a la misma cuenta de correo, actualizando todos los cambios que se efectúen de forma inmediata, para dar mayor flexibilidad a aquellos usuarios que utilizan dispositivos móviles.

1.3.3. SEGURIDAD EN CORREO ELECTRÓNICO

El correo electrónico es una aplicación cuya simplicidad de uso y funcionamiento, lo han transformado en un estándar de comunicación, pero es precisamente esta característica la que lo convierte en vulnerable, considerando que por este medio circula gran flujo de tráfico de datos sin ningún tipo de protección.

Una alternativa de seguridad es proteger la transferencia de correo empleando protocolos de transporte seguro como TLS, mediante una extensión STARTTLS (definida en la RFC 3207 para SMTP y RFC 2595 para POP3 e IMAP). Esto implica que para garantizar fiabilidad en la comunicación extremo a extremo, será necesario en algunos casos asegurar enlaces establecidos entre MTAs intermedios.

El problema con ello es que el correo electrónico está diseñado para operar bajo un esquema almacenamiento-reenvío, de esta manera, TLS protege a los datos en tránsito a través de las redes, pero durante su almacenamiento en nodos intermedios o finales (MDA) quedan totalmente vulnerables, pudiendo ser revisados o alterados antes de que lo haga el destinatario legítimo.

Esto ha generado el desarrollo de técnicas de seguridad que protejan al correo electrónico durante todo el proceso de transferencia hacia el destinatario, sin necesidad de implantar adicionalmente mecanismos complejos de seguridad a nivel de capa transporte o red, o peor aún modificando la infraestructura de correo.

Actualmente la mayoría de plataformas de correo electrónico seguras emplean técnicas criptográficas en los agentes MUA, que generen correos auto-protegidos mediante cifrado y/o firma digital en capa aplicación, de modo que los MTA los transfieran de forma convencional a su destino. Algunos de estos sistemas de seguridad usados comúnmente son PGP y S/MIME.

1.3.3.1. S/MIME (SECURE / MULTIPURPOSE INTERNET MAIL EXTENSIONS)

Las Extensiones Multipropósito de Correo Electrónico (MIME) son una serie de estándares desarrollados para mejorar la capacidad de transferencia de correo, posibilitando la inserción, envío e interpretación de archivos, como imágenes, audio, video, entre otros. Están definidas en las RFCs 2045, 2046, 2047, 4288, 4289 y 2077.

Secure MIME (S/MIME) es una especificación de seguridad para correo electrónico inicialmente desarrollada por RSA Data Security (RFC 2632-2634), empleada para la transferencia de mensajes MIME protegidos mediante técnicas criptográficas, de acuerdo al formato estandarizado PKCS#7³⁵.

PKCS#7 es el formato de los mensajes MIME con protección criptográfica, caracterizado por soportar la integración de certificados digitales X.509, para avalar la relación usuario – clave pública, en comunicaciones seguras. Establece la estructura de este tipo de mensajes, y representa a su contenido mediante un identificador, para definir si está firmado digitalmente, cifrado, cifrado y firmado, firmado y cifrado, o simplemente datos en texto plano.

³⁵ **Public Key Cryptography Standards** – Estándar Criptográfico de Clave Pública

Entonces en un mensaje S/MIME pueden existir tres tipos de contenido PKCS#7: Data, SignedData o EnvelopedData.

1.3.3.1.1. Data

Este es el formato convencional de los mensajes, cuando se generan sin ningún tipo de protección criptográfica. En S/MIME mensajes de este tipo deben complementarse con contenidos SignedData o EnvelopedData para ser transferidos por correo electrónico de manera segura.

1.3.3.1.2. SignedData

Este formato representa la estructura del contenido de un mensaje firmado digitalmente, contiene diversos campos como lo muestra la Tabla 12.

1.3.3.1.3. EnvelopedData

Este formato representa al contenido del mensaje cuando está en un sobre digital, esto significa que fue cifrado con una clave de sesión simétrica, que a su vez es cifrada con la clave pública del destinatario (sobre digital); tanto el mensaje como el sobre son enviados conjuntamente, de forma que el receptor abra este sobre empleando su clave privada y tenga acceso a la clave de sesión para descifrar el mensaje. La estructura de este formato lo muestra la Tabla 13.

Tabla 12. Estructura PKCS#7 de un mensaje S/MIME firmado digitalmente

CAMPO	TIPO	DESCRIPCIÓN
version	Entero	Especifica la versión del formato con estructura SignedData.
digestAlgorithms (rep.)		Es una lista de algoritmos hash empleados para firmar los datos.
algorithm parameters	Identificador único (Depende del algoritmo)	
contentInfo	Mensaje PKCS#7	Son los datos a firmar en formato PKCS#7, puede ser Data para firmar datos en texto plano, o Enveloped-Data para datos cifrados.
certificates (opc. rep.)	Certificado X.509	Contiene certificados o cadenas de certificados empleados para comprobar la legitimidad de las claves públicas de los firmantes.
crls (opc. rep.)	CRL	Contiene CRLs que complementan la operación anterior.
signerInfos (rep.)		Está integrado por una estructura con diversos campos para cada firmante.
version	Entero	Es la versión del formato de esta estructura.
issuerAndSerialNumber		Identifica la clave pública del firmante, empleando el nombre de la CA (DN=Distinguished Name) y el número de serie del certificado.
issuer serialNumber	DN Entero	
digestAlgorithm		Es el algoritmo hash usado por el firmante, tiene que ser uno de los que contiene el campo digestAlgorithm del inicio
algorithm parameters	Identificador único (Depende del algoritmo)	
authenticatedAttributes (opc. rep.)	Atributo X.501	Es un conjunto de atributos añadidos a los datos sobre los que se calcula la firma.

CAMPO	TIPO	DESCRIPCIÓN
digestEncryptionAlgorithm		Es el algoritmo con el que el firmante ha cifrado el hash.
algorithm parameters	Identificador único (Depende del algoritmo)	
encryptedDigest	Cadena de bytes	Es la firma digital, el hash cifrado con la clave privada del firmante.
unauthenticatedAttributes (opc. rep.)	Atributo X.501	Es un conjunto de atributos adicionales que no son empleados en la firma.

Nota. El parámetro opc. significa que es un campo opcional, y rep. que es repetible.

Fuente: Creado a partir de Perramon. X. Aplicaciones Seguras. Recuperado de http://ocw.uoc.edu/computer-science-technology-and-multimedia/advanced-aspects-of-network-security/advanced-aspects-of-network-security/P06_M2107_01772.pdf

Tabla 13. Estructura PKCS#7 de un mensaje S/MIME contenido en un sobre digital

CAMPO	TIPO	DESCRIPCIÓN
version	Entero	Especifica la versión del formato con estructura EnvelopedData.
recipientInfos (rep.)		Contiene una estructura con diferentes campos para cada destinatario del mensaje.
version	Entero	Es la versión del formato de la estructura
issuerAndSerialNumber		Sirve para identificar al destinatario al que le corresponde esta estructura, comparando si el nombre de la CA (DN=Distinguished Name) y el número de serie del certificado de este campo coinciden con los suyos.
issuer	DN	
serialNumber	Entero	
keyEncryptionAlgorithm		Identifica al algoritmo de clave pública con el que se ha cifrado la clave de sesión.
algorithm	Identificador único	
parameters	(Depende del algoritmo)	
encryptedKey	Cadena de bytes	Contiene la clave de sesión cifrada con la clave pública del destinatario.
encryptedContentInfo		Contiene información de los datos cifrados.
contentType	Identificador único	Indica que tipo de mensaje PKCS#7 hay en los datos cifrados, Data cuando se ha cifrado el mensaje en texto plano, y SignedData para datos previamente firmados.
contentEncryptionAlgorithm		Es el algoritmo simétrico usado para cifrar los datos, empleando la clave de sesión.
algorithm	Identificador único	
parameters	(Depende del algoritmo)	
encryptedContent (opc.)	Cadena de bytes	Son los datos cifrados en formato de mensaje PKCS#7.

Nota. El parámetro opc. significa que es un campo opcional, y rep. que es repetible.

Fuente: Creado a partir de Perramon. X. Aplicaciones Seguras. Recuperado de http://ocw.uoc.edu/computer-science-technology-and-multimedia/advanced-aspects-of-network-security/advanced-aspects-of-network-security/P06_M2107_01772.pdf

De acuerdo al tipo de protecciones criptográficas aplicadas a los mensajes, estos contenidos se combinan para representar: mensajes con datos firmados (SignedData [Data]), mensajes con datos cifrados (EnvelopedData [Data]), mensajes con datos cifrados y firmados (SignedData [EnvelopedData [Data]]) o mensajes con datos firmados y cifrados (EnvelopedData [SignedData [Data]]).

Esto depende completamente de lo que se quiere priorizar, por ejemplo un mensaje firmado que contiene datos en texto plano (SignedData [Data]), garantiza su integridad y la autenticidad del emisor, pero un mensaje firmado que contenga datos cifrados (SignedData [EnvelopedData [Data]]), garantiza integridad, autenticidad y confidencialidad.

De igual forma, un mensaje cifrado que contiene datos en texto plano (EnvelopedData [Data]), garantiza confidencialidad, pero un mensaje cifrado que contenga datos firmados (EnvelopedData [SignedData [Data]]), garantiza confidencialidad, autenticación e integridad.

1.3.3.2. PGP (PRETTY GOOD PRIVACY)

Es un mecanismo diseñado para proteger cualquier tipo de información mediante técnicas criptográficas, en base a la gestión de claves. Desarrollado por Philip Zimmermann en 1990, su uso fue difundido principalmente para la transferencia de mensajes cifrados y/o firmados digitalmente, a través de correo electrónico.

Su modelo de confianza no implica demasiada complejidad de funcionamiento, en comparación con S/MIME que se basa en jerarquías de entidades certificadoras, por la razón de que al ser distribuido, otorga a cada usuario la potestad de generar su par clave y

emplearlas para establecer comunicaciones seguras. Sin embargo, es precisamente esta característica la que lo torna vulnerable, al no emplear mecanismos como los certificados digitales, para avalar la vinculación legítima entre el usuario y su clave pública.

Una de sus fortalezas es que implementa una transferencia de mensajes de correo eficiente, debido a que en lo posible, los datos son comprimidos antes de ser cifrados, y después de haber sido firmados. Su debilidad es que no está diseñado para soportar la integración de certificados digitales.

CAPÍTULO 2. ANÁLISIS SITUACIONAL DE LA RED INTERNA DE DATOS DE LA INSTITUCIÓN

2.1. CUERPO DE INGENIEROS DEL EJÉRCITO (CEE)

El Cuerpo de Ingenieros del Ejército es una unidad de ingeniería militar encargada de desarrollar obras civiles, viales, petroleras y desminado humanitario en territorio ecuatoriano, con el compromiso de minimizar hasta niveles tolerables, los riesgos a los que están expuestos permanentemente las personas y los recursos ambientales implícitos en este propósito, y aportar de esta forma al desarrollo del país.

Además, conjuntamente con Chile, forman parte de un grupo de naciones que llevan a cabo misiones de paz, para apoyar a la Organización de las Naciones Unidas (ONU) en la reestructuración vial y civil de Haití, tras el desastre natural por el que fue afectado.

2.1.1. MISIÓN INSTITUCIONAL

Ejecutar operaciones de Ingeniería Militar en apoyo a Fuerzas Armadas, al desarrollo nacional, acción del estado y cooperación internacional.

2.1.2. VISIÓN AL 2021

Unidad de Ingeniería Militar líder a nivel regional en apoyo a las operaciones de seguridad, defensa, desarrollo nacional y misiones de paz, con personal altamente capacitado y comprometido, tecnología de punta y flexibilidad para enfrentar nuevos escenarios.

2.2.DESCRIPCIÓN FÍSICA

La sucursal matriz del Cuerpo de Ingenieros del Ejército se encuentra situada en Quito, en la Av. Rodrigo de Chávez Oe4-19 y Jacinto Collahuazo, lugar desde el cual se administran todas las actividades que lleva a cabo esta institución.

Está conformada por personal civil y militar, que comparten las instalaciones de un edificio, y de un campamento adjunto a éste, para cumplir con sus labores cotidianas. Además, cuenta con grupos de trabajo distribuidos en distintos lugares del país, desde los cuales se efectúan las obras y proyectos programados.

El personal militar que desempeña funciones administrativas en esta institución, está constituido por aquellos con rangos superiores en su jerarquía (como sargentos, oficiales, mayores, capitanes, etc.), y ocupan generalmente cargos como las Jefaturas Departamentales. Al personal civil lo integran funcionarios y médicos (personal administrativo), personal de limpieza, obreros y choferes.

Existen aproximadamente cerca de 1000 personas que forman parte del personal administrativo, considerando aquellos que laboran en el edificio, en el campamento, y los grupos de trabajo.

2.2.1. DISTRIBUCIÓN DE ÁREAS

La organización de las oficinas del edificio y el campamento, es en base a la agrupación de diferentes áreas que tienen cierta afinidad o dependencia en las labores que realizan, para formar departamentos.

Mediante una inspección en los racks de backbone, se obtuvo información referente a los puntos de voz y datos existentes, para determinar la cantidad de usuarios que tienen acceso a la red. La Tabla 14 muestra algunos resultados obtenidos.

Tabla 14. Distribución Departamental y Terminales de Red – Edificio

Planta	Departamentos	Puntos de Datos	Puntos de Voz
Subsuelo	Comunicación Social Salud Ocupacional	28	15
Planta Baja	Logística Seguridad Recursos Humanos	80	52
Primer Piso	Sistemas Financiero		
Segundo Piso	Comando Jefatura de Estado Mayor Asesoría Jurídica Comité de Contrataciones Ayudanturía General	55	31
Tercer Piso	Técnico Planificación Institucional		
Cuarto Piso	Obras Viales DEPSIS Obras Civiles	65	37
Quinto Piso	Inteligencia Operaciones SEPRAC Inspectoría		
Total Terminales de Red		228	135

Fuente: Elaborado con la ayuda del Departamento de Sistemas del CEE (2013)

El campamento es un área distribuida en su mayor parte para actividades militares, pero también existen oficinas que mantienen conexión con los dispositivos de red del edificio, para que el personal administrativo que labora en este sector pueda acceder a los servicios que demanden sus actividades de trabajo. La Tabla 15 contempla los resultados que se obtuvieron luego de la inspección de los racks de comunicaciones.

Tabla 15. Distribución Departamental y Terminales de Red – Campamento

Dependencia	Departamentos	Puntos de Datos	Puntos de Voz
Policlínico	Planta Baja Administración y Estadística Estación de Enfermería Emergencia Médico Residente Traumatología Rayos X Laboratorio Clínico Bacteriológico Fisioterapia y Rehabilitación	15	9
	Planta Alta Dirección Secretaría Ginecología Psicología Clínica Medicina General Pediatría Oftalmología Audiometría y Optometría Odontología		
Campamento	Ductos y Refinería	42	14
	UMAT	25	8
	Oficina de Comunicaciones	12	4
	Oficinas Oficiales - Yachay	17	5
	Guardería	1	
Total terminales de red		112	40

Fuente: Elaborado con la ayuda del Departamento de Sistemas del CEE (2013)

2.3.DESCRIPCIÓN DE LA RED

La red interna de datos del edificio matriz es una red conmutada, estructurada por una zona de red desmilitarizada que protege los servidores, un segmento de red para los usuarios LAN, y un segmento que contiene los puntos de última milla de proveedores de enlaces contratados, distribuidos en una topología de red en estrella, cuyo punto central es un switch de capa 3 (véase Figura 23).

Este switch Ethernet, marca H3C modelo S7506E (véase Tabla 16), tiene instalada (en el primer slot - soporta 8) una tarjeta que dispone de 24 puertos de fibra óptica y 12 de cobre, admitiendo la interconexión de los segmentos de red, y la administración de los servicios empleando Vlans.

Tabla 16. Switch Capa 3 – Especificaciones Técnicas

Item	Descripción
Dimensiones (altura x ancho x profundidad)	575 x 436 x 420 mm
Peso máximo (configuración completa)	77 Kg
Total de Slots	8
LPU slots	6
Fuente de Alimentación	-48 VDC to -60 VDC 100 VAC to 240 VAC
Entorno de Funcionamiento	Temperatura: 0°C a 45°C (32°F a 113°F) Humedad (sin condensación): 10% a 95%
Capacidad de Conmutación	2.56 Tbps
Throughput	1920 Mpps
Funciones de Capa 2	IEEE 802.1p (CoS priority), IEEE 802.1Q (VLAN), IEEE 802.1d (STP)/802.1w (RSTP)/802.1s (MSTP), IEEE 802.1ad (QinQ), selective QinQ, and VLAN mapping, IEEE 802.3x (full-duplex flow control) and

	backpressure flow control (half-duplex), IEEE 802.3ad (link aggregation) and multi-card link aggregation, IEEE 802.3 (10BASE-T)/802.3u (100BASE-T), IEEE 802.3z (1000BASE-X)/802.3ab (1000BASE-T), IEEE 802.3ae (10G base), IEEE 802.3af (PoE), IEEE 802.3at (PoE+), RRRP Inter-card port mirroring and flow mirroring, Port broadcast/multicast/unknown unicast storm suppression, Jumbo Frame, Port VLAN, protocol VLAN, subnet VLAN, and MAC VLAN, Super VLAN, PVLAN, Multicast VLAN+, Point-to-point single-VLAN cross-connection and dual-VLAN cross-connection, VLAN-ID-based forwarding without involving MAC address learning, Maximum VLAN mapping and selective QinQ entries, 1:1, 2:1,1:2, and 2:2 VLAN mappings, GVRP, LLDP
Enrutamiento IPv4	ARP proxy, DHCP relay, DHCP server, Static routing, RIPv1/v2, OSPFv2, IS-IS, BGPv4, OSPF/IS-IS/BGP Graceful Restart, ECMP, Policy-based, routing, Routing policy
Enrutamiento IPv6	ICMPv6, ICMPv6 redirection, DHCPv6, ACLv6, OSPFv3, RIPng, BGP4+, IS-ISv6, Manual tunnels, ISATAP, 6to4 tunnels, IPv6/IPv4 dual stack
Multicast	IGMPv1/v2/v3, IGMPv1/v2/v3 snooping, IGMP filter, IGMP fast leave, PIM-SM/PIM-DM/PIM-SSM, MSDP, AnyCast-RP, MLDv2/MLDv2 , nooping, PIM-SMv6, PIM-DMv6, and PIM-SSMv6
ACL/QoS	Up to 16K ACLs per card, Basic ACLs and advanced ACLs, VLAN-based ACL, Ingress ACLs and egress ACLs, Ingress CAR and egress CAR with the granularity of 8 kbps, Two levels of meter, Aggregate CAR based on VLANs and MAC addresses, Traffic shaping, IEEE 802.1p/DSCP priority marking and remarking, H-QoS and three-level queue scheduling, Queue scheduling mechanisms, including SP, WRR, SP+WRR and CBWFQ, Congestion avoidance mechanisms, including Tail-Drop and WRED, Mirroring
MPLS/VPLS	Layer 3 MPLS VPN, Layer 2 VPN: VLL (Martini and Kompella), MCE, MPLS OAM, VPLS and VLL, Hierarchical VPLS and QinQ+VPLS access, P/PE, LDP
Seguridad	EAD solution, Portal authentication, MAC authentication, IEEE 802.1X and IEEE 802.1X server, AAA/RADIUS, HWTACACS and command line authentication, SSHv1.5/SSHv2, ACL-based flow filtering, Plaintext and MD5 authentication for OSPF, RIPv2, and BGPv4, Hierarchical protection of command lines to prevent unauthorized users and grant different configuration rights to different levels of users, Telnet login control through IP address and password, Multiple binding combinations of IP address, VLAN ID, MAC address, and port number, uRPF, Primary/secondary data backup, Fault alarm and automatic recovery, Data logs
Administración del Sistema	FTP, TFTP, and XMODEM, SNMP v1/v2/v3, sFlow traffic statistics, RMON, NTP clocks, NetStream traffic statistics, Intelligent power management, Online monitoring of MPU engine, backplane, chip, and storage

Fuente: Elaborado a partir de H3C. (2014). *Products and Solutions*. Recuperado de http://www.h3c.com/portal/Products___Solutions/Products/Switches/H3C_S7500E_Series_Switches/Detail_Material_List/201311/804645_57_0.htm

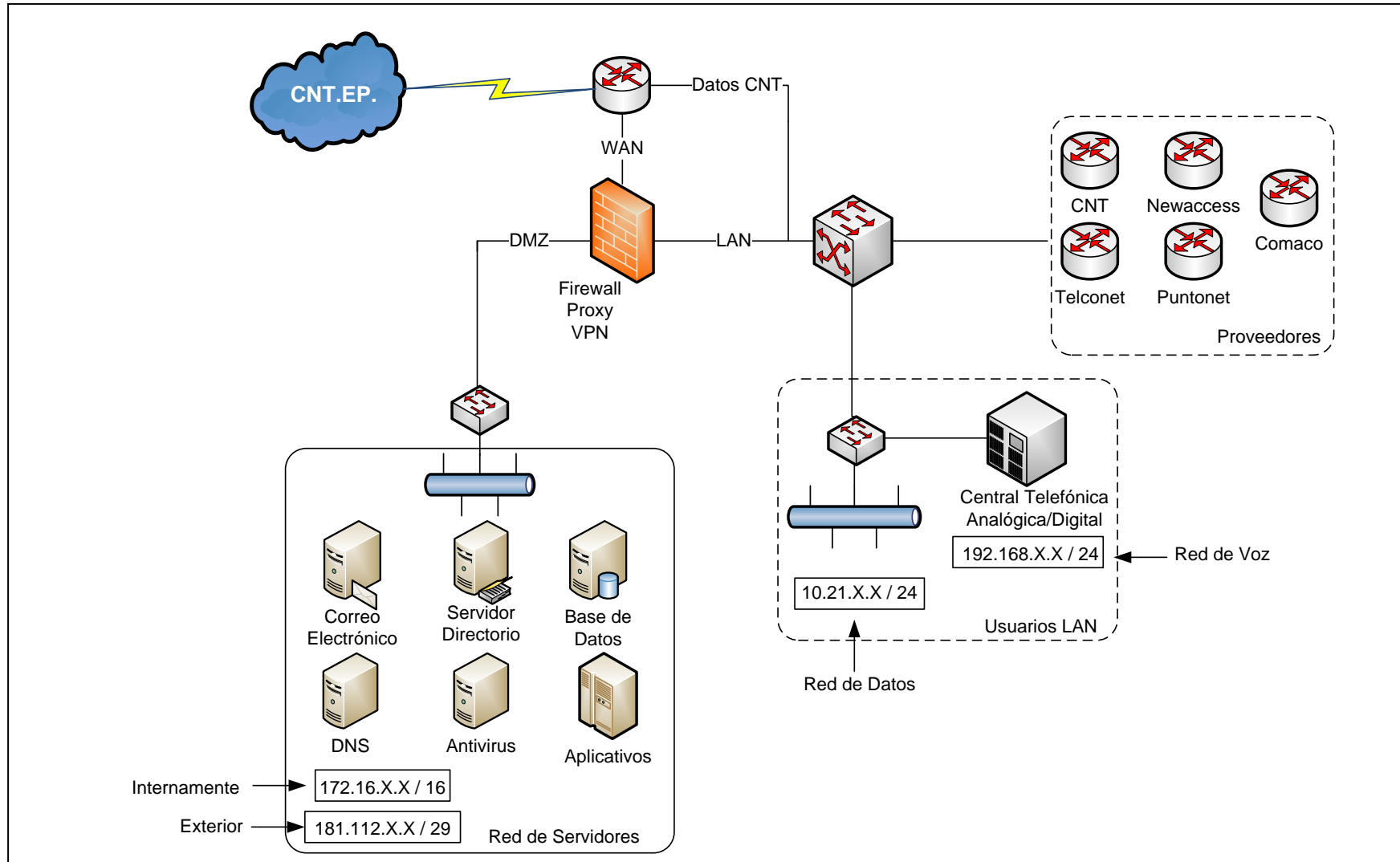


Figura 23. Diagrama de la Topología Lógica de la Red de Datos del CEE - Quito

Fuente: Elaborado a partir de información facilitada por el Departamento de Sistemas del CEE (2013)

El firewall dispone de tres interfaces de fibra óptica, que se conectan al router del proveedor de internet CNT. EP., a la interfaz LAN del switch capa 3, y a la DMZ. Desarrollado bajo la aplicación ISA³⁶ Server propietaria de Windows, configurado para operar como firewall, proxy y VPN (véase Tabla 17). Estos tres servicios están vinculados al dominio de la organización, para administrar permisos y restricción de páginas.

Tabla 17. Firewall - Características de Hardware y Software

Descripción	Detalle
Servidor	Hewlett-Packard (HP)
Sistema Operativo	Windows 2003
Memoria RAM	2 GB
Procesador	Intel Xeon 2,8 GHz

Fuente: Elaborado a partir de información facilitada por el Departamento de Sistemas del CEE (2013).

En lo referente a sistemas de almacenamiento de respaldos de energía, esta organización dispone de dos UPS instalados en el subsuelo (FERRUPS Series – véase Tabla 18), que se encuentran habilitados para operar al suscitarse inconvenientes de provisión de energía eléctrica, pero el sistema principal que se activa en estas instancias es la planta eléctrica, su generador se encuentra instalado en los exteriores del edificio.

Tabla 18. UPS – Especificaciones Técnicas

Item	Descripción
Rango de Energía	500 VA a 18 kVA
Voltaje	120/208/240
Frecuencia	60 Hz
Configuración	Torre
Serie del Producto	Powerware

Fuente: EATON. (2014). *Productos y Servicios*. Recuperado de <http://powerware.eaton.com/Products-services/Backup-Power-UPS/FERRUPS.aspx?cx=116&GUID=5704F961-4815-4C8F-A938-48C994CB023E>

³⁶ Internet Security and Acceleration

La desventaja es que estos sistemas están diseñados para abastecer de energía a todo el edificio, no existe un sistema destinado específicamente para proveer respaldo de energía a los equipos de comunicación. El cuarto de equipos dispone de un sistema de calefacción que suministra aire de precisión entre 19 -21° C.

2.3.1. BACKBONE Y CABLEADO HORIZONTAL

El backbone de la red se encuentra estructurado por racks distribuidos en ciertas plantas del edificio, y los departamentos del campamento (véase Figura 24). El cuarto de equipos se encuentra en la primera planta, departamento de sistemas, desde el cual se distribuye el cableado horizontal hacia las estaciones finales de esta, y la planta baja.

El cableado del rack de la tercera planta, se distribuye también hacia las estaciones finales de la segunda, el de la quinta planta también hacia la cuarta, y el del subsuelo únicamente hacia esa planta.

Todas las plantas del edificio tienen instalado un access point TP-Link para acceso inalámbrico, como una alternativa de conexión, siendo la red cableada el medio de transmisión principal, pero en el subsuelo el departamento de Comunicación Social no dispone de red cableada, el acceso es totalmente inalámbrico, este es el motivo por el cual el rack de esa planta es el más pequeño.

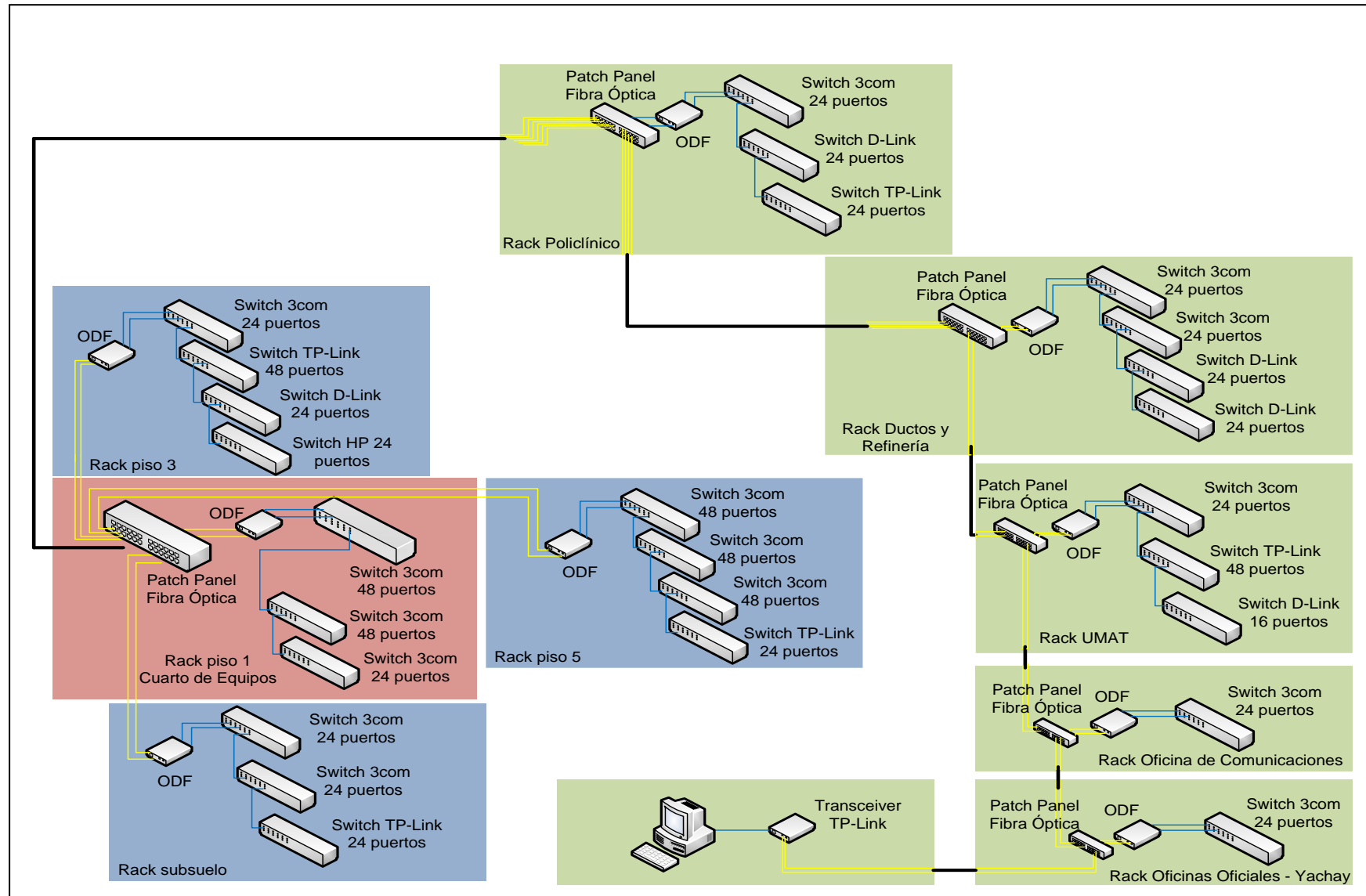


Figura 24. Diagrama de Backbone de la Red de Datos del CEE - Quito

Fuente: Elaborado a partir de información facilitada por el Departamento de Sistemas del CEE (2013).

La zona del campamento a diferencia del edificio, tiene dispersas las oficinas, la distribución de los racks se extiende por toda esta zona. El rack más cercano al edificio es el del Policlínico, y únicamente los departamentos Ductos y Refinería, y UMAT, se encuentran en oficinas contiguas entre sí. El rack de la guardería por el momento no tiene switchs activos, debido a que únicamente utilizan una computadora.

Todo el backbone se conecta mediante dos hilos de Fibra Óptica Multimodo, dispuestos uno como enlace principal y otro de respaldo, llegan a un ODF³⁷, y luego a los switchs de cada rack. Hacia el campamento se distribuyen 6 hilos de fibra por tubería subterránea, destinados a enlazar las dependencias principales, Policlínico, Ductos y Refinería, y UMAT. Las otras tres dependencias también mantienen la misma distribución de dos hilos de fibra subterránea, que se derivan a partir de las principales.

Se emplean cuatro tipos de switch: 3com 5500, TP-Link modelo TL-SG2224, hp Procurve y D-Link, de 16, 24, 48 o 52 puertos. Para normalizar el uso de los puertos de los switchs, se utilizan los últimos para conexiones en cascada, y los iniciales para enlaces principales.

El cableado horizontal está implementado con cable UTP categoría 5e, tanto para los ordenadores, como para los teléfonos IP. Cada funcionario de esta organización cuenta normalmente con un ordenador de escritorio y un teléfono IP, pero existen algunos que utilizan computadoras portátiles, en especial el personal militar, y también hay quienes utilizan teléfonos convencionales adaptados a la red IP.

³⁷ Distribuidor de Fibra óptica

El sistema operativo bajo el cual operan los ordenadores es Windows en varias versiones (98, XP y Windows 7), sobre este corren diversos aplicativos de la organización como Autocad, destacando que todo está legalmente licenciado.

2.4.DESCRIPCIÓN DE SERVICIOS

Los servidores de esta organización están en un proceso de migración, hacia servidores blade de mayor capacidad, actualmente el chasis IBM dispone de dos cuchillas blade IBM HS22, con similares características de hardware, en las que se ha implementado el servidor de correo electrónico, una aplicación web para acceso al correo, el servidor de Directorio y el Servidor de Nombres de Dominio DNS.

2.4.1. CORREO ELECTRÓNICO

En esta institución el uso del correo electrónico es prioritario para el personal administrativo, permitiendo agilizar actividades laborales como trámites, peticiones, solicitudes, aprobaciones, contratos, proyectos, entre otras. Actualmente se administran 1020 cuentas de usuario bajo un único dominio que es cee.gob.ec, considerando al personal administrativo del edificio, del campamento y los grupos de trabajo.

Está implementado sobre el sistema operativo Windows Server 2008, con la aplicación Microsoft Exchange 2010 Server, configurado para generar diariamente respaldos (backups) tanto de los datos de configuración y actualizaciones del servidor, como también de los buzones de usuario creados (mensajería, contactos, calendario), que son almacenados en un arreglo de discos duros (storage), y en un disco duro externo.

Este es uno de los servicios que fue migrado al servidor blade IBM HS22, que tiene las siguientes propiedades (véase Tabla 19).

Tabla 19. Características de Hardware

Descripción	Detalle
Procesador	Dos procesadores Intel Xeon 5500 de 2.93 GHz
Memoria RAM	Utiliza una de las doce ranuras para módulos de Memoria, emplea una memoria DIMM DDR-3 de 10 GB. La capacidad total del servidor es 96 GB, con velocidades de hasta 1333 MHz.
Almacenamiento Interno	Utiliza una de las dos bahías hot-swap de disco duro, con una capacidad de 300 GB de almacenamiento, el valor máximo es 600 GB.
Interfaz de Red	2 puertos Gigabit Ethernet
Formato	Ancho 30 mm

Fuente: Elaborado a partir de información facilitada por el Departamento de Sistemas del CEE (2013).

Los agentes de cliente de correo MUA, se configuran empleando Microsoft Outlook para acceder a cada buzón de usuario, en el entorno de la institución.

Complementariamente se ha utilizado la propia aplicación de Exchange Server 2010, para posibilitar el acceso webmail de los usuarios a sus buzones desde cualquier lugar, sin necesidad de utilizar un ordenador con un agente MUA previamente instalado y configurado.

2.4.2. DNS Y DIRECTORIO

Estos servicios conjuntamente con el servidor web IIS³⁸ del correo electrónico, están alojados en máquinas virtuales instaladas en el segundo servidor blade IBM HS22. El dominio de la organización es cee.gob.ec, y el servidor de nombres de dominio (DNS) está desarrollado como un servicio complementario de Active Directory en Windows Server 2008.

El servicio de Directorio opera bajo la aplicación Active Directory propietaria de Microsoft, y vincula al personal de cada departamento del edificio, del campamento y los grupos de trabajo, con el usuario y contraseña generados y proporcionados por el administrador de red para cada uno, y su correspondiente dirección IP privada.

De esta manera es como se administran los inicios de sesión en los ordenadores que forman parte del dominio de la red, y los permisos para acceder a determinados servicios de la misma, como la vpn, el acceso Wireless, restricción de páginas empleando al proxy o administración de puertos mediante el firewall; todos estos servicios están vinculados al servidor de directorio.

2.4.3. WEB

La página web del cuerpo de ingenieros del ejército está hosteada, y es administrada desde un servidor remoto del proveedor, desarrollada en base a Joomla y Base de Datos MySQL. La dirección URL es <http://www.cuerpodeingenierosdelejercito.mil.ec/>.

³⁸ Internet Information Services

2.4.4. TELEFONÍA IP

La central telefónica que provee este servicio, es una MITEL con líneas analógicas modelo 3300 ICP, cuya característica principal es que es híbrida, es decir, provee el servicio a usuarios que disponen de teléfonos IP, y lo adapta para aquellos con línea convencional.

Actualmente existen 20 troncales telefónicas analógicas, y se administran 250 usuarios de la organización que utilizan este servicio. Los modelos de teléfonos IP empleados son marca MITEL, modelo 5212 y 5312, pero también existe gran cantidad de usuarios que utilizan teléfonos convencionales integrados a la red IP.

La administración de esta central es efectuada a través de una consola de central IP, instalada en un ordenador de la red.

2.4.5. ANTIVIRUS

El antivirus que protege los ordenadores y las actividades de la organización es Kaspersky, del cual se han adquirido las licencias para obtener la máxima protección. Está configurado para obtener las actualizaciones necesarias desde internet y almacenarlas en el servidor, de manera que los clientes únicamente se conectan a éste para descargarlas.

Este es uno de los servicios que todavía no ha sido migrado al servidor blade, está instalado en un HP ProLiant ML370, con procesador Intel Xeon, y es gestionado vía consola de administración.

2.5.ENLACES WAN

La red WAN del Cuerpo de Ingenieros del Ejército está conformada por el enlace principal del proveedor de internet y datos de la organización, CNT.EP., conjuntamente con los enlaces de comunicación alquilados para establecer conexión con los grupos de trabajo.

La velocidad del enlace de acceso a internet contratado es 6 Mbps compartición 1:1, los grupos de trabajo y los proveedores con los que opera la organización, se muestran en la Tabla 20.

2.6.MECANISMOS DE SEGURIDAD

Hoy en día existe gran dependencia de los sistemas informáticos y las redes de comunicación, para que las organizaciones puedan llevar a cabo todas sus actividades laborales; por ello en esta institución, existen proyectos como la migración total de los servidores hacia unos de mayor capacidad, para lograr más efectividad en los servicios, adecuar el cuarto de equipos con sistemas de respaldo de energía eléctrica (ups, baterías, generador), y sustituir el cableado horizontal para normalizarlo con categoría 6.

La seguridad perimetral es provista por el firewall y el proxy, controlando en un sentido accesos generados desde redes externas, con destino a determinados servidores de la zona desmilitarizada u ordenadores de usuario final, y en otro aquellos accesos generados en la red interna para utilizar sus servicios, o destinados hacia redes externas.

Tabla 20. Grupos de Trabajo del CEE - Quito

GRUPO DE TRABAJO	ÚLTIMA MILLA	PROVEEDORES
GT Manabí		COMACO
GT Loja		
GT Cética	Multiacceso	CNT.EP.
GT Jaramijó		
BE-67 Montufar		NEWACCESS
GT Amazónico		PUNTONET S.A.
GT Frontera Norte	Cable Modem	TELCONET
CDR – Chaco	Cobre	
CDR – Montufar		
GT Zapotillo	Satelital	
GT Saquisilí		
GT Sucua - Macas		
GT Arenillas		
GT Esmeraldas	Radio Enlace	
GT Tababela		
GT CIA Puentes		
GT Baños		
GT Yachay		
GT Bolívar		
GT Guaranda		
GT Guayaquil		
GT Morona		
GT Asamblea	Fibra óptica	
GT Shyris		
GT Ambato		
GT Latacunga		
GT Guayaquil - SENAE		
Grupo Loja - 2		

Fuente: Elaborado a partir de información facilitada por el Departamento de Sistemas del CEE (2013).

La red privada virtual es otro mecanismo que complementa la seguridad perimetral, asegurando la privacidad en aquellas comunicaciones de suma importancia con oficinas remotas.

Internamente el principal mecanismo de protección disponible es el antivirus, que brinda un elevado nivel de seguridad por las licencias adquiridas; también se emplean técnicas habituales de protección de acceso por contraseñas, tanto en los inicios de sesión de los ordenadores, acceso inalámbrico, a la vpn, a las cuentas de correo electrónico y administración de servidores y dispositivos de red.

El direccionamiento IP es administrado con segmentaciones virtuales VLANS, garantizando con ello la restricción de cierto tipo de tráfico, entre los funcionarios que manipulan información prioritaria. Desventajosamente todavía no se han implementado políticas de seguridad, primordialmente para controlar que las actividades de los usuarios en la red, sean las adecuadas para no generar vulnerabilidades.

Por tal motivo, existe la necesidad de integrar en la organización, un mecanismo de seguridad que complemente a los existentes y compense en gran parte sus vulnerabilidades. Éste se basa en la emisión y gestión de certificados digitales, para emplearlos cifrando y firmando digitalmente, la información que circula por determinadas aplicaciones, garantizando de este modo confidencialidad, integridad, autenticación y no repudio sobre la misma.

En este proyecto de titulación, los certificados digitales X.509 van a ser aplicados en la protección de los mensajes transferidos por el correo electrónico institucional, pero al ser un

mecanismo muy versátil, su uso puede ser enfocado posteriormente en proteger información generada o manipulada por diversas aplicaciones y servicios de red, tratando de implantar la seguridad en profundidad basada en capas o niveles de seguridad.

CAPÍTULO 3. DISEÑO DE LA INFRAESTRUCTURA PKI Y DE LA PLATAFORMA DE CORREO ELECTRÓNICO

En este capítulo se diseñará la PKI conjuntamente con la plataforma de Correo Electrónico para el CEE de Quito, lo que implica establecer requerimientos de hardware y el análisis de herramientas de software libre que permitan desarrollar este proyecto.

3.1.CRITERIOS DE DISEÑO

El propósito primordial de este proyecto es la certificación de los funcionarios y militares del Cuerpo de Ingenieros del Ejército de Quito, mediante la emisión y gestión de certificados digitales X.509, que vinculen su identidad con su clave pública legítima generada, demostrando de esta forma ante los demás que son entidades fiables.

Para ello el requerimiento es configurar una Autoridad Certificadora Raíz que auto-genera su certificado, convirtiéndose desde este momento en una entidad legítimamente autorizada para prestar servicios de certificación, en el entorno del CEE. Sin embargo, esta entidad no solo estará destinada a emitir certificados, también deberá estar en capacidad de gestionarlos, complementándose con componentes adicionales para integrar una Infraestructura de Clave Pública (véase Tabla 21).

Dentro de las consideraciones de diseño de una PKI, los aspectos referentes a su funcionamiento están muy ligados a la (s) vía (s) de entrega de los certificados que se tenga planificado; esto debido a que la CA puede ser configurada para entregarlos a sus propietarios empleando medios tanto de hardware como de software.

Tabla 21. Componentes Estructurales necesarios para desplegar la PKI del CEE

COMPONENTE	DESCRIPCIÓN
Autoridad de Registro (RA)	Será la vinculación entre los funcionarios y militares del CEE, con la CA, atendiendo solicitudes de registro, recuperación de claves o certificados, gestión del ciclo de vida de los certificados, actualización de información de usuario, entre otras.
Directorio de Publicación de Certificados	Almacenarán los certificados de usuario emitidos, para que los funcionarios y militares los obtengan y utilicen en el establecimiento de comunicaciones seguras de correo.
Listas de Revocación de Certificados	Es un documento que publicará y actualizará permanentemente la CA, para dar a conocer los certificados que han sido revocados (invalidados).

Los tokens criptográficos usb, por ejemplo, son dispositivos de hardware comúnmente empleados para almacenar de forma segura certificados digitales y claves privadas. En cuanto a las herramientas de software una de las alternativas más usuales es emitirlos en un formato p12 o pfx para que sean almacenados en los ordenadores de usuario final.

En tal virtud, en el entorno PKI del CEE los certificados de usuario serán distribuidos empleando el formato p12, posteriormente cuando los funcionarios y autoridades de esta entidad estén más relacionados con este sistema, se podría implementar la distribución en tokens usb; por el momento los certificados serán almacenados conjuntamente con su clave criptográfica privada, en los ordenadores de usuario final del edificio matriz, el campamento adjunto y los grupos de trabajo.

Esto debido a que se ha considerado como medida de seguridad, que el usuario final (funcionario público o militar del CEE) no debe formar parte del proceso de solicitud e instalación de certificados en el entorno de la institución, ellos únicamente estarán destinados y serán capacitados para utilizar este mecanismo de seguridad, en la protección de

información transferida por el correo electrónico institucional; será el administrador de red conjuntamente con un grupo capacitado quienes lleven a cabo estas actividades.

La razón es prevenir que se generen posibles vulnerabilidades en el sistema debido al mal uso, tal vez por su desconocimiento o negligencia; de todas formas, y aunque este requerimiento demande un gran esfuerzo por parte del Administrador, es en beneficio de precautelar la operatividad de este sistema.

En tal virtud, las actividades que tendrá que desempeñar el Administrador de red en el proceso de certificación son las que se muestran en la Figura 25, considerando la interacción de los componentes que integrarán la PKI del CEE.

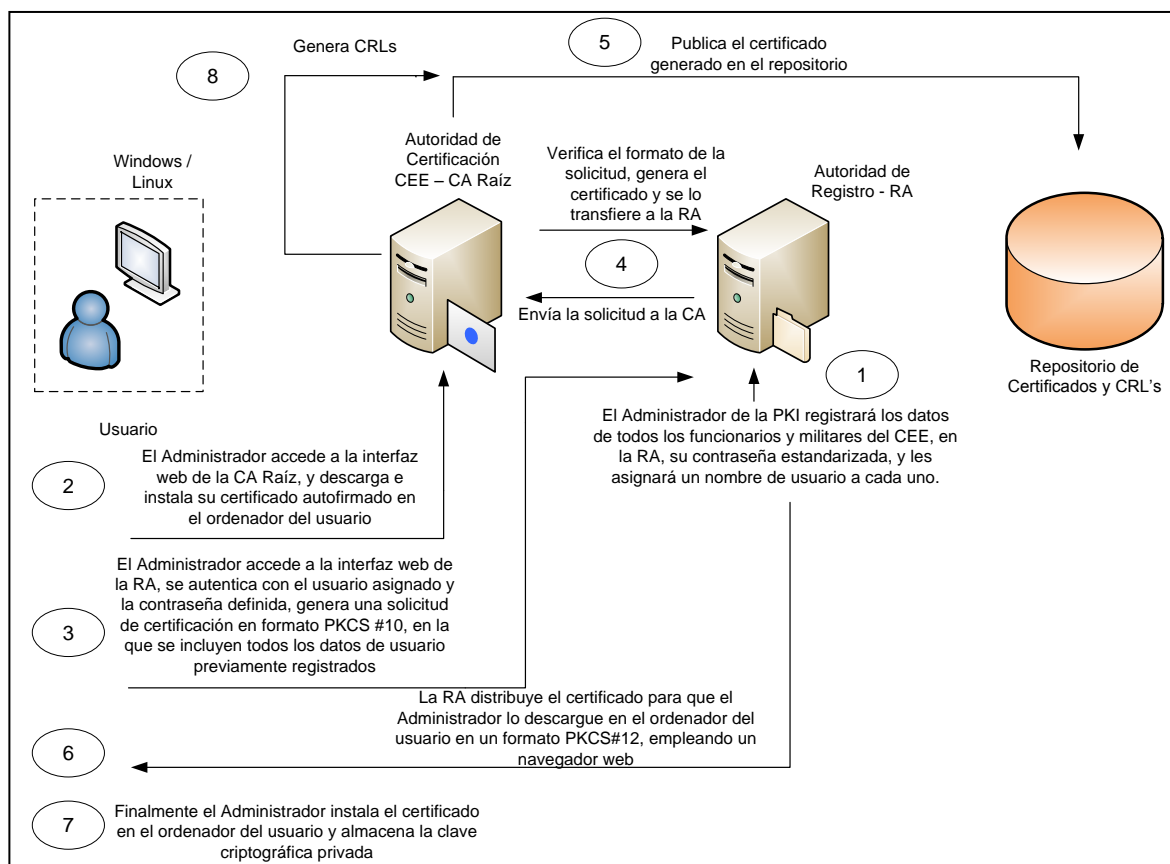


Figura 25. Proceso de certificación en el entorno PKI del CEE - Quito

1. Como se puede apreciar es el Administrador quien va a interactuar con la PKI, e inicia con el proceso de registro que se lleva a cabo para personalizar cada certificado, con la información correspondiente a cada usuario. La ventaja es que esta institución dispone del servicio de Directorio Activo, y será indispensable también la colaboración del Departamento de Recursos Humanos, para obtener la información necesaria de cada usuario y agilizar este proceso.

Además en esta etapa es imprescindible asignarles independientemente un nombre de usuario y una contraseña estandarizada, para utilizarlos como desafío que los autentique ante la RA, previo la generación del certificado. El nombre de usuario será el mismo que se les ha asignado en el dominio Active Directory, pero ellos deberán generar sus contraseñas personales de acuerdo a ciertas consideraciones expuestas en el Anexo A, y darlas a conocer al Administrador únicamente para el registro.

2. Es indispensable confiar en la Autoridad Certificadora Raíz del CEE antes de obtener e instalar los certificados de usuario, caso contrario los ordenadores lo reconocerán como no fiable; para ello, el administrador descargará el certificado de esta CA en el ordenador del usuario, y lo ejecutará para activar el asistente de importación de certificados de Windows, que le guíaran paso a paso para almacenarlo en los repositorios de certificados. Este procedimiento es posible debido a que los certificados que emitirá la PKI del CEE están basados en el estándar X.509, por ese motivo se asegura su compatibilidad con la mayoría de aplicaciones de seguridad basadas en certificados digitales.

En la Institución todos los ordenadores operan sobre Windows, pero en el caso de que se incluyan posteriormente ordenadores Linux y Mac, también es posible obtener esta certificación, aunque el proceso de importación puede diferir de cierta forma.

3. El proceso de registro finaliza en el momento en que el Administrador desde el ordenador cliente accede a la interfaz web de la RA, y luego de haberse autenticado con el usuario y contraseña predefinidos, genera una solicitud de certificación en formato PKCS#10, que contiene los datos del usuario que han sido registrados previamente.
4. La RA transfiere esta solicitud a la entidad certificadora que verificará su formato, generará el certificado, y se lo transferirá a la RA para que lo distribuya al usuario.
5. La CA publica el certificado emitido en el repositorio local, para que el resto de usuarios lo descarguen y empleen su clave pública en la transferencia fiable de mensajes de correo electrónico.
6. Desde el ordenador de usuario el Administrador descargará el certificado, en formato PKCS#12.
7. Instala el certificado de usuario con la ayuda del asistente de importación de Windows, de manera similar a la instalación del certificado de la CA Raíz, pero con la diferencia de que en este caso también se almacenará y protegerá, mediante la contraseña establecida para el registro, la clave criptográfica privada.

8. Para complementar la gestión del certificado la CA Raíz emitirá periódicamente las Listas de Revocación de Certificados CRLs y las publicará en el repositorio local, con el propósito de revelar cuáles de los certificados bajo su administración, han sido invalidados o suspendidos.

Tras este proceso los usuarios dispondrán de certificados digitales personales almacenados en sus ordenadores, conjuntamente con sus claves privadas, pero su aplicación en este proyecto será al emplearlos para generar técnicas de cifrado y firma digital, sobre los mensajes transferidos por el correo electrónico institucional.

La segunda parte del proyecto es diseñar una plataforma de correo electrónico basada en herramientas de software libre, que provea las funcionalidades de la actual desarrollada sobre Exchange, aportando de esta manera con la migración hacia nuevos sistemas que proporcionan servicios similares a los privativos, pero que requieren de menor inversión para implementarlos, o en el mejor de los casos no tienen costo.

La alternativa más habitual para proteger el correo electrónico es utilizar el protocolo de capa transporte SSL/TLS; sin embargo, para garantizar una comunicación segura extremo a extremo sería necesario cifrar todos los enlaces intermedios que puedan intervenir durante la transferencia.

El problema con ello es que el correo electrónico está diseñado para operar bajo un esquema almacenamiento-reenvío, de esta manera, SSL/TLS protege a los datos en tránsito a través de las redes, pero durante su almacenamiento en nodos intermedios o finales (MDA)

quedan totalmente vulnerables, pudiendo ser revisados o alterados antes de que lo haga el destinatario legítimo.

La solución más idónea es generar correos auto-protegidos mediante cifrado y/o firma digital, en capa aplicación, de manera que los MTA los transfieran de forma convencional a su destino, con ello se garantiza la protección durante todo el proceso de transferencia, incluso mientras están alojados en el buzón de los destinatarios.

Los métodos de seguridad que utilizan actualmente las plataformas de correo seguro son PGP y S/MIME, el primero basado en claves criptográficas autogeneradas, y el segundo en certificados digitales. En tal virtud, la seguridad del correo electrónico institucional del CEE, a diseñarse, será implementada utilizando en primera instancia el protocolo SSL/TLS para securizar los enlaces de comunicación establecidos entre cliente/servidor, pero el mecanismo prioritario de protección será la implementación de S/MIME para generar correos auto-protegidos.

La interacción de los ordenadores de los funcionarios y militares del CEE, al enviar un mensaje firmado digitalmente, es mostrada en la Figura 26.

1. El emisor a través del agente de correo de usuario (MUA) Outlook, genera un mensaje con estructura S/MIME, al cual lo firmará con su clave criptográfica privada; previamente el MUA debió haber sido configurado por el Administrador de la PKI para activar la funcionalidad S/MIME, y el certificado digital del usuario debe estar instalado en su ordenador.

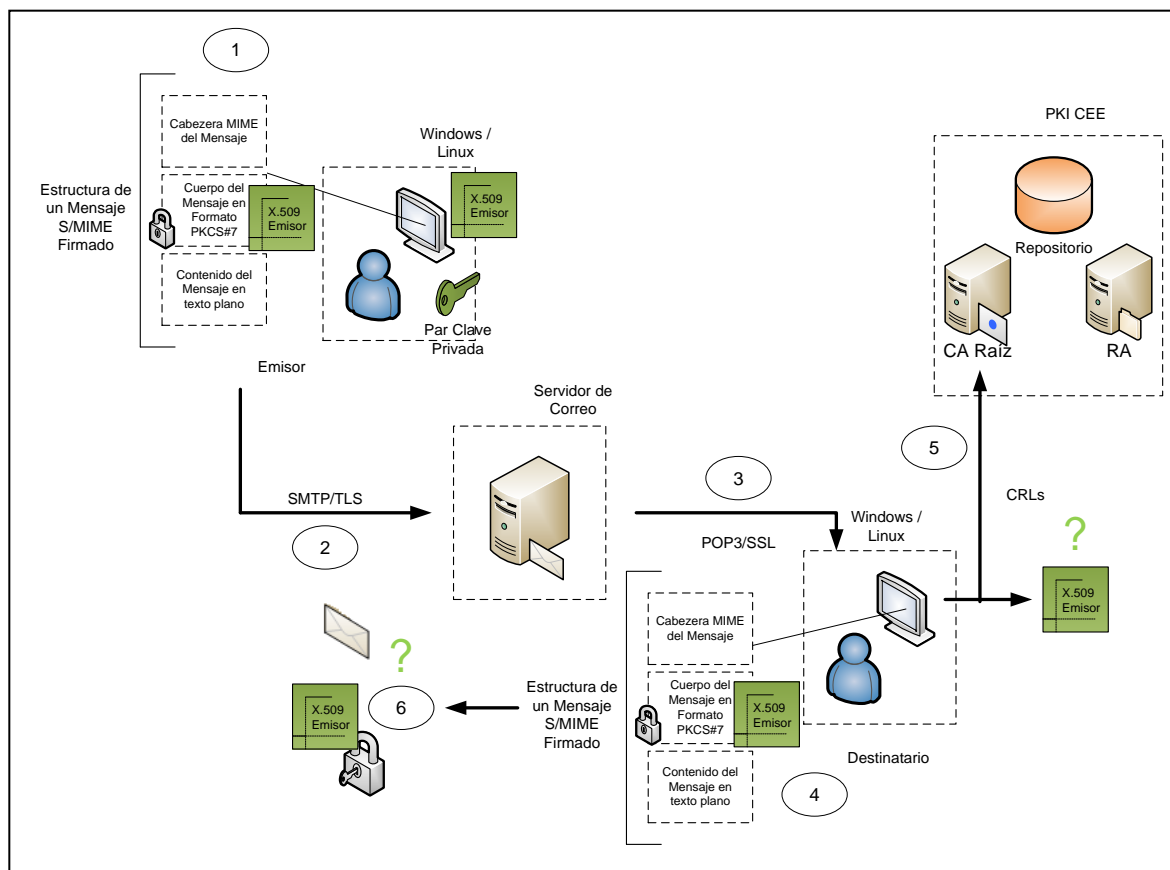


Figura 26. Interacción del Usuario, la PKI y el Sistema de Correo en el entorno del CEE – Mensaje Firmado

2. Este mensaje auto-protegido será transferido de manera habitual, empleando el protocolo de transporte SMTP, y TLS para cifrar el canal de comunicación, almacenándose finalmente en el servidor de correo de forma convencional.
3. El destinatario accederá a su buzón y descargará su mensajería pendiente utilizando el protocolo POP3, con seguridad SSL para cifrar la conexión.
4. Obtendrá el mensaje S/MIME.
5. El agente MUA detectará su estructura y obtendrá el certificado digital X.509 del emisor, que contiene este mensaje, para verificar su validez empleando las listas de revocación de certificados (CRLs) que la PKI del CEE publicará constantemente,

luego verificará su vigencia y finalmente la firma digital que contiene, generada por la CA.

- Si el certificado es legítimo verificará la firma digital del mensaje para determinar si no ha presentado ningún tipo de alteración desde que fue creado, e implícitamente la autenticidad del emisor. Además, el receptor debe agregar a sus contactos de Outlook al emisor, almacenándolo conjuntamente con su certificado digital, que será utilizado desde ese momento para enviarle mensajes cifrados, y garantizar que sólo él pueda revisarlos.

En el caso del envío de mensajes cifrados es el mismo proceso de transferencia, pero difieren las operaciones criptográficas (véase Figura 27).

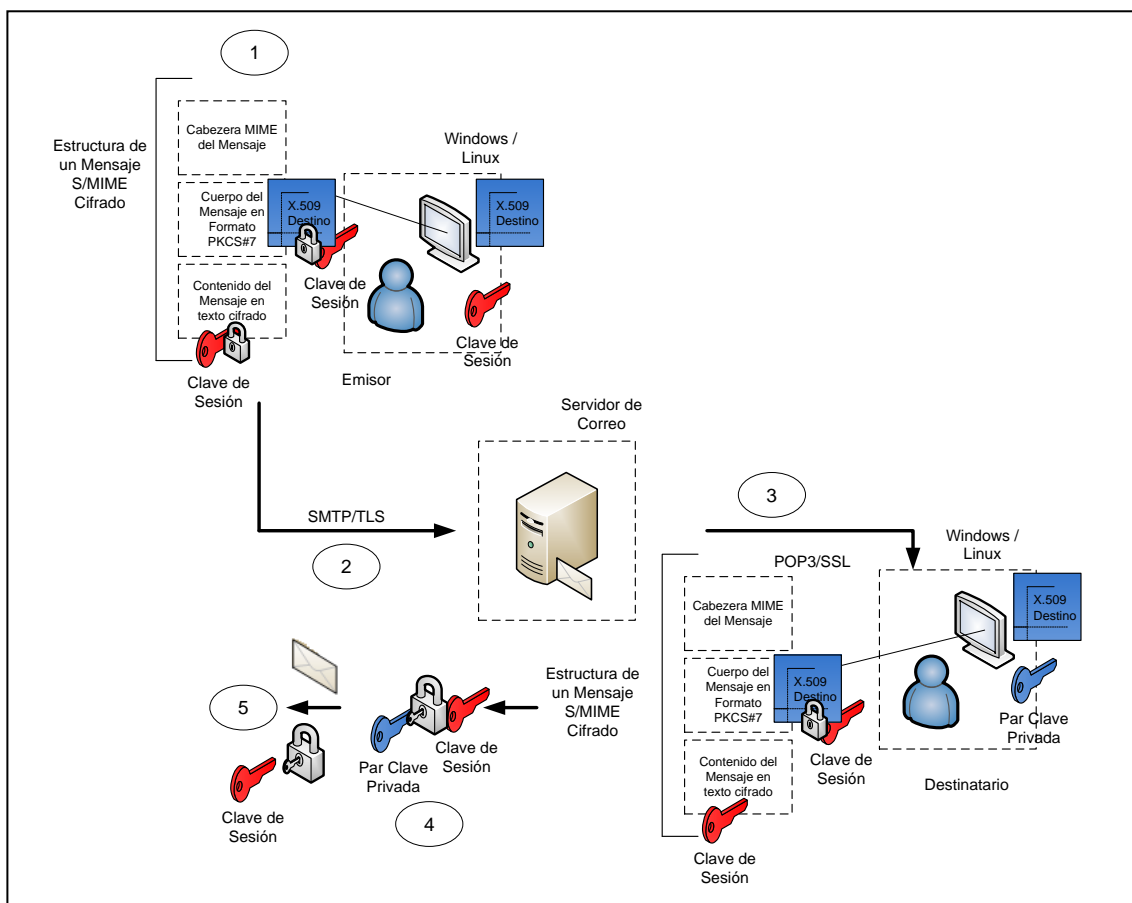


Figura 27. Interacción del Usuario, la PKI y el Sistema de Correo en el entorno del CEE – Mensaje Cifrado (Sobre Digital)

- El ordenador del emisor generará una clave de sesión que será cifrada utilizando el certificado del destinatario, garantizando de esta forma que sólo él pueda descifrarla con su clave privada. El contenido del mensaje será cifrado con la clave de sesión.
- El destinatario con su par clave privada descifra la clave de sesión, y finalmente el mensaje para revelar su contenido.

Finalmente uno de los requerimientos primordiales de este proyecto es migrar la información de los buzones creados en servidor de correo actual (mensajería, contactos, calendario), desarrollado sobre Microsoft Exchange, hacia la nueva plataforma sobre software libre, para garantizar que durante la transición los usuarios conservarán toda su información.

Estos son los criterios y requerimientos de diseño que se considerarán para desarrollar este proyecto, la siguiente etapa consiste en elegir argumentativamente, las herramientas de software libre, y el dimensionamiento de hardware que permitan implementarlos.

Finalmente, vale la pena recalcar que los sistemas de seguridad generalmente están diseñados para ser robustos y neutralizar los ataques que intenten vulnerar los servicios que protegen, pero muchas veces las vulnerabilidades provienen de las personas que manipulan constantemente estos servicios, tal vez por desconocimiento o negligencia.

Por este motivo, para preservar la operatividad del sistema de seguridad diseñado en este proyecto, se establecerán Políticas de Seguridad que controlen las actividades de los usuarios de la institución:

1. Los funcionarios públicos, militares y autoridades que formen parte activa del CEE, deben participar de este proceso de certificación, con el propósito de salvaguardar el activo de mayor validez con el que dispone esta entidad, su información.
2. Desde el momento en el que el sistema de seguridad se encuentre operativo, todos los mensajes que se transfieran por el correo electrónico institucional deben ser protegidos criptográficamente (cifrados y firmados digitalmente), caso contrario, se los considerará inválidos; excepto los que estén dirigidos a destinatarios externos, es decir, que no dispongan de un buzón de correo en el servidor institucional.

3.2.INFRAESTRUCTURA DE CLAVE PÚBLICA PKI

Para el diseño de la PKI del CEE de Quito es necesario definir ciertos parámetros referentes a su arquitectura, los requerimientos de hardware, y las herramientas software que permitan su despliegue.

3.2.1. ARQUITECTURA DE LA PKI

En una PKI todo gira en torno a las Autoridades Certificadoras, que establecen la cadena de confianza certificándose unas a otras, formando jerarquías en las que la fiabilidad radica en la CA raíz. Se llama raíz porque emite un certificado auto-firmado que la distinguen como la cúspide de esta cadena, habilitándola para generar certificados destinados a CAs intermedias que formarán nuevas jerarquías independientes, o a subordinadas que certificarán directamente a usuarios y dispositivos finales; pero que en cualquier situación, operan bajo la misma administración.

Mediante la Certificación Cruzada esta cadena de confianza se puede extender aún más, al establecer comunicación con CAs externas que no operan bajo la misma administración, de manera que un determinado usuario admita un certificado generado por una CA que no forma parte de la jerarquía, pero que previamente ha sido inspeccionada y reconocida como fiable por la CA a la que este usuario pertenece.

Existen proveedores de servicios de certificación reconocidos internacionalmente, como VeriSign, Safelayer, Entrust, Microsoft, IBM, Baltimore, entre otros, que generan diversos tipos de certificados que pueden ser validados globalmente, dependiendo de los reglamentos dispuestos por los entes reguladores de cada país; pero son proveedores tan difundidos que en ocasiones sus certificados de CAs raíz o intermedias están integrados por defecto en el repositorio de certificados de los sistemas operativos (pueden visualizarse empleando los navegadores web, véase Figura 28), principalmente para establecer conexiones seguras mediante el protocolo https.

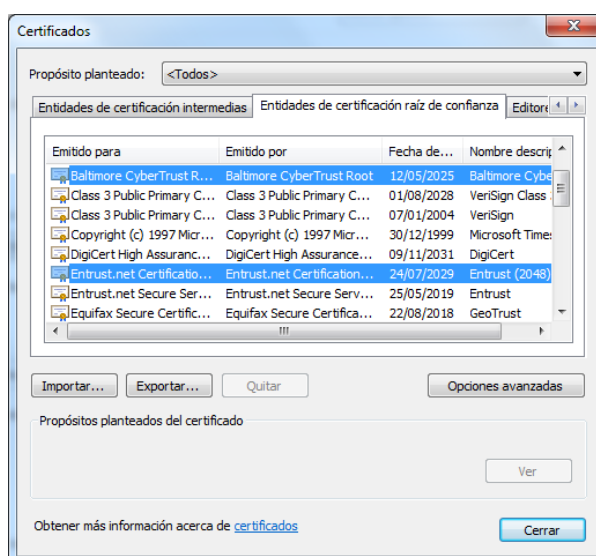


Figura 28. Repositorio de Certificados Digitales de Windows 7 Ultimate - Navegador Google Chrome

Sin embargo, es posible implementar una PKI que emita certificados digitales que sean válidos localmente, dentro de una institución, una empresa, un campus universitario o cualquier dependencia; es decir, que tengan únicamente validez interna. Este tipo de infraestructura se denomina aislada porque no está destinada a establecer enlaces de confianza con CAs externas a la jerarquía.

Para extender su uso y proveer servicios de certificación no sólo a una dependencia, sino a toda una región, una provincia o un país, es necesario legalizarla ante los entes de regulación pertinentes. En Ecuador de acuerdo a la Ley 67: Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, analizada en el capítulo 1, el organismo de regulación, autorización y registro de entidades de certificación, es el CONATEL, y el organismo de control de estas entidades es la SUPERTEL.

El Decreto 1356 que contiene Reformas al Reglamento General a la Ley 67, incluye información relacionada con los requisitos, procedimientos, y el periodo de validez de la acreditación para las entidades de certificación solicitantes; como el control de operación, la renovación y la extinción de la acreditación para entidades previamente autorizadas. De igual manera, se establece la información necesaria para autorizar el funcionamiento de Autoridades de Registro (terceros vinculados) destinadas a operar conjuntamente con las Certificadoras acreditadas.

La SENATEL³⁹ entre sus diversas funciones, se encarga de elaborar un documento denominado “Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y terceros vinculados”, reglamentado por el CONATEL,

³⁹ Secretaría Nacional de Telecomunicaciones

en el que se publican todas aquellas entidades que han sido aprobadas para proveer servicios de certificación en territorio ecuatoriano, conjuntamente con los terceros vinculados. El Anexo B muestra la última versión actualizada de este documento.

Actualmente el Banco Central del Ecuador, la ANF - Autoridad de Certificación Ecuador S.A. y Security Data - Seguridad en Datos y Firma Digital S.A., son las tres entidades de certificación acreditadas en el país; algunos de los terceros vinculados son: Telconet, la Cámara de Comercio de Guayaquil, Megadatos S.A., entre otros.

En tal virtud, el diseño de la PKI que satisface los requerimientos de certificación propuestos en este proyecto, de acuerdo a aspectos legales, es una infraestructura PKI aislada, considerando que éstos van a ser de uso exclusivamente interno en el entorno del Cuerpo de Ingenieros del Ejército, y estarán destinados para la seguridad del correo electrónico institucional.

De todas formas se han expuesto también documentos que constituyen las leyes y reglamentos emitidos por los organismos de regulación, y en base a ellos también ciertos criterios, dando a conocer los requerimientos y procesos que demandaría la legalización de la entidad certificadora.

En lo referente a aspectos de funcionamiento, una PKI puede estar estructurada por la CA raíz, y varias CAs intermedias y subordinadas dependiendo del alcance del entorno sobre el que se requiera implantar la certificación. En el caso de este proyecto la certificación está destinada a los funcionarios y militares del CEE, por lo que una arquitectura PKI plana es la adecuada para satisfacer este requerimiento, al integrarse por una sola CA raíz que genere y

distribuya certificados directamente a usuarios y dispositivos finales empleando una RA de por medio.

Esto se ha decidido considerando que esta institución mantiene todas sus actividades centralizadas en la sucursal matriz en Quito, desde allí se controlan y planifican todas las actividades de los grupos de trabajo a nivel nacional, por ello no sería necesario implantar CAs adicionales; posteriormente de acuerdo al crecimiento y dispersión de sus dependencias se podría incorporar CAs intermedias y subordinadas para garantizar el servicio.

3.2.2. SOFTWARE PARA EL DISEÑO DE LA PKI

Gran parte de las soluciones propietarias en diversos campos de la seguridad informática como en muchos otros, permiten efectuar implementaciones en ambientes reales de producción, garantizando su funcionamiento y en ocasiones algunas funcionalidades complementarias; sin embargo, los costos por las licencias de funcionamiento representan generalmente una gran inversión para las organizaciones.

Esto ha impulsado la investigación y desarrollo de herramientas de software libre, para generar soluciones alternativas que equiparen las funcionalidades que proveen las privativas, pero con la ideología de que puedan ser utilizadas, adaptadas y modificadas libremente, sin necesidad de pagar por ello; aunque existen versiones comerciales que pueden tener algún costo, en compensación por el soporte técnico que pueden ofrecer, o por alguna funcionalidad complementaria.

En el ámbito de las Autoridades de Certificación no existe gran variedad de estas alternativas que permitan implementar una PKI, las soluciones más conocidas y estables son OpenSSL, OpenCA, NewPKI y EJBCA; la Tabla 22 expone las características más importantes de cada una.

Tabla 22. Descripción de las Soluciones Open Source en entornos PKI

SOLUCIÓN	CARACTERÍSTICAS
OpenSSL	<ul style="list-style-type: none"> ▪ Desarrollada en base a un entorno de colaboración. ▪ Provee de un conjunto de librerías criptográficas. ▪ Es una aplicación sobre la que se han desarrollado aplicaciones de seguridad como OpenSSH y HTTPS. ▪ Es una aplicación de línea de comandos, por lo que utilizarla como base para implementar una PKI, resultaría un proceso de gran complejidad.
OpenCA	<ul style="list-style-type: none"> ▪ Desarrollada en base a OpenSSH, OpenLDAP y Apache ▪ Permite implementar una PKI a pequeña escala, con propósitos de evaluación. ▪ La administración puede ser llevada a cabo únicamente a través de interfaces web. ▪ No es escalable ante la gran demanda de usuarios.
NewPKI	<ul style="list-style-type: none"> ▪ Desarrollada en base a OpenSSL sobre C++. ▪ Esto la convierte en una solución dependiente de la plataforma sobre la que se ejecute.
EJBCA⁴⁰	<ul style="list-style-type: none"> ▪ Desarrollada sobre JAVA Enterprise. ▪ Esto la convierte en una solución independiente de la plataforma, es decir, que puede ser ejecutada sobre cualquier sistema operativo que soporte JAVA (Windows, Linux o Mac). ▪ Permite implementar una PKI completamente funcional, de alcance empresarial. ▪ Es altamente escalable debido a que puede integrarse con otras aplicaciones basadas en JAVA. ▪ La administración puede ser llevada a cabo a través de una interfaz web con autenticación en base a certificados digitales (no al tradicional mecanismo usuario contraseña), como también mediante una interfaz de línea de comandos. ▪ Es considerada como la solución del futuro en entornos PKI, debido a que soporta algoritmos criptográficos de curva elíptica ECDSA, que serán la sustitución del algoritmo criptográfico de clave pública actual más empleado por aplicaciones telemáticas, RSA, considerando que en algún momento éste podrá ser vulnerado para descifrar el intercambio de claves criptográficas.

Fuente: Creado a partir de Ayesha, I. G. & Asra, P. (2006). *PKI Administration using EJBCA and OpenCA*. Recuperado de http://teal.gmu.edu/courses/ECE646/project/reports_2006/IL-3-report.pdf
 Plaza, D. *Soluciones PKI basadas en Cryptlib*. (Trabajo de fin de Carrera). Universidad Politécnica de Madrid, Madrid, España.

⁴⁰ Enterprise Java Beans Certification Authority

De este modo, la alternativa más viable y conveniente para desarrollar este proyecto es utilizar EJBCA.

3.2.2.1. EJBCA

EJBCA es un proyecto que fue desarrollado en el 2001 por Tomas Gustavsson y Philip Vendil, año en el cual se publicó su versión inicial, actualmente existen más de cincuenta versiones, de las cuales las más recientes están alojadas en uno de los repositorios de gran popularidad a nivel mundial, SourceForge.

Su uso se ha difundido enormemente al disponer de foros públicos, un sitio web oficial (www.ejbca.org) al cual está vinculado su sitio wiki y su blog, y complementariamente en sus paquetes de instalación existe mucha información disponible, que brinda soporte de instalación, configuración y funcionamiento.

EJBCA es una Autoridad Certificadora construida en base a J2EE⁴¹ con la capacidad de desempeñar todas las funciones de una CA (Autoridad Certificadora, de Registro y emisión de CRLs), sin necesidad de emplear herramientas adicionales que la complementen (es multifuncional), esto es debido a que está estructurada por componentes que cumplen cada uno con su función designada.

Esta herramienta posibilita la emisión y gestión de diversos tipos de certificados digitales, dependiendo de sus propósitos, por ejemplo para autenticar a usuarios y dispositivos que

⁴¹ Java 2 Platform, Enterprise Edition

intervienen en una comunicación telemática, proteger mensajes de correo electrónico mediante cifrado y firmado digital, acceso a recursos y sistemas de una red, etc.

3.2.2.1.1. Arquitectura

Enterprise Java Beans (EJB) es una arquitectura de desarrollo desplegada por Sun Microsystems, que permite construir aplicaciones altamente robustas y escalables orientadas para implementaciones empresariales. Es un componente esencial de la plataforma J2EE, que es el soporte sobre el cual se despliegan aplicaciones de alto rendimiento, multinivel y basadas en componentes.

Los componentes que integran EJB ejecutan sus funciones dentro de un contenedor (EJB Container) utilizando como plataforma un servidor de aplicaciones J2EE como JBOSS o Web Logic. Este contenedor proporciona servicios a las aplicaciones desarrolladas, por ejemplo comunicaciones por red, transacciones, persistencia, gestión de logs, seguridad, gestión de recursos, entre otras.

EJBCA es una Autoridad Certificadora desarrollada sobre J2EE, que posibilita el despliegue de una PKI completamente robusta, fiable y flexible, debido a que al estar basada en componentes, éstos pueden ser personalizados o sustituidos, de acuerdo a las necesidades de las entidades.

La Figura 29 esquematiza la arquitectura multinivel de EJBCA, en la que se distinguen tres niveles: Web y EJB estructurados en contenedores, y el de Datos. El nivel Web es la interfaz a través de la cual los usuarios finales interactúan con la CA o RA (front-end), para iniciar un

proceso de solicitud de certificación, verificación del estado de un certificado, obtención del certificado de la CA raíz, etc. El contenedor Web está integrado por componentes estructurados por servlets⁴², para ejecutar acciones en función de las solicitudes realizadas por los clientes, a través de los navegadores web.

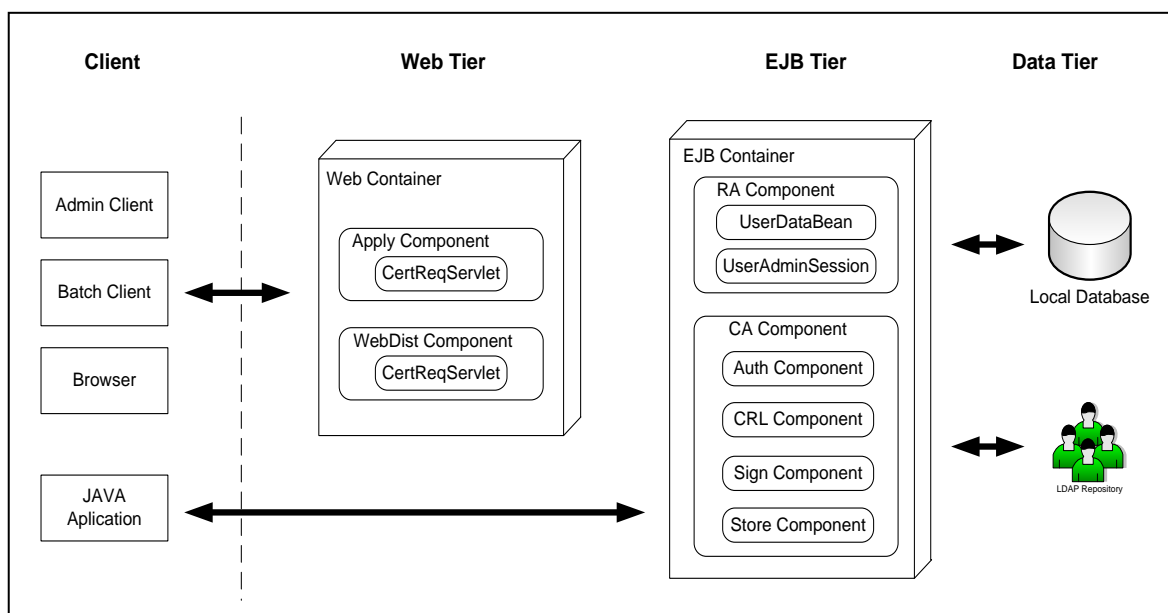


Figura 29. Arquitectura de EJBCA

Fuente: Ghori, A. I. & Parveen, A. (2006). PKI Administration using EJBCA and OPENCA. Recuperado de http://teal.gmu.edu/courses/ECE646/project/reports_2006/IL-3-report.pdf

En situaciones en las que la CA haya sido implementada integrándose con alguna aplicación J2EE, el contenedor EJB puede comunicarse directamente con el front-end propio de esta aplicación, sin necesidad de emplear los servlets.

En el contenedor EJB el componente CA desempeña todas las funciones referentes a una Autoridad Certificadora, al generar la CA raíz, y formar a partir de ella Autoridades Intermedias, Subordinadas y de Registro, como también la emisión y gestión de Certificados Digitales y CRLs, y su publicación en repositorios digitales.

⁴² Son programas java utilizados por los servidores de aplicaciones, para procesar las solicitudes provenientes de usuarios.

El componente RA administra la información proporcionada por los usuarios finales, certificados o en proceso de certificación, generalmente se conecta con la base de datos local para almacenar esta información.

El nivel de Datos se refiere al almacenamiento de información de los usuarios que requieren y han solicitado la certificación, de los Certificados Digitales y las CRLs. EJBCA por defecto está vinculada a una base de datos destinada a almacenar principalmente los certificados y las CRLs, pero también existe la posibilidad de integrarse con repositorios digitales como LDAP o Active Directory para publicar esta información.

3.2.2.2. Herramientas de Software Complementario

Son aquellas herramientas necesarias para la compilación e instalación de EJBCA, como la base de datos, el Servidor de Aplicaciones, herramientas de desarrollo Java JDK, librerías criptográficas, un servidor de dominio configurado con el dominio actual del Cuerpo de Ingenieros del Ejército (cee.gob.ec), con propósitos de efectuar la simulación de este proyecto, entre otras. La tabla 23 detalla estas herramientas complementarias necesarias para desplegar la PKI.

Tabla 23. Software complementario para la compilación e instalación de EJBCA

HERRAMIENTA	DESCRIPCIÓN	VERSIÓN
JDK (Java Development Kit)	Herramientas java de desarrollo	1.6.0_27
JCE Unlimited Strength (Jurisdiction Policy Files)	Librerías Criptográficas	6
JBoss	Servidor de Aplicaciones	5.1.0.GA
MySQL	Servidor de Base de Datos	5.5
JDBC (Java Database Connectivity)	Conector de la Base de Datos MySQL con Java	5.1.26
BIND	Servidor de Dominio (DNS)	9

3.2.3. DESPLIEGE DE LA PKI

La instalación de EJBCA, como lo muestra la Tabla 23, requiere de un conjunto de aplicaciones complementarias configuradas para operar de tal modo que permitan la implementación de una Autoridad Certificadora Raíz. Todo este proceso de instalación es detallado en el Anexo C.

3.2.3.1. Servidor de Dominio – DNS

Este servidor de dominio ha sido desplegado empleando el dominio actual del Cuerpo de Ingenieros del Ejército (cee.gob.ec), utilizando el software de código abierto BIND9⁴³, debido a uso generalizado, simplicidad de funcionamiento y la abundante información referente a su configuración.

Este DNS ha sido configurado para resolver nombres únicamente en la red local de servidores de este proyecto 192.168.0.0/24, con propósitos de efectuar su simulación; el Anexo D contiene información detallada referente a su instalación y configuración. Para implementar este servicio de certificación el administrador de red del CEE debe incluir al servidor PKI en la red DMZ de servidores 172.16.0.0/16 de la institución, y agregarlo en los registros de configuración del DNS operativo, garantizando la resolución tanto desde la red local, como desde la pública.

⁴³ Berkeley Internet Name Domain

3.2.3.1.1. Virtualización

La virtualización de plataforma es una técnica que permite desplegar varios servidores virtuales compartiendo un sólo servidor físico, de esta forma, cada máquina o servidor virtual podrá interactuar con diversas aplicaciones, datos, usuarios o dispositivos, de forma independiente, tal como si fuese un recurso físico destinado para ello (véase Figura 30).



Figura 30. Virtualización de Servidores

Fuente: CAPACITY Blog Corporativo. Qué es la Virtualización y cuáles son sus beneficios. Recuperado de <http://blog.capacityacademy.com/2012/08/07/que-es-la-virtualizacion-y-cuales-son-sus-beneficios/>

Cada máquina virtual que se implemente sobre el equipo físico, tiene la característica de ser independiente de las demás, por este motivo, distintas máquinas virtuales pueden ejecutar simultáneamente diversos sistemas operativos y aplicaciones, sin el riesgo de que si alguna falla pueda afectar al resto.

Esto es posible debido al administrador de virtualización hypervisor, que al encontrarse entre el hardware y el sistema operativo, los separa independizándolos y determina el acceso que las aplicaciones y los sistemas operativos tendrán sobre los recursos físicos de hardware como el procesador, la memoria, disco duro, etc.

Existen diversos proveedores de software de virtualización como VMware, Citrix, IBM, Microsoft, Red Hat, Oracle (Virtualbox), entre otras.

Para desarrollar este proyecto se ha decidido virtualizar el servidor DNS y los servidores de correo Zimbra y Exchange, sobre Virtualbox, por ser una herramienta de código abierto, con el propósito de simular los sistemas que requiere el diseño propuesto, priorizando el factor económico.

3.2.3.2. Jerarquía PKI

EJBCA es una herramienta muy versátil que permite modificar su apariencia para adaptarlo más al entorno sobre el que se va a implementar, en este caso se han efectuado ciertas modificaciones, relativamente sencillas, que representen de mejor manera al Cuerpo de Ingenieros del Ejército, tratando de demostrar que se pueden hacer muchos cambios para mejorar y adecuar su apariencia; el numeral 1 del Anexo E muestra todas estas modificaciones.

Tras la instalación de EJBCA se creará una Autoridad Certificadora, un Usuario Super-administrador y un certificado digital de cliente SSL, que son componentes de carácter

temporal que le permiten a este usuario acceder a la interfaz EJBCA de administración para que la gestione, y desde este punto constituir la jerarquía PKI, e iniciar su operación.

Sin embargo, una de las consideraciones para desarrollar este proyecto, es emplear de manera momentánea estos componentes, la intención es crear a partir de ellos los componentes reales que integrarán la PKI del CEE.

Se ha determinado previamente que una jerarquía plana de CAs satisface los requerimientos de certificación de la institución, esto significa la creación de una CA raíz que emitirá certificados directamente a usuarios finales, con la ayuda de una RA; el numeral 2 del Anexo E detalla los procedimientos necesarios para crear esta entidad.

3.2.3.2.1. Diseño del Certificado Digital

La estructura del certificado está definida por el estándar X.509 versión 3, que establece los campos que debe contener un certificado para que sea admitido por las aplicaciones (cada uno de estos ha sido analizado en el primer capítulo), pero existen ciertos parámetros que varían dependiendo de las consideraciones de cada entidad certificadora.

El DN⁴⁴ es un parámetro que identifica tanto a la entidad emisora del certificado, como a su titular, por ese motivo puede contener varios atributos que los describan de mejor manera; por ejemplo, el CN⁴⁵, Organización, Unidad Organizacional, Dirección de Correo Electrónico, Calle de Dirección, Código Postal, País, Estado o Localidad.

⁴⁴ **Distinguished Name** – Nombre Distintivo

⁴⁵ **Common Name** – Nombre Común

Estos atributos dependen del tipo de certificado, es decir, si está destinado a una persona natural, jurídica, a un funcionario público o a un servidor seguro SSL; las entidades de certificación comercial definen los requisitos personales o institucionales para cada tipo. En el caso de este proyecto debido a que los funcionarios, militares y servidores pertenecen a la misma institución, se ha determinado que los atributos necesarios para identificarlos son los descritos en la Tabla 24.

Tabla 24. Nombre Distintivo que contendrán los certificados del CEE

ATRIBUTO	DESCRIPCIÓN	
	Servidor (Autoridad Certificadora)	Usuario Titular
CommonName (CN)	Autoridad Certificadora CEE	Nombre del Funcionario Público o Militar
Unique Identifier (UID)	-	Departamento Institucional al que pertenece
Organizational Unit (OU)	Servidor CEE	Entidad Final CEE
Organization (O)	Cuerpo de Ingenieros del Ejército	Cuerpo de Ingenieros del Ejército
Country (C) ISO 3166	EC	EC
DNS Name	cee.gob.ec	-

El certificado también contiene un campo (KeyUsage) que especifica los usos para los que fue emitido, por ejemplo: Firma Digital, No Repudio, Cifrar claves o datos, Autenticación de Cliente/Servidor o Protección de Correo Electrónico; la Tabla 25 describe los usos definidos para los certificados que emitirá la PKI del CEE.

Todas las configuraciones realizadas para generar este tipo de certificados, se detallan ampliamente en los numerales 3, 4, 5 y 6 del Anexo E, tanto para el certificado de entidades finales, como para los servidores.

Tabla 25. Usos para los que serán emitidos los certificados del CEE

USO	Servidores (Autoridad Certificadora)	Usuarios
Digital Signature	Si	Si
Non-repudiation	No	Si
Key encipherment	Si	Si
Data encipherment	No	Si
Client Authentication	No	Si
Email Protection	No	Si
Server Authentication	Si	No

3.2.3.3. Iniciar la Operación de la Entidad Certificadora

A esta altura del proyecto se ha creado la CA Raíz y se han definido los campos que contendrán los certificados que emitirá esta entidad, ahora por seguridad se deben reemplazar los certificados temporales emitidos durante la instalación de EJBCA, por certificados emitidos por la CA real de este proyecto (Autoridad Certificadora CEE).

Esto implica la emisión de nuevas Claves y del Certificado para el nuevo usuario Super-administrador, asignarle privilegios de administración de la entidad certificadora, crear un nuevo repositorio de claves (keystore) para el servidor web EJBCA, un repositorio de confianza (truststore) utilizado por Java, deshabilitar la CA temporal creada durante la instalación y finalmente revocar todos los certificados temporales.

Los numerales 7 y 8 del Anexo E contienen información relacionada con todas estas configuraciones efectuadas para iniciar la operación de la PKI del CEE.

3.2.4. DIMENSIONAMIENTO DE HARDWARE

Internet ofrece una gran variedad de aplicaciones que se ejecutan interactuando de forma diferente cada una, pero en la actualidad existe una tendencia a desarrollarlas en base a servicios que requieren de una arquitectura cliente – servidor.

El fundamento en esta arquitectura es que el servidor desempeña un rol pasivo, recibiendo peticiones, procesándolas y respondiendo; a diferencia, el cliente es activo, generando las peticiones y esperando respuestas.

La ventaja se ve reflejada absolutamente en la centralización del servicio y la información, pero la contraparte es el riesgo de saturar al servidor debido al exceso de peticiones, por ello, es de suma importancia establecer los requerimientos de hardware adecuados para garantizar un servicio de red.

Los parámetros de hardware relevantes que deben considerarse al implementar un servidor son: el procesador, la memoria RAM y la capacidad de almacenamiento; para dimensionar este servidor se ha considerado las principales aplicaciones necesarias para implementar EJBCA, como también el sistema operativo anfitrión.

Debido a que la documentación oficial del proyecto EJBCA (EJBCA PKI by Primekey) no expone ninguna especificación técnica del hardware necesario para su implementación, se ha considerado las recomendaciones del proyecto Jboss propuestas por Kopalova, Dickenson, Morgan, Mumford & Penicka (2012), en su guía de instalación sobre redhat, en la que establece una capacidad de almacenamiento de disco mínima de 1.5 GB, la memoria RAM

del sistema debe ser al menos de 1.5 GB para ejecutar esta plataforma sobre un sistema operativo de 64 bits, y un procesador Intel Pentium de 1 Ghz para ejecutar aplicaciones sencillas. Sin embargo, estas características son una referencia que variarán de acuerdo a la cantidad de usuarios con necesidad de certificación.

3.2.4.1. Dimensionamiento del Procesador

La capacidad de procesamiento es determinada mediante el análisis del comportamiento de un usuario común frente al servicio de red, en este caso de certificación, e involucra conocer las operaciones que ejecuta, el tiempo que demanda hacerlo y la frecuencia con que las realiza. El cálculo del procesador entonces, se fundamenta en las siguientes ecuaciones.

$$Utilización_{CPU} / usuario = \frac{Operaciones / sesión}{Tiempo de sesión en segundos} \times \frac{Uso_{CPU} \times Peticiones / operación}{Peticiones / segundo}$$

Ecuación 1. Utilización del CPU por usuario (1)

Operaciones por sesión/Tiempo de sesión en segundos se refieren al cálculo de las operaciones por segundo que un usuario realizará sobre la interfaz web pública de EJBCA. Un usuario previamente certificado, o con propósitos de hacerlo, usualmente realizará las siguientes operaciones en cada sesión: ingreso a la página web y sondeo de los enlaces e información que dispone, descarga del certificado de la CA, descarga de la CRL, búsqueda del estado de certificados, creación de la solicitud de petición de certificación, descarga de sus certificados, entre otras, por lo que se estima que realizará alrededor de 10 diferentes operaciones.

(1) Cedeño, S. A. & Robalino, J. A. (2008). *Rediseño de la Infraestructura del proveedor de servicios de Internet ONNET S.A para la optimización del servicio en el Distrito Metropolitano de Quito*. Proyecto de Titulación, Escuela Politécnica Nacional, Quito, Ecuador.

El tiempo promedio que permanecerá en una sesión web para efectuar todas estas operaciones, es aproximadamente 9 minutos (540 s).

El parámetro Uso CPU involucra los siguientes datos para su cálculo:

$$Uso_{CPU} = Velocidad_{CPU} \times Número_{CPU} \times Disponibilidad_{CPU}$$

Ecuación 2. Uso del CPU (2)

Esto implica definir un procesador referencial para su cálculo, y como la guía de apoyo de JBoss establece que debe ser al menos 1 GHz para ejecutar aplicaciones sencillas, se ha decidido emplear un procesador de 3 GHz para incrementar el rendimiento. La disponibilidad del procesador para un óptimo rendimiento está determinada por el 95%, entonces:

$$Uso_{CPU} = 3000 [MHz] \times 1 \times 0,95 = 2850 [MHz]$$

Peticiones por operación hace referencia al número de peticiones que se realizarán sobre la página web de la entidad certificadora, para completar una operación; de esta forma, pueden generarse solicitudes al sitio web y en ocasiones será necesario búsquedas en la base de datos, para procesar las respectivas respuestas, entonces en promedio se realizarán 4 peticiones por cada operación.

Peticiones por segundo es el producto entre la velocidad del procesador, el número de procesadores y las peticiones por ciclo que un procesador puede resolver; considerando que en cada ciclo (Hz = 1 ciclo/seg.) se procesa aproximadamente el 65% de una solicitud de

(2) Cedeño, S. A. & Robalino, J. A. (2008). *Rediseño de la Infraestructura del proveedor de servicios de Internet ONNET S.A para la optimización del servicio en el Distrito Metropolitano de Quito*. Proyecto de Titulación, Escuela Politécnica Nacional, Quito, Ecuador.

Servicio HTTP.

$$Peticiones_{/segundo} = Velocidad_{CPU} \times Número_{CPU} \times Peticiones_{CPU/ciclo}$$

Ecuación 3. Peticiones por Operación (3)

Para dimensionar la frecuencia óptima del procesador que soporte la demanda de peticiones simultáneas por concepto de solicitudes de certificación, o cualquier consulta, es necesario establecer un valor umbral de utilización del CPU entre el 60% y 80% de la capacidad total, para garantizar su operación en condiciones normales y evitar que colapse.

Tras realizar los cálculos empleando las ecuaciones anteriores sólo si se cumple con la siguiente condición el procesador es el adecuado.

$$Umbral\ Utilización_{CPU} \geq Usuarios\ Concurrentes \times Utilización_{CPU} / Usuario$$

Ecuación 4. Consideración Umbral de utilización del CPU (4)

El Cuerpo de Ingenieros del Ejército cuenta con aproximadamente 1020 usuarios entre funcionarios, militares y autoridades que laboran bajo su dependencia, de los cuales se estima que en horas pico cerca del 90% accederán simultáneamente al sitio web de la entidad certificadora, para descargar la CRL actualizada, considerando que cada mensaje firmado y/o cifrado contendrá un certificado digital que debe ser validado.

En tal virtud:

(3) (4) Cedeño, S. A. & Robalino, J. A. (2008). *Rediseño de la Infraestructura del proveedor de servicios de Internet ONNET S.A para la optimización del servicio en el Distrito Metropolitano de Quito*. Proyecto de Titulación, Escuela Politécnica Nacional, Quito, Ecuador.

$$Utilización_{CPU} / usuario = \frac{10}{540 [s]} \times \frac{2850 [MHz] \times (10 \times 4)}{3000 [MHz] \times 1 \times 0,65}$$

$$Utilización_{CPU} / usuario = 1,0826 [MHz]$$

$$Umbral Utilización_{CPU} \geq (1020 * 0,9) \times 1,0826 [MHz]$$

Considerando un valor umbral del 75% de utilización del procesador se tiene:

$$2250 [MHz] \geq 993,85 [MHz]$$

Con esto se deduce que el procesamiento que generará el servidor PKI en el entorno del CEE será aproximadamente de 1 [GHz] para abastecer del servicio a 1020 usuarios; a esto se le puede agregar el procesamiento requerido por sistema operativo anfitrión Ubuntu 12.04 LTS Server Edition de 64 bits, que de acuerdo a Ubuntu Official Documentation (s.f.) es 300 [MHz]. De este modo se concluye que el procesador de 3 [GHz] seleccionado como referencia abastecerá la demanda del servicio de certificación, pero sería importante considerar un procesador estructurado por varios núcleos (2, 4, 6, 8) para garantizar la operatividad del servicio y brindar una grado considerable de escalabilidad.

3.2.4.2. Dimensionamiento del Disco Duro

Para dimensionar la capacidad de almacenamiento del servidor de certificación, se considera que debe ser capaz de albergar el sistema operativo, la base de datos mysql que almacena los certificados digitales de usuario y CA emitidos, el par clave criptográfico para cada certificado y las CRLs emitidas, como también los ficheros de instalación y configuración de EJBCA y del resto de aplicaciones.

El proceso de almacenamiento será crítico principalmente durante la etapa de emisión de certificados para todos los funcionarios de la institución, posteriormente la mayoría de actividades serán de administración, por ello se recomienda un disco con capacidad de almacenamiento referencial de 160 GB.

3.2.4.3. Dimensionamiento de la Memoria RAM

Análogamente al procesamiento, la etapa crítica para el funcionamiento del servidor pki es precisamente durante la emisión de certificados para todos los funcionarios, posteriormente estará destinado a consultas, emisión y actualización periódica de CRLs, suspensión o revocación de certificados, recuperación de llaves criptográficas y otras actividades relacionadas con la gestión del sistema, razón por la que se recomienda una memoria RAM referencial de 4 GB.

3.3.SISTEMA DE CORREO ELECTRÓNICO

Para el diseño del sistema de correo del CEE de Quito es necesario definir ciertos parámetros referentes a la migración de los buzones de usuario, configurados en el servidor actual basado en Exchange, y toda la información que contiene cada uno, los requerimientos de hardware y las herramientas de software que permitan implementar todos los agentes estructurales y protocolos necesarios para el despliegue de este servicio.

3.3.1. SOFTWARE PARA EL SISTEMA DE CORREO

El diseño de un sistema de correo electrónico implica el análisis de herramientas que implementen los protocolos que emplean sus componentes estructurales, denominados agentes, y ciertas funcionalidades que complementan su funcionamiento:

1. El agente de transferencia de correo (MTA – Mail Transfer Agent) encargado de transferir los mensajes de correo electrónico entre los ordenadores, empleando el protocolo SMTP. Estos agentes utilizan programas adicionales que gestionan los mensajes de correo, preparándolos para su posterior entrega y lectura, se denominan agentes de entrega de correo (MDA – Mail Delivery Agent).
2. El agente de usuario de correo (MUA – Mail User Agent) que desempeña dos roles importantes: permite crear mensajes de correo electrónico para su posterior envío en el extremo del emisor, e implementa funcionalidades de acceso a correo mediante los protocolos POP3 (offline) e IMAP (online), para posibilitar la recuperación y lectura de los mensajes en el lado del receptor. Además, debe soportar extensiones MIME (Multipurpose Internet Mail Extensions) para interpretar o insertar texto no ASCII en el cuerpo del mensaje.
3. Una funcionalidad complementaria que posibilite a los usuarios una alternativa de acceso webmail hacia sus buzones, mediante el protocolo HTTP, para revisar su mensajería, descartando la necesidad de configurar previamente programas de cliente de correo como Outlook, Mozilla Thunderbird, Eudora, entre otros.

4. Funcionalidades que contribuyen a la seguridad del servicio de correo, como antivirus, antispam, autenticación y gestión de usuarios.

Los sistemas de correo electrónico modernos deben estar protegidos por mecanismos que neutralicen, hasta niveles tolerables, problemas relacionados con el spam, los virus informáticos o cualquier tipo de correos masivos generados ilegítimamente para intentar obtener información confidencial; debido a que están enfocados a afectar la operatividad de este servicio.

Además, su seguridad ya no radica solamente en cifrar el contenido de los mensajes transferidos por este medio (PGP), se han incluido nuevos servicios que garantizan su integridad (firmas digitales), la autenticidad de emisor, receptor y servidor, empleando certificados digitales X.509, y la protección de los enlaces establecidos para conectarse con el servidor de correo (SSL/TLS); con ello se tiene la certeza de confiar en este servicio, y la legitimidad de los correos y usuarios.

Actualmente el desarrollo de soluciones de software libre, que cumplen con estos requerimientos, mantienen un alto grado de aceptación por gran parte de empresas e instituciones a nivel mundial, que han optado por migrar sus servidores privativos a soluciones de código abierto. La razón principal es obtener beneficios y funcionalidades similares respecto al servicio, o quizás superiores, a las que pueden ofrecer las soluciones privativas, pero reduciendo considerablemente los costos de implementación, que son principalmente en representación del soporte técnico para su instalación, configuración y administración, e inclusive en algunos casos no se debe pagar por licencias de funcionamiento.

Es así que existe gran diversidad de soluciones de software libre destinadas para distintos propósitos, que equiparan o mejoran las funcionalidades provistas por las privadas, en especial en entornos de servicios de red.

En el ámbito de los sistemas de correo electrónico existen varias alternativas de herramientas linux que permiten implementar los protocolos y funcionalidades que emplean los agentes estructurales de este servicio, la Tabla 26 muestra algunas de ellas.

Tabla 26. Soluciones Linux que permiten implementar un sistema de correo electrónico

Protocolo o Funcionalidad	Herramientas de Software Libre
SMTP	Sendmail Postfix Qmail Exim
POP3/IMAP	Cyrus-IMAP Dovecot Courier UW-IMAP
Webmail	Squirrelmail Horde IMP Ilohamail Openwebmail
Antivirus	Amavisd Clamav MailScanner
Antispam	SpamAssassin
Gestor de Usuarios	OpenLDAP phpLDAPadmin

Fuente: Creado a partir de *Implementación de un Servicio de Correo Electrónico Seguro*. Recuperado de http://www.iered.org/joiner/docfinal/2-e_correo-seguro/

En tal virtud, la implementación de este servicio involucra elegir las herramientas de software necesarias, que garanticen fiabilidad y estabilidad de funcionamiento, pero fundamentalmente compatibilidad para operar en conjunto, debido a que en su mayoría se instalan y configuran independientemente.

Favorablemente existen herramientas como zimbra, que integran todos los componentes, protocolos y funcionalidades necesarias, en un solo proyecto, para establecer un sistema de correo robusto y completamente operacional, garantizando su compatibilidad de funcionamiento.

Zimbra es una alternativa que permite implantar una solución completa de correo electrónico corporativo, debido a que ha sido desarrollada en base a un conjunto de servicios Linux de reconocido prestigio por su eficiencia y seguridad, como Postfix, Courier, Mysql, Openldap, Apache y Lucene, integrados entre sí para proveer una solución eficiente.

Además, zimbra provee una funcionalidad especial llamada Zimbra Migration Tools, que permite la migración de correos electrónicos, calendarios, contactos y tareas, desde Microsoft Exchange; esta es una ventaja muy significativa para este proyecto, debido a que uno de los requerimientos es la migración de las cuentas de usuario creadas en el sistema de correo actual del Cuerpo de Ingenieros del Ejército, desarrollado bajo esta plataforma privativa, hacia el nuevo sistema desplegado sobre software libre.

Con estos antecedentes se ha decidido utilizar la plataforma de código abierto Zimbra Server para desarrollar este sistema de correo.

3.3.1.1. El Proyecto Zimbra - Zimbra Collaboration Suite

Zimbra Collaboration Suite (ZCS) es un proyecto de colaboración que ha desarrollado un software completo de mensajería de código abierto, que ofrece un servicio de correo electrónico fiable y de alto rendimiento, con funcionalidades complementarias como libretas de direcciones, agendas y diversas tareas adicionales (icti, 2011).

3.3.1.1.1. Arquitectura

El núcleo de este proyecto es el servidor zimbra, que ha sido desarrollado en base a JAVA, utilizando Jetty como servidor de aplicaciones, está integrado por varios sistemas, el MTA basado en Postfix, almacenes de datos para información de usuarios en base a OpenLDAP y MySQL, soporte para protocolos de cifrado SSL/TLS, incorpora mecanismos de seguridad como antivirus y antispam, y un potente motor de búsqueda de mensajes basado en Lucene. Los componentes de esta arquitectura son descritos en la Tabla 27.

Zimbra proporciona varias funcionalidades complementarias, entre las cuales destaca la posibilidad de acceso webmail hacia los buzones de usuario desde cualquier lugar, simplemente con disponer de conexión a internet, o también operar como cliente de correo tradicional con herramientas como Outlook o Thunderbird, que utilizan los protocolos POP/IMAP.

Tabla 27. Componentes de la Arquitectura Zimbra Server

COMPONENTE	DESCRIPCIÓN
a. MTA	Es el núcleo del sistema que implementa el protocolo SMTP para enrutar los mensajes de correo, y LMTP para entregarlos al almacén de correos correspondiente, provee un almacén de buzones con soporte de acceso POP e IMAP, y cifrado de canal SSL. Emplea la herramienta SpamAssassin como filtro antispam, ClamAV como antivirus, y Amavis como filtro de contenidos, con la posibilidad de personalizarlo para emplear cualquier otra herramienta de filtrado.
b. Core	Este componente contiene librerías, ficheros de configuración y herramientas de monitorización.
c. LDAP (OpenLDAP)	Zimbra emplea este directorio para almacenar y gestionar información de autenticación de las cuentas de usuario. Debido a su versatilidad es posible integrar al sistema de correo con directorios externos LDAP, como Active Directory u OpenLDAP.
d. Store	Este componente utiliza el servidor de aplicaciones Jetty, desarrollado en base a JAVA, como contenedor de servlets para almacenar el correo electrónico. Zimbra contiene varios almacenes vinculados entre sí para administrar el correo, los más importantes son el almacén de datos (una base de datos MySQL) que contiene información del buzón del usuario (carpetas, citas del calendario, contactos y el estado de los mensajes, es decir, leídos y no leídos), y el almacén de mensajes que contiene los mensajes y sus adjuntos en formato MIME.
e. SNMP y Logger	La instalación de estos paquetes contribuye a la gestión del servidor, incluyendo herramientas de monitorización periódica y reportes de seguimiento de mensajes mediante logs e informes.

Fuente: Creado a partir de Rave et al. (2008). Instalación y Configuración de Zimbra 5 Suite de Mensajería y Colaboración. Recuperado de http://www.redes-linux.com/manuales/Servidor_correo/Instalacion-y-Configuracion-de-Zimbra-en-Debian-Ecth.pdf

Además, incorpora un cliente web de correo que se ejecuta sobre AJAX⁴⁶, garantizando su compatibilidad con los navegadores web más populares como Mozilla Firefox o Internet Explorer.

Por mencionar, algunas de sus prestaciones son:

- Correo Electrónico

⁴⁶ Asynchronous Javascript and XML

- Libreta de Direcciones
- Agendas / Calendarios
- Tareas
- Bloc de Notas
- Maletín de Documentos
- Mensajería Instantánea / Chat
- Búsquedas avanzadas en todos sus componentes y módulos
- Herramientas de importación de datos desde entornos Exchange o Outlook
- Compartir contenido en el wiki corporativo
- Interfaz web de usuario intuitiva y fácil de manejar

3.3.2. DESPLIEGUE DEL SISTEMA DE CORREO

La instalación de Zimbra Server involucra que todo el tema referente a resolución de nombres de dominio (DNS) esté configurado de tal manera que permita la implementación de este servicio; esto se refiere a que si existen peticiones sobre el dominio `cee.gob.ec`, en este caso un dominio local configurado para simular este proyecto, en busca del intercambiador de correo (mail exchange - MX), éstas sean direccionadas hacia el host sobre el cual se ha desplegado este sistema para que las administre.

También es necesario instalar herramientas preliminares para asegurar la ejecución de los procesos posteriores en la instalación de zimbra. La primera parte del Anexo F (Preparación del Entorno) contiene información detallada acerca de la instalación de estas herramientas, como también de la configuración del DNS y el host anfitrión del sistema de correo, ambos desplegados sobre máquinas virtuales, resaltando que se ha utilizado el Sistema Operativo GNU/Linux de distribución Centos 6.4 de 64 bits para el servidor de correo, y Ubuntu Server 12.04 LTS de 64 bits para el DNS.

Otra consideración de importancia es detener de manera definitiva la ejecución de postfix, que viene instalado como MTA por defecto para centos, si no se detiene se generarán conflictos al utilizar el puerto 25 durante la instalación. La segunda parte del Anexo F (Instalación de Zimbra) contiene información detallada referente a la instalación del sistema de correo.

3.3.2.1. Interfaces de Administración y Webmail de Zimbra

La interfaz web de administración posibilita la gestión del sistema de correo zimbra, a través de ella se puede verificar el estado de los servicios, creación de cuentas de correo, monitorización de eventos, logs y varias actividades que contribuyen a la seguridad, como habilitar S/MIME por ejemplo; para acceder a ella es necesario autenticarse en la dirección <https://mail.cee.gob.ec:7071/zimbraAdmin> (véase Figura 31).

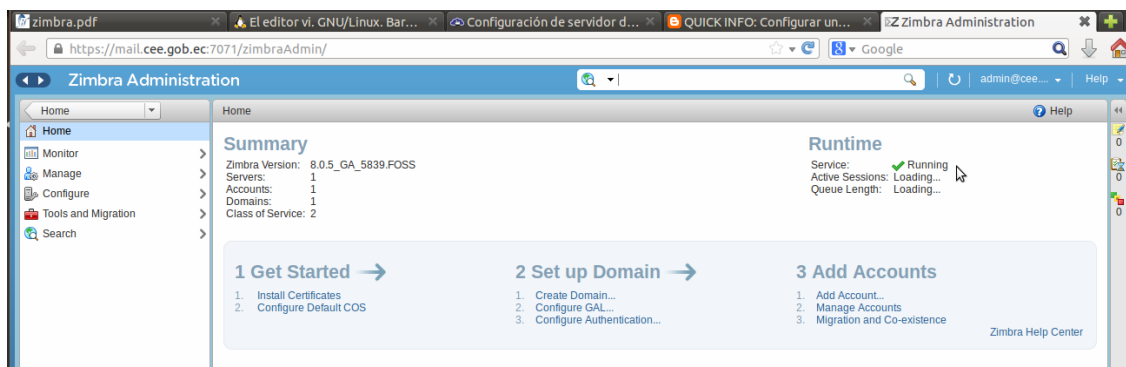


Figura 31. Visualización de la interfaz de administración

La interfaz Webmail se basa completamente en AJAX, para permitir el acceso web a los buzones de correo de los usuarios, la dirección URL de acceso es <https://mail.cee.gob.ec> (véase Figura 32), su función principal es permitir la interacción de los clientes de correo con sus buzones, y todas las prestaciones que provee.

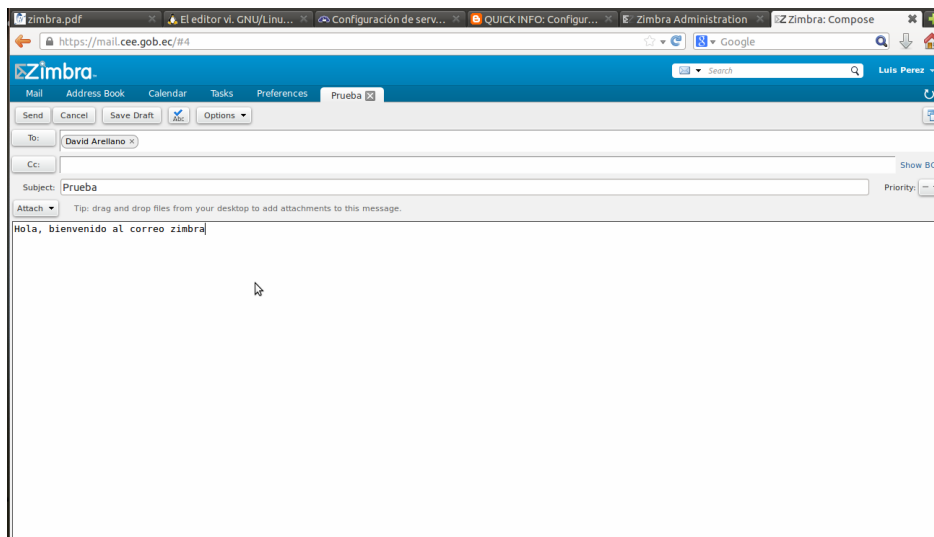


Figura 32. Visualización de la interfaz webmail – Creación de un correo

3.3.2.2. Clase de Servicio (COS)

Es un componente prioritario de zimbra que permite establecer los atributos que deben tener, y las características que se permiten o deniegan, en las cuentas de correo de usuario. Mediante su gestión se controlan parámetros como el tiempo de vida de los mensajes alojados en el servidor, restricciones de contraseñas de usuario, el manejo de archivos adjuntos en los correos, el tamaño que deben tener los buzones de usuario para almacenamiento de mensajes, y varias configuraciones del servidor.

Esto es de importancia para este proyecto debido a que en el servidor de correo actual del CEE de Quito, existen distintos tipos de cuentas de usuario configuradas con ciertas prioridades dependiendo del rol que desempeñan los funcionarios y militares en la institución, en especial referentes a la capacidad permitida para el almacenamiento de mensajes en los buzones; la tercera parte del Anexo F (Clase de Servicio COS) detalla los procedimientos para configurar esta característica en el servidor zimbra.

3.3.2.3. Certificación del servidor Zimbra

Uno de los requerimientos de seguridad del servidor de correo en desarrollo es que debe implementar el protocolo seguro SSL/TLS para cifrar los enlaces de comunicación establecidos entre cliente/servidor, y proteger de esta forma el tráfico referente a este servicio que circulará por la red; para ello, durante el proceso de instalación de zimbra se genera de forma predeterminada un certificado digital auto-firmado con el cual se puede llevar a cabo este proceso de seguridad.

Sin embargo, este certificado es de carácter temporal y en entornos de implementación real es imprescindible sustituirlo por uno generado y personalizado específicamente para este servidor, y zimbra es una solución tan versátil que provee dos alternativas para realizarlo (véase Figura 33).

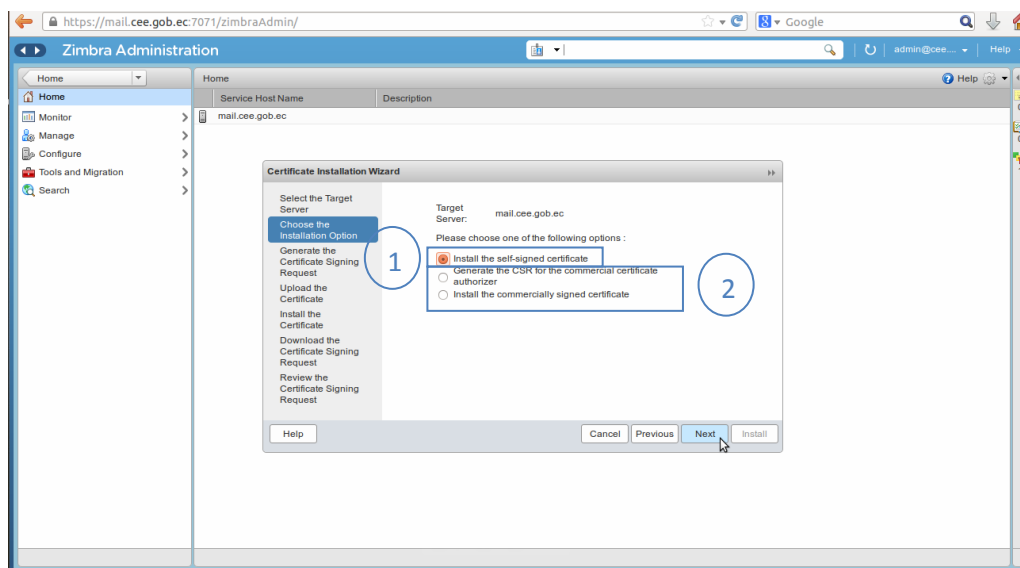


Figura 33. Alternativas para sustituir el certificado digital predeterminado de zimbra

La primera (Install the self-signed certificate) consiste en generar un certificado digital auto-firmado empleando el propio servidor zimbra, esto es posible debido a

una funcionalidad de carácter complementario con la que dispone (una Autoridad Certificadora), que posibilita la implementación de seguridad SSL/TLS a través de la emisión de certificados que identifican únicamente a este servidor; ésta CA no está en capacidad de emitir cualquier otro tipo de certificados, en vista de que no es administrable (véase Figura 34).

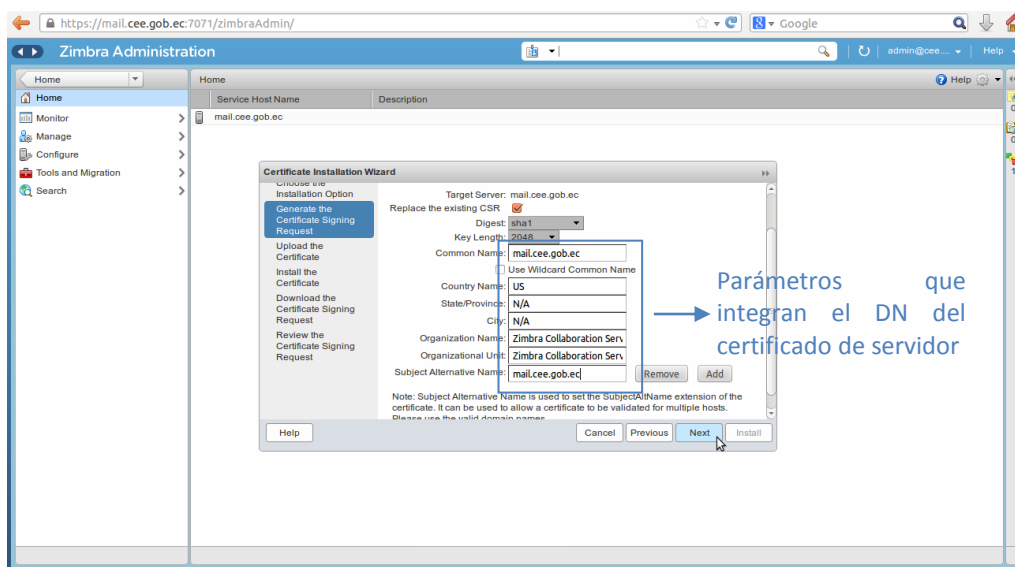


Figura 34. Parámetros que identifican y personalizan al certificado SSL de zimbra

La ventaja de emplearla radica en que este certificado se instala automáticamente en el servidor, para identificarlo ante los clientes de correo. De todos modos, esta funcionalidad de zimbra, a pesar de todos sus beneficios, no será implementada en este proyecto, considerando que a esta altura de su desarrollo, el Cuerpo de Ingenieros del Ejército dispone de una Autoridad Certificadora completamente funcional, diseñada para certificar a los funcionarios y militares que laboran en esta entidad, y en este caso al servidor de correo en desarrollo.

La segunda funcionalidad (Generate the CSR for the comercial certificate authorizer) en cambio permite generar una solicitud de certificación (CSR⁴⁷) para que una entidad certificadora comercial la procese, y emita y gestione el certificado requerido (véase Figura 33).

Básicamente esta solicitud contiene parámetros que identifican a la entidad solicitante, en este caso al servidor zimbra, de hecho son los mismos que se muestran en la Figura 34, pero la diferencia es que al finalizar este proceso se obtendrá un fichero `current.csr` (solicitud de certificación) que deberá ser entregada a la entidad certificadora (véase Figura 35).

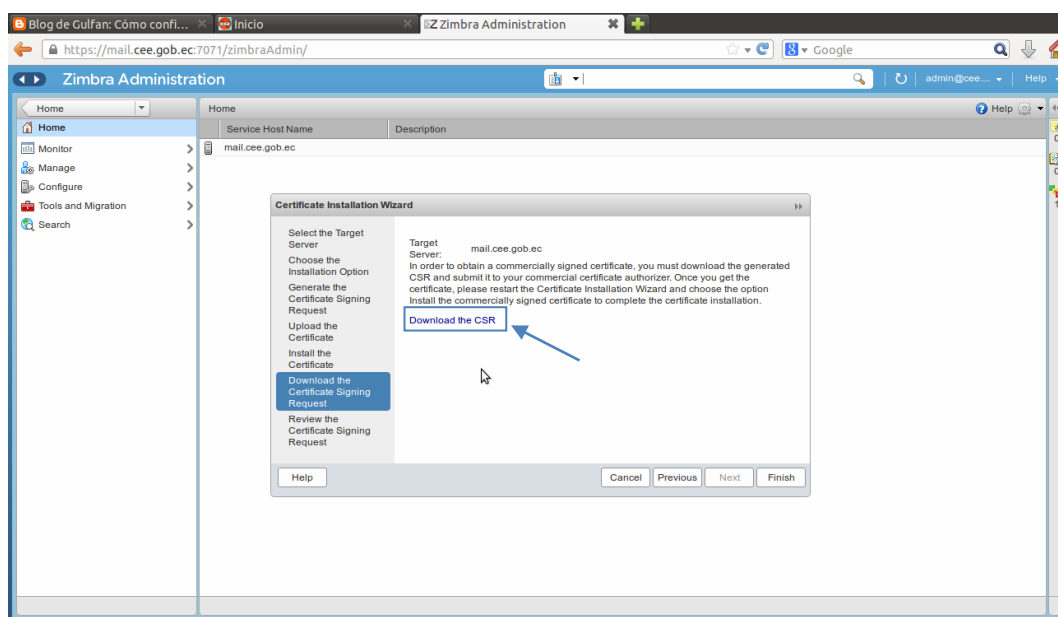


Figura 35. Generar una solicitud de firma de certificado - CSR

Pero este proceso puede omitirse en el caso de este proyecto, teniendo en cuenta que no se va a solicitar una certificación de una entidad externa, el propósito es emplear la PKI del CEE diseñada para obtener el certificado, y realizar todo el proceso de instalación de manera que éste sustituya al que se está utilizando actualmente en el servidor zimbra, convirtiéndose de

⁴⁷ Certificate Signing Request – Solicitud de Firma de Certificado

esta forma en la etapa inicial de aplicación de los certificados en el entorno de esta entidad; todo este procedimiento se describe detalladamente en la cuarta parte del Anexo F (Generación e instalación del certificado para el servidor zimbra).

La siguiente etapa de aplicación se llevará a cabo al instalar los certificados digitales en los ordenadores de los funcionarios y militares del CEE, y configurar los clientes de correo para aplicar firmas digitales y cifrar los mensajes mediante técnicas S/MIME, este procedimiento a diferencia del anterior se explica en el capítulo 4 conjuntamente con las pruebas de funcionamiento de todo el proyecto.

3.3.2.4. Migración de las Cuentas de Correo del Servidor Exchange hacia Zimbra

Es uno de los requerimientos primordiales de este proyecto de titulación, planteado con el objetivo de sustentar su desarrollo, considerando que actualmente el Cuerpo de Ingenieros del Ejército dispone de una plataforma de correo operativa, basada en Microsoft Exchange, con datos reales que deben salvaguardarse durante la transición hacia la nueva plataforma open source, para garantizar que los clientes conserven sus buzones y la información que estos contienen, específicamente las bandejas de mensajes y los contactos.

Este fue uno de los factores que influyeron directamente en la elección de Zimbra Server como solución para implementar este servicio en el CEE, debido a que provee, adicionalmente a las prestaciones de un sistema de correo convencional, funcionalidades que posibilitan efectuar la migración de este tipo de información desde Exchange, cumpliendo de esta forma con este requerimiento del sistema.

El propósito es dar a conocer a las autoridades de esta entidad que existen soluciones, basadas en software libre, lo suficientemente estables como para soportar la demanda generada por las implementaciones en ambientes reales de producción, a tal punto que están en capacidad de proveer servicios y funcionalidades similares a las privativas, pero reduciendo los costos de implementación.

Para este proceso de migración se ha estimado la severidad de los riesgos a los que se puede exponer a esta entidad en caso de afectar la operatividad del servidor Exchange, o pero aún la pérdida de su información; además, es comprensible que el administrador de red por salvaguardar los bienes de la misma, y cumplir con sus actividades laborales y políticas de seguridad informática, restrinja el acceso al mencionado servidor, necesario para efectuar configuraciones y pruebas de funcionamiento.

Este es el motivo por el cual se ha decidido simular una plataforma de correo empleando las mismas herramientas de software que la actual, el sistema operativo, la versión de Exchange, un sistema de directorio Active Directory, y todo lo que el proceso implique. El objetivo es crear una base de datos administrada bajo este nuevo sistema a la cual se vinculen direcciones de correo que representarán a la de cada funcionario, se agregarán contactos, se enviarán y recibirán mensajes, y finalmente toda esta información del servidor será migrada hacia Zimbra.

Mediante el desarrollo de este proceso se demostrará que es posible su ejecución desde el sistema real, garantizando a las autoridades de esta entidad que no existirá ningún percance de por medio, y que se tiene muy claro lo que se quiere hacer y cómo hacerlo. El Anexo G contiene toda la información en detalle de esta etapa del proyecto, la simulación de la

plataforma de correo Exchange, su configuración, la creación de la base de datos y las cuentas de usuario, y por último la migración hacia zimbra.

3.3.3. DIMENSIONAMIENTO DE HARDWARE

El servidor de correo actual del Cuerpo de Ingenieros del Ejército administra aproximadamente 1020 cuentas de usuario, destinadas a los funcionarios públicos y militares de la institución, los cuales por cuestiones laborales acceden reiteradamente a ellas, para diferentes fines como agilizar trámites, peticiones, solicitudes, aprobaciones, contratos, proyectos, presupuestos, etc., que son actividades obligatorias que demanda su trabajo.

Esto da a entender que en momentos determinados del día, cerca del 90 % de estos usuarios de correo, estarán conectados simultáneamente a sus cuentas, e interactuando con el servidor, por tal motivo, éste debe ser dimensionado para soportar este umbral de procesos, de alrededor de 918 cuentas activas.

De acuerdo a las recomendaciones propuestas por Zimbra and VMware (2011), los requerimientos de hardware referenciales para implementar Zimbra Collaboration Server en ambientes reales de producción, son los descritos en la Tabla 28.

Es así que, se emplearán estos datos para realizar el cálculo del procesador, de acuerdo al análisis del comportamiento de los usuarios de correo, análogamente a como se lo realizó en el dimensionamiento del servidor PKI.

Tabla 28. Requerimientos de Hardware - Zimbra Server

Parámetro	Descripción
Procesador	Mínimo Intel/AMD 2.0 GHz, de preferencia implementarlo en sistemas operativos de 64 bits.
Memoria RAM	Mínimo 2 GB (recomendado 4GB).
Capacidad de Almacenamiento	10 GB de espacio libre para software y logs. Espacio adicional para almacenamiento de correo: zimbra-store requiere 5 GB, adicionalmente el espacio para almacenamiento de correo; el resto de componentes de la arquitectura de zimbra requieren 100 MB.

Fuente: Creado a partir de Zimbra and VMware. (2011). System Requirements for Zimbra Collaboration Server. Recuperado de http://www.zimbra.com/docs/ne/latest/single_server_install/wwhelp/wwhimpl/common/html/wwhelp.htm#context=NE_QuickStart_7_1&file=System%20Requirements.html

3.3.3.1. Dimensionamiento del Procesador

Un usuario de correo electrónico usualmente realiza operaciones como: acceso a la cuenta, revisión de la mensajería del buzón de entrada, agregar contactos, crea, almacena y elimina correos, programa su calendarización, genera notas, entre otras; se puede promediar entonces que realizará alrededor de 15 operaciones. De esta forma, el tiempo estimado que este usuario permanecerá en una sesión con el servidor de correo para efectuar estas operaciones es 15 minutos (900s).

El procesador referencial para el cálculo del parámetro Uso_{CPU} , de acuerdo a la Tabla 28 debe ser de 2GHz, pero para incrementar el rendimiento y garantizar la operatividad del servicio se ha decidido emplear un procesador de 3 GHz.

$$Uso_{CPU} = Velocidad_{CPU} \times Número_{CPU} \times Disponibilidad_{CPU}$$

$$Uso_{CPU} = 3000 [MHz] \times 1 \times 0,95 = 2850 [MHz]$$

El número de peticiones que se realizarán sobre el servidor de correo en una sesión establecida para completar una operación, son 4, debido a que se generarán solicitudes que deberán ser atendidas por el servidor, y en ocasiones será necesario realizar búsquedas en la base de datos, para procesar las respuestas esperadas.

En tal virtud:

$$Utilización_{CPU} / usuario = \frac{Operaciones / sesión}{Tiempo de sesión en segundos} \times \frac{Uso_{CPU} \times Peticiones / operación}{Peticiones / segundo}$$

$$Utilización_{CPU} / usuario = \frac{15}{900 [s]} \times \frac{2850 [MHz] \times (15 \times 4)}{3000 [MHz] \times 1 \times 0,65}$$

$$Utilización_{CPU} / usuario = 1,462 [MHz]$$

El número de usuarios de correo concurrentes es 918.

$$Umbral Utilización_{CPU} \geq 918 \times 1,462 [MHz]$$

Considerando un valor umbral del 75% de utilización del procesador se tiene:

$$2250 [MHz] \geq 1341,69 [MHz]$$

Con esto se concluye que el procesamiento que generará el servidor de correo en el entorno del Cuerpo de Ingenieros del Ejército es aproximadamente 1,5 [GHz] para abastecer la demanda del servicio a 1020 personas; a esto se le puede incluir el procesamiento requerido por el sistema operativo anfitrión Centos 6.4 de 64 bits, que de acuerdo a Red Hat (2008) en su Soporte de Guía de Instalación, es de 500 [MHz].

De manera que el procesador referencial seleccionado de 3 [GHz] está en capacidad de soportar la demanda de este servicio, pero para mayor grado de escalabilidad es preferible elegir un procesador con varios núcleos (2, 4, 6, 8) para mejorar el rendimiento y garantizar su operatividad.

3.3.3.2. Dimensionamiento del Disco Duro

Para dimensionar la capacidad de almacenamiento del servidor de correo, se considera que debe ser capaz de albergar el sistema operativo, los buzones de correo, y los ficheros de instalación y configuración de Zimbra Server, y la de todos sus componentes.

El tamaño de los buzones del servidor actual del CEE (Microsoft Exchange) es descrito en la Tabla 29; es así que se dimensionará la capacidad de almacenamiento de zimbra server para mantener estos tamaños referenciales.

Tabla 29. Tamaño de los buzones de usuario - Exchange

Tipo de Usuario (Perfil)	Espacio de Buzón	Estimación de Usuarios
Comando – Estado Mayor	Ilimitado	30
Jefes Departamentales	50 MB	50
Coordinadores	45 MB	20
Usuarios en General	30 MB	Los restantes (920)

Fuente: Elaborado con la ayuda del Departamento de Sistemas del CEE (2013)

Con esto se puede determinar que la capacidad de almacenamiento requerida por cada perfil de usuario es: Jefes Departamentales 2,5 GB, Coordinadores 900 MB, Usuarios en

general 27,6 GB; en el caso de las autoridades de Estado Mayor los buzones deben ser privilegiados, por establecer un valor referencial para el dimensionamiento de este servidor, se ha considerado que deberían ser de al menos 100 MB, generando una capacidad de almacenamiento de 3 GB, para este tipo de usuarios.

En lo referente al sistema operativo anfitrión del servidor, Centos 6.4 de 64 bits, Red Hat (2008) en su Soporte de Guía de Instalación, propone que la capacidad de almacenamiento debe ser de 4 GB para entornos de producción considerablemente grandes.

Finalmente, los requerimientos de almacenamiento necesarios para implementar zimbra server son los que se han expuesto en la Tabla 28; en tal virtud, la capacidad de almacenamiento total del servidor se detalla en la Tabla 30.

Tabla 30. Cálculo de la Capacidad de Almacenamiento

Parámetro	Tamaño del Disco	
Comando – Estado Mayor	3 GB	
Jefes Departamentales	2,5 GB	
Coordinadores	900 MB	
Usuarios en General	27,6 GB	
Sistema Operativo	4GB	
Capacidad Parcial		
	38 GB	
Zimbra Server	Espacio libre para software y logs	10 GB
	Zimbra Store	5 GB
	Almacenamiento de Correo	38 GB
	Componentes de Zimbra	100 MB
Capacidad Total		
	53,1 GB	

Este es un valor referencial de la capacidad de almacenamiento necesaria para implementar este servicio, pero se debe estimar cierto grado de escalabilidad para garantizar que no se pierda ningún tipo información perteneciente a los buzones, en especial aquellos destinados a las autoridades; por ello se recomienda emplear un disco con capacidad referencial de 160GB.

3.3.3.3. Dimensionamiento de la Memoria RAM

Análogamente al procesamiento, los procesos del servidor irán aumentando gradualmente, de acuerdo a los requerimientos y necesidades de los funcionarios, razón por la que se recomienda una memoria RAM referencial de 8 GB, considerando los requerimientos de zimbra server de la Tabla 28, y las recomendaciones propuestas por Red Hat (2008) para alojar el sistema operativo.

CAPÍTULO 4. PRUEBAS DE FUNCIONAMIENTO

En esta etapa del proyecto se exponen ciertas actividades y configuraciones que contribuyen a la demostración del funcionamiento de los sistemas desarrollados, y su interacción, para constituir un mecanismo de seguridad basado en una de las herramientas más fiables empleadas en transacciones de comercio electrónico, los certificados digitales.

Este mecanismo contribuirá a la implantación de un sistema de correo electrónico seguro para la red de datos del Cuerpo de Ingenieros del Ejército de Quito, a través de métodos de criptografía asimétrica. Para que sea más evidente esta tarea se efectuará técnicas de hacking ético, empleando el analizador de paquetes de red Wireshark, para intentar vulnerar la confidencialidad de los mensajes transferidos por este sistema, y mediante el análisis del contenido de los paquetes capturados demostrar su grado de protección.

4.1.PROCESO DE CERTIFICACIÓN

La primera parte del proceso de certificación se llevó a cabo al generar un certificado SSL/TLS tanto para el servidor web de EJBCA, como también para el servidor de correo zimbra, ahora es momento de certificar a los funcionarios y militares del CEE; para ello, todas las actividades que involucra este proceso las efectuará el administrador de red de esta institución, con la ayuda de personal capacitado, los funcionarios únicamente serán instruidos para utilizar sus buzones de correo y generar mensajes protegidos por técnicas de cifrado y firma digital.

4.1.1. REGISTRO

Este es el proceso en el cual el administrador registra en el componente RA de la PKI, la información del usuario que ha solicitado certificación, después de haber constatado su legitimidad, aunque en este caso, al tratarse de solicitantes que laboran en la misma entidad, este proceso es mucho más sencillo.

Acceder al apartado RA Functions de la admin web, elegir Add End Entity e ingresar los datos del solicitante (véase Figura 36).

The screenshot shows the 'Add End Entity' form in the EJBCA Administration interface. The form is divided into several sections:

- End Entity Profile:** PERSONAS (Required)
- Username:** Fabian Pazmiño (Required)
- Password:** [Redacted] (Required)
- Confirm Password:** [Redacted] (Required)
- E-mail address:** fpazmino@cee.gob.ec (Not Required)
- Subject DN Attributes:**
 - CN, Common name:** Mayor Fabián Pazmiño (Required)
 - UID, Unique Identifier:** Departamento de Sietemas (Required)
 - O, Organization:** Cuerpo de Ingenieros del Ejercito (Not Required)
 - OU, Organizational Unit:** Entidad Final CEE (Not Required)
 - C, Country (ISO 3166):** EC (Not Required)
- Other subject attributes:** (None)
- Subject Alternative Name:** (None)
- RFC 822 Name (e-mail address):** Use data from E-mail address field (Not Required)
- Main certificate data:**
 - Certificate Profile:** PERFIL_ENTIDAD_FINAL (Required)
 - CA:** Autoridad Certificadora CEE (Required)
 - Token:** P12 file (Required)
- Other data:**
 - Key Recoverable:** [Checked] (Not Required)

Buttons: Add, Reset

Customized by David Ricardo Valencia de la Torre, Sep. 2013.

Figura 36. Proceso de registro del usuario solicitante

4.1.2. CONFIAR EN LA CA RAÍZ DE LA PKI

En un ambiente de certificación se debe considerar que la fiabilidad de la jerarquía radica en la Autoridad Certificadora Raíz, de manera que previamente a instalar un certificado

personal, es necesario establecerla como una entidad fiable, para garantizar la interacción con cualquier certificado que ésta gestione. Para ello se debe instalar el certificado auto-firmado de esta CA, en cada uno de los ordenadores de usuario que requieran utilizar este sistema de seguridad.

4.1.2.1. Instalación del Certificado

Acceder a la interfaz web pública de EJBCA, seleccionar la opción Fetch CA & OCSF Certificates y pulsar en Download to Internet Explorer para obtenerlo (véase Figura 37).

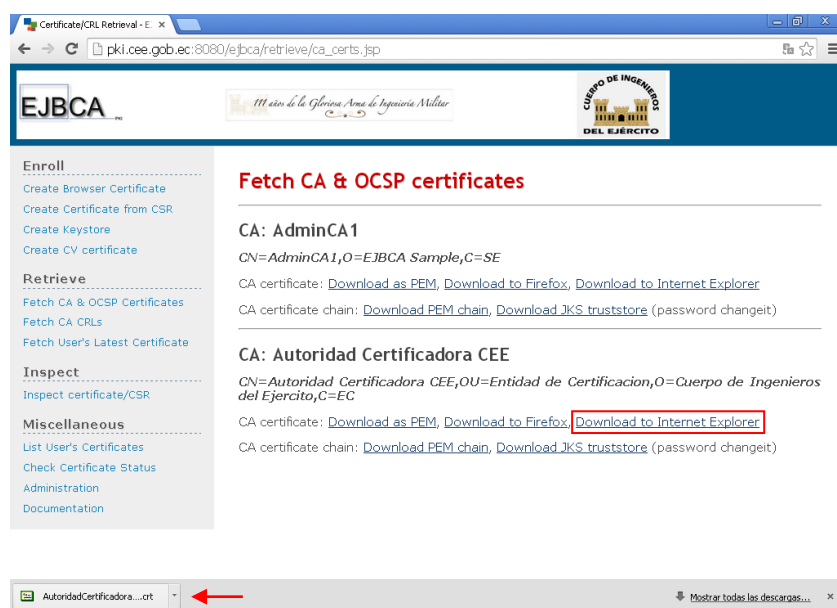


Figura 37. Descargar el certificado de la CA Raíz

Mozilla Firefox utiliza su propio almacén de certificados, a diferencia de Internet Explorer o Google Chrome que emplean el almacén de Windows, por ello es recomendable descargar el certificado de la CA para este tipo de navegadores web. Ejecutar el archivo descargado para iniciar el asistente de importación de certificados de Windows, y al finalizar este proceso se

puede comprobar si este certificado se ha importado, empleando el administrador de certificados del navegador web (véase Figura 38).

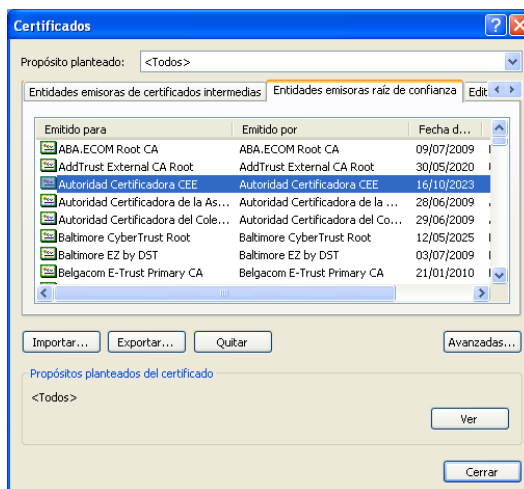


Figura 38. Administrador de Certificados de Google Chrome

4.1.3. EMISIÓN E INSTALACIÓN

Para obtener el certificado del usuario solicitante, previamente registrado, acceder a la opción Create Browser Certificate de la interfaz web pública, y autenticarse con el usuario y la contraseña acordados durante el registro (véase Figura 39).

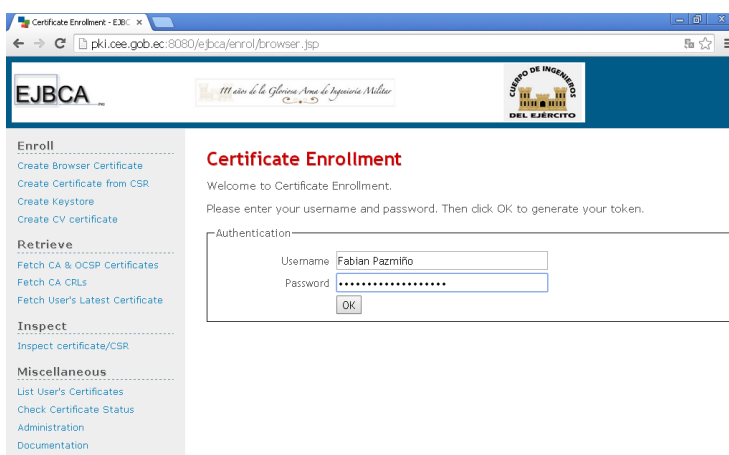


Figura 39. Usuario y contraseña del solicitante

Si la autenticación ha sido exitosa se procede a definir la longitud del par clave criptográfico RSA a ser creado, para generar la solicitud de certificación, y obtener el certificado (véase Figura 40).

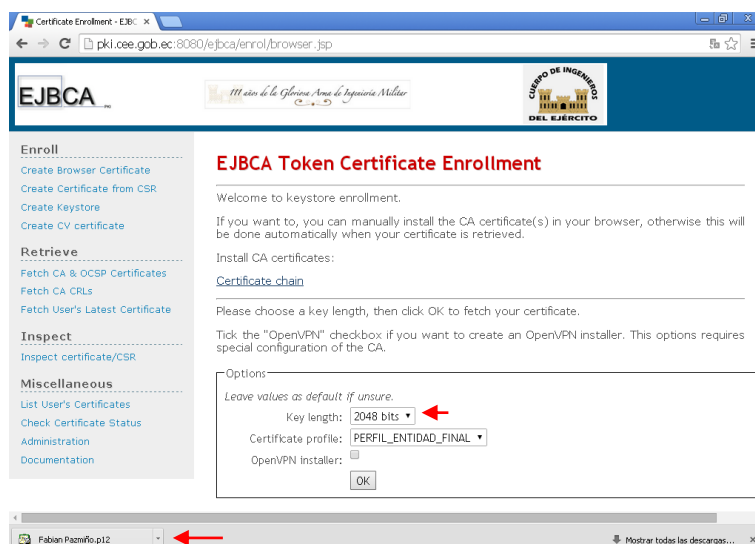


Figura 40. Establecer la longitud del par clave

Se obtendrá un archivo de extensión .p12 que contiene la clave pública de este usuario, alojada en su certificado, y la clave privada que ha sido cifrada con la contraseña de autenticación de registro; al ejecutarlo activará al asistente de importación de certificados de Windows, y solicitará esta contraseña (véase Figura 41).

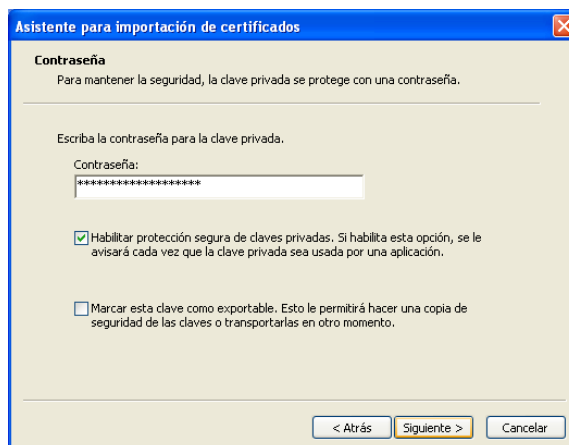


Figura 41. Descifrar la clave criptográfica privada

Al finalizar este proceso iniciará una aplicación para proteger la clave privada durante su almacenamiento en el sistema operativo (véase Figura 42), se debe seleccionar Nivel de seguridad y fijar la opción Alto, esto hace que cada vez que se requiera emplear esta clave privada sea necesario ingresar la contraseña establecida.

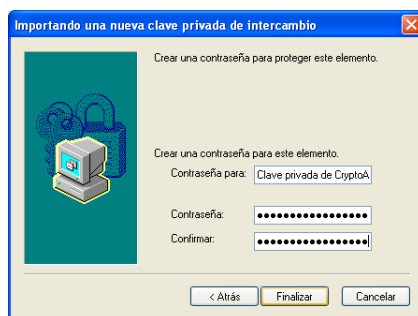


Figura 42. Contraseña de protección de la clave privada

Con esto se ha completado la solicitud, emisión e instalación del certificado personal, disponiendo desde este momento de un mecanismo de seguridad fiable, que puede ser empleado para diversos propósitos (véase Figura 43), pero en lo que se refiere a este proyecto será empleado específicamente para la seguridad del correo institucional.

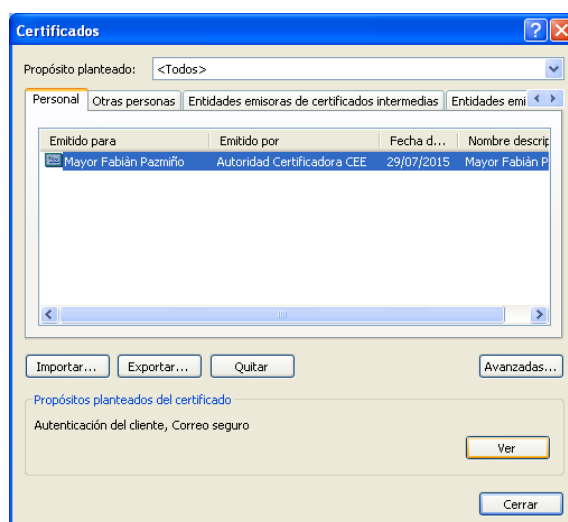


Figura 43. Certificado Personal instalado en el repositorio Windows visualizado empleando Google Chrome

4.2.EJECUCIÓN DEL SISTEMA DE CORREO ELECTRÓNICO

Cuando zimbra esté en ejecución es importante supervisar el estado de los servicios que éste provee, accediendo a la consola de administración (véase Figura 44).

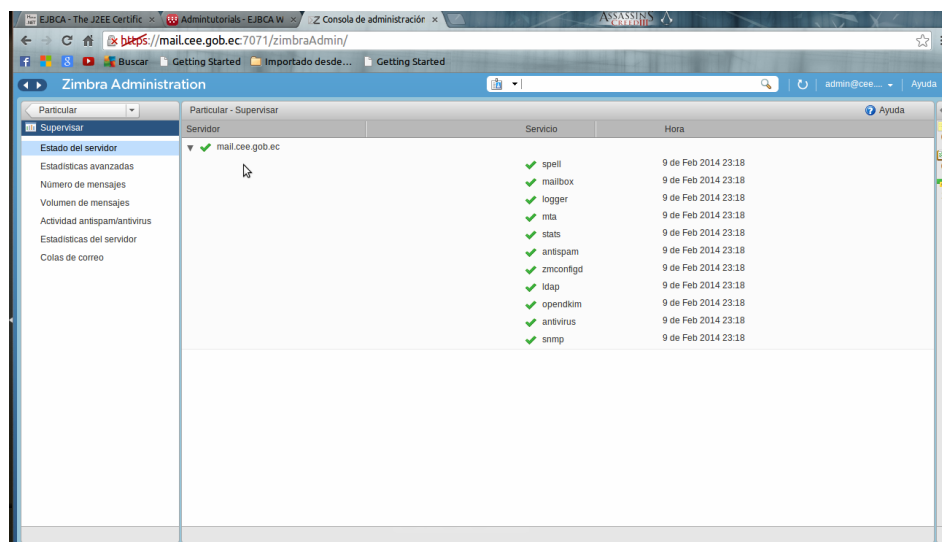


Figura 44. Supervisar la ejecución de los servicios de zimbra

4.2.1. CREACIÓN DE UNA CUENTA DE USUARIO

En la sección Administrar del panel de administración de zimbra, seleccionar Cuentas, añadir una cuenta nueva y proporcionar los datos del buzón de correo a crearse (véase Figura 45). Las cuentas que han sido configuradas para realizar estas pruebas se muestran en la Figura 46.

4.2.2. CONFIGURACIÓN DE LA CUENTA

Los parámetros de configuración de la cuenta deben definirse de acuerdo a la Figura 47, en un entorno de cliente Microsoft Outlook.

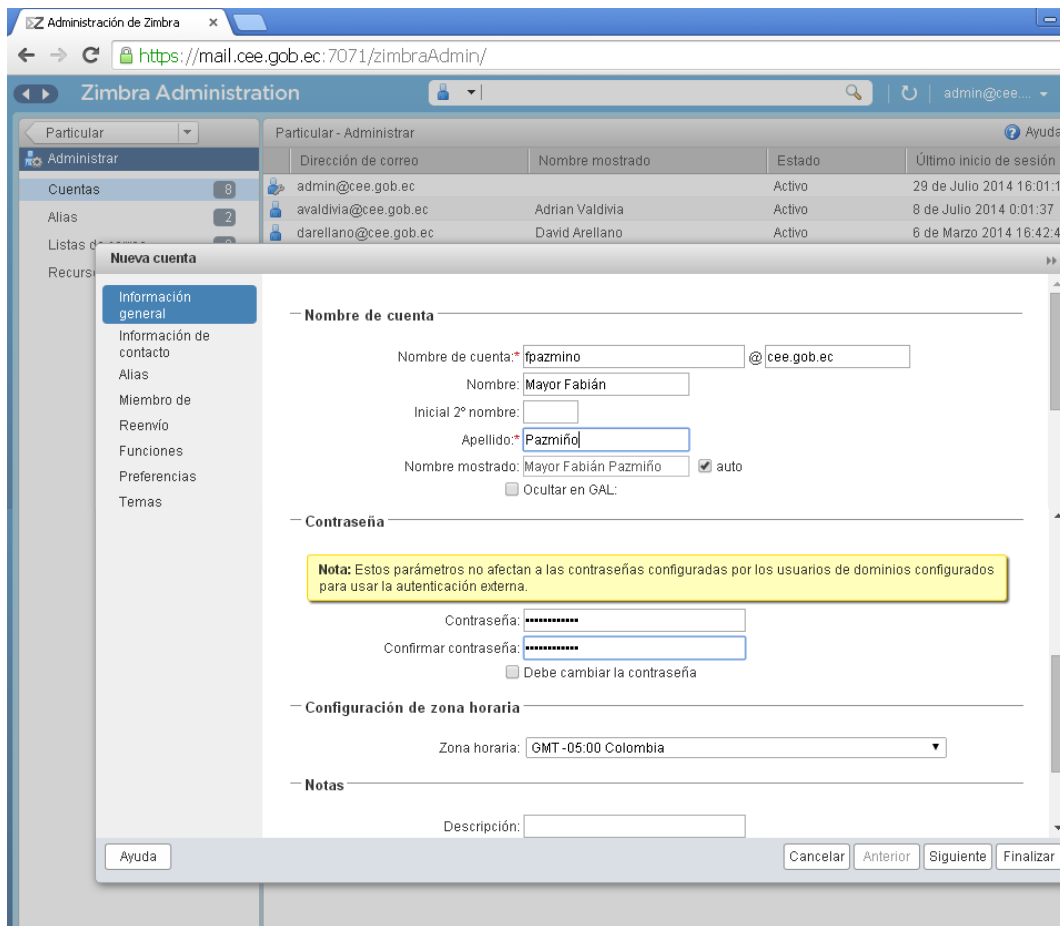


Figura 45. Creación de una cuenta de correo

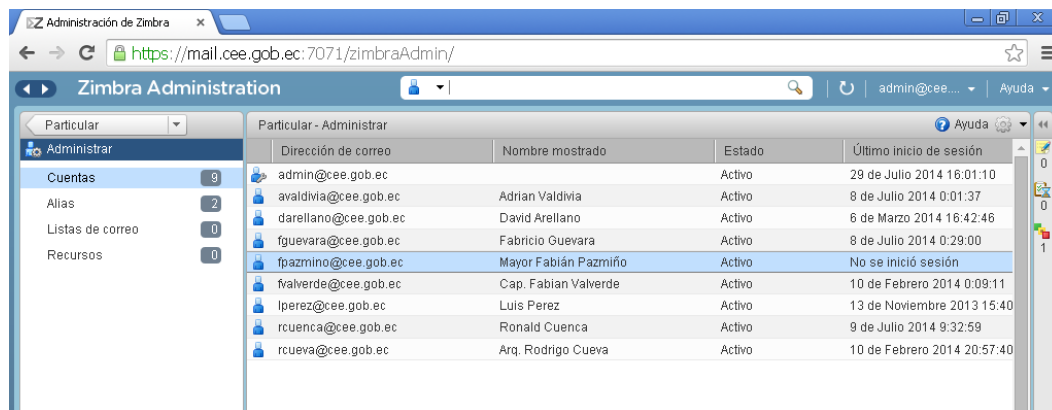


Figura 46. Buzones administrados por el servidor Zimbra

Figura 47. Parámetros de configuración de la cuenta

Además, la configuración de los puertos SMTP, POP y sus seguridades, se la realiza accediendo a Más configuraciones en la pestaña Avanzadas (véase Figura 48).

Figura 48. Configuración de puertos

Se observa que se ha utilizado POP3 para descargar una copia de la mensajería en el ordenador cliente, empleando SSL para cifrar esta conexión temporal establecida con el servidor, y SMTP como protocolo usual de transporte de mensajería, pero complementado con TLS para cifrar el canal de comunicación y proteger la información en tránsito.

4.2.3. CONFIGURAR EL CLIENTE DE CORREO PARA ACTIVAR LOS MECANISMOS DE CIFRADO Y FIRMA DIGITAL

La funcionalidad que deben disponer los agentes de usuario de correo MUA para proveer seguridad en base a certificados digitales, es S/MIME, y en el caso de este proyecto Outlook la incorpora.

En el panel Herramientas de Outlook seleccionar Centro de Confianza, en él dirigirse a Seguridad del Correo Electrónico y habilitar las tres primeras casillas (véase Figura 49), esto activará las técnicas de cifrado y firma digital.

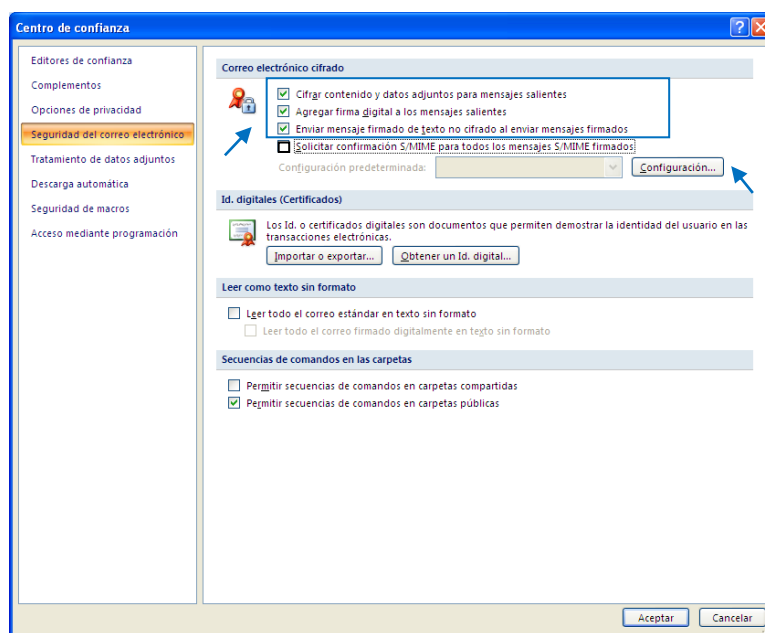


Figura 49. Habilitar las técnicas S/MIME de cifrado y firma digital

La cuarta casilla habilita una respuesta de confirmación S/MIME, eso significa que cada vez que un funcionario envíe un mensaje con su firma digital, recibirá un mensaje notificando que éste ha sido revisado por el receptor, pero se ha considerado que al enviar mensajes a una

lista de destinatarios simultáneamente, esto generaría demasiadas respuestas e incrementaría el flujo de tráfico innecesario en la red, por ello no ha sido habilitada esta opción.

Sobre la misma pantalla Seguridad del Correo Electrónico seleccionar Configuración y elegir el certificado de usuario que se va a utilizar desde este momento para firmar digitalmente los mensajes que se originen en esta cuenta de correo, y también los algoritmos criptográficos tanto de firma, como de cifrado (véase Figura50).

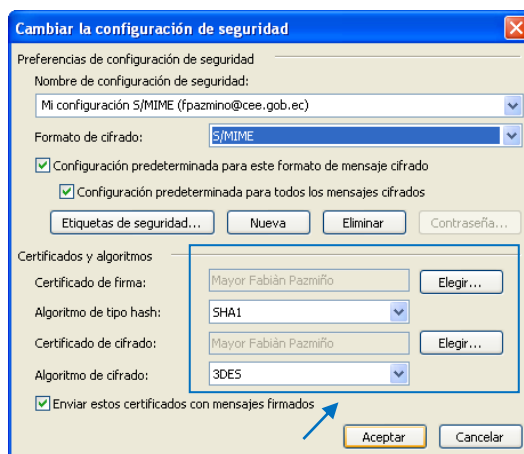


Figura 50. Certificado de firma digital

4.2.4. OBTENER LOS CERTIFICADOS DE LOS USUARIOS DE LA PKI

Es necesario disponer de los certificados de los destinatarios con quienes se requiera establecer comunicaciones seguras, para cifrar los mensajes dirigidos hacia ellos y que puedan revisarlos únicamente empleando su par clave privada respectiva. La manera más sencilla de hacerlo es enviando un mensaje firmado digitalmente para que el destinatario agregue a sus contactos de correo al funcionario emisor, e implícitamente importe su certificado en el repositorio de Windows; la otra forma sería realizando una búsqueda de cualquier certificado en la base de datos de la PKI, descargarlo e instalarlo en el repositorio de certificados de

Windows; obviamente este proceso resulta mucho más complicado, es más factible el primero.

Entonces desde el buzón configurado anteriormente, se enviará un mensaje firmado de prueba (véase Figura 51). El ícono del sobre con un sello rojo marcado indica que este mensaje contendrá una firma digital, y el de candado azul en cambio representa un mensaje cifrado.

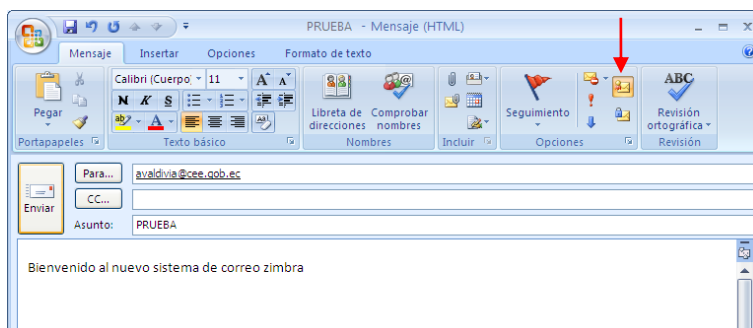


Figura 51. Enviar un mensaje firmado digitalmente

Para generar la firma de este mensaje, de acuerdo a las configuraciones realizadas, es necesario ingresar la contraseña de protección del par clave privada (véase Figura 52).

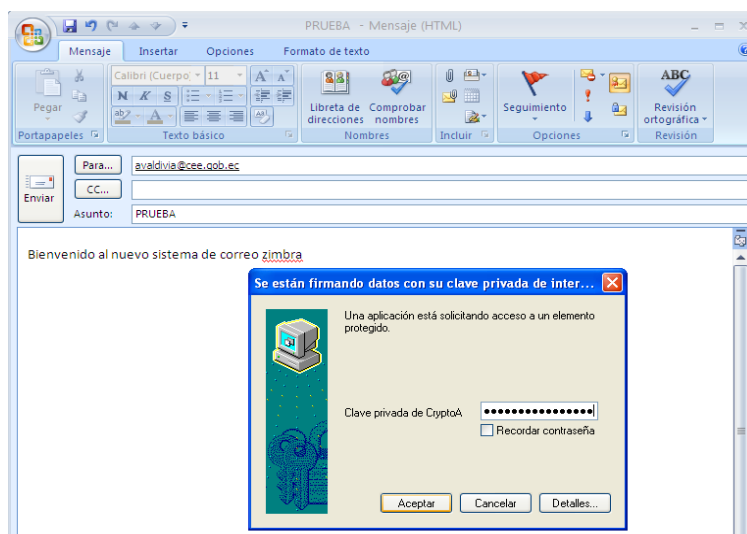


Figura 52. Contraseña de protección de la clave privada - emisor

En el extremo del destinatario se visualiza el contenido del mensaje, y para verificar la firma digital basta con acceder al botón rojo a la derecha de la bandeja de entrada (véase Figura 53).

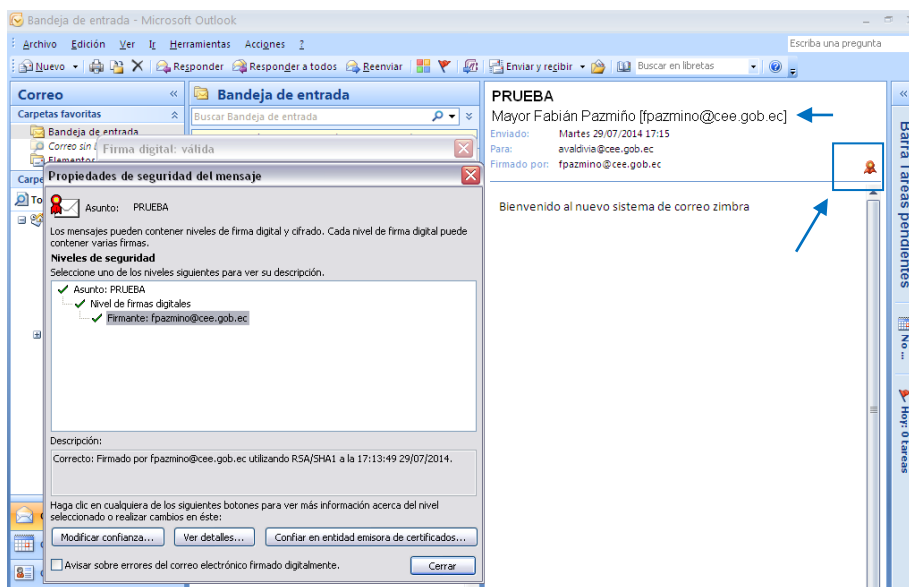


Figura 53. Comprobación de la firma del mensaje

En este caso la firma ha sido validada y se puede considerar que este mensaje no ha sufrido ningún tipo de modificación desde que fue creado, garantizando su integridad, y el no repudio por parte del emisor responsabilizándolo por el contenido del mensaje que ha generado.

Para complementar este proceso sobre el mismo mensaje, clic derecho sobre la dirección de correo electrónico del emisor (Mayor Fabián Pazmiño [fpazmino@cee.gob.ec] – véase Figura 53) y agregarlo a los contactos de Outlook, con ello se almacenará el contacto incorporando su certificado (véase Figura 54).

Al disponer del certificado de este funcionario, es posible enviarle desde este momento mensajes cifrados (véase Figura 55).

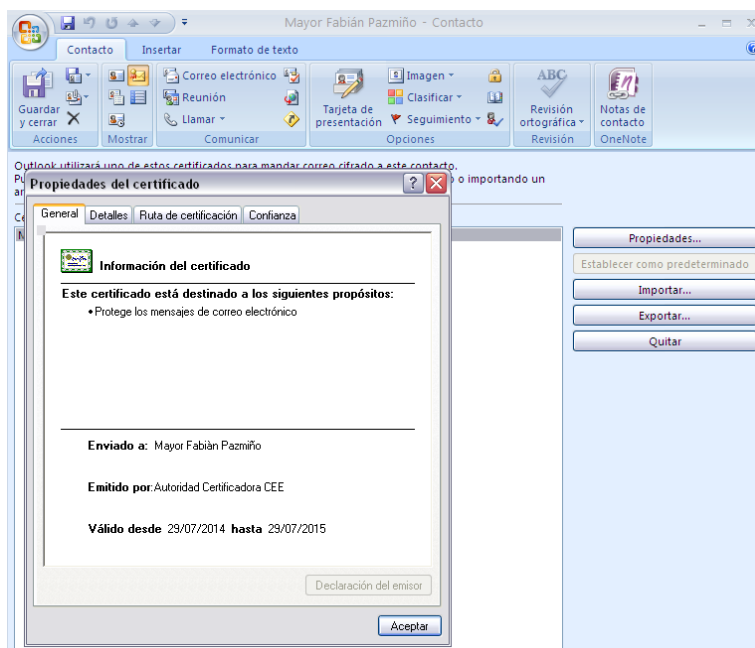


Figura 54. Agregar un contacto incluyendo su certificado

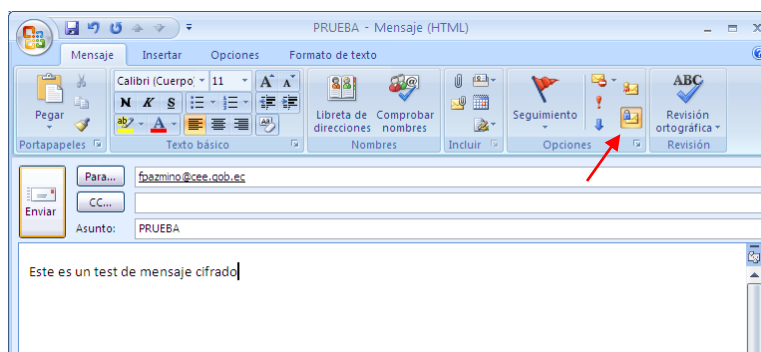


Figura 55. Envío de un mensaje cifrado

En el extremo del destinatario se puede apreciar que no se muestra ningún elemento en el panel de lectura, de manera que si no se ingresa la contraseña que protege el par clave privada, que va a ser empleada para descifrar este mensaje, no se tendrá acceso éste (véase Figura 56).

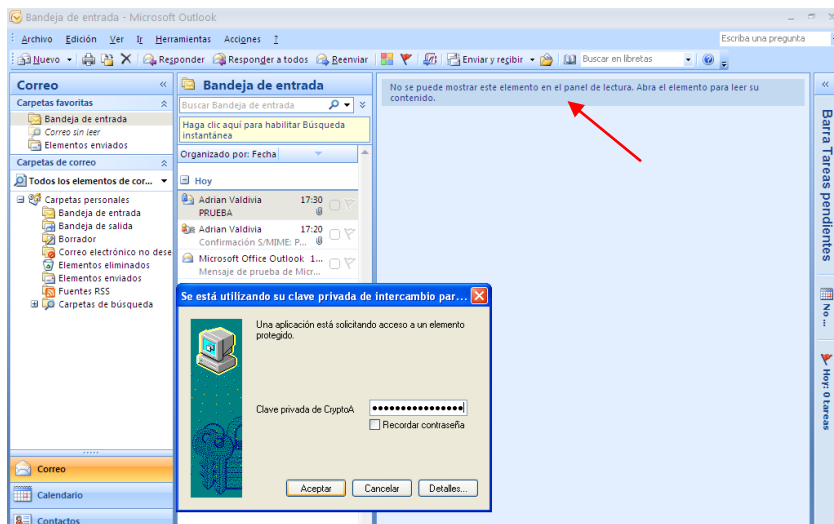


Figura 56. Contraseña para utilizar la clave privada

Al ingresarla se desplegará este panel para visualizar el mensaje, y al presionar sobre el símbolo del candado azul, se verificará el algoritmo de cifrado y hacia quién está dirigido (véase Figura 57).

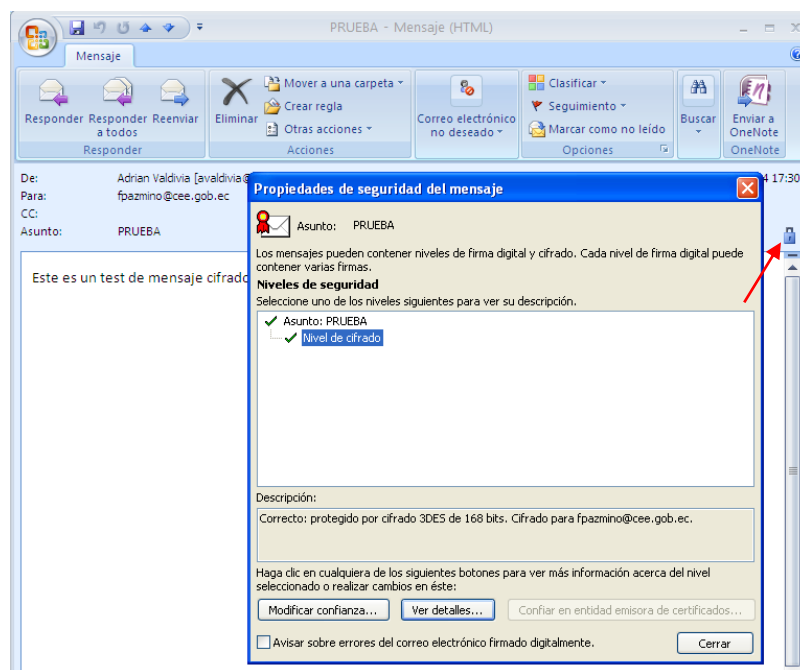


Figura 57. Visualizar el mensaje cifrado

Con esto se garantiza la confidencialidad del mensaje, y la autenticación del destinatario.

En el caso de recibir mensajes cifrados con documentos adjuntos, de igual forma no se muestra ningún elemento en el panel de lectura (véase Figura 58).

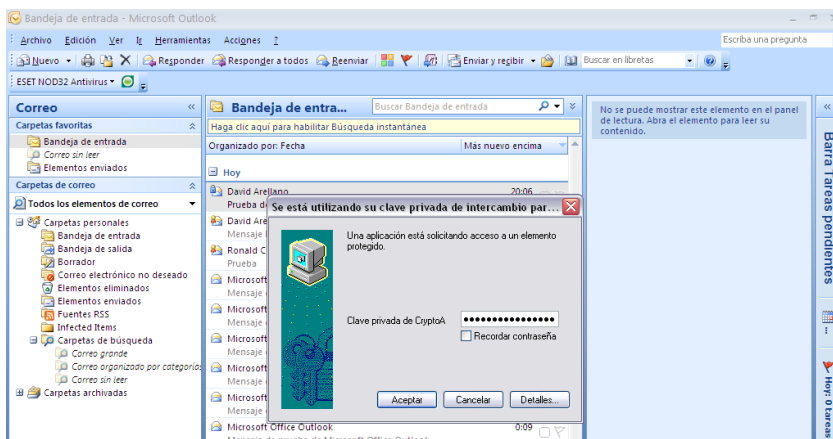


Figura 58. Mensaje cifrado que contiene documentos adjuntos

Sólo al ingresar la contraseña que protege el par clave privada se podrá revisar su contenido (véase Figura 59).

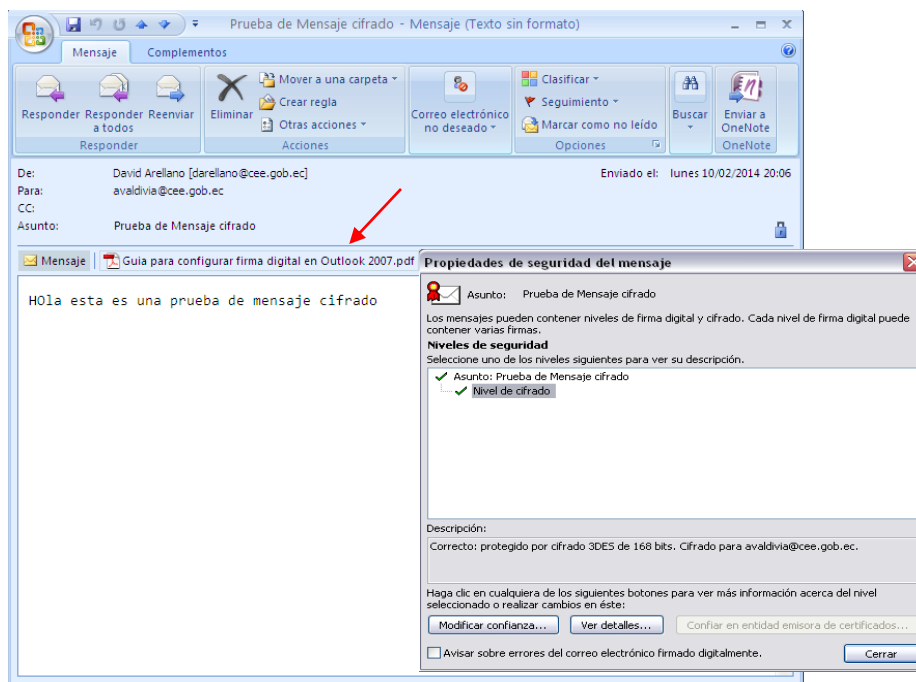


Figura 59. Visualizar un mensaje cifrado con documentos adjuntos

Análogamente al recibir un mensaje que ha sido firmado y cifrado, el proceso es el mismo, pero al visualizarlo se apreciará que existen los dos símbolos, el candado y el botón rojo, al acceder a cada uno se verifica tanto el nivel de firma, como el de cifrado (véase Figura 60).

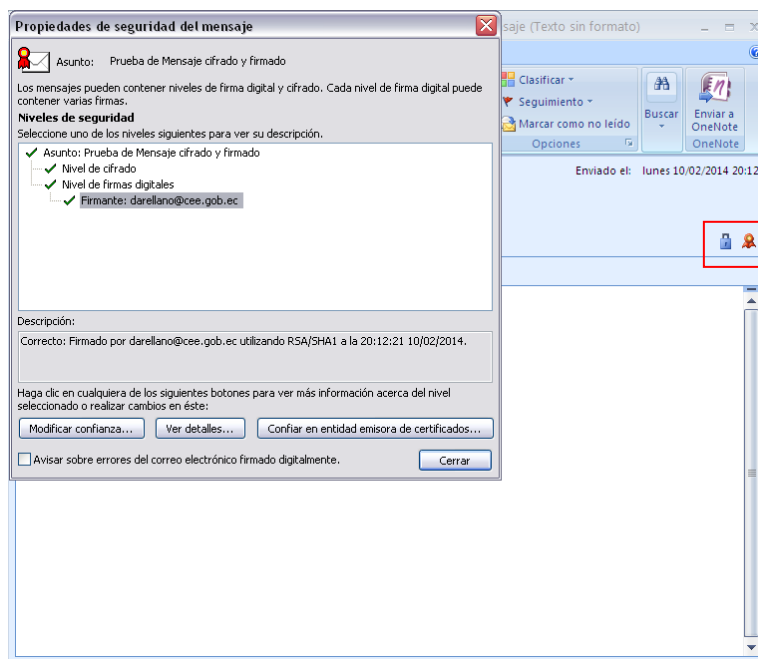


Figura 60. Visualizar un mensaje firmado y cifrado

Si la firma digital es validada se garantiza la integridad del mensaje, y el no repudio del emisor; y si el nivel de cifrado es válido se garantiza la confidencialidad del mensaje, y la autenticación del destinatario, logrando de esta manera implantar cuatro dimensiones de seguridad por cada mensaje transferido sobre esta plataforma de correo institucional.

4.3. ESCENARIOS DE PRUEBA

Se realizará la captura y el análisis de paquetes para intentar vulnerar la confidencialidad de los mensajes transferidos, y la verificación del comportamiento del sistema ante certificados caducados y revocados.

4.3.1. CAPTURA DE PAQUETES Y ANÁLISIS DEL PROTOCOLO SMTP

Este análisis se ha realizado con el propósito de vulnerar los mensajes de correo en proceso de transferencia, e intentar revelar la información que contienen. Esto se ha realizado empleando el analizador de tráfico de uso generalizado (Wireshark), sobre varios tipos de mensajes.

El primero es un mensaje enviado en texto plano (véase Figura 61).

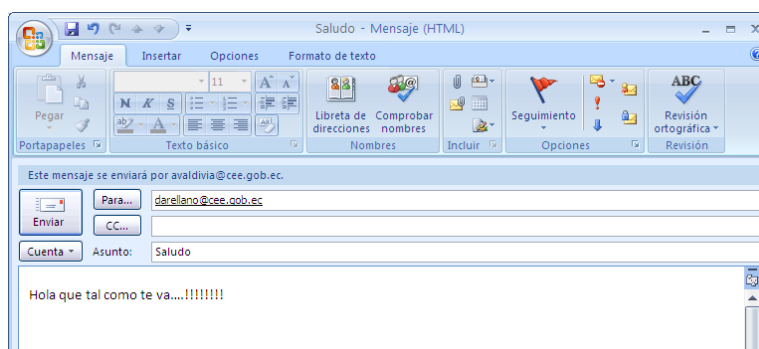


Figura 61. Mensaje sin ningún tipo de protección

En el analizador se aplica un filtro sólo para capturar paquetes del protocolo SMTP que es lo que interesa; cuando inicia la captura sobre cualquier paquete hacer click derecho y elegir la opción `Follow TCP stream`, esto permite visualizar la conversación tal como ocurrió (véase Figura 62).

En esta captura se ha podido revelar las direcciones de correo electrónico tanto del emisor, como del receptor, y además es posible visualizar el mensaje en sí, es decir lo que ha redactado el emisor; por lo que se concluye que este tipo de mensajes convencionales no imponen ningún tipo de oposición ante técnicas que intenten vulnerarlos.

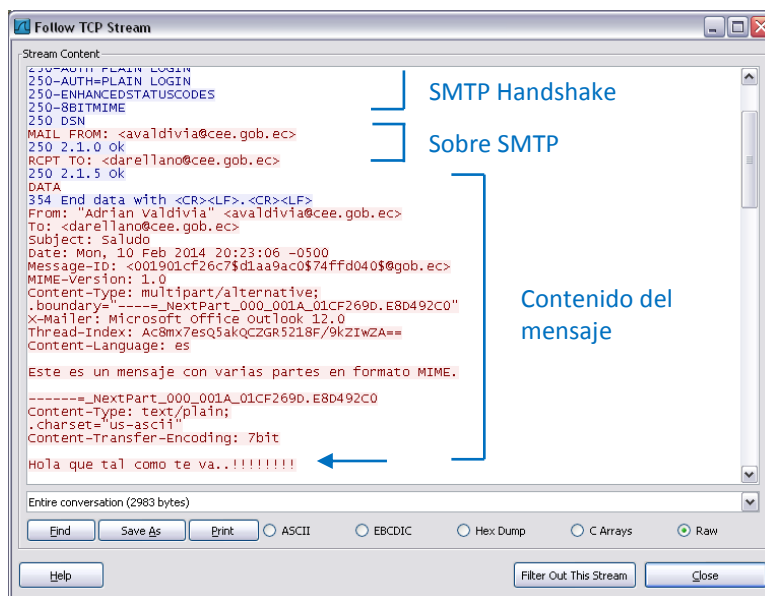


Figura 62. Captura SMTP con Wireshark de un mensaje en texto plano

Se efectuará el mismo procedimiento para vulnerar un mensaje cifrado (véase Figura 63).

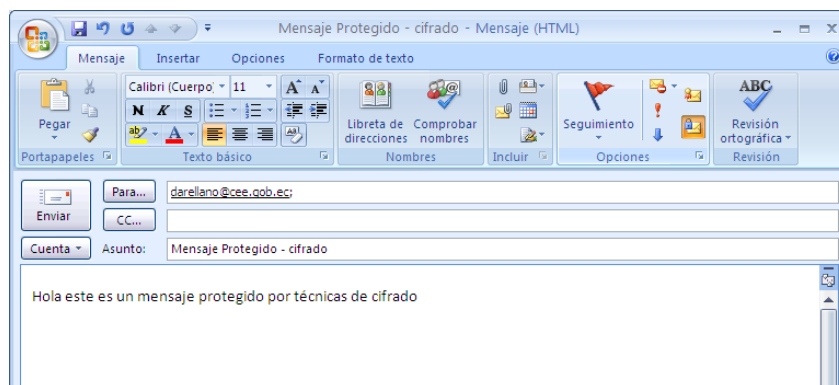


Figura 63. Mensaje Cifrado

La captura de paquetes se muestra en la Figura 64, en la que se puede apreciar que los dos primeros campos estructurales del mensaje (handshake y el sobre) no han variado, pero el cuerpo del mensaje ha sido transformado a un formato ilegible, generando de esta forma mensajes auto-protegidos que pueden ser transferidos convencionalmente por el servidor de correo, como en este caso, y que van a ser almacenados de ésta forma en este servidor.

```

Follow TCP Stream
Stream Content
220 mail.cee.gob.ec ESMTP Postfix
EHLO americanblack
250-mail.cee.gob.ec
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN LOGIN
250-AUTH PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
MAIL FROM: <avaldivia@cee.gob.ec>
250 2.1.0 ok
RCPT TO: <darellano@cee.gob.ec>
250 2.1.5 ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: "Adrian Valdivia" <avaldivia@cee.gob.ec>
To: <darellano@cee.gob.ec>
Subject: Mensaje Protegido - cifrado
Date: Mon, 10 Feb 2014 20:27:33 -0500
Message-ID: <002501c2f6c857079aa105516cfe30@gob.ec>
MIME-Version: 1.0
Content-Type: application/x-pkcs7-mime;
.smime-type=enveloped-data;
.name="smime.p7m"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
.filename="smime.p7m"
X-Mailer: Microsoft office outlook 12.0
Thread-Index: Ac8myHAaVr7ob8hjQv2NtVCYiG24tw==
Content-Language: es

MTAGCSGSIB3DQEH4GCAAMIACAQAQggNYMIIBQAIADCBjzCBGjEkMCIGAIUEAwbbQxV0b3jPzGFK
IEN1cnRpm2llywRvcmEgQOVFMSEWHYDQQLDBHfBnrPzGFKIGR1IEN1cnRpm2llywbb24xk1Ao
T3jWPCeAng/Ceebch+815gnsjR1PRasQMBTqvrYDS7x/11AXV/X89TGIGKzV6CMBDFE9IBjz
e51UrXV+B3Ew917mB5h10r31/IROMY7p8HH8nAHCNNS1AHQmsYzu+dPslu8JmFALVIVPQzBvQup
3mg558hd+kux8Jf6/qe++untWU52LdZkKqC9Jga1owRv3ahgecPPT13fP0CQwAF/+ySu1nkowbsq
jg/4j6R0v21qphvtH+c/wQNoFjxxk0MwIGiTUA3+xHvsakyQF1dQdc7omosxzRntx4BorvssDsP0
1fSdJ/Cwuap+QmU8x8ni9c11f/fJho0AOMFrrtc+98pef1xB4qzFPptg1MLjg5q62IjZ1mxvqjL
JxvHwD2MNN/qLBCD78d1qyB1b7ncFDvEAXRdWk5GVTWY+28j191r483F1xueKPRFcj/KaSIgTYIF
u08FU89evjWwDvT5Hf35ly6PTL1011x8tCOcZGF5Vbs2yCJTFMxUz9NqtqaC2rdq2YlywP9014
a9g3youbp9TmkR5sm5YGM1dQpJkejFZPLkw9lwsxt6QL6eHQ+4CMOKLdkva86spsv5E30ucfQ7k
V5V3jrUn7bQqrErw9UfHrg7+MvQpD0hyPby4FE1+5322S2jvFxeIy9KG6k854NSdhGufBgB25hFA
T/XpUfP09qPvJ4sb11tqzBbcxYY/mcn/H3xwELQ1AmXDSx5EA8I7Grb8E+n1DvTpxJm1F4Bys
LS2FeTxxhNofZAGuUr2UdE11Tfogy7csRBj8CRUXJQMF84woAu1b1eNqmaN0tyk0/5x5Ivs/8ftK
Ssoo021TATyGq3n+Bc04F4odeYph2eook7vv1TeY+gPL9seq1eEPWTGowhq+z7L5+Qx58ULeN2dg
tp59EovE1hlpM/1T7XecLOH/TbwnJIP1hAM+7FzrHH1pYNTv1PZ1gx9P9Mwpqov07q+0UlyImj3
217kFcsXkSb5ayr2WHUFTRodTCovrpaYdocrDvFwY580dIy7uj1Vb8EjAuc92tfb1QyAkzmdC0GZ
520T7V1grQe9P5KQSCA4hmfWogeUjgqFDu0wXtzXFVNF22FUCYxL1h1D/GwkELNIgNSMFW5U
/avCEf32KNbA9xLc1hx14kqpceT5DLHUJtjTVb6u+ct9qnt/Am1NoFAPBiv5er+hk5k7df97n
kMLB6Z/0m5k1UgdmeEn9ZUfCW+432R0UPH3HTByFOzCzr9PAJ1vULsubk5onDDK7044kw0692I
rBdMFAOKKxthvY1Q1NC32ot57Fgvy2ymot1hovSE2X8FMgkmtIBV+EdAxgcecy20kLIT2Aj03FW
3NC1Ax4dKngF52mukwJnR5F18+mn3S9BDixCwM4ouQM6qu/JQMAJjHv1779qtPx0GL2afVf
HN47ju/Zsc9AH/bh5h0wrjMFRW0BLb56WfZyyep5diX0KLCCLC+ggf0jPcuknosBA1y9XE190QMKx
I35YmW/YOpEoknA1tqhgbk3yPwC2900gep7k4/ak63E9uv+FHNond+b6RLzbvkeZg53DHD5U6P5
59ot3oyUT1GFdn1rERA7TyrkZPVADT7Q5dyq//JZ2N9sp8wr1kqAu311tbpqbxQP/QgvvJ6kIbws
K38fK0U1J6B4mYtn10IH2UrFXCYH7wnrR13esPwsGqpw9IXsvtMyG2xVPvbaqcbpP44FV/
NXC+AK8fCkqosCATPGxHIGTITttn2Fvw0r59QDdyqQ5WPLFOELz6y/h5DQ/ehokCAW59CI7p50
wQa2yph011vgn5kvxwq5ILMF22tj/1k101gA8K4mehp50UMFREP/LH1S+1K0/7X/ATMDW30
p3KIQKprdq20x23m10xUwB11FnP+2311A40ut23wD0ydoggCFI6et/UGKgs9y1MA48xmA1iCOOB
31uxd9Ae4T233ecnsmhkox5x64JD94vfwLDEWISPk09p2ocI30D6ggaovpcaFuyvyywMon6RAD
6TBPpy30MD2Vjgk8z+1m5J4SKovvtck5r7ssplXF7sckLvUswR1ve6v/9VnCXgxfq4YYDRwmp0Uv
0wrHyYUkagnnD4weesqt4G7MEaTRWF9/duy13gVjQvdygdque1XAGksxgk6PamkHBF5dvGdxix
hyysFDKf7pWimr1verYSU87//r5xyfKpDvLjN/G1gehwd9XbTFQehwd32JQJ5X+Py+U1wbpgMUG+
eL3MwGrC8ZV2AAAAA=
.
250 2.0.0 ok: queued as 5B99D1624AF
QUIT
221 2.0.0 Bye

```

Entire conversation (9101 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Filter Out This Stream Close

Figura 64. Captura SMTP con Wireshark de un mensaje cifrado

El mecanismo de seguridad complementario que se debe implementar en esta plataforma de correo electrónico seguro, es proteger la transferencia de información con el protocolo TLS; entonces, se generará un mensaje cifrado con S/MIME (véase Figura 65), que será transferido con la protección de éste protocolo habilitada.

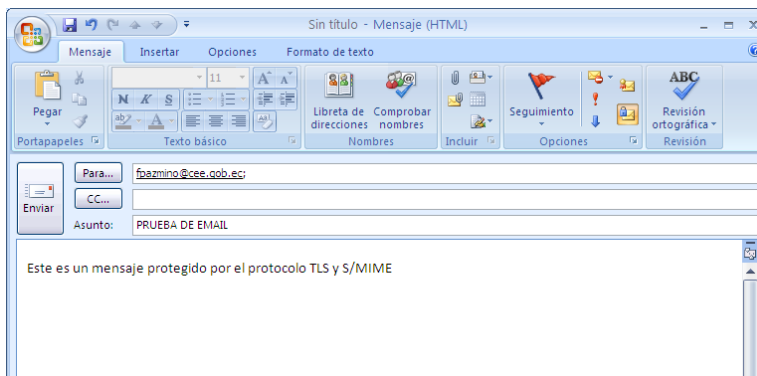


Figura 65. Mensaje cifrado transferido por un canal protegido por TLS

La captura de paquetes de este mensaje se ilustra en la Figura 66.

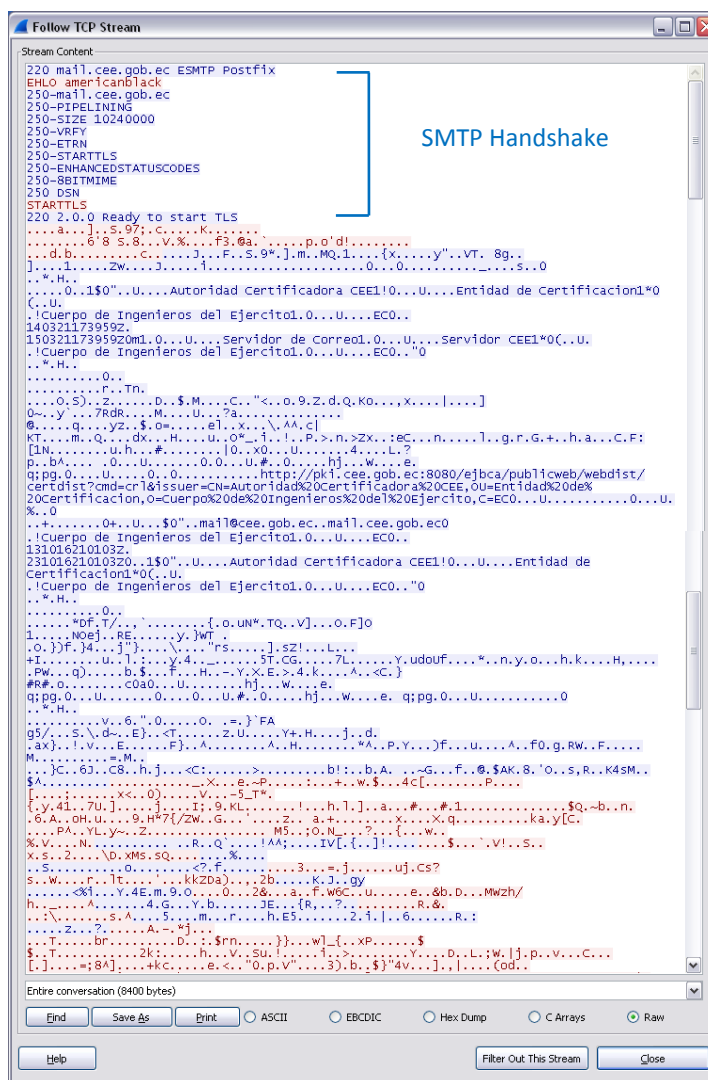


Figura 66. Captura SMTP con Wireshark de un mensaje cifrado - TLS activado

Se puede observar que este mecanismo complementa la seguridad del sistema, ocultando el sobre SMTP que contiene las direcciones de correo origen y destino; esto resulta útil porque en ocasiones a los hackers no les interesa revelar el contenido de mensajes al azar, sino determinar de quién provienen y hacia quién están dirigidos, para ejecutar seguimientos especiales sobre la información que manipula alguien en específico.

Con esto se concluye que las herramientas desarrolladas, y las configuraciones realizadas en este proyecto, cumplen con su propósito principal, la seguridad del correo electrónico institucional.

4.3.2. COMPORTAMIENTO ANTE CERTIFICADOS CADUCADOS

La interacción del agente de correo tanto para generar un mensaje firmado o cifrado, como para recibirlo, es verificar si el certificado digital (empleado, o que va a ser empleado) proviene de una Autoridad Certificadora de confianza, accede a la URL del certificado que contiene la publicación de CRLs emitidas por esta entidad para verificar su validez, y comprueba su fecha de vigencia; si falla alguna de estas pruebas mostrará alertas que lo identificarán como no fiable.

En este caso se ha utilizado un certificado válido para generar un mensaje firmado digitalmente, pero que caducó minutos después de haberlo enviado; lo que ocurre es que en el extremo del destinatario la firma no podrá validarse (véase Figura 67).

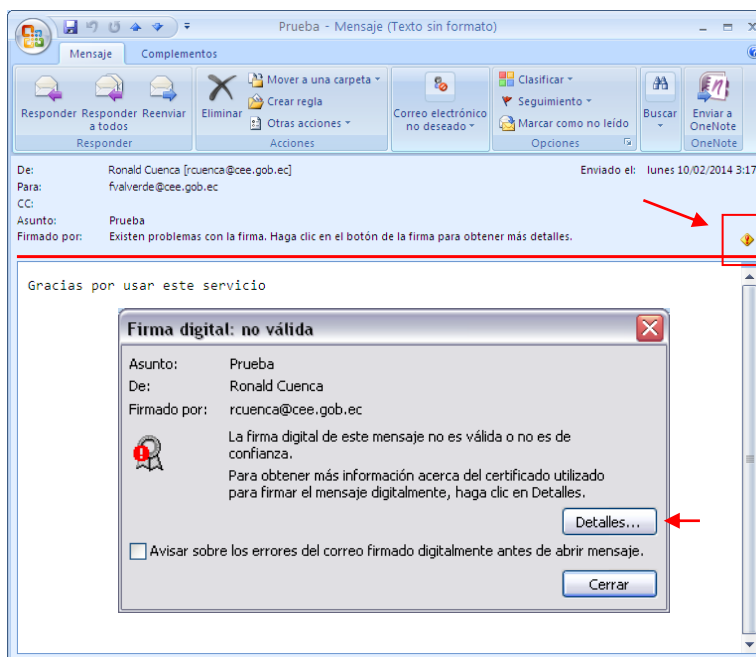


Figura 67. Firma Digital invalidada

Al acceder a Detalles se podrá ver que el error se debe a la vigencia del certificado (véase Figura 68).

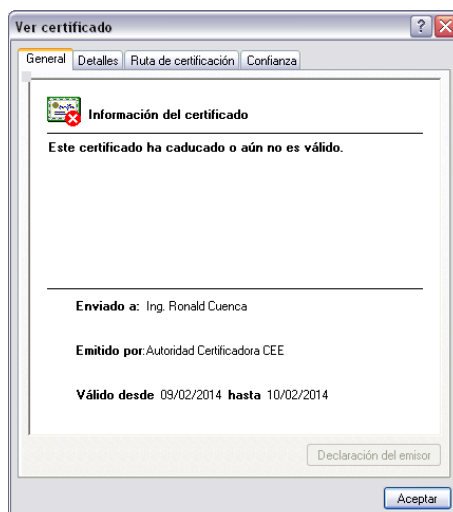


Figura 68. Certificado Digital caducado

Desde este momento este certificado no tendrá validez, pero su titular puede solicitar una renovación a la administración de la PKI del CEE, para mantener la misma clave criptográfica

privada que le permitan firmar nuevos mensajes, y descifrar los anteriores; y ser identificado por un certificado renovado que contenga la clave pública anterior.

4.3.3. COMPORTAMIENTO ANTE CERTIFICADOS REVOCADOS

En este caso lo que se requiere es enviar un mensaje firmado digitalmente utilizando un certificado digital que ha sido revocado, para demostrar el comportamiento del agente cliente de correo (véase Figura 69).

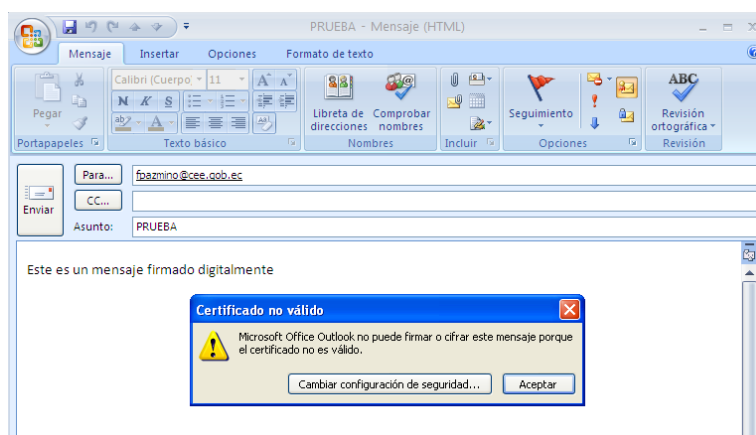


Figura 69. Intentar firmar un mensaje con un certificado revocado

Se obtiene un error que no permite enviar este mensaje, y al acceder a las características del certificado se observa que el problema no es su vigencia, entonces se entenderá que es su validez (véase Figura 70).

Para cerciorarse identificar el número de serie del certificado, descargar la CRL actualizada de la PKI, desde la interfaz web pública de EJBCA, y verificar si éste número de serie consta en la lista de certificados revocados (véase Figura 71); este proceso, transparente

para el usuario, lo realiza Outlook automáticamente cada vez que se requiera verificar la validez de un certificado.

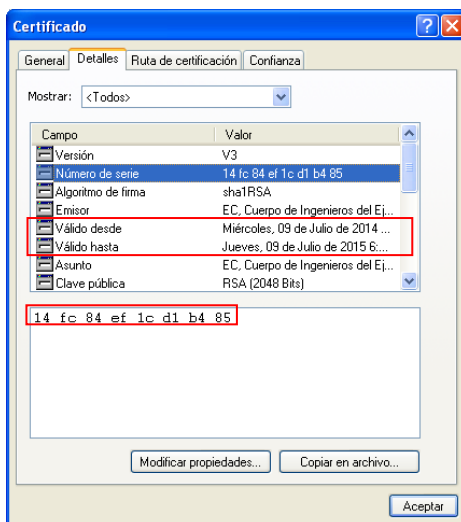


Figura 70. Vigencia y Número de Serie del Certificado

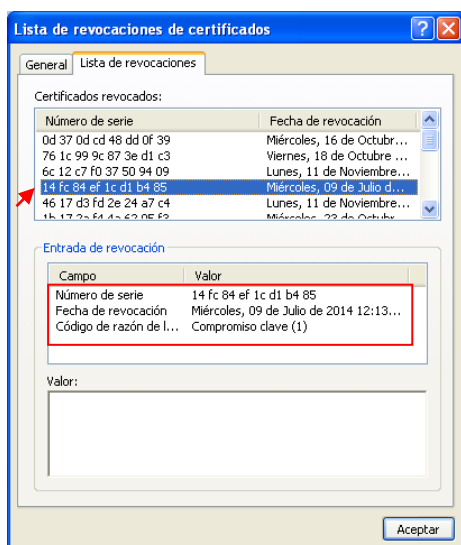


Figura 71. CRL actualizada publicada por la CA

Se puede apreciar que en efecto éste certificado ha sido revocado, y la razón fue el compromiso del par clave privada, por lo que ya no podrá ser utilizado o validado para

securizar los mensajes transferidos por este sistema de correo; cumpliendo de esta forma con la gestión del ciclo de vida de los certificados.

Con estas pruebas de funcionamiento se puede concluir que se dispone de un sistema que no solo emite certificados digitales, sino que permite su gestión controlando las actividades de sus titulares; es decir, que un certificado no sólo deja de ser válido por haber expirado, también pueden existir otras circunstancias que los invaliden contribuyendo para su revocación, como por ejemplo el compromiso o la pérdida de su par clave privada, o la pública almacenada en el certificado, el cese de la afiliación del titular con la entidad certificadora, o la modificación de sus datos.

Por otra parte, se ha logrado integrar éste sistema de seguridad con uno de los servicios informáticos de comunicación más difundidos en la actualidad, el correo electrónico; garantizando la confidencialidad, integridad, autenticación y el no repudio, en cada uno de los mensajes transferidos por este sistema diseñado para el entorno del Cuerpo de Ingenieros del Ejército de Quito, estableciendo de esta forma, una plataforma de correo electrónico seguro.

CAPÍTULO 5. PRESUPUESTO REFERENCIAL

En este capítulo se expone el presupuesto referencial del proyecto, en base a los servidores sugeridos durante la etapa del dimensionamiento de hardware, y su administración, una vez se hayan implementado los servicios de Infraestructura de Clave Pública y el Sistema de Correo Electrónico, en el entorno del Cuerpo de Ingenieros del Ejército de Quito.

5.1. ANÁLISIS DE COSTOS

Se consideran parámetros como los costos generados por motivo del equipamiento, la implementación y la administración de estos servicios, para definir un presupuesto referencial del proyecto desarrollado.

5.1.1. COSTOS DEL EQUIPAMIENTO

Estos costos involucran el análisis, tanto del hardware como del software, necesarios para implantar la Infraestructura de Clave Pública y el Sistema de Correo Electrónico.

5.1.1.1. Análisis del costo referencial de hardware de los servidores

El tipo de servidor recomendado debido a su eficiencia de trabajo, uso generalizado y soporte técnico disponible, es un HP ProLiant modelo ML310e, con características de hardware acordes al dimensionamiento del servidor PKI desarrollado en el Capítulo 3; además, su elección resultará familiar debido a que en esta institución ya se han

implementado anteriormente varios servicios sobre esta gama de servidores; la Tabla 31 expone sus características.

Tabla 31. Características de Hardware del Servidor PKI

HARDWARE	TIPO
Procesador	Intel Xeón E3 – 1220 v3 (3,1 GHz/4 núcleos/8MB/80W)
Memoria Caché	8 MB
Número de Procesadores	1
Memoria RAM	4GB
Tipo de Memoria	UDIMM DDR3
Disco Duro	500 GB
Tipo /Chasis	Micro Torre AX
Adaptador de Red	Adaptador HP Ethernet 1 Gb
Fuente de Alimentación	350W
Garantía	Incluye un año de garantía en piezas, un año de mano de obra y un año de cobertura de soporte técnico a domicilio.

Fuente: Creado a partir de Hewlett Packard. (2014). HP ProLiant ML310e Generation 8 (Gen8) v2. Recuperado de <http://www8.hp.com/h20195/v2/GetDocument.aspx?docname=c04123183>

Si bien es cierto que la institución está en un proceso de migración de servicios hacia el chasis de servidores IBM HS22, para centralizar su infraestructura de red, es importante que el servidor PKI permanezca físicamente aislado del resto de servidores, por cuestiones de seguridad. La razón es por proteger la clave criptográfica privada de la Autoridad Certificadora, por ello se recomienda restringir el acceso físico hacia este servidor, mediante mecanismos de control de acceso.

Respecto al servicio de correo se han realizado los cálculos y apreciaciones necesarias para el dimensionamiento de hardware, pero no se sugerirá ningún tipo de marca o modelo específico de servidor, al conocer que todos los servicios de red serán centralizados en el chasis IBM; de manera que este servicio debe ser virtualizado sobre esta plataforma, tomando como referencia los requerimientos de hardware sugeridos.

5.1.1.2. Análisis del costo referencial del software de los servicios

Este proyecto ha sido desarrollado empleando herramientas de código abierto, como JBoss, EJBCA y MySQL, que son soluciones de software que se las puede implementar libremente, con el propósito de abaratar los costos. En el caso de Zimbra existe la versión Open Source que también es de libre distribución, y la versión Network que es pagada básicamente por el soporte durante la instalación y la administración; de todas formas la versión bajo la cual se ha desarrollado este proyecto es la libre.

5.1.2. COSTOS DE IMPLEMENTACIÓN

Este análisis involucra factores como el presupuesto que la institución destine a la implantación de estos servicios, si deciden incluir o reducir algunas funcionalidades, y la propuesta de empresas que se postulen en el portal de compras públicas para implementarlos.

Además, hay que considerar el costo del mantenimiento de hardware de los servidores, que es un valor impuesto netamente por las empresas proveedoras, de acuerdo a la regularidad con que se los realice, normalmente una vez por año, y las garantías que puedan incluirse.

Referente al software, el diseño de estos servicios garantiza un tiempo de operatividad de 10 años, tomando como referencia la vida útil del hardware de un servidor, y las actualizaciones de las herramientas open source empleadas; con este parámetro se ha emitido tanto el certificado digital de la Autoridad Certificadora Raíz del CEE, como del Sistema de Correo Electrónico Zimbra, obviamente con la posibilidad de renovarlos si se requiere una vez cumplida esta etapa.

5.1.3. COSTOS DE ADMINISTRACIÓN

Este parámetro puede ser apreciado únicamente si los servicios se han implementado empleando las herramientas de software con las que se ha desarrollado este proyecto, brindando la capacitación adecuada al administrador de red de esta institución, y al personal que ellos consideren pertinente; de manera, que se designe una persona en esta entidad que desempeñe las labores de administración de estos servicios, generándose un costo aproximado de 900 USD mensuales, que es el salario promedio de un profesional.

El costo de la capacitación es de 500 USD, y si se requiere soporte adicional que amerite el traslado hacia las instalaciones de la entidad el costo sería evaluado por 20 USD cada hora.

5.1.4. PRESUPUESTO REFERENCIAL DEL PROYECTO

Definidos estos parámetros del análisis de costos, el presupuesto del proyecto se detalla en la Tabla 32.

Tabla 32. Presupuesto Referencial del Proyecto

PARÁMETROS	COSTO REFERENCIAL (USD)
Costo del Hardware	2.092 (referencial)
Costo del Software	0
Costo Implementación	No se ha definido
Costo de Capacitación	500 (sin incluir soporte adicional)
TOTAL	2.592

CAPÍTULO 6

CONCLUSIONES Y RECOMENDACIONES

6.1.CONCLUSIONES

- La transferencia fiable de mensajes de correo electrónico es garantizada mediante la implementación de mecanismos criptográficos que los protegen usualmente mientras están en tránsito a través de las redes, en base al protocolo TLS; pero la alternativa más efectiva que además los protege durante su almacenamiento en los buzones avalando una comunicación segura extremo a extremo, son las extensiones S/MIME, que operan en capa aplicación para generar mensajes auto-protegidos, y permiten implementar el mecanismo de firma digital.

- Previo a comprender el propósito de implementar una Infraestructura de Clave Pública PKI, es necesario conocer qué son y cómo se aplican las técnicas criptográficas de cifrado y firma digital sobre un documento electrónico que se requiera proteger; en este caso un certificado digital X.509, emitido por una entidad imparcial autorizada, que lo vinculan legítimamente con la identidad de su titular mientras se efectúe cualquier transacción o trámite electrónico ante determinadas aplicaciones telemáticas.

- Las técnicas de seguridad que permiten implantar una plataforma de correo electrónico seguro, son las extensiones S/MIME, cuyo propósito es proteger la mensajería empleando técnicas criptográficas, como el cifrado y la firma digital, que se basan en la aplicación de certificados digitales X.509 para avalar la autenticidad de sus titulares.

- Este proyecto va a ser de gran utilidad en el entorno del Cuerpo de Ingenieros del Ejército, considerando que complementará la seguridad otorgada por los mecanismos existentes, al estar destinado a salvaguardar la información transferida por el correo electrónico institucional, que por cuestiones laborales representa al activo de mayor importancia con el que cuenta esta entidad.
- Durante el diseño de la Infraestructura de Clave Pública es trascendental definir una ubicación estratégica para la CA Raíz, aislándola de la granja de servidores del CEE, para preservar la operatividad del sistema de certificación; el objetivo es restringir el acceso hacia este servidor, tratando en lo posible de proteger su clave criptográfica privada.
- La Jerarquía de Certificación configurada para el Cuerpo de Ingenieros del Ejército, está basada en una arquitectura plana, siendo la CA Raíz quien certifica directamente a usuarios finales, con la posibilidad de complementarla con CAs subordinadas o intermedias, para ampliar eficientemente el servicio de certificación, hacia los grupos de trabajo remotos de esta institución.
- EJBCA emite certificados digitales en base a plantillas de certificado y entidad final, que se complementan para definir qué tipo de información contendrá el certificado, en este proyecto se los ha configurado para que la mayoría de campos coincidan, entendiéndose que los usuarios pertenecen a la misma entidad, algunos campos que difieren son el nombre, el departamento en el que labora, su dirección de correo electrónico, y algunos datos de carácter personal.

- La interfaz de administración de EJBCA provee funcionalidades de seguridad en base al número de serie de los certificados, para restringir el acceso de usuarios que intenten vulnerarla empleando un certificado digital fraudulento; esto significa que únicamente los administradores tendrán autorizado el acceso a los diversos recursos de la PKI, tras autenticarse con el certificado autorizado.

- La Infraestructura de Clave Pública diseñada cumplió con los propósitos de emisión y gestión de certificados digitales X.509 efectuados durante la etapa de pruebas de funcionamiento, resaltando la compatibilidad que se logró con los agentes de usuario de correo MUA, para cifrar y firmar digitalmente los mensajes transferidos por este medio.

- Con este trabajo de investigación se ha demostrado que es posible integrar un mecanismo de seguridad basado en certificados digitales personales, sobre una de las plataformas de comunicación más generalizadas en la actualidad, el correo electrónico, para proteger el flujo de información que circula a través de este medio.

- Se pudo comprobar que en realidad los mensajes fueron protegidos durante todo el proceso de su transferencia, siendo únicamente los destinatarios legítimos quienes pudieron revertir los mensajes cifrados, verificar la integridad de la firma digital y la autenticidad del emisor.

6.2.RECOMENDACIONES

- Considerando la situación actual referente a los mecanismos de seguridad implantados en la red de datos del CEE de Quito, se deberán establecer políticas de seguridad que definan los procedimientos apropiados de los usuarios en este entorno para evitar que se generen vulnerabilidades sobre cualquier sistema de la red, en especial respecto al uso adecuado de los certificados digitales, debido a que de ello depende su eficiencia.
- Es indispensable instalar el servidor de certificación en un entorno aislado de las instalaciones del Cuerpo de Ingenieros del Ejército, que disponga de algún mecanismo de control de acceso, con el interés de proteger la CA Raíz de la PKI, puntualmente de preservar la confidencialidad de su clave privada, debido a que si alguien logra revelarla podría apropiarse de su identidad invalidando desde este momento la legitimidad del sistema.
- Este proyecto de investigación establece el fundamento de una solución de seguridad basada en mecanismos criptográficos, que de ser implementada se recomienda personalizar los puertos de acceso hacia las interfaces web pública y privada de EJBCA, y habilitarlos en el firewall de la institución; esto implica adicionalmente la recomendación de utilizar preferentemente la interfaz web pública segura HTTPS por cuestiones de seguridad.
- Es de suma importancia concientizar y capacitar al personal que labora en esta institución, para que utilicen este sistema de manera adecuada y responsable,

considerando que ellos forman parte activa de la Infraestructura de Clave Pública y el Sistema de Correo Electrónico Seguro.

- El servidor que se ha dimensionado y presupuestado para implementar la PKI, deberá destinarse para alojar únicamente a este servicio, de ningún modo se debe pensar en virtualizar sobre éste cualquier otro servicio adicional de red, para que opere en conjunto, esto podría generar vulnerabilidades que degraden al servicio, o poner en riesgo su operatividad.

REFERENCIAS BIBLIOGRÁFICAS

LIBROS, RECURSOS BIBLIOGRÁFICOS EN LÍNEA Y TESIS

Alfárez, J.A. (s.f.). *Instalación, Configuración y Administración del Servidor de Aplicaciones JBoss*.

Recuperado de <http://www.alferez.es/documentos/Jboss.pdf>

Ayesha, I. G. & Asra, P. (2006). *PKI Administration using EJBCA and OpenCA*. Recuperado de

http://teal.gmu.edu/courses/ECE646/project/reports_2006/IL-3-report.pdf

Barrantes, H. (2009). *Instalar y Configurar un Servidor DNS en Ubuntu Linux*. Recuperado de

<http://www.codigofantasma.com/blog/instalar-y-configurar-servidor-dns-en-ubuntu-linux/>.

Bobadilla, J. (s.f.). *Aplicaciones Web en Servidor: Servlets*. Recuperado de

<http://138.100.152.2/~jbobi/jbobi/Libro2Java/42Apuntes.pdf>

Cedeño, S. A. & Robalino, J. A. (2008). *Rediseño de la Infraestructura del proveedor de servicios de Internet ONNET S.A para la optimización del servicio en el Distrito Metropolitano de Quito*.

Proyecto de Titulación, Escuela Politécnica Nacional, Quito, Ecuador.

Cuesta, J., & Puñales, M. (2002). *Seguridad en Redes Telemáticas-Infraestructura de Clave Pública (PKI)*. Recuperado de <http://es.scribd.com/doc/116154580/Infraestructura-de-clave-publica-PKI>

Comunicación de Datos II. (2005). *Tema 4: Firmas Digitales*. Recuperado de

http://personales.upv.es/~fjmartin/cdii_web/traspas/Firmas_sin_fondo_2x.pdf

Educoas. (s.f.). *Capítulo 4: Correo Electrónico*. Recuperado de

<http://www.educoas.org/portal/bdigital/contenido/valzacchi/ValzacchiCapitulo-4New.pdf>

EJBCA PKI BY PRIME KEY. (2013). *PrimeKey Support, Development and Maintenance Services – EJBCA Installation*. Recuperado de <http://www.ejbca.org/installation.html>.

Escuela de Sistemas Informáticos. (2004). *Tecnologías de la Comunicación en Internet*. Recuperado de http://www.falconmarbella.com/esigranada/dmdocuments/Punto_235_Correo_electronico.pdf

Escuela Politécnica Nacional. (s.f.). *Fundamentos de Seguridad de la Información y de Redes Inalámbricas*. Recuperado de <http://dspace.epn.edu.ec/bitstream/15000/8917/5/10762CAP1.pdf>

Fernández, A. (2007). *Seguridad en Redes – Intercambio de Claves DIFFIE-HELLMAN*. Recuperado de <http://fernandezg.wordpress.com/2007/08/11/intercambio-de-claves-de-diffie-hellman/>

González, M. & González, V. (s.f.). *El Algoritmo Diffie-Hellman: Introducción*. Recuperado de <http://serdis.dis.ulpgc.es/~ii-cript/PAGINA%20WEB%20CLASICA/CRIPTPGRAFIA%20MODERNA/ALGORITMO%20DE%20DEFFI-HELLMAN.html>

Gonzales, R. (2005). *Infraestructura de Clave Pública PKI con Software Libre*. Recuperado de http://www.criptored.upm.es/guiateoria/gt_m115a.htm

Hewlett-Packard. (2014). *HP ProLiant ML310e Generation 8*. Recuperado de <http://www8.hp.com/h20195/v2/GetDocument.aspx?docname=c04123183>

INDRA Sistemas, S.A. (2005). *Infraestructura de Clave Pública (PKI)*. Recuperado de http://www.inteco.es/extfrontinteco/es/pdf/Formacion_PKI.pdf

Internet Engineering Task Force, (1999). *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*. Recuperado de <http://tools.ietf.org/html/rfc2560>

Internet Engineering Task Force, (2000). *Internet Security Glossary*. Recuperado de <https://www.ietf.org/rfc/rfc2828.txt>

Internet Engineering Task Force, (2001). *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*. Recuperado de <http://www.ietf.org/rfc/rfc3161.txt>

- Jara, F. A. (2012). *Sistema Selectivo de Correos Electrónicos Orientado a Dispositivos Móviles NMM: No More Mails (Tesis de Pregrado)*. Universidad Austral de Chile, Valdivia, Chile.
- Lucena, M. J. (2009). *Criptografía y Seguridad en Computadores*. Recuperado de <http://es.scribd.com/doc/39400098/Criptografia>
- Lara, E. (s.f.). *10º Unidad Didáctica: Correo Electrónico*. Recuperado de <http://personals.ac.upc.edu/elara/documentacion/INTERNET%20-%20UD10%20-%20Correo%20Electronico.pdf>
- Lopez, M. R. (2011). *Las Variables de Entorno en Ubuntu*. Recuperado de <http://marcosrobertos.blogspot.com/2011/09/las-variables-path-y-classpath.html>
- Lopez, J. C. (2014). *Recomendaciones para crear contraseñas robustas*. Recuperado de <http://www.eduteka.org/ContrasenasRobustas.php>
- Llorente, L. (s.f.). *Instalación y Configuración del Servidor DNS Bind*. Recuperado de http://www.sergio-gonzalez.com/personales/ingenieria_informatica/sistemas_informaticos/documentacion/bind/bind.pdf
- MAJIC.RS. (2011). *Revision of Setting-up EJBCA as Certification Authority*. Recuperado de <http://majic.rs/node/50/revisions/52/view>.
- Microsoft – Support. (2006). *Introducción a Lightweight Directory Access Protocol (LDAP)*. Recuperado de <http://support.microsoft.com/kb/196455/es>.
- Microsoft – Support. (2014). *Sugerencias para crear una contraseña segura*. Recuperado de <http://support.microsoft.com/kb/196455/es> <http://windows.microsoft.com/es-419/windows-vista/tips-for-creating-a-strong-password>.
- Ministerio de Ciencia y Tecnología. (2008). *Dirección de Certificadores de Firma Digital. Política de Sellado de tiempo del Sistema Nacional de Certificación Digital*. Recuperado de <http://www.firmadigital.go.cr/Documentos/PoliticadeSelladodetiempover100.pdf>

Nando, A. (2010). *Seguridad en Sistemas de Información*. Recuperado de <http://www.slideshare.net/nyzapersa/curso-seguridad-en-sistemas-de-informacion>

Osorio, J. M. (s.f.). *Evaluación de la Herramienta EJBCA para un prestador de Servicios de Certificación*. (Proyecto Final de Carrera). Universidad Politécnica de Cataluña, Barcelona, España.

Perramon, X. (s.f.). *Aplicaciones Seguras*. Recuperado de http://ocw.uoc.edu/computer-science-technology-and-multimedia/advanced-aspects-of-network-security/advanced-aspects-of-network-security/P06_M2107_01772.pdf

Plaza, D. (s.f.). *Soluciones PKI basadas en Cryptlib*. (Trabajo de fin de Carrera). Universidad Politécnica de Madrid, Madrid, España.

Quer System Informática. (s.f.). *Comparativa de Soluciones Open Source Groupware (Zimbra, Open-Xchange, Scalix)*. Recuperado de [http://www.versystem.com/docs/Comparativa%20soluciones%20Groupware%20\(Zimbra,%20Open-Xchange,%20Scalix\).pdf](http://www.versystem.com/docs/Comparativa%20soluciones%20Groupware%20(Zimbra,%20Open-Xchange,%20Scalix).pdf)

Ramió, J. (2006). *Funciones Hash en Criptografía (Tema 6)*. Recuperado de http://criptosec.unizar.es/doc/tema_c7_criptosec.pdf

Red Hat Enterprise Linux. (s.f.). *Seguridad de las Estaciones de Trabajo (Capítulo 4)*. Recuperado de <http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-wstation-pass.html>

Red Hat Enterprise Linux. (s.f.). *Operating System Requirements*. Recuperado de http://www.centos.org/docs/5/html/CDS/install/8.0/Installation_Guide-Support-Platforms.html

Salazar, J. E. (s.f.). *Desarrollo de una guía práctica para la implantación y manejo de la Infraestructura de Clave Pública (PKI) en la WEB*. Recuperado de <http://ftp.puce.edu.ec/handle/22000/1368>

Salvador, L. (s.f.). *Herramientas de Validación de Certificados en PKI con tarjeta inteligente*. (Tesis de Pregrado). Universidad Carlos III de Madrid, Madrid, España.

SENATEL. (s.f.). *Firma Electrónica – Regulación Vigente*. Recuperado de <http://www.regulaciontelecomunicaciones.gob.ec/firma-electronica-regulacion-vigente/>

Stallings, W. (2006). *Cryptography and Network Security Principles and Practice*. Recuperado de [http://evilzone.org/ebooks/cryptography-and-network-security-principles-\(5th-edition\)/](http://evilzone.org/ebooks/cryptography-and-network-security-principles-(5th-edition)/)

Talens-Oliag, S. (s.f.). *Introducción a los certificados digitales*. Recuperado de http://www.uv.es/~sto/articulos/BEI-2003-11/certificados_digitales.pdf

Tutorials Point. (s.f.). *Enterprise Java Bean (EJB) Tutorial*. Recuperado de http://www.tutorialspoint.com/ejb/ejb_tutorial.pdf

Ubuntu Guia. (s.f.). *Instalar Oracle Java 7 en Ubuntu 12.04*. Recuperado de <http://www.ubuntu-guia.com/2012/04/instalar-oracle-java-7-en-ubuntu-1204.html>

UIT-T. (2003). *La Seguridad de las Telecomunicaciones y las Tecnologías de la Información*. Recuperado de <http://www.itu.int/itudoc/itu-t/85097-es.pdf>

UIT-T. (2008). *Information Technology – Open Systems Interconnection – The Directory: Public-Key and attribute certificate frameworks*. Recuperado de <http://www.itu.int/rec/T-REC-X.509-200811-l/es>

Valzacchi. (s.f.). *Capítulo 4: Correo Electrónico*. Recuperado de <http://www.educoas.org/portal/bdigital/contenido/valzacchi/ValzacchiCapitulo-4New.pdf>

Veiga, M. (2008). *Redes y Servicios Telemáticos - Aplicaciones*. Recuperado de <http://www-gris.det.uvigo.es/wiki/pub/Main/PaginaRst/Tema3.pdf>

VMware Zimbra Collaboration Server. (2011). *System Requirements for Zimbra Collaboration Server*. Recuperado de http://www.zimbra.com/docs/ne/latest/single_server_install/wwhelp/wwhimpl/common/html/wwhelp.htm#context=NE_QuickStart_7_1&file=System%20Requirements.html

Wol, A. (s.f.). *Telemática*. Recuperado de <http://es.scribd.com/doc/49816497/Telematica>

Zimbra Guide. (s.f.). Managing Classes of Service. Recuperado de http://zimbra.imladris.sk/download/src/HELIX-711/ZimbraWebClient/WebRoot/help/en_US/admin/html/cos/class_of_service.htm

Zimbra Guide. (s.f.). Account Advanced Features. Recuperado de http://zimbra.imladris.sk/download/src/HELIX-711/ZimbraWebClient/WebRoot/help/en_US/admin/html/managing_accounts/account_advanced_features.htm

ANEXO A

GENERACIÓN DE CONTRASEÑAS ROBUSTAS

En este anexo se presentan varias recomendaciones que los funcionarios del CEE deben acatar, para el establecimiento de contraseñas robustas. Estas recomendaciones han sido definidas en base a sugerencias provenientes de corporaciones como Microsoft o Red Hat Enterprise Linux, adaptándolas al entorno de esta entidad y este proyecto.

1. CONSIDERACIONES PARA LA CREACIÓN DE CONTRASEÑAS

Las contraseñas son el mecanismo de seguridad de uso más habitual en sistemas informáticos, debido fundamentalmente a su simplicidad de funcionamiento; por ello representan la principal barrera de defensa ante accesos no autorizados hacia ordenadores o sistemas en la red, de manera que mientras más robustas sean, más los protegerán.

Todos los funcionarios, militares y autoridades que formen parte activa del Cuerpo de Ingenieros del Ejército de Quito, deben crear una contraseña robusta acatando las pautas y recomendaciones que se describen en este apartado del proyecto.

Estas contraseñas serán empleadas inicialmente en el registro y autenticación ante la entidad certificadora del CEE, para generar la solicitud de certificación, posteriormente serán empleadas también para proteger la clave privada en los ordenadores de usuario final al instalar su certificado; por ello se genera la necesidad establecer una contraseña robusta.

1.1. Caracteres

El primer requerimiento para que una contraseña sea aprobada por la Administración de la PKI del CEE, es estar conformada por las cuatro categorías de caracteres expuestas en la Tabla A1.

Tabla A1. Caracteres que integran una contraseña robusta

Categoría	Ejemplo
Letras Mayúsculas	A, B, C
Letras Minúsculas	a, b, c
Números	0, 1, 2, 3, 5, 6, 7, 8, 9
Símbolos del teclado (todos los caracteres del teclado que no se definen como letras o números) y espacios	`~!@#\$%^&*()_ - + = { } [] \ : ; " ' < > , . ? /

Fuente: Microsoft. (2014). Sugerencias para crear una contraseña segura. Recuperado de <http://windows.microsoft.com/es-419/windows-vista/tips-for-creating-a-strong-password>

1.2. Tamaño

No existe una norma estandarizada que defina el tamaño que debe tener una contraseña para que sea robusta, aunque es obvio que la complejidad para revelarla aumentará de acuerdo a la cantidad de caracteres por los que esté compuesta.

Pozadzides (citado por López, 2011) ha elaborado una tabla en la que se estima el tiempo que emplea un ordenador moderno en ejecutar los procesos y combinaciones de caracteres necesarios para revelar una contraseña, dependiendo de la cantidad y el tipo de caracteres que la integran (véase Tabla A2).

Tabla A2. Tiempo que emplea un ordenador en revelar una contraseña

Tamaño (caracteres)	Mayúsculas Minúsculas y Números	Sólo minúsculas
3	0,86 segundos	0,02 segundos
4	1,36 segundos	0,046 segundos
5	2,15 horas	11,9 segundos
6	8,51 días	5,15 minutos
7	2,21 años	2,23 horas
8	2,10 siglos	2,42 días
9	20 milenios	2,07 meses
10	1,899 milenios	4,48 años

Fuente: Adaptado de Pozadzidez. (Citado por López, 2011).
Recomendaciones para crear contraseñas robustas. Recuperado de [http://www.eduteka.org/Contrasenhas Robustas.php](http://www.eduteka.org/ContrasenhasRobustas.php)

La Autoridad Certificadora del CEE ha sido diseñada para soportar el manejo de contraseñas que contengan largas cadenas de caracteres, de hecho pueden contener más de 7; por lo tanto, el segundo y último requerimiento es que las contraseñas que definan los funcionarios, militares y autoridades del CEE como estándar deben contener 15 caracteres.

2. SUGERENCIAS

- La intención es que los usuarios de esta entidad generen sus propias contraseñas para que les resulte mucho más fácil memorizarlas, y no exista la necesidad de que las apunten para recordarlas.
- Utilice acrónimos para crear una contraseña que sea fácil de recordar. Por ejemplo, piense en una frase que le suene familiar, le recuerde algo, o sea célebre, como Me gradué en Ibarra el 8 de Junio del año 2005, y cree un acrónimo como MgeIe8dJunda005.

- Para cumplir con las consideraciones de contraseña robusta establecidas, reemplazar algunas letras del acrónimo por símbolos y números, como Mg3I38%Jun%@005.
- No utilice patrones del teclado para crear la contraseña, como una V por ejemplo, iniciando por el tres (3eDCFt6), o una W (3eDCFt6yHNJi9); esto de cierta forma es una ventaja por el hecho de que no sería necesario memorizarla, pero a la larga resultará siendo demasiado vulnerable.
- No incluya información de carácter personal en las contraseñas, como su nombre, el de la organización, un miembro de su familia, su dirección domiciliaria, mascota, fecha de nacimiento, o cualquiera de este tipo; es mejor pensar en algo mucho más aleatorio como el título o frases de un libro, canción, película, o alguna serie de preferencia.
- Por ningún motivo utilice palabras completas, éstas pueden resultar reconocibles, aunque estén escritas en otro idioma, o se invierta su orden.
- Por último, no emplee ninguna de las contraseñas que han sido tomadas como ejemplo.

ANEXO B

AC Y AR LEGALIZADOS EN ECUADOR



Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y Terceros Vinculados a cargo de la Dirección General de Gestión de los Servicios de Telecomunicaciones de la Secretaría Nacional de Telecomunicaciones, SENATEL

ENTIDADES DE CERTIFICACIÓN DE INFORMACIÓN Y SERVICIOS RELACIONADOS (AUTORIDADES DE CERTIFICACIÓN AC o CA) ACREDITADAS POR EL CONSEJO NACIONAL DE TELECOMUNICACIONES, CONATEL (ENTIDAD ACREDITADORA):

#	Entidades de Certificación de Información y Servicios Relacionados Acreditadas	Web	Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y Terceros Vinculados
1	Banco Central del Ecuador	http://www.eci.bce.ec/	Resolución 481-20-CONATEL-2008 (08/OCT/2008) SECCIÓN 1, TOMO 1 a FOJAS 1 OF-DGGST-2008-1006 (06-NOV-2008)
2	ANF Autoridad de Certificación Ecuador S.A.	https://www.anf.es/ec/	Resolución 639-21-CONATEL-2010 (22/OCT/2010) SECCIÓN 1, TOMO 2 a FOJAS 1 OF-DGGST-2010-1794 (21-DIC-2010)
3	SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A.	https://www.securitydata.net.ec/	Resolución 640-21-CONATEL-2010 (22/OCT/2010) SECCIÓN 1, TOMO 3 a FOJAS 1 OF-DGGST-2010-1802 (23-DIC-2010)

TERCEROS VINCULADOS (AUTORIDADES DE REGISTRO AR o RA) CON LAS ENTIDADES DE CERTIFICACIÓN DE INFORMACIÓN Y SERVICIOS RELACIONADOS ACREDITADAS (AC o CA):

#	Terceros vinculados con Security Data	Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados
---	---------------------------------------	---



	S.A.	Acreditadas y Terceros Vinculados
1	Cámara de Comercio de Guayaquil	SECCIÓN 2, TOMO 1 a FOJAS 1 OF-DGGST-2011-0799 (03-06-2011)
2	Kruger Corporation S.A.	SECCIÓN 2, TOMO 2 a FOJAS 1 OF-DGGST-2011-1169 (10-08-2011)
3	Telconet S.A.	SECCIÓN 2, TOMO 4 a FOJAS 1 OF-DGGST-2012-0329 (10-03-2012)
4	Optimsoft Software & Hardware CIA. LTDA.	SECCIÓN 2, TOMO 5 a FOJAS 1 OF-DGGST-2012-0373 (19-03-2012)
5	Federación Ecuatoriana De Exportadores FEDEXPOR	SECCIÓN 2, TOMO 6 a FOJAS 1 OF-DGGST-2012-0372 (19-03-2012)
6	Cámara de Industrias de Guayaquil	SECCIÓN 2, TOMO 7 a FOJAS 1 OF-DGGST-2012-0639 (02-05-2012)
7	EXPOFLORES	SECCIÓN 2, TOMO 8 a FOJAS 1 OF-DGGST-2012-0792 (17-05-2012)
8	TRANSASIA PACIFIC S.A.	SECCIÓN 2, TOMO 9 a FOJAS 1 OF-DGGST-2012-1329 (31-07-2012)
9	ESDINÁMICO CIA. LTDA.	SECCIÓN 2, TOMO 10 a FOJAS 1 OF-DGGST-2012-1848 (15-11-2012)
10	Cámara de Comercio de Cuenca	SECCIÓN 2, TOMO 11 a FOJAS 1 OF-DGGST-2013-0426 (15-01-2013)
11	Cámara de Comercio de Quito	SECCIÓN 2, TOMO 12 a FOJAS 1 OF-DGGST-2013-1255 (20-05-2013)
12	Megadatos S.A.	SECCIÓN 2, TOMO 13 a FOJAS 1 OF-DGGST-2013-1256 (20-05-2013)



#	Terceros vinculados con ANF	Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y Terceros Vinculados
1	CÁMARA DE INDUSTRIAS DE CUENCA	SECCIÓN 2, TOMO 14 a FOJAS 1 OF-DGGST-2013-2322 (24-10-2013)

ANEXO C

INSTALACIÓN DE EJBCA VERSIÓN 4.0.10

En este anexo se detallan los procedimientos de instalación de EJBCA para la implementación de la Infraestructura de Clave Pública PKI, sobre el Sistema Operativo GNU/Linux distribución Ubuntu Server 12.04 LTS, organizada mediante un esquema que contiene todas las actividades implícitas en este proceso (véase Figura C1).

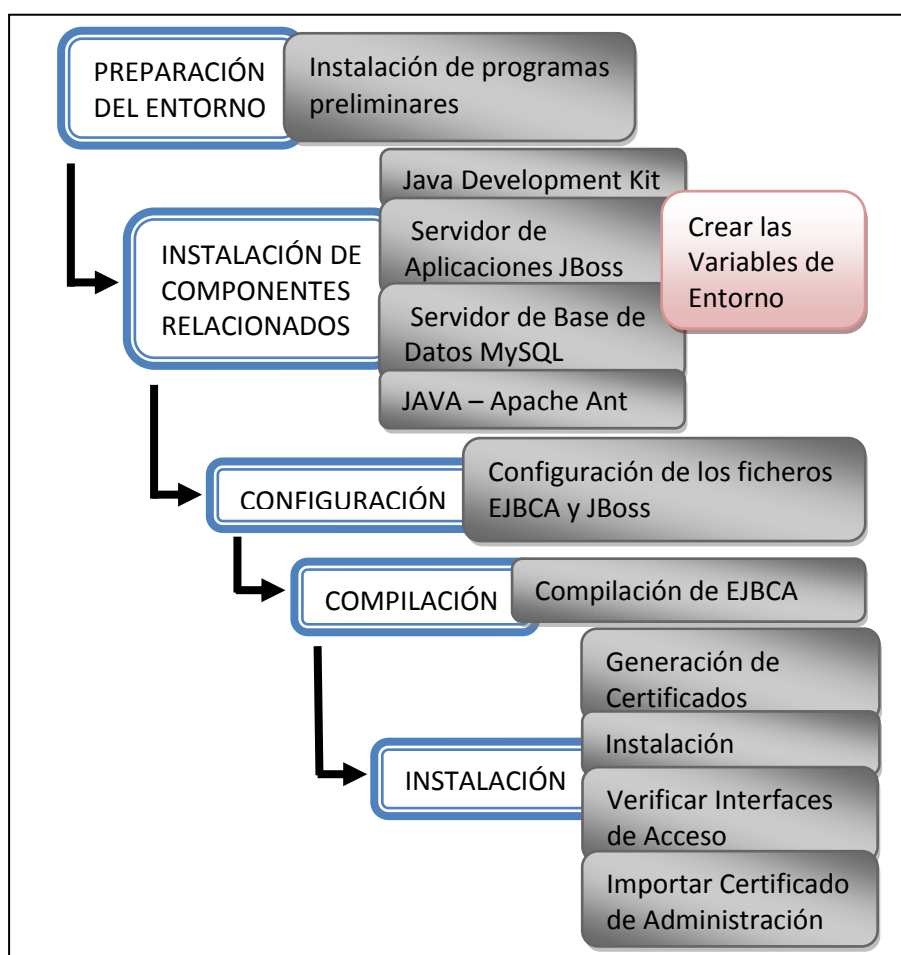


Figura C1. Etapas para la instalación de la Infraestructura de Clave Pública

1. PREPARACIÓN DEL ENTORNO

Antes de proceder a instalar los distintos tipos de servicios que necesita EJBCA, es necesario verificar que se encuentren instaladas en el Sistema Operativo ciertas herramientas como zip y unzip, librerías SSL y otras preliminares, para garantizar su ejecución.

Entonces abrir una sesión de consola de terminal y ejecutar los siguientes comandos como usuario privilegiado, cerciorándose previamente de tener acceso a internet desde este servidor:

```
apt-get install autoconf lynx zip unzip tofrodos ldap-utils  
apt-get install db4.8-util libldap2-dev libssl-dev libnet-ldap-perl  
apt-get install libapache2-mod-jk tdsodbc sqsh junit libapr1 slapd
```

Con esto aquellas herramientas que no se encuentren en el sistema operativo serán instaladas, y algunas de las que se encuentren se mantendrán o serán actualizadas.

2. INSTALACIÓN DE COMPONENTES RELACIONADOS

Son aquellos servicios necesarios para compilar e instalar EJBCA, como el de Base de Datos, el servidor de Aplicaciones o el de Compilación e Instalación, librerías criptográficas, entre otros.

2.1. Java Development Kit (JDK)

Java en sus repositorios provee dos tipos de paquetes destinados a propósitos específicos, JRE (Java Runtime Environment) que es un entorno de ejecución de aplicaciones Java, y JDK un entorno para desarrollarlas. EJBCA al estar estructurado en base a J2EE, necesita JDK

para desarrollar la aplicación de Autoridad de Certificación destinada a operar en el entorno del Cuerpo de Ingenieros del Ejército.

Al instalar JDK también se incluye el compilador `javac`⁴⁸, el entorno de ejecución JRE, y también la máquina virtual de java JVM, que en conjunto ejecutan las aplicaciones java desarrolladas y previamente compiladas.

Para instalar JDK se puede descargarlo directamente de sus repositorios oficiales en la página <http://www.oracle.com/technetwork/index.html>, para su posterior instalación, o también existe la posibilidad de unificar este proceso con la ayuda del comando `apt-get install openjdk-6-jdk` (véase Figura C2).

```

root@ubuntu-server:/home/david-admin# apt-get install openjdk-6-jdk
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
 libice-dev libpthread-stubs0 libpthread-stubs0-dev libsm-dev libx11-dev libx11-doc libxau-dev libxcb1-dev libxdmcp-dev libxt-dev
 x11proto-core-dev x11proto-input-dev x11proto-kb-dev xorg-sgml-doctools xtrans-dev
Paquetes sugeridos:
 libxcb-doc openjdk-6-demo openjdk-6-source visualvm
Se instalarán los siguientes paquetes NUEVOS:
 libice-dev libpthread-stubs0 libpthread-stubs0-dev libsm-dev libx11-dev libx11-doc libxau-dev libxcb1-dev libxdmcp-dev libxt-dev
 openjdk-6-jdk x11proto-core-dev x11proto-input-dev x11proto-kb-dev xorg-sgml-doctools xtrans-dev
0 actualizados, 16 se instalarán, 0 para eliminar y 2 no actualizados.
Necesito descargar 15,9 MB de archivos.
Se utilizarán 52,7 MB de espacio de disco adicional después de esta operación.
¿Desea continuar [s/n]?

```

Figura C2. Instalación de JDK versión 6

Luego de instalar java JDK se debe verificar que esta versión del paquete es la que se está ejecutando, en el caso de que existan otras versiones instaladas en el sistema; para ello ingresar el comando `update-alternatives --config java` (véase Figura C3), si están disponibles algunas versiones permitirá elegir la que se requiera.

```

root@ubuntu-server:/home/david-admin# update-alternatives --config java
Solo hay una alternativa en el grupo de enlaces java: /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
Nada que configurar.
root@ubuntu-server:/home/david-admin#

```

Figura C3. Comprobar que versión de JDK está ejecutándose

⁴⁸ **java compiler** – compila el código java a una representación intermedia denominada bytecode

Es un requerimiento indispensable cerciorarse de tener instalada la misma versión de java, y del compilador javac, para evitar problemas posteriores de compatibilidad, ejecutando los comandos `java -version` y `javac -version` respectivamente (véase Figura C4).

```
root@ubuntu-server:/home/david-admin# java -version
java version "1.6.0_27"
OpenJDK Runtime Environment (IcedTea6 1.12.6) (6b27-1.12.6-1ubuntu0.12.04.2)
OpenJDK 64-Bit Server VM (build 20.0-b12, mixed mode)
root@ubuntu-server:/home/david-admin#
root@ubuntu-server:/home/david-admin# javac -version
javac 1.6.0_27
root@ubuntu-server:/home/david-admin#
```

Figura C4. Verificar la versión de java y el compilador javac

Para comprobar que java está ejecutándose correctamente en el servidor, con la ayuda del navegador web de preferencia acceder a la dirección `http://www.java.com/es/download/testjava.jsp` y ejecutar el test (véase Figura C5).



Figura C5. Comprobar el funcionamiento de java utilizando Mozilla Firefox

2.1.1. Creación de la Variable de Entorno

Estas son variables que pueden ser creadas para almacenar diversos tipos de datos, como un nombre, un valor, o una ruta de alguna librería o partes de código almacenados en el sistema, destinados para cumplir distintos propósitos. Las aplicaciones que han de usarlas deben interpretar el formato de los datos que almacenan estas variables, y su significado.

En Ubuntu se pueden definir variables locales disponibles para un usuario específico, para un grupo, o pueden ser globales para todos los usuarios. Generalmente los sistemas operativos tienen predefinidas algunas variables de entorno que las utilizan para su propio funcionamiento. La Tabla C1 muestra algunas de las variables más usuales.

Tabla C1. Variables de Entorno habitualmente definidas en los sistemas Linux

Variable	Descripción
PATH	Es una variable global que almacena rutas para localizar directorios dentro del sistema operativo donde se encuentran los archivos necesarios para ejecutar un programa.
HOSTNAME	Guarda el nombre del equipo (host).
HOME	Es la ruta del directorio personal del usuario activo con el que se ha iniciado la sesión.
USER	Almacena el nombre del usuario que ha iniciado la sesión.
DESKTOP-SESSION	Es el tipo de sesión iniciada, por ejemplo Gnome, KDE, etc.

Fuente: Elaborado a partir de Pavón, L. (2010). Robótica, Software y Telecomunicaciones. Recuperado de <http://landerpfc.wordpress.com/2010/09/28/variables-de-entorno-en-gnulinux/>

Para desarrollar aplicaciones java, es necesario definir una variable de entorno global PATH, estableciendo el directorio en el que se encuentra la ruta de ejecución y el compilador javac, de manera que el sistema pueda localizarlas y emplearlas cuando sean requeridas.

Además, el Servidor de Aplicaciones JBoss y EJBCA, tienen definidas en sus archivos de compilación variables de entorno como JAVA_HOME, JBOSS_HOME o EJBCA_HOME, las cuales las utilizan para acceder directamente hacia directorios que deben contener librerías, compiladores, ejecutables, etc., que posibiliten la compilación e instalación de la Autoridad Certificadora.

Para ello, en Ubuntu se debe modificar como usuario privilegiado el archivo de configuración /etc/environment, y añadir la variable JAVA_HOME con la ruta del directorio donde se han almacenado los archivos del paquete JDK de java, e incluir esta variable en PATH precedido del signo \$ (véase Figura C6).

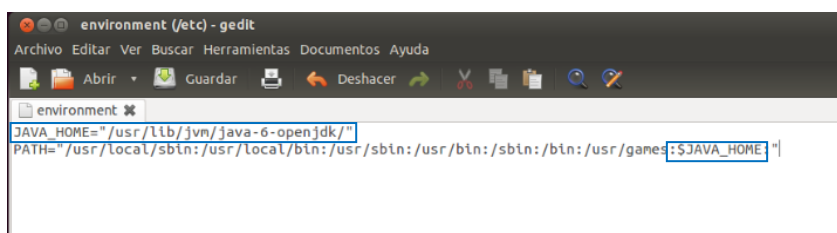


Figura C6. Declaración de la variable de entorno java

Se debe actualizar este valor ejecutando en una nueva sesión del terminal de consola, el comando `echo $PATH` y luego `echo $JAVA_HOME` (véase Figura C7) para que sea reconocida por el sistema la ruta del directorio de esta variable.

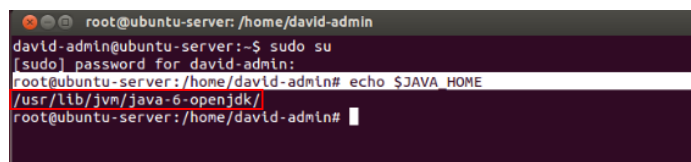


Figura C7. Actualización de la variable de entorno java

2.1.2. Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files

Por razones de seguridad las versiones más recientes de java han incluido entre sus funcionalidades el manejo de criptografía, pero debido a las restricciones legales que existen en algunos países referentes a su uso generalizado, no han sido desarrolladas completamente para proveer de gran cantidad de algoritmos criptográficos.

Sin embargo, EJBCA al haber sido desarrollada como una aplicación de código abierto, está exenta de cualquier restricción criptográfica, admitiendo la utilización de una gran variedad de algoritmos criptográficos “strong cryptography”. Entonces java necesita tener instalada esta extensión JCE para aprovechar todos los beneficios de seguridad de EJBCA, como la implementación de strong cryptography, o el manejo de almacenes de claves “keystores passwords” con soporte para longitudes mayores a 7 caracteres.

Esta extensión está disponible para su descarga en los repositorios oficiales de Oracle <http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html>, asegurándose de que la versión sea compatible con la de java, en este caso es la versión 6 de JCE es la correspondiente para java 1.6.0 (véase Figura C8).

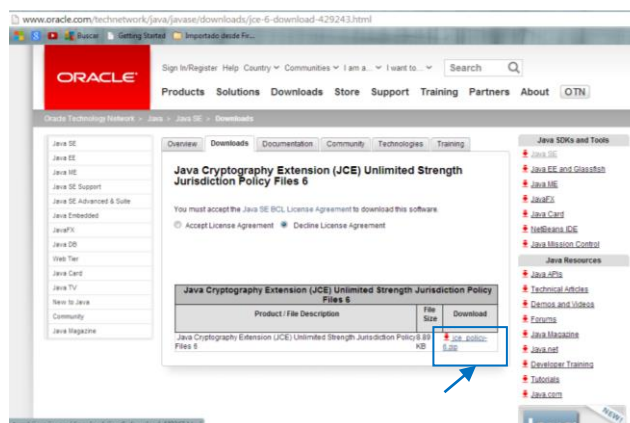


Figura C8. Descarga JCE de la Página Oficial de Oracle

Descomprimir el archivo descargado, y copiar los ficheros con extensiones .jar que contiene, en el directorio de java correspondiente, de la siguiente forma:

```
unzip jce_policy-6.zip
cd jce_policy-6
cp local_policy.jar US_export_policy.jar JAVA_HOME/jre/lib/security
```

2.2. Servidor de Aplicaciones Jboss

Este servidor es un software diseñado para proveer de aplicaciones a ordenadores cliente a través de internet, mediante el protocolo http. Su principal función consiste en gestionar la mayor parte de la lógica de las aplicaciones desarrolladas, y el acceso a sus datos; con la ventaja de que para su desarrollo no es necesario programarlas, sino más bien ensamblarlas a partir de módulos provistos por este servidor.

Debido a su uso masificado uno de los servidores de aplicaciones más usuales es el de JAVA desarrollado en base a la plataforma J2EE, algunos servidores Java EE de carácter privativo son WebSphere (IBM) y WebLogic de Oracle, JOnAS fue el primer servidor de código abierto desarrollado para ser compatible con esta plataforma, JBoss y GlassFish son los servidores de código abierto más populares en la actualidad.

JBoss AS es un servidor de aplicaciones diseñado para soportar el despliegue de aplicaciones empresariales de alto rendimiento sobre J2EE, que al operar bajo una licencia de código abierto, posibilita su descarga, instalación, ejecución y libre distribución sin ningún tipo de restricciones, este es el motivo por el cual es una de las plataformas más usuales en aplicaciones reales de producción.

Se ha considerado la recomendación publicada en la página oficial de EJBCA (<https://www.ejbca.org>) de utilizar la versión JBoss 5.1.0.GA compatible con jdk6, que se puede obtener desde <http://sourceforge.net/projects/jboss/files/JBoss/JBoss5.1.0.GA/jboss-5.1.0.GA-jdk6.zip>, aunque cualquier versión en el rango 5.1.x o 6.0.x funcionan para esta versión de java. Descomprimir este archivo en el directorio de usuario local mediante el comando:

```
unzip jboss-5.1.0.GA-jdk6.zip -d /usr/local/
```

Añadir en el archivo de configuración `/etc/environment` una variable de entorno `JBOSS_HOME` que direcciona hacia los ficheros donde se almacenó jboss, e incluir esta variable en el `PATH` precedida del signo `$` (véase Figura C9).

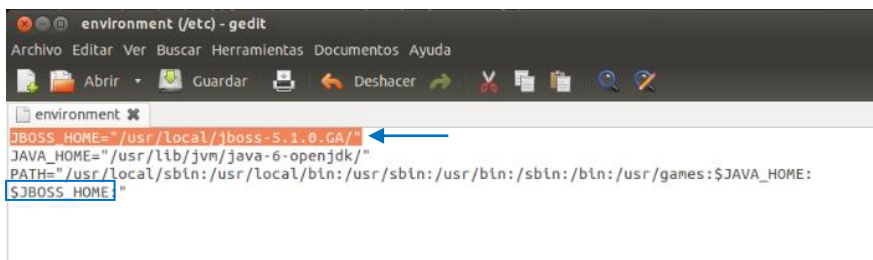


Figura C9. Declaración de la variable de entorno de Jboss

Actualizar este valor ejecutando en una nueva sesión del terminal de consola, el comando `echo $PATH` y luego `echo $JBOSS_HOME` (véase Figura C10) para que sea reconocido por el sistema la ruta del directorio de esta variable.

```

root@ubuntu-server: /home/david-admin
david-admin@ubuntu-server:~$ sudo su
[sudo] password for david-admin:
root@ubuntu-server: /home/david-admin# echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:$JAVA_HOME:$JBASS_HOME:
root@ubuntu-server: /home/david-admin# echo $JAVA_HOME
/usr/lib/jvm/java-6-openjdk/
root@ubuntu-server: /home/david-admin# echo $JBASS_HOME ←
/usr/local/jboss-5.1.0.GA/
root@ubuntu-server: /home/david-admin#

```

Figura C10. Actualización de la variable de entorno Jboss

Iniciar la operación del servidor de aplicaciones, en una sesión de terminal, desde el directorio `$JBASS_HOME/bin` ejecutando el fichero `run.sh` mediante el siguiente comando, percatándose de no obtener ningún tipo error en las operaciones que se efectúan luego de ejecutarlo:

```
./run.sh
```

Si la ejecución ha sido satisfactoria, es posible visualizar la interfaz web del servidor accediendo desde un navegador a la dirección `http://localhost:8080/` (véase Figura C11), verificando de esta manera su funcionamiento. Para detenerlo simplemente hay que digitar `control + C` en el terminal que fue ejecutado.

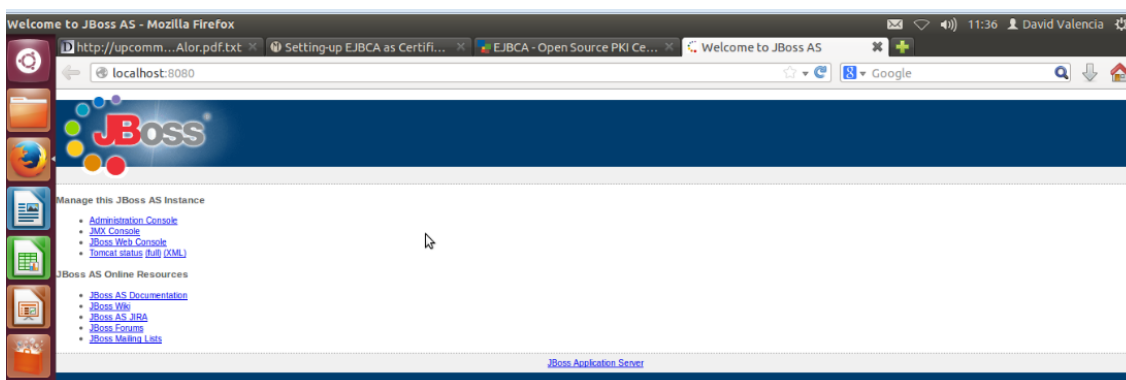



Figura C11. Ejecución de Jboss

2.3. Servidor de Base de Datos MySQL

Jboss de forma predeterminada dispone de la base de datos “Hypersonic Database” para llevar a cabo el desarrollo de aplicaciones; sin embargo, esta base de datos se caracteriza por ser in-memory (en memoria), esto significa que consumirá mayores recursos de memoria RAM de manera gradual, de acuerdo a como aumenten las operaciones de la Autoridad Certificadora. Además, esta base de datos no está en capacidad de soportar todos los comandos SQL, lo cual comprometerá su operación en algún momento.

Ventajosamente existe la posibilidad de integrarlo con un gestor de base de datos como MySQL para solventar estos inconvenientes, pensando en priorizar en todo momento la disponibilidad del servidor de certificación del CEE.

Para establecer el servidor de base de datos MySQL, es necesario inicialmente instalar `mysql-server` (véase Figura C12).



```

root@ubuntu-server: ~
root@ubuntu-server:~# apt-get install mysql-server
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
 libdbd-mysql-perl libdbi-perl libhtml-template-perl libnet-daemon-perl liblprc-perl libterm-readkey-perl
 mysql-client-5.5 mysql-client-core-5.5 mysql-server-5.5 mysql-server-core-5.5
Paquetes sugeridos:
 libipc-sharedcache-perl tinyca mailx
Se instalarán los siguientes paquetes NUEVOS:
 libdbd-mysql-perl libdbi-perl libhtml-template-perl libnet-daemon-perl liblprc-perl libterm-readkey-perl
 mysql-client-5.5 mysql-client-core-5.5 mysql-server mysql-server-5.5 mysql-server-core-5.5
0 actualizados, 11 se instalarán, 0 para eliminar y 0 no actualizados.
Necesito descargar 26,2 MB de archivos.
Se utilizarán 93,8 MB de espacio de disco adicional después de esta operación.
¿Desea continuar [S/n]? █

```

Figura C12. Instalación del servidor MySQL

Durante la instalación de este paquete se deberá ingresar una contraseña (véase Figura C13) para crear al usuario root del sistema gestor de base de datos.

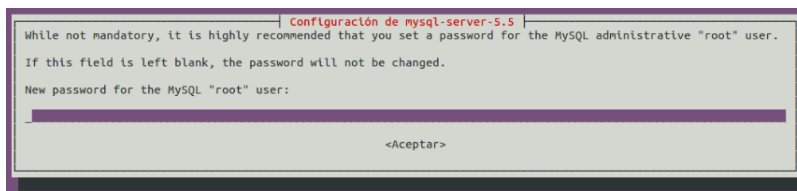


Figura C13. Establecer la contraseña del usuario root

También se debe instalar el paquete complementario `mysql-client` (véase Figura C14).

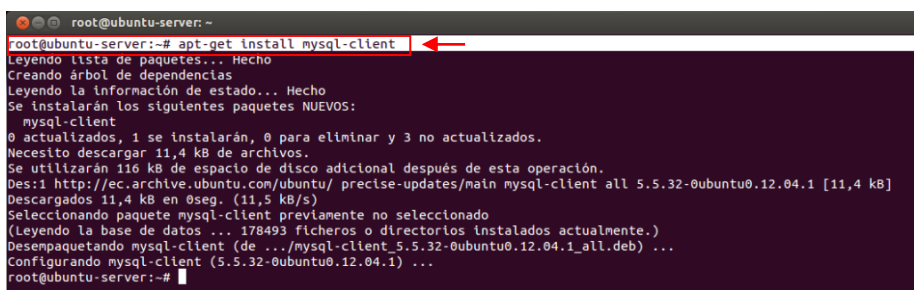


Figura C14. Instalación del cliente MySQL

Las herramientas gráficas de administración MySQL Administrator y MySQL Query Browser actualmente no están disponibles en los repositorios de Ubuntu, pero existen en repositorios alternativos los cuales deben ser añadidos a los de Ubuntu para su posterior instalación (véase Figura C15).

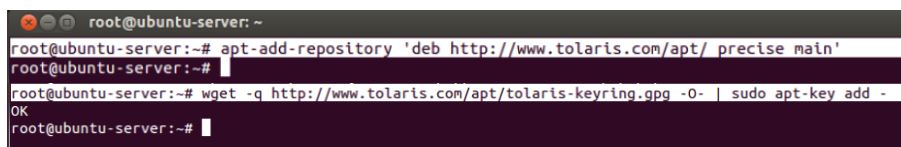


Figura C15. Añadir el repositorio tolaris a Ubuntu

Con esto, es posible actualizar el sistema `apt-get update`, y proseguir con la instalación de estas herramientas (véase Figura C16).

```

root@ubuntu-server: -
root@ubuntu-server:~# apt-get install mysql-query-browser
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
 libbonobo2-0 libbonobo2-common libglade2-0 libgnome2-0 libgnome2-bin libgnomevfs2-0 libgnomevfs2-common
 libgtkhtml3.14-19 libgtkmm-2.4-1c2a libidl-common libidl0 libmysqlclient16 liborbit2 mysql-admin
 mysql-gui-tools-common
Paquetes sugeridos:
 libbonobo2-bin libgnomevfs2-bin libgnomevfs2-extra gamin fam gnome-mime-data libgtkhtml3.14-dbg
Se instalarán los siguientes paquetes NUEVOS:
 libbonobo2-0 libbonobo2-common libglade2-0 libgnome2-0 libgnome2-bin libgnomevfs2-0 libgnomevfs2-common
 libgtkhtml3.14-19 libgtkmm-2.4-1c2a libidl-common libidl0 libmysqlclient16 liborbit2 mysql-admin
 mysql-gui-tools-common mysql-query-browser
0 actualizados, 16 se instalarán, 0 para eliminar y 3 no actualizados.
Necesito descargar 8.642 kB de archivos.
Se utilizarán 30,0 MB de espacio de disco adicional después de esta operación.
¿Desea continuar [S/n]?

```

Figura C16. Instalación de Herramientas Gráficas de Administración

Además, es necesario crear un nuevo usuario destinado a desempeñar todas las actividades relacionadas con EJBCA, y una base de datos sobre la que éste tenga todos los privilegios, para almacenar las tablas y datos que se generarán posteriormente durante la instalación y operación de la CA, para esto:

Iniciar sesión como usuario root:

```
mysql -u root -p
```

Crear la base de datos ejbca_4_0_10:

```
mysql> create database ejbca_4_0_10;
```

Crear el usuario ejbca, establecer su contraseña y asignarle todos los privilegios sobre la base de datos creada:

```
mysql> grant all privileges on ejbca_4_0_10.* to 'ejbca'@'localhost'
identified by 'contraseña de acceso';
```

De esta forma el usuario ejbca puede iniciar su sesión y acceder a la base de datos ejbca_4_0_10 (véase Figura C17).

```

root@ubuntu-server:~
root@ubuntu-server:~# mysql -u ejbca -p ← Inicio de sesión
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 52
Server version: 5.5.32-0ubuntu0.12.04.1 (Ubuntu)

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> use ejbca 4.0.10; ← Acceso a la base de datos
Database changed
mysql>

```

Figura C17. Inicio de sesión y acceso a la base de datos creada

2.3.1. Conector de Base de Datos JDBC

JDBC⁴⁹ es un API⁵⁰ que establece una librería estándar para acceder desde aplicaciones desarrolladas en base a JAVA, hacia bases de datos relacionales que implementan SQL. Esto permitirá que la base de datos MySQL opere adecuadamente con Java en el despliegue de la PKI del CEE.

Este controlador está disponible en su página oficial <http://dev.mysql.com/downloads> en la sección MySQL Connectors con el nombre Connector/J, en este caso la última versión actualizada en el repositorio fue la 5.1.26 (véase Figura C18).

Descomprimir el archivo descargado y copiar el fichero .jar en el directorio del servidor de aplicaciones que almacena sub-directorios de configuración, de la siguiente forma:

```

unzip mysql-connector-java-5.1.26.zip
cd mysql-connector-java-5.1.26
cp mysql-connector-java-5.1.26-bin.jar $JBOSS_HOME/server/default/lib

```

⁴⁹ Java Database Connectivity

⁵⁰ Interfaz de Programación de Aplicaciones

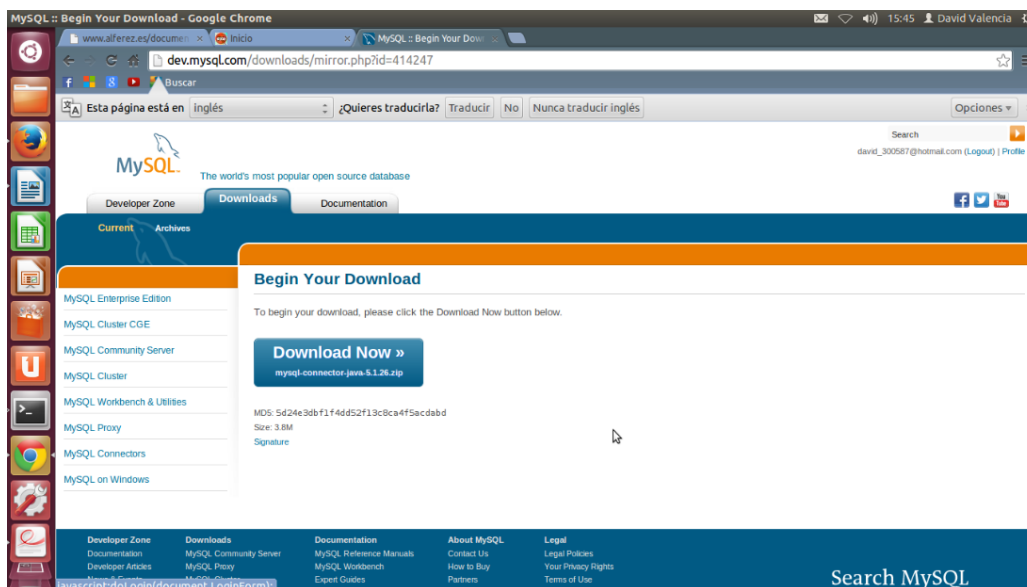


Figura C18. Paquete JDBC para MySQL

JBoss está estructurado de acuerdo a directorios que contienen información específica para su ejecución, la Tabla C2 detalla cuales son estos directorios y la información que cada uno almacena.

2.4. Apache Ant

Esta es una herramienta utilizada en programación durante la fase de compilación y construcción de aplicaciones desarrolladas sobre java. La ejecución del comando ant localiza y ejecuta el archivo build.xml almacenado en el servidor de aplicaciones y EJBCA, para compilarlos y construir la aplicación de Autoridad Certificadora del CEE.

Para asegurarse de que todas las funcionalidades y librerías de esta herramienta sean instaladas, ejecutar el siguiente comando:

```
apt-get install ant ant-doc ant-gcj ant-optional ant-optional-gcj
```

Tabla C2. Estructura de Directorios del Servidor de Aplicaciones JBoss

Directorio	Descripción
bin	Contiene archivos ejecutables que emplea JBoss para su operación, por ejemplo el script de arranque run.sh
client	Posee diversos archivos de extensión .jar que serán usados por diversos clientes de los contenedores EJB empleados en Jboss.
docs	Almacena documentación relacionada con JBoss, y algunos ejemplos de conexión con diversos servidores de bases de datos.
lib	Este directorio contiene archivos .jar necesarios para que JBoss se ejecute en diferentes modalidades de funcionamiento.
server	Almacena tres sub-directorios con distintos archivos de configuración para ejecutar JBoss en diferentes modalidades de funcionamiento (all, default y minimal), acotando que la de default es la que habitualmente se ejecuta, las otras se ejecutan modificando el script de arranque run.sh. All presenta funcionalidades adicionales, y minimal se ejecuta con requerimientos mínimos del servidor de aplicaciones.
Sub-directorios residentes en la modalidad de ejecución Default	
conf	Contiene varios archivos de configuración de JBoss dependiendo de la modalidad en la que se ejecute.
Archivos de Configuración	
Directorio	Descripción
jboss-service.xml	Archivo que contiene los parámetros principales para la configuración Default de jboss. Define los valores para la variable CLASSPATH, el puerto para el servidor JNDI, el directorio donde se almacenarán los contenedores EJBs, entre otros parámetros.
jbossmq-state.xml	Contiene los usuarios y roles disponibles para emplear el sistema "Messaging" que provee jboss.
jndi.properties	Son propiedades para realizar búsquedas JNDI.
login-config.xml	Contiene parámetros JAAS empleados por JBoss para autenticar/verificar usuarios.
server.policy	Referente a parámetros de seguridad
standardjaws.xml	Es un motor de mapeo empleado por JBoss
standardjboss.xml	Son parámetros de configuración estándar como el tamaño de pools para los contenedores EJBs, valores de caché, número de pools para bases de datos, clases empleadas para el control de transacciones, entre otros.
data	Almacena parámetros y archivos de configuración para la base de datos Hypersonic proporcionada por defecto por JBoss, generalmente se utiliza para pequeñas aplicaciones demostrativas.
deploy	Este directorio es de suma importancia, debido a que almacena los archivos JAR de las aplicaciones en forma de EJB, para que sean ejecutados por JBoss
	Guarda los archivos JAR de acuerdo a la modalidad de funcionamiento
	Contiene los registros de las actividades llevadas a cabo al ejecutarse JBoss

tmp	Son archivos creados de manera temporal
work	Almacena clases y archivos ejecutados por JBoss

Fuente: Creado a partir de Alférez S, J. A. Instalación, Configuración y Administración del Servidor de Aplicaciones JBoss. Recuperado de <http://www.alferez.es/documentos/Jboss.pdf>

3. CONFIGURACIÓN

Hasta este punto se encuentran instaladas y almacenadas en el sistema, todas las herramientas de software preliminares y relacionadas, indispensables para implementar la CA, ahora es necesario obtener los paquetes de EJBCA. De acuerdo a la guía de instalación de su página oficial, una de las versiones estables y recomendables de utilizar para desarrollar el servidor de certificación es la 4.0.10.

Es posible obtenerla desde http://sourceforge.net/projects/ejbca/files/ejbca4/ejbca_4_0_10/ejbca_4_0_10.zip, descargar este archivo y descomprimirlo en el directorio de usuario local, que contiene también los archivos del servidor de aplicaciones, de la siguiente forma:

```
unzip.ejbca_4_0_10.zip -d /usr/local
```

Análogamente a las anteriores herramientas se debe declarar una variable de entorno que localice los archivos de EJBCA en el sistema, durante el proceso de compilación, construcción e instalación de la Autoridad Certificadora.

Esto implica modificar el archivo de configuración `/etc/environment` e incluir la nueva variable (véase Figura C19), y en una nueva sesión de terminal de consola ejecutar el comando `echo $PATH` y luego `echo $EJBCA_HOME`, para actualizar este valor y que sea reconocido por el sistema.

A screenshot of a text editor window titled 'environment'. The window shows several environment variables defined in a single line: `ANT_HOME="/usr/local/ant-1.9.4"`, `EJBCA_HOME="/usr/local/ejbc4 4 0 10"`, `JBoss_HOME="/usr/local/jboss-5.1.0.GA"`, `JAVA_HOME="/usr/lib/jvm/java-6-openjdk"`, and `PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:$JAVA_HOME:$JBoss_HOME:$EJBCA_HOME:$ANT_HOME"`. The `EJBCA_HOME` variable and its value are highlighted with a blue selection box.

Figura C19. Declaración de la variable de entorno de EJBCA

Estas son todas las herramientas de software que deben estar almacenadas e instaladas en el sistema, ahora se deben realizar algunas configuraciones previas a la instalación de EJBCA.

3.1. Ficheros EJBCA

Los ficheros de configuración de esta herramienta se encuentran en el directorio `EJBCA_HOME/conf` y deben realizarse ciertas configuraciones sobre varios de ellos previo a la instalación de la CA, resaltando que éstos mantienen un nombre estándar en este directorio, de la forma `nombre_del_archivo.properties.sample`.

Entonces se deben crear inicialmente los ficheros que serán personalizados, a partir de los ya existentes, por ejemplo copiar el fichero `database.properties.sample` y guardarlo con el nombre `database.properties`; de esta forma el sistema utilizará este nuevo fichero con todas sus modificaciones en el proceso de instalación, en lugar del predeterminado `.sample`.

Las configuraciones por defecto de estos ficheros funcionan bien para entornos de prueba, pero para una producción real es necesario personalizar `ejbca.properties.sample`, `database.properties.sample`, `web.properties.sample` e `install.properties.sample`, debido a que fijan ciertos parámetros importantes de instalación, como el establecimiento de contraseñas personales, la conexión con la base de datos, el servidor de aplicaciones, entre otros.

3.1.1. Fichero `ejbca.properties`

En este fichero se definen el tipo del servidor de aplicaciones y el directorio en el cual se encuentran almacenados sus archivos, como las contraseñas que protegerán los repositorios de claves en la base de datos. Las modificaciones que se realizaron sobre este fichero y los valores que fueron asignados son:

* El servidor de aplicaciones elegido para el despliegue, y la ruta del directorio donde se almacenan sus archivos

```
appserver.type=jboss
appserver.home=/usr/local/jboss-5.1.0.GA
appserver.home=${env.JBOSS_HOME}
```

* Establecer contraseñas para proteger los almacenes de claves (keystores) de la CA, XKMS y CMS en la base de datos

```
ca.keystorepass= contraseña de protección
ca.xkmskeystorepass= contraseña de protección
ca.cmskeystorepass= contraseña de protección
```

Estas contraseñas deben ser definidas acatando las consideraciones y recomendaciones expuestas en el Anexo A.

3.1.2. Fichero database.properties

Se deben establecer los valores para el gestor de base de datos, como también la dirección y los datos de acceso (usuario y contraseña) a la base de datos creada para almacenar toda la información relacionada con EJBCA. Las modificaciones que se realizaron sobre este fichero y los valores que fueron asignados son:

* El nombre de la base de datos elegida para el despliegue

```
database.name=mysql
```

*La dirección de acceso a la base de datos creada para almacenar información relacionada con EJBCA

```
database.url=jdbc:mysql://127.0.0.1:3306/ejbca_cee
```

*El driver JDBC correspondiente al gestor de base de datos

```
database.driver=com.mysql.jdbc.Driver
```

*Usuario y contraseña del administrador de la base de datos

```
database.username=ejbca_admin  
database.password=contraseña de acceso
```

3.1.3. Fichero web.properties

Contiene parámetros que establecen la configuración de conexión web hacia JBoss (puertos e interfaces web), el nombre del host (hostname), el DN⁵¹ para el certificado SSL del servidor de certificación, las contraseñas para protegerlo, el certificado del Superadministrador temporal, y el almacén de claves (keystore) de confianza de java. Las modificaciones que se realizaron sobre este fichero y los valores que fueron asignados son:

⁵¹ **Distinguished Name** – Nombre Distintivo

*Definir la contraseña que protege el almacén de claves (keystore) de java (JDK) utilizado por EJBCA.

```
java.trustpassword=contraseña de protección
```

* Los valores de los campos Common Name y Distinguished Name que se incluirán en el certificado digital del Superadministrador temporal, y servirán para identificarlo.

```
superadmin.cn=PKISuperAdmin
superadmin.dn=CN=${superadmin.cn}
```

*Contraseña para proteger el certificado digital del Superadministrador temporal (superadmin.p12), que será utilizada como desafío de autenticación al importarlo sobre cualquier ordenador.

```
superadmin.password= contraseña de protección
```

*El siguiente parámetro debería estar en true si se desea recuperar el certificado de superadmin utilizando la interfaz web pública del servidor, en lugar de la importación manual desde el directorio \$EJBCA_HOME/p12

```
superadmin.batch=true
```

*La contraseña para proteger el certificado del servidor web (HTTPS), análoga al del Superadministrador temporal, que emplea EJBCA para permitir el acceso público al servicio, y también la administración del mismo (son las interfaces web pública y de administración).

```
httpsserver.password= contraseña de protección
```

*El nombre del host (hostname) sobre el cual se han instalado todas las herramientas de software para la instalación de EJBCA, si existe un servidor DNS configurado previamente se debe escribir el dominio con el cual se identifique al host.

```
httpsserver.hostname=localhost
```

*El DN (Distinguished Name) para el certificado del servidor web (HTTPS) de este servidor de certificación, con la consideración de que el campo del certificado CN (Common Name) debería llevar el nombre del hostname para identificarlo de mejor manera; y también deben definirse los campos Organización (O) y País (C - Country). Estos valores por el momento no tienen mucha relevancia teniendo en cuenta que van a formar parte de un certificado digital que en procesos posteriores de esta implementación será reemplazado por uno con datos más representativos.

```
httpsserver.dn=CN=127.0.0.1,O=EJBCA Sample,C=SE
```

*Los puertos de las interfaces públicas y privada por las que EJBCA aceptará las peticiones de certificación http y https, la privada requiere un certificado de autenticación ante el servidor SSL (en este caso, el que va a ser generado para el Superadministrador)

```
httpserver.pubhttp=8080
httpserver.pubhttps=8442
httpserver.privhttps=8443
```

*Los interfaces públicas EJBCA deberán permitir conexiones desde host remotos provenientes de cualquier red, para que los usuarios de los grupos de trabajo tengan la posibilidad de acceder al servicio; mientras que la privada únicamente debe ser accesible desde la red local del edificio CEE.

```
httpserver.bindaddress.pubhttp=0.0.0.0
httpserver.bindaddress.pubhttps=0.0.0.0
httpserver.bindaddress.privhttps=192.168.0.0/24
```

3.1.4. Fichero install.properties

Este fichero contiene parámetros para definir valores referentes a la Autoridad Certificadora raíz que va a ser creada, como su nombre, el DN de su certificado digital, o si la generación de claves será efectuada empleando hardware criptográfico HSM⁵² o token software, y varias propiedades para la generación de su certificado digital. Las modificaciones que se realizaron sobre este fichero y los valores que fueron asignados son:

* Definir el nombre de la CA root que será creada y el Distinguished Name de su certificado

```
ca.name=AdminCA1
ca.dn=CN=AdminCA1,O=EJBCA Sample,C=SE
```

*Fijar si la generación de claves se llevará a cabo empleando herramientas de software (token software), que es el método más usual, o con módulos de soporte físico (HSM – Hardware Security Module).

```
ca.tokenype=soft
ca.tokenpassword=null
```

*Establecer las propiedades del certificado digital de la CA raíz (la longitud y el algoritmo para la generación de claves, el algoritmo para la firma digital, y la validez en días del certificado).

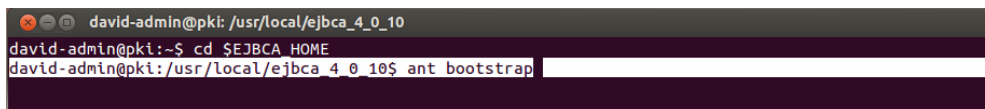
```
ca.keyspec=2048
ca.keytype=RSA
ca.signaturealgorithm=SHA1WithRSA
ca.validity=3650
ca.policy=null
```

⁵² **Hardware Security Module** – Módulo de Seguridad de Hardware

La mayoría de las configuraciones sobre todos los ficheros almacenados en el directorio EJBCA_HOME/conf, pueden ser modificadas después de la instalación si fuese necesario, excepto las del fichero `install.properties`.

4. COMPILACIÓN

En esta etapa de desarrollo del servidor de certificación como en la de instalación, se empleará la herramienta Apache Ant instalada previamente. Para efectuar la compilación de los ficheros EJBCA es necesario detener el servidor de aplicaciones JBoss si ha estado ejecutándose, acceder al directorio de la herramienta y ejecutar `ant bootstrap` (véase Figura C20).



```
david-admin@pki: /usr/local/ejbca_4_0_10
david-admin@pki:~$ cd $EJBCA_HOME
david-admin@pki: /usr/local/ejbca_4_0_10$ ant bootstrap
```

Figura C20. Comando para la compilación de los ficheros EJBCA

Tras la ejecución de este comando se desplegarán una serie de procesos para generar y almacenar ficheros en directorios específicos, si todo ha ido bien debería mostrar un mensaje como el de la Figura C21 al finalizar este proceso.

Lo que hace este comando es generar un fichero EAR que será almacenado en el directorio `JBOSS_HOME/server/default/deploy` como un servicio `ejbca.ear`, conjuntamente con `ejbca-ds.xml` y `ejbca-mail-service.xml`; mientras que en el directorio `EJBCA_HOME/` se generarán los sub-directorios `dist/`, `hwtoken/` y `tmp/` (véase Figura C22).

```

root@ubuntu-server: /usr/local/ejbca_4_0_10

websphere-specials:
signjar:
  [echo] Specify -Dsignjar.keystore=/path/keystore.jks if you want to sign the release.
signjar.internal:
build:
inputDeployPasswords:
inputBootstrapAndDeployPasswords:
  [input] skipping input as property database.password has already been set.
deploy:
j2ee:check:
  [echo] Using appserver.home : /usr/local/jboss-5.1.0.GA/
j2ee:web-configure:
j2ee:configure:
j2ee:deployBase:
  [copy] Copying 2 files to /usr/local/jboss-5.1.0.GA/server/default/deploy
  [mkdir] Created dir: /usr/local/ejbca_4_0_10/dist/datasources
  [copy] Copying 1 file to /usr/local/jboss-5.1.0.GA/server/default/deploy
j2ee:deploy:
showtime:
  [echo] Task completed 2013-09-17 22:28:48 -0500.

BUILD SUCCESSFUL
Total time: 35 seconds
root@ubuntu-server: /usr/local/ejbca_4_0_10#

```

Figura C21. Ejecución exitosa del proceso de compilación

```

david-admin@pki:~$ cd $JBASS_HOME/
david-admin@pki:~/usr/local/jboss-5.1.0.GA$ cd server/default/deploy
david-admin@pki:~/usr/local/jboss-5.1.0.GA/server/default/deploy$ ls
admin-console.war          hsqldb-ds.xml          legacy-invokers-service.xml  schedule-manager-service.xml
cache-invalidation-service.xml  http-invoker.sar      mail-ra.rar                scheduler-service.xml
ejb2-container-jboss-beans.xml  jboss-local-jdbc.rar  mail-service.xml           security
ejb2-timer-service.xml        jbossweb.sar         management                 sqlexception-service.xml
ejb3-connectors-jboss-beans.xml  jbossws.sar         messaging                  transaction-jboss-beans.xml
ejb3-container-jboss-beans.xml  jboss-xa-jdbc.rar    monitoring-service.xml     transaction-service.xml
ejb3-interceptors-aop.xml      jca-jboss-beans.xml  profileservice-jboss-beans.xml  uuid-key-generator.sar
ejb3-timer-service-jboss-beans.xml  jms-ra.rar          profileservice-secured.jar   vfs-jboss-beans.xml
ejbca-ds.xml                  jmx-console.war      properties-service.xml     xnio-provider.jar
ejbca.ear                    jmx-invoker-service.xml  quartz-ra.rar              remoting-jboss-beans.xml
ejbca-mail-service.xml        jmx-remoting.sar     ROOT.war
hdscanner-jboss-beans.xml      jsr88-service.xml
david-admin@pki:~$ cd $EJBCA_HOME
david-admin@pki:~/usr/local/ejbca_4_0_10$ ls
bin      conf      dist      docs.xml  lib      p12      README  test.xml  velocity.log
build.xml  Changelog.txt  doc      hwtoken  modules  propertyDefaults.xml  src      tmp
david-admin@pki:~/usr/local/ejbca_4_0_10$

```

Figura C22. Generación y alojamiento de ficheros y sub-directorios durante la instalación

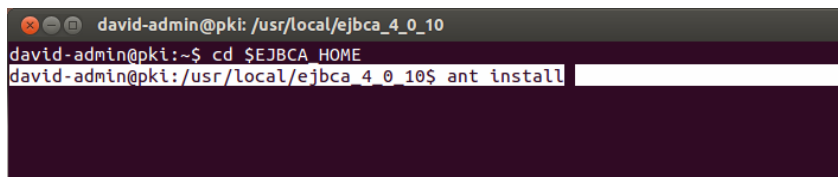
Este fichero EAR es trasladado para incluirse con los de JBoss y posibilitar de esta forma la integración con el servidor de aplicaciones.

5. INSTALACIÓN

Se generarán los certificados de Superadministrador, del servidor web SSL de la entidad certificadora, de la entidad certificadora, y será creada la entidad certificadora, de acuerdo a los valores establecidos en los ficheros de configuración EJBCA.

5.1. Generación de Certificados

Si la compilación ha sido exitosa se deberá arrancar el servidor de aplicaciones JBoss y percatarse de que no se presenten errores durante su ejecución, de esta forma acceder al directorio EJBCA, sin detener JBoss y con el servidor de base de datos en operación, ejecutar `ant install` (véase Figura C23).



```
david-admin@pki: /usr/local/ejbca_4_0_10
david-admin@pki:~$ cd $EJBCA_HOME
david-admin@pki: /usr/local/ejbca_4_0_10$ ant install
```

Figura C23. Comando para la generación de Certificados y Repositorios

Tras este proceso se creará el certificado de Superadministrador (`superadmin.p12`), y también los repositorios de claves de java y del servidor SSL (`truststore.jks` y `tomcat.jks`), que son almacenados en el directorio `EJBCA_HOME/p12` (véase Figura C24). Este comando debido a que genera certificados, sólo puede ejecutarse una sola vez durante la instalación de EJBCA, si ya se instaló y se ejecuta nuevamente generará errores.

```

david-admin@pki:~$ cd $EJBCA_HOME
david-admin@pki:/usr/local/ejbca_4_0_10$ ls
bin          conf          dist          docs.xmlli   lib          p12          README      test.xmlli   velocity.log
build.xml   Changelog.txt doc           hwtoken     modules     propertyDefaults.xml  src         tmp
david-admin@pki:/usr/local/ejbca_4_0_10$ cd p12/
david-admin@pki:/usr/local/ejbca_4_0_10/p12$ ls
superadmin.p12  tomcat.jks  truststore.jks
david-admin@pki:/usr/local/ejbca_4_0_10/p12$

```

Figura C24. Directorio del certificado de Superadministrador y los repositorios de claves

5.2. Instalación

Para finalizar el proceso de instalación es necesario detener el servidor de aplicaciones, y desde el directorio de EJBCA ejecutar `ant deploy` (véase Figura C25).

```

david-admin@pki: /usr/local/ejbca_4_0_10
david-admin@pki:~$ cd $EJBCA_HOME
david-admin@pki:/usr/local/ejbca_4_0_10$ ant deploy

```

Figura C25. Comando para la instalación de EJBCA

Este comando creará copias de los ficheros de configuración EJBCA y los repositorios de claves, sobre JBoss; además, se volverán a generar los ficheros de servicios (EAR) que fueron creados durante el proceso de compilación. Lo que queda es iniciar el servidor de aplicaciones para comprobar el funcionamiento de la Autoridad Certificadora creada.

5.3. Verificar Interfaces de Acceso

EJBCA implementa por seguridad tres interfaces de acceso destinadas a diferentes propósitos, la primera es la public web que es una interfaz gráfica accesible públicamente para que los usuarios puedan obtener los certificados que han solicitado previamente, el certificado y las CRLs de la CA, entre otras cosas; la segunda es la admin web, también es gráfica pero

es accesible únicamente para los administradores de la PKI, debido a que es necesario un certificado SSL de autenticación ante el servidor; y la tercera la CLI⁵³ es una interfaz de consola de administración, de gran utilidad si se requiere llevar a cabo actividades mediante scripts.

Como la public web no necesita autenticación, se puede acceder a ella mediante la dirección <http://localhost:8080/ejbca> (véase Figura C26), o también existe la posibilidad de realizarlo en modo seguro mediante <https://localhost:8442/ejbca> (véase Figura C27).

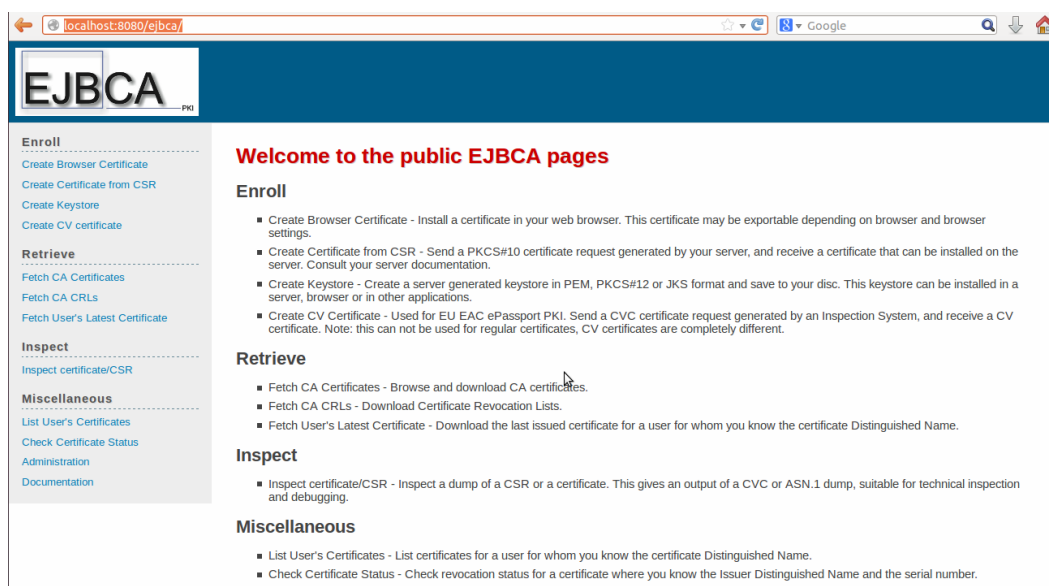


Figura C26. Interfaz web pública de EJBCA

En ella el apartado Enroll es empleado para finalizar el proceso de certificación de un usuario, generándose el par clave criptográfico y el certificado pertinente; Retrieve permite descargar las CRLs y los certificados de las CAs creadas en la jerarquía PKI, como también

⁵³ Command Line Interfaz

los certificados de usuario final emitidos; Miscellaneous posibilita verificar el estado de un certificado.

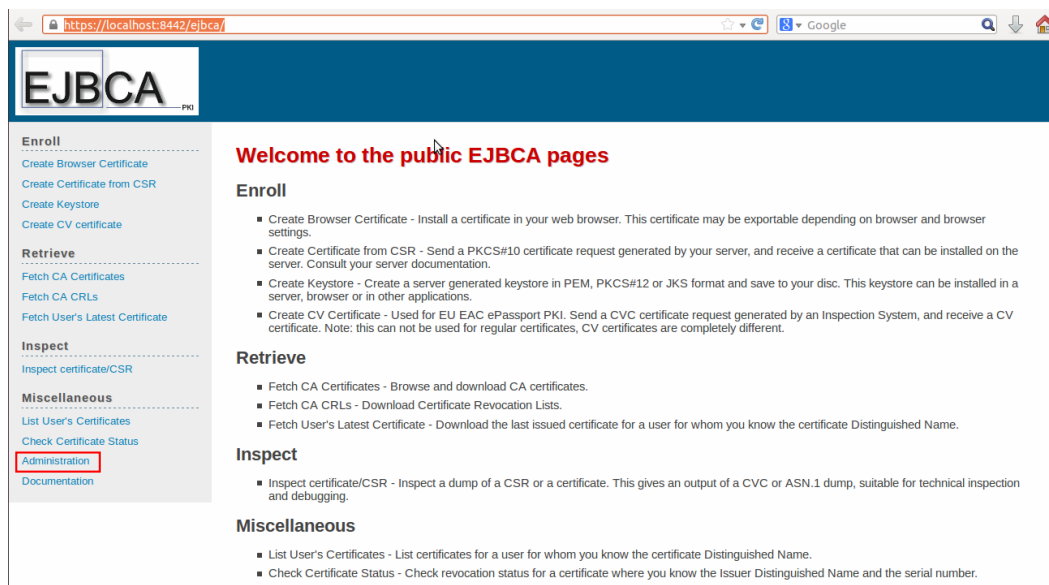


Figura C27. Interfaz web pública de EJBCA en modo seguro

En esta interfaz existe la opción Administration que permite acceder hacia la admin web, pero para ello es necesario disponer del certificado de Superadministrador emitido, caso contrario tratará de acceder a ésta a través del puerto 8442, lo que generará un error, debido a que de acuerdo a las configuraciones en web.properties el puerto de acceso debe ser el 8443. Esto garantiza un filtro de seguridad para que únicamente el Administrador designado de la CA Raíz del CEE, pueda acceder a ella.

5.4. Importar Certificado de Administración

La admin web por su parte requiere de autenticación, por ello es necesario importar el certificado Superadministrador desde el directorio EJBCA_HOME/p12 generado durante la

instalación, hacia el navegador web que se esté empleando para acceder a esta interfaz gráfica de administración.

Entonces es necesario acceder al administrador de certificados del navegador de nuestra preferencia (se recomienda utilizar Internet Explorer o Google Chrome porque emplean el almacén de certificados del sistema operativo, en el caso de Windows) e importarlo; en el caso de Firefox seleccionar Edit + Preferences + Advanced + Certificates, en la opción View Certificates, seleccionar Your Certificates, elegir import (véase Figura C28) y buscar este fichero (véase Figura C29).

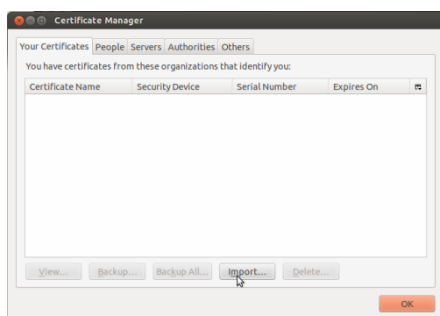


Figura C28. Administrador de Certificados de Mozilla Firefox

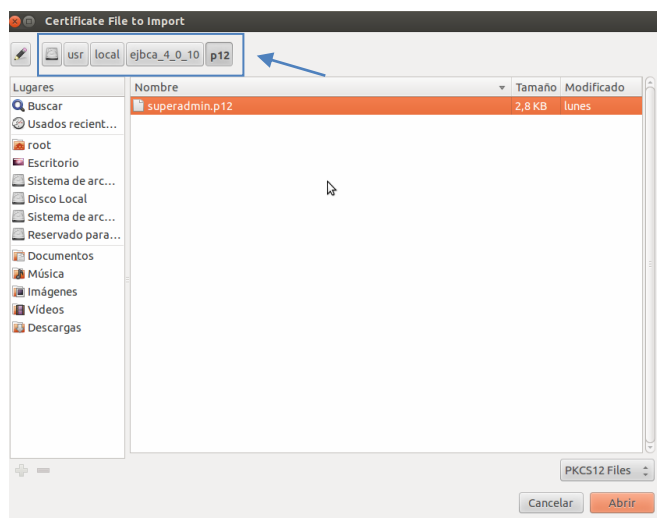


Figura C29. Fichero que contiene el certificado de administración

Al importarlo el sistema solicitará la contraseña empleada para proteger este certificado (véase Figura C30), ésta debe ser la misma que fue establecida en el fichero `web.properties` de EJBCA, en el campo `superadmin.password`.

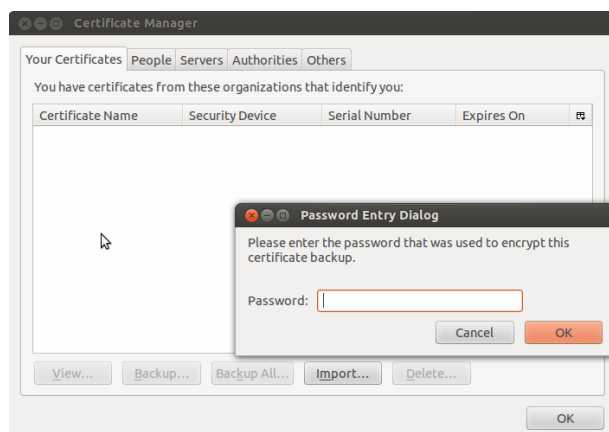


Figura C30. Solicitud de contraseña que protege al certificado de administración

Entonces si se ha importado correctamente este certificado es posible acceder a la interfaz admin web (véase Figura C31), a través de la cual es posible generar la CA real para el CEE y posteriormente la emisión y gestión de certificados digitales de usuarios finales.

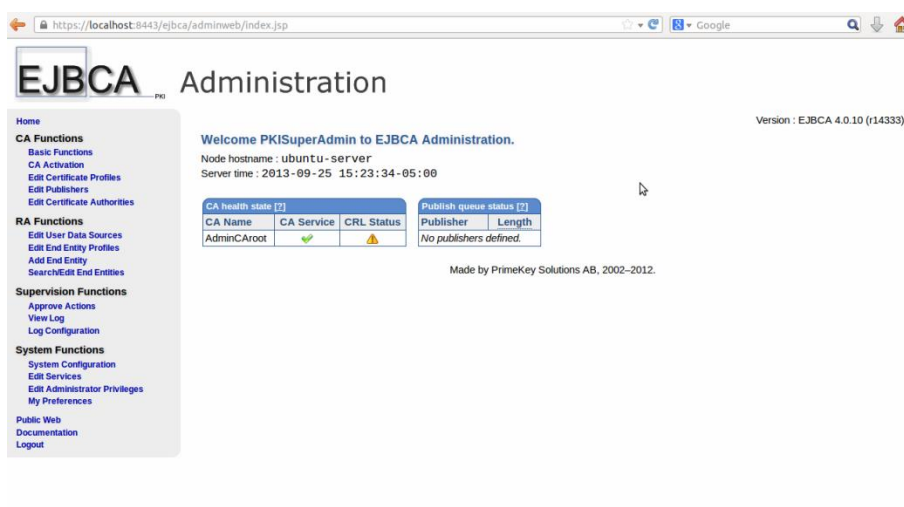


Figura C31. Interfaz de Administración de EJBCA

ANEXO D

INSTALACIÓN Y CONFIGURACIÓN DE BIND 9

En este anexo se detallan los procedimientos de instalación y configuración de Bind9, para simular el Servicio de Nombres de Dominio (DNS) necesario en el desarrollo de este proyecto, sobre el Sistema Operativo GNU/Linux distribución Ubuntu Server 12.04 LTS.

1. INSTALACIÓN

Para implantar un servidor de dominio es necesario inicialmente cerciorarse de que el ordenador anfitrión, disponga de una configuración de red con una dirección IP estática, en este caso al estar implementado sobre Ubuntu server 12.04 LTS, se debe editar el fichero de configuración en el directorio `/etc/network/interfaces`, y establecer los valores del adaptador de red (véase Figura D1).

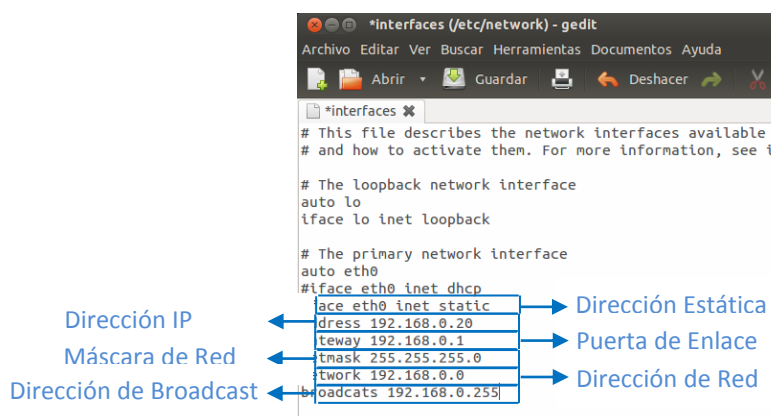
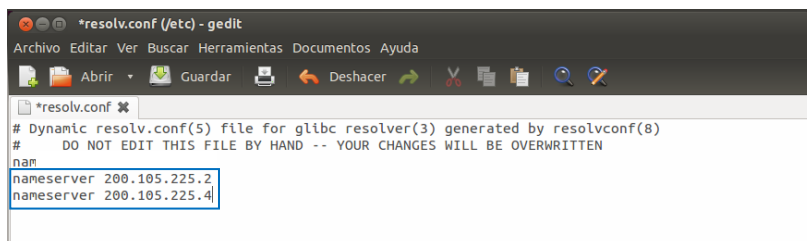


Figura D1. Configuración de la Tarjeta de Red del Servidor

Para garantizar el acceso a internet se debe configurar temporalmente el adaptador de red, con el servidor DNS proporcionado por el proveedor del servicio, en el fichero

/etc/resolv.conf (véase Figura D2), de manera que permita descargar más adelante los archivos de bind requeridos.

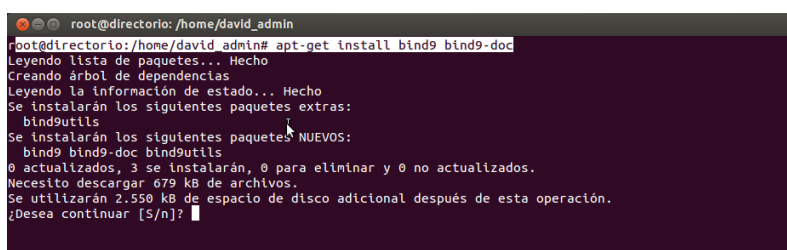


```
*resolv.conf (/etc) - gedit
Archivo Editar Ver Buscar Herramientas Documentos Ayuda
Abrir Guardar Deshacer
*resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
# DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 200.105.225.2
nameserver 200.105.225.4
```

Figura D2. Configuración de los Servidores DNS del proveedor

Finalizada la configuración es necesario reiniciar el adaptador ejecutando `/etc/init.d/networking restart`, para que se reconfigure e inicie su operación con los nuevos valores establecidos.

La instalación de bind es relativamente sencilla, al estar disponible en los repositorios de Ubuntu para su descarga, entonces mediante el comando `apt-get install bind9 bind9-doc` se instalarán y almacenarán todos los ficheros necesarios para su ejecución (véase Figura D3).



```
root@directorio: /home/david_admin
root@directorio:/home/david_admin# apt-get install bind9 bind9-doc
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
 bind9utils
Se instalarán los siguientes paquetes NUEVOS:
 bind9 bind9-doc bind9utils
0 actualizados, 3 se instalarán, 0 para eliminar y 0 no actualizados.
Necesito descargar 679 kB de archivos.
Se utilizarán 2.550 kB de espacio de disco adicional después de esta operación.
¿Desea continuar [S/n]:
```

Figura D3. Instalación de Bind 9

Adicionalmente se debe instalar un servidor web, por ejemplo apache, para iniciar la operación de bind, ejecutando `apt-get install apache2` (véase Figura D4).

```

root@directorio:/home/david_admin
root@directorio:/home/david_admin# apt-get install apache2
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
 apache2-mpm-worker apache2-utils apache2.2-bin apache2.2-common libapr1 libaprutil1
 libaprutil1-dbd-sqlite3 libaprutil1-ldap
Paquetes sugeridos:
 apache2-doc apache2-suexec apache2-suexec-custom
Se instalarán los siguientes paquetes NUEVOS:
 apache2 apache2-mpm-worker apache2-utils apache2.2-bin apache2.2-common libapr1 libaprutil1
 libaprutil1-dbd-sqlite3 libaprutil1-ldap
0 actualizados, 9 se instalarán, 0 para eliminar y 0 no actualizados.
Necesito descargar 1.843 kB de archivos.
Se utilizarán 5.590 kB de espacio de disco adicional después de esta operación.
¿Desea continuar [S/n]?

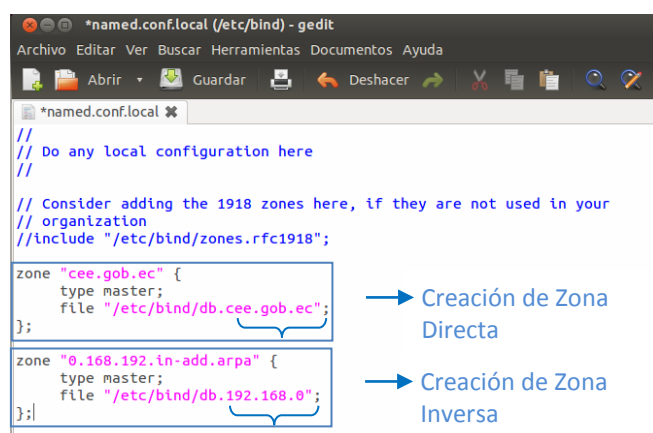
```

Figura D4. Instalación de Apache

2. CONFIGURACIÓN

La traducción de nombres de los ordenadores (servidores) de la red implica crear dos zonas, una para resolución directa, y otra para resolución inversa. La primera traducirá del dominio (pki.cee.gob.ec) a la dirección IP del servidor de certificación (192.168.0.10), y la segunda en cambio receptorá la búsqueda en la red de la dirección 192.168.0.10, y la direccionará hacia este servidor sobre el cual se está ejecutando la pki.

La configuración de estas zonas se realiza en el fichero del directorio /etc/bind/named.conf.local (véase Figura D5).



```

*named.conf.local (/etc/bind) - gedit
Archivo Editar Ver Buscar Herramientas Documentos Ayuda
Abrir Guardar Deshacer
*named.conf.local
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "cee.gob.ec" {
    type master;
    file "/etc/bind/db.cee.gob.ec";
};
zone "0.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192.168.0";
};

```

Figura D5. Configuración de zonas del servidor DNS

Los ficheros `db.cee.gob.ec` (véase Figura D6) y `db.192.168.0` (véase Figura D7) contendrán datos referentes a los servidores accesibles en la red. Para crear estos ficheros es posible usar como plantilla `/etc/bind/db.local` y `/etc/bind/db.127` respectivamente, a partir de los cuales modificar y personalizar con los datos requeridos. El directorio en el cual deben ser creados es `/etc/bind`.

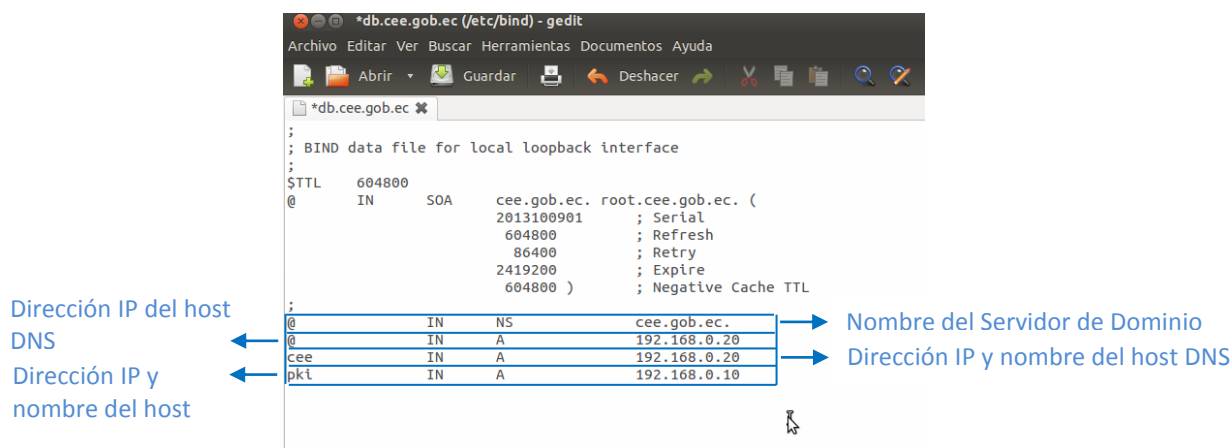


Figura D6. Fichero de configuración zona directa

Los parámetros que intervienen en este fichero indican que el dominio a resolver es `cee.gob.ec.`, el punto al final del dominio representa la raíz de éste.

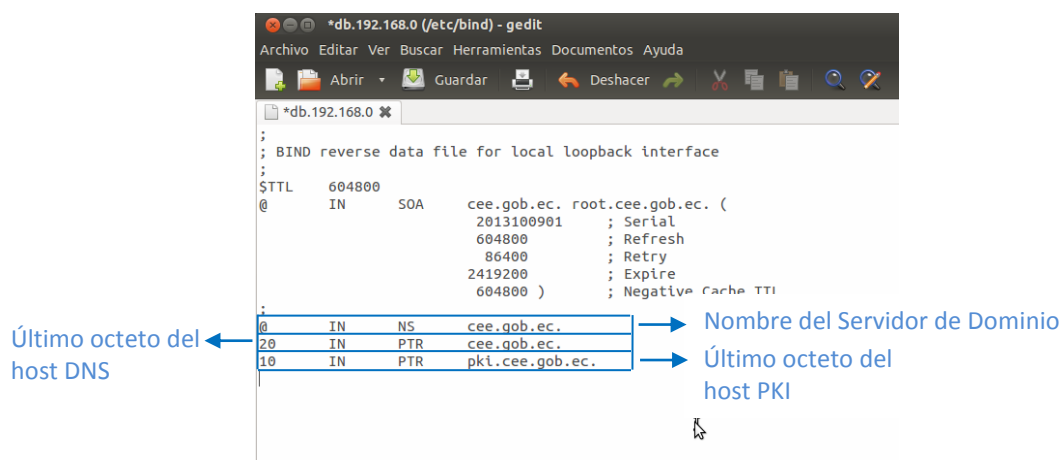


Figura D7. Fichero de configuración zona inversa

El registro PTR indica que la dirección IP para el servidor `cee.gob.ec` es `192.168.0.20`, pero omitiendo los tres primeros octetos, debido que fueron establecidos en la zona inversa del fichero `named.conf.local`; de igual manera para el servidor `pki.cee.gob.ec` (`192.168.0.10`), y todos los servidores que se requiera incluir.

La Tabla D1 describe los parámetros y registros de estos ficheros de configuración de zonas.

Una vez concluido habrá que reiniciar el servicio DNS mediante el comando `/etc/init.d/bind9 restart`, para asegurar que inicie su operación con las configuraciones efectuadas.

Finalmente hay que configurar el servidor de nombres de dominio primario en el adaptador de red, tanto del ordenador anfitrión DNS, como de todos los que conforman la red. Para el primero se debe emplear la dirección de loopback `127.0.0.1`, mientras que para el resto de servidores y ordenadores, la dirección IP del servidor `192.168.0.20`.

3. PRUEBAS DE FUNCIONAMIENTO

Al arrancar el servidor de aplicaciones, que implementa EJBCA, mediante el comando `./run.sh` desde el directorio `JBOSS_HOME/bin`, se ejecuta para acceder únicamente desde el host local, pero para acceder mediante la dirección IP de ordenador o su dominio, se debe ejecutarlo mediante `./run.sh -b 192.168.0.10`, siendo esta la dirección IP del servidor de certificación.

Tabla D1. Parámetros y Registros del fichero de configuración de zonas

Parámetros	Descripción
Serial	Es un identificador del archivo, puede tener un valor arbitrario pero se recomienda que tenga la fecha con una estructura AAAA-MM-DD y un consecutivo.
Refresh	Número de segundos que un servidor de nombres secundario debe esperar para comprobar de nuevo los valores de un registro.
Retry	Número de segundos que un servidor de nombres secundario debe esperar después de un intento fallido de recuperación de datos del servidor primario.
Expire	Número de segundos máximo que los servidores de nombre secundarios retendrán los valores antes de expirarlos.
Negative Cache TTL	Es el número de segundos que los registros se mantienen activos en los servidores NS caché antes de volver a preguntar su valor real.
<hr/> Registros <hr/>	
A (Address)	Es el registro más usado que define una dirección IP y el nombre asignado al host. Generalmente existen varios en un dominio.
MX (Mail eXchanger)	Se usa para identificar servidores de correo, se pueden definir dos o más servidores de correo para un dominio, siendo que el orden implica su prioridad. Debe haber al menos uno para un dominio.
CNAME (Canonical Name)	Es un alias que se asigna a un host que tiene una dirección IP válida y que responde a diversos nombres. Pueden declararse varios para un host.
NS (Name Server)	Define los servidores de nombre principales de un dominio. Debe haber al menos uno y pueden declararse varios para un dominio.
SOA (Start Of Authority)	Especifica el servidor DNS primario del dominio, la cuenta de correo del administrador y tiempo de refresco de los servidores secundarios (todos los parámetros anteriores).

Fuente: Creado a partir de Barrantes, H. (2009). Instalar y Configurar un servidor DNS en Ubuntu Linux. Recuperado de <http://www.codigofantasma.com/blog/instalar-y-configurar-servidor-dns-en-ubuntu-linux/>

De esta forma se puede acceder a la interfaz pública de este servidor a través del dominio <https://pki.cee.gov.ec:8442/ejbc> (véase Figura D8).

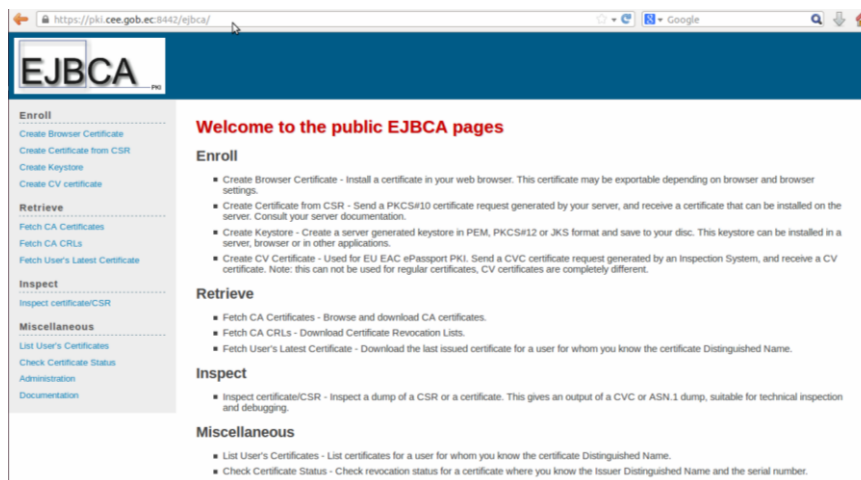


Figura D8. Interfaz de Pública de EJBCA

Para acceder a la interfaz de administración es necesario el certificado de Superadministrador que ha sido autorizado para ello, desde la opción Administration de la interfaz pública, con lo que se direccionará a través del puerto 8443 (véase Figura D9).

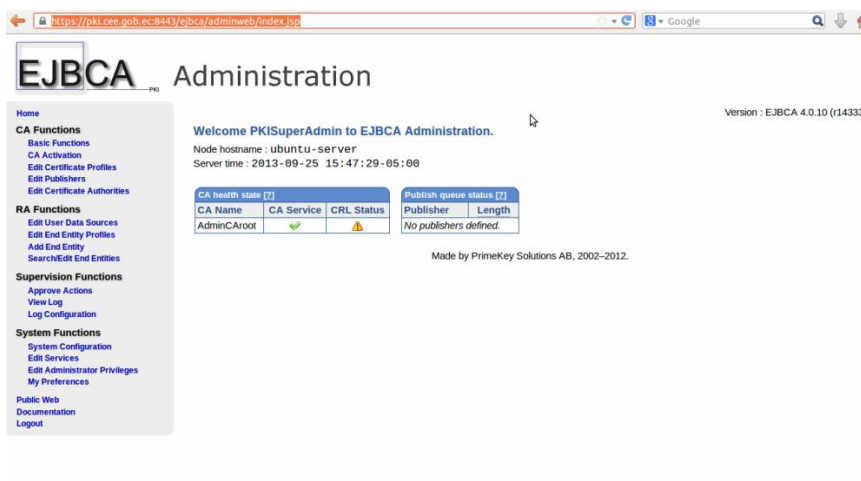


Figura D9. Interfaz de Administración de EJBCA

ANEXO E

CONFIGURACIÓN DE EJBCA VERSIÓN 4.0.10

En este anexo se detallan los procedimientos de configuración de EJBCA para iniciar su operación como servidor de certificación en el entorno del Cuerpo de Ingenieros del Ejército, y está organizada de acuerdo a un esquema que contiene las actividades implícitas en este proceso (véase Figura E1).

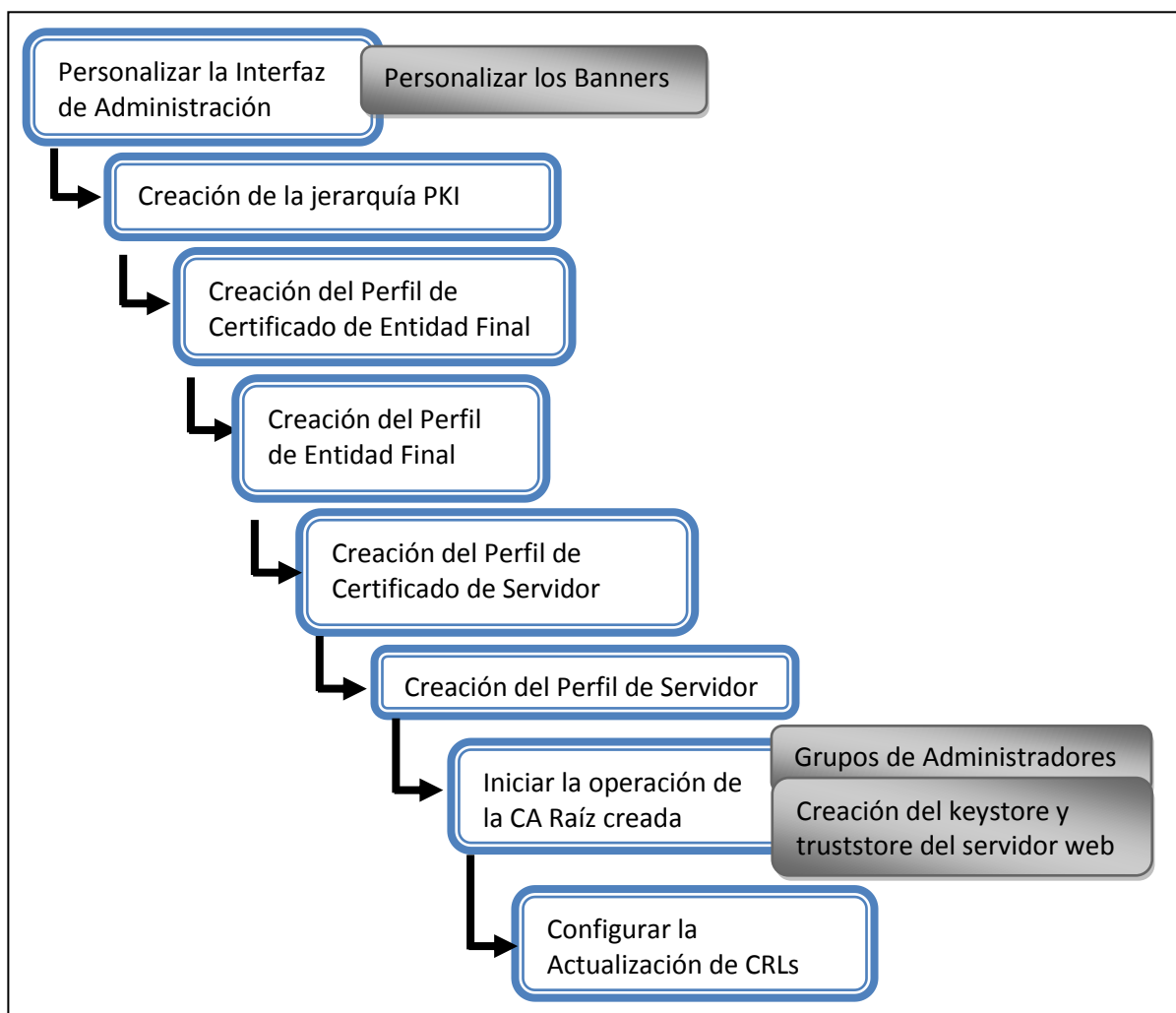


Figura E1. Etapas para habilitar la operación de la Infraestructura de Clave Pública

1. PERSONALIZAR LA INTERFAZ DE ADMINISTRACIÓN

La admin web contiene cuatro apartados que organizan sus funcionalidades, funciones de CA, de RA, de Supervisión, y del Sistema, que estarán disponibles de acuerdo al tipo de usuario administrador que se haya autenticado, en el caso del Superadministrador como usuario privilegiado, todas estas funcionalidades deben estar habilitadas.

La funcionalidad System Configuration del apartado System Functions contiene parámetros para definir las características de apariencia y funcionamiento del sistema, la Tabla E1 describe estos parámetros y los valores que fueron configurados en este proyecto.

Tabla E1. Configuración Web EJBCA

Funcionalidad	Descripción
Title	Define el título del sitio
Head Banner Foot Banner	Es el nombre del archivo JSP o HTML que contiene las imágenes que aparecen en la cabecera y fin de página, almacenados en el directorio de los banners
Enable End Entity Profile Limitations	Permite mantener un control de acceso sobre entidades finales para definir cuáles pueden administrar una RA por ejemplo. Habilitado
Enable Key Recovery	Posibilita la recuperación de par claves en caso de pérdida. Habilitado
Issue Hardware Tokens	Si se tiene planificado emitir tokens de hardware. Deshabilitado
Use Approval Notifications	Para enviar emails cada vez que se procese una aprobación, en este caso no se usará esta funcionalidad
Enable Command Line Interface Access	Permitir el acceso para el Superadministrador, hacia la Interface de Línea de Comandos local (CLI). Habilitado
Preferred Language Secondary Language	Es el lenguaje por defecto y secundario que se usará en la página web

Fuente: Elaborado a partir de Osorio, J. M. (s.f.). *Evaluación de la Herramienta EJBCA para un prestador de Servicios de Certificación*. (Proyecto Final de Carrera). Universidad Politécnica de Cataluña, Barcelona, España.

1.1. Personalizar los Banners

Los banners son ficheros que contienen código e imágenes que definen la apariencia de la página web de administración, por ejemplo la imagen que aparece en el encabezado, o el texto al pie de la página. Pueden ser de extensión HTML o JSP y están almacenados en el sistema con la posibilidad de ser reemplazados o personalizados de acuerdo a las necesidades.

La manera más sencilla es reemplazar parámetros que emplean los ficheros actuales, como la imagen de cabecera en `head_banner.jsp`, o el texto del pie de página en `foot_banner.jsp`, evitando de esta forma la edición del código de los mismos. Están almacenados en `EJBCA_HOME /modules/admin-gui/resources/banners/`.

El directorio `EJBCA_HOME/modules/admin-gui/resources/images` contiene la imagen de encabezado, es posible reemplazarla conservando el nombre original `banner_ejbca-admin.png` (véase Figura E2), para que se muestre una imagen representativa del CEE.

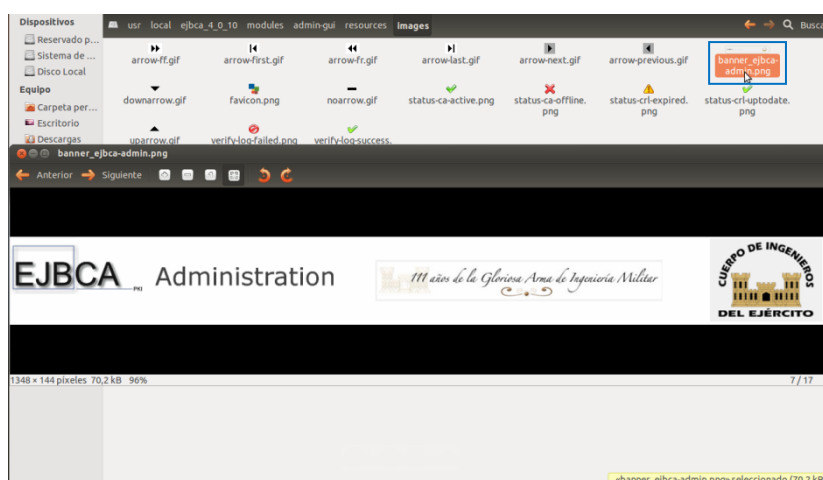


Figura E2. Personalizar la imagen de encabezado de la interfaz web de administración

En el pie de página de la interfaz web de administración se muestra una secuencia de texto configurado en `foot_banner.jsp`, para modificarlo acceder al directorio `EJBCA_HOME/modules/admin-gui/resources/languages`, y editar el parámetro `MADEBYPRIMEKEY`.

Este directorio contiene todos los lenguajes disponibles para la interfaz gráfica, de manera que este parámetro tendrá un valor diferente para cada uno de los idiomas, de esta forma, se ha editado tanto en el idioma primario que es el inglés (`languagefile.en.properties`), como en el secundario español (`languagefile.es.properties`) (véase Figura E3).

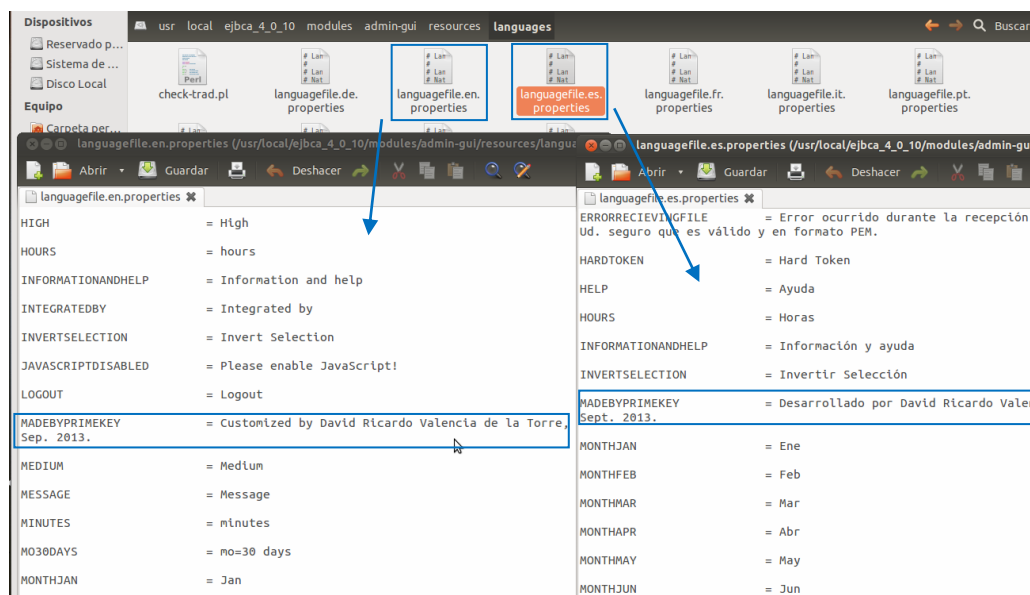


Figura E3. Personalizar el texto del pie de página de la interfaz web de administración

De igual manera, se ha modificado la imagen de encabezado de la interfaz web pública de EJBCA, accediendo al directorio `EJBCA_HOME/modules/publicwebgui/resources/images`, y reemplazando la imagen `logotype.png` por una representativa del CEE, conservando el mismo nombre (véase Figura E4).

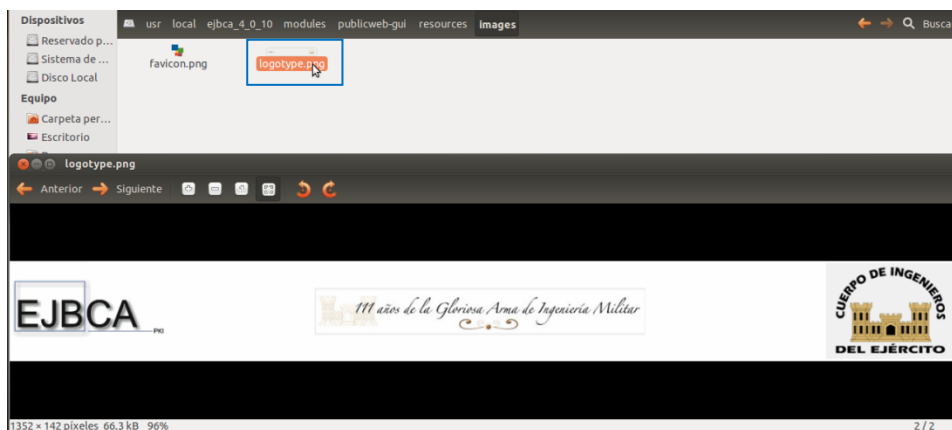


Figura E4. Personalizar la imagen de encabezado de la interfaz web pública

Finalmente para visualizar estas modificaciones se debe ejecutar el comando `ant deploy` de acuerdo a como se lo realizó en el proceso de instalación de EJBCA. Las Figuras E5 y E6 muestran la personalización de la interfaz de administración y pública, respectivamente.

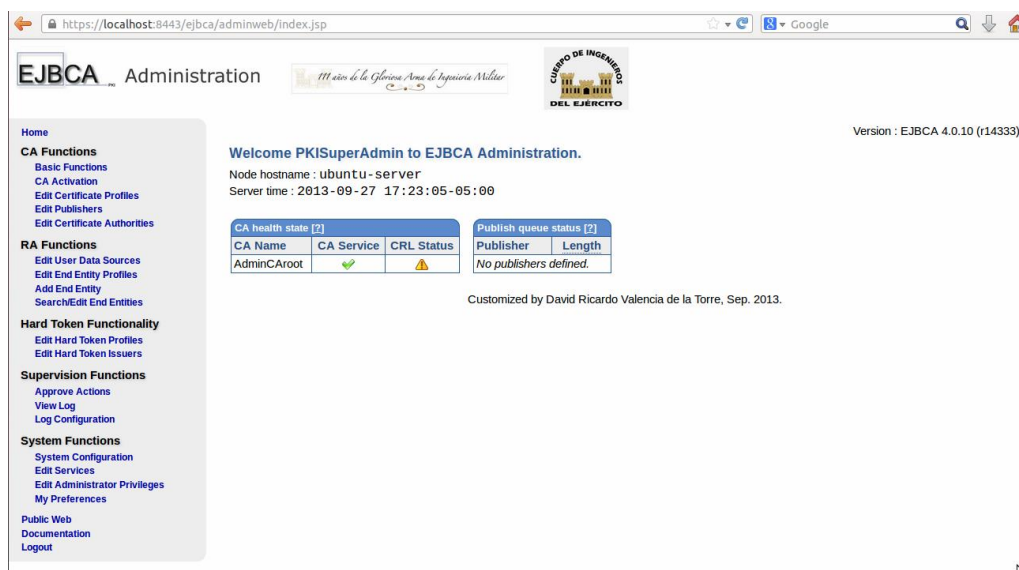


Figura E5. Cambios realizados en la interfaz de administración

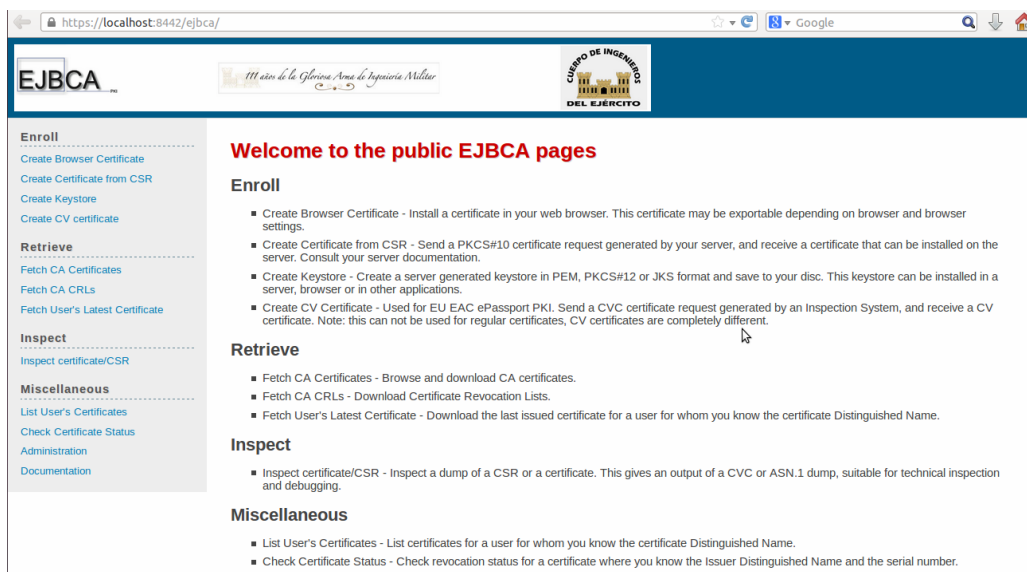


Figura E6. Cambios realizados en la interfaz pública

2. CREACIÓN DE LA JERARQUÍA PKI

La creación de la CA raíz del CEE se la realiza desde la opción Edit Certificate Authorities del apartado CA Functions, definir el nombre de la nueva autoridad en Add CA (en este caso Autoridad Certificadora CEE) y luego clic en Create (véase Figura E7).

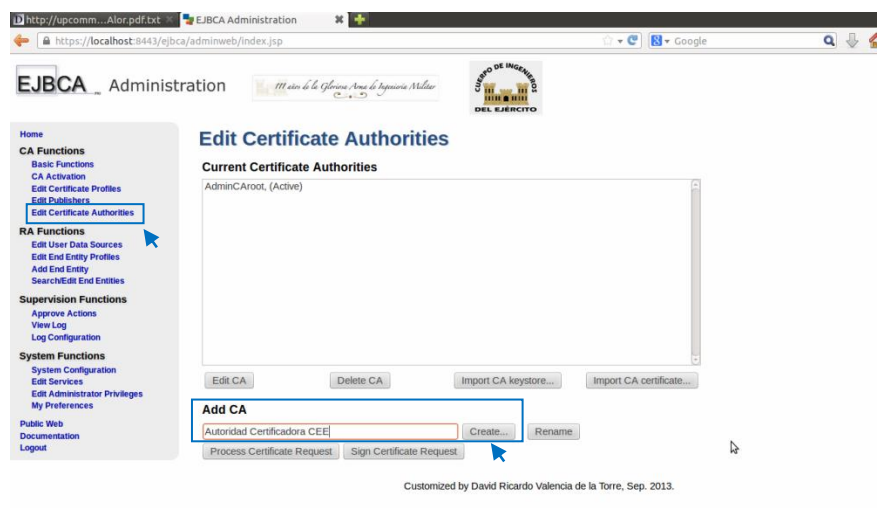


Figura E7. Creación de la nueva CA raíz

La mayoría de las configuraciones definidas por defecto al crear la CA, permiten su operatividad, pero se han realizado algunos cambios para que se ajusten más a nuestros propósitos (véase Tabla E2); para ello seleccionar la CA creada y Edit CA.

Tabla E2. Creación y Configuración de la CA

Parámetro	Valor
Type of CA	X.509 (CA que emite certificados basados en el estándar oficial X.509, pero EJBCA permite también el establecimiento de una CVC, que es una CA que emite certificados de CV, que son especiales para pasaportes electrónicos)
CA token Type	Soft
Signing Algorithm	SHA1WithRSA (Algoritmo de firma digital del certificado de la CA)
RSA key size	2048 (longitud del par clave criptográfico RSA)
Description	Entidad de Certificación CEE
Validity	3650d (10 años de validez del certificado de la CA)
Subject DN (del certificado)	CN=Autoridad Certificadora CEE,OU=Entidad de Certificación,O=Cuerpo de Ingenieros del Ejército,C=EC
Signed By	Self Signed (autofirmar el certificado)
Certificate Profile	ROOTCA (Tipo de CA – raíz, intermedia o subordinada)
Use Issuing Distribution Point on CRLs	Habilitado (Habilitar los repositorios de distribución de CRLs)
Default CRL Dist. Point	http://pki.cee.gob.ec:8080/ejbca/publicweb/webdist/cerdist?cmd=crl&issuer=CN=Autoridad%20CEE,OU=Entidad%20de%20Certificación,O=Cuerpo%20de%20Ingenieros%20del%20Ejército,C=EC (Este valor se autogenera)
CRL Expire Period	1d (para que se genere la actualización de las CRLs diariamente)
CRL Overlap Time	10m (para que la nueva CRL se genere 10 minutos antes de que expire la anterior)

Fuente: Elaborado a partir de Osorio, J. M. (s.f.). *Evaluación de la Herramienta EJBCA para un prestador de Servicios de Certificación*. (Proyecto Final de Carrera). Universidad Politécnica de Cataluña, Barcelona, España.

3. CREACIÓN DEL PERFIL DE CERTIFICADO DE ENTIDAD FINAL

Previo a iniciar la emisión de certificados para los funcionarios, militares del CEE, es necesario definir ciertos parámetros del certificado y de estos usuarios, que van a ser empleados en su creación. Este perfil de certificado contendrá los parámetros netamente referentes al certificado, por ejemplo su periodo de validez, o los propósitos para los que fue emitido (cifrado, firma digital, no repudio, etc.).

EJBCA de forma predeterminada contiene plantillas de estos perfiles de certificado (de nombre FIXED), a partir de los cuales se puede crear y configurar los nuevos perfiles; para ello acceder a la opción **Edit Certificate Profiles** del apartado **CA Functions**, escribir el nombre del perfil (en este caso **PERFIL_ENTIDAD_FINAL**), seleccionar como plantilla **ENDUSER (FIXED)**, y **Use selected as template** (véase Figura E8).

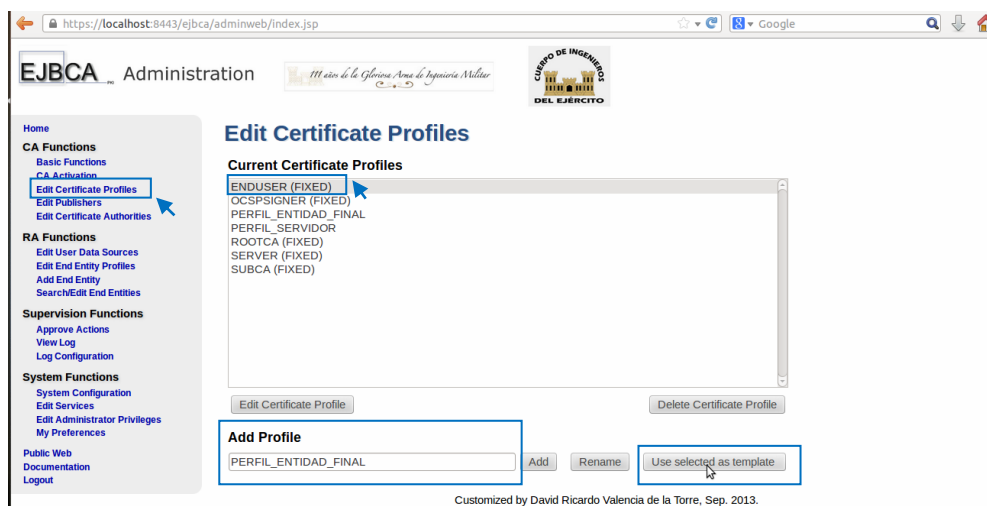


Figura E8. Creación de un nuevo perfil de certificado en base a una plantilla

Con esto se ha creado y está disponible el nuevo perfil, acceder a su página de edición mediante la opción **Edit Certificate Profile** y realizar los cambios necesarios, en el caso de este proyecto la Tabla E3 muestra sus parámetros de configuración.

Tabla E3. Configuración del Perfil del Certificado – Entidad Final

Parámetro	Valor
Available bit lengths	1024, 2048, 4096 (los valores disponibles para definir la longitud del par clave criptográfica)
Validity (*y *mo *d) or end date of the certificate	365d (periodo de validez en días)
Key Usage	Digital Signature, Non-repudiation, Key encipherment, Data encipherment (significa que ha sido emitido para efectuar estas operaciones)
Extended Key Usage	Client Authentication, Email Protection (son operaciones adicionales)
CRL Distribution Points	Use (para que la CA publique permanentemente las CRLs en repositorios)
Use CA defined CRL Dist. Point	Habilitado (para que estos certificados sean incluidos en la CRL publicada permanentemente por la CA)
Authority Information Access	Habilitado
Use CA defined OCSP locator	Habilitado
Available CAs	Autoridad Certificadora CEE (es la CA disponible que emitirá estos certificados de usuario)

Fuente: Elaborado a partir de EJBCA PKI BY PRIME KEY. (2013). *PrimeKey Support, Development and Maintenance Services – EJBCA Installation*. Recuperado de <http://www.ejbca.org/installation.html>
MAJIC.RS. (2011). *Revision of Setting-up EJBCA as Certification Authority*. Recuperado de <http://majic.rs/node/50/revisions/52/view>

4. CREACIÓN DEL PERFIL DE ENTIDAD FINAL

Este perfil complementa el certificado de usuario final, al contener información referente al usuario, por ejemplo los atributos del Distinguished Name, la organización a la que pertenece, su correo electrónico, el país, entre otros.

Para crear este perfil acceder a la opción Edit End Entity Profile del apartado RA Functions, escribir el nombre del perfil (en este caso PERSONAS) y adicionarlo. Ingresar en la página de edición del perfil creado y personalizarlo con los datos requeridos, para este

proyecto se consideraron los datos del Cuerpo de Ingenieros del Ejército como entidad (véase Tabla E4).

Tabla E4. Configuración del Perfil de Entidad Final

Parámetro	Valor
Subject DN Attributes	
E-mail Domain	cee.gob.ec (es el dominio de correo del Cuerpo de Ingenieros del Ejército)
O, Organization	Cuerpo de Ingenieros del Ejército
C, Country (ISO 3166)	EC
RFC 822 Name (e-mail address)	Required (para que el campo del correo de usuario forme parte del certificado)
Default Certificate Profile	PERFIL_ENTIDAD_FINAL (este perfil de entidad va a estar disponible de forma predeterminada para este perfil de certificado)
Available Certificate Profiles	PERFIL_ENTIDAD_FINAL (si se ha creado algunos perfiles de certificado, es posible habilitar este perfil de entidad para algunos de ellos)
Default CA	Autoridad Certificadora CEE (es la CA por defecto que emitirá y gestionará certificados con este perfil)
Available CAs	Autoridad Certificadora CEE (para utilizarlo en más de una CA de la jerarquía)
Default Token	P12 file (es el tipo de extensión con la que se generará el certificado)
Number of allowed requests	1 (se permitirá al usuario previamente registrado, descargar su certificado una sola vez, la siguiente vez que intente hacerlo se generará un error y no permitirá la descarga)
Key Recoverable	Use (posibilita la recuperación del par clave criptográfico, obviamente en casos justificados)

Fuente: Elaborado a partir de EJBCA PKI BY PRIME KEY. (2013). *PrimeKey Support, Development and Maintenance Services – EJBCA Installation*. Recuperado de <http://www.ejbca.org/installation.html>
 MAJIC.RS. (2011). *Revision of Setting-up EJBCA as Certification Authority*. Recuperado de <http://majic.rs/node/50/revisions/52/view>

En la sección **Subject DN Attributes**, de esta página de edición del perfil, se pueden adicionar y remover campos que integran el Distinguished Name, y se ha definido con anterioridad que los que deben incluirse para este proyecto son el Common Name (CN),

Unique Identifier (UID), Organization (O), Organizational Unit (OU), y el Country (C); adicionalmente en la sección Other Subject Attributes es necesario incluir el campo RFC 822 Name (e-mail address), para que en el certificado se incluya la dirección de correo electrónico del usuario.

En cada uno de estos campos, como en muchos otros de esta página de edición, existen las opciones Required y Modifiable, si se habilita la primera significa que este es un campo que debe ser llenado obligadamente durante el proceso de registro de usuarios, en el caso de habilitar la segunda, el campo generalmente debe aparecer vacío, para ingresar los datos del usuario, pero si se ha escrito algún texto de sugerencia sobre él, podrá ser modificado libremente.

También existen las opciones Use y Default para algunos campos, de manera que al habilitar la primera se incluye este campo en la página de registro de usuarios finales efectuada por la RA, y la segunda para que el texto ingresado aparezca por defecto y no sea modificable.

De esta forma se ha configurado este perfil con las opciones Required y Modifiable habilitadas en los campos Common Name (CN), Unique Identifier (UID), para permitir ingresar el nombre del usuario y el departamento de la institución en el que labora el funcionario o militar, respectivamente; los demás campos del Subject DN Attributes tendrán valores predefinidos en la Tabla E4, que no podrán ser modificados, debido a que son valores que identifican a la institución.

5. CREACIÓN DEL PERFIL DE CERTIFICADO DE SERVIDOR

También se debe generar un perfil de certificado para los servidores de la organización, en este proyecto se utilizará para generar certificados SSL destinados a la CA Raíz configurada con anterioridad, y al servidor de correo zimbra que será diseñado posteriormente. Los pasos a seguir son los mismos que en el de entidad final, lo que difiere es la definición del nombre del perfil, en este caso PERFIL_SERVIDOR, y seleccionar como plantilla el perfil SERVER (FIXED). La Tabla E5 muestra las configuraciones que se realizaron sobre éste perfil, y varias explicaciones.

Tabla E5. Configuración del Perfil del Certificado - Servidor

Parámetro	Valor
Available bit lengths	1024, 2048, 4096 (los valores disponibles para definir la longitud del par clave criptográfica)
Validity (*y *mo *d) or end date of the certificate	365d (periodo de validez en días)
Key Usage	Digital Signature, Key encipherment (significa que ha sido emitido para efectuar estas operaciones)
Extended Key Usage	Server Authentication (son operaciones adicionales)
CRL Distribution Points	Use (para que la CA publique permanentemente las CRLs en repositorios)
Use CA defined CRL Dist. Point	Habilitado (para que estos certificados sean incluidos en la CRL publicada permanentemente por la CA)
Authority Information Access	Habilitado
Use CA defined OCSP locator	Habilitado
Available CAs	Autoridad Certificadora CEE (es la CA disponible que emitirá estos certificados de usuario)

Fuente: Elaborado a partir de EJBCA PKI BY PRIME KEY. (2013). *PrimeKey Support, Development and Maintenance Services – EJBCA Installation*. Recuperado de <http://www.ejbca.org/installation.html>
 MAJIC.RS. (2011). *Revision of Setting-up EJBCA as Certification Authority*. Recuperado de <http://majic.rs/node/50/revisions/52/view>

6. CREACIÓN DEL PERFIL DE SERVIDOR

Por su parte este perfil complementa el certificado de dispositivo final, al contener información referente a los servidores. En la opción **Edit End Entity Profile** del apartado **RA Functions**, escribir el nombre del perfil (en este caso **SERVIDORES**), adicionarlo y acceder a la página de edición del perfil creado para personalizarlo. La Tabla E6 muestra las configuraciones que se realizaron sobre éste perfil, y varias explicaciones.

Tabla E6. Configuración del Perfil de Servidor

Parámetro	Valor
Batch generation (clear text pwd storage)	Use
E-mail Domain	cee.gob.ec (es el dominio de correo del Cuerpo de Ingenieros del Ejército)
O, Organization	Cuerpo de Ingenieros del Ejército
C, Country (ISO 3166)	EC
RFC 822 Name (e-mail address)	Required (para que el campo del correo de usuario forme parte del certificado)
Default Certificate Profile	PERFIL_SERVIDOR (este perfil de entidad va a estar disponible de forma predeterminada para este perfil de certificado)
Available Certificate Profiles	PERFIL_SERVIDOR (si se ha creado algunos perfiles de certificado, es posible habilitar este perfil de entidad para algunos de ellos)
Default CA	Autoridad Certificadora CEE (es la CA por defecto que emitirá y gestionará certificados con este perfil)
Available CAs	Autoridad Certificadora CEE (para utilizarlo en más de una CA de la jerarquía)
Default Token	PEM file (es el tipo de extensión con la que se generará el certificado)
Number of allowed requests	1 (se permitirá al usuario previamente registrado, descargar su certificado una sola vez, la siguiente vez que intente hacerlo se generará un error y no permitirá la descarga)
Key Recoverable	Deshabilitado (posibilita la recuperación del par clave criptográfico, obviamente en casos justificados)

Fuente: Elaborado a partir de EJBCA PKI BY PRIME KEY. (2013). *PrimeKey Support, Development and Maintenance Services – EJBCA Installation*. Recuperado de <http://www.ejbca.org/installation.html>
 MAJIC.RS. (2011). *Revision of Setting-up EJBCA as Certification Authority*. Recuperado de <http://majic.rs/node/50/revisions/52/view>

7. INICIAR LA OPERACIÓN DE LA CA RAÍZ CREADA

La emisión del certificado para el nuevo usuario Super-administrador se la realiza desde la opción Add End Entity del apartado RA Functions, de la interfaz de administración, seleccionar el perfil de entidad final PERSONAS creado en los procesos anteriores, y definir los datos de este usuario de la PKI del CEE (véase Figura E9).

The screenshot shows the 'Add End Entity' form in the EJBCA Administration interface. The form is titled 'Add End Entity' and is located in the 'RA Functions' section. The 'End Entity Profile' is set to 'PERSONAS'. The 'Username' is 'SuperAdministrador', the 'Password' and 'Confirm Password' are masked, and the 'E-mail address' is 'sadmin@cee.gob.ec'. The 'Subject DN Attributes' section includes 'CN, Common name' (Administrador Autoridad Certificadora), 'UID, Unique Identifier' (Departamento de Sistemas), 'O, Organization' (Cuerpo de Ingenieros del Ejercito), 'OU, Organizational Unit' (Entidad Final CEE), and 'C, Country (ISO 3166)' (EC). The 'Other subject attributes' section includes 'Subject Alternative Name' (RFC 822 Name (e-mail address) is checked). The 'Main certificate data' section includes 'Certificate Profile' (PERFIL_ENTIDAD_FINAL), 'CA' (Autoridad Certificadora CEE), and 'Token' (P12 file). The 'Other data' section includes 'Key Recoverable' (unchecked). The 'Add' button is highlighted with a blue arrow.

Figura E9. Registro de un usuario con requerimientos de certificación - Superadministrador

Al finalizar este registro se mostrará un mensaje End Entity SuperAdministrador added successfully indicando que todo se ha realizado con normalidad, el parámetro RFC 822 Name (e-mail address) fue habilitado para que el correo del usuario forme parte de su certificado.

De este modo el usuario, en este caso Super-administrador, puede obtener su certificado desde su ordenador e importarlo en el sistema operativo, a través de la interfaz web pública,

accediendo a la opción Create Browser Certificate del apartado Enroll, e ingresando las credenciales (usuario y contraseña) que fueron acordadas durante el registro (véase Figura E10).

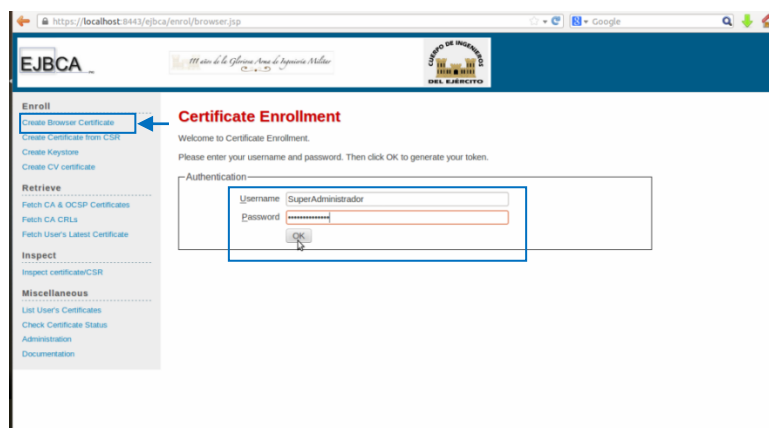


Figura E10. Ingresar las credenciales para generar el certificado

Con ello habrá que definir la longitud del par clave criptográfico que va a ser creado, y cerciorarse de que el perfil de certificado asignado sea el de entidad final, en el caso que esté asignado otro por defecto (véase Figura E11).

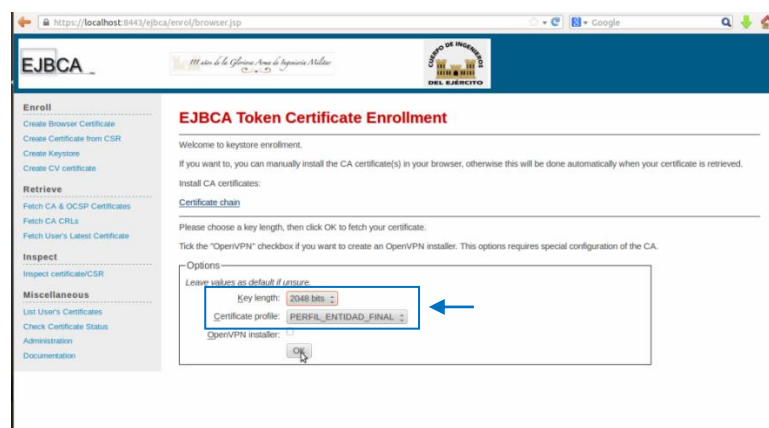


Figura E11. Definir la longitud del par clave

Se obtendrá un archivo de extensión .p12 que deberá ser importado al sistema operativo del ordenador cliente, y al navegador web (en el caso de utilizar Mozilla Firefox, debido a que

no utiliza el almacén de certificados de Windows), en el momento que solicite la contraseña, ésta debe ser la que se ha predefinido en el registro. Si se ha realizado correctamente la importación aparecerá un mensaje como el de la Figura E12.

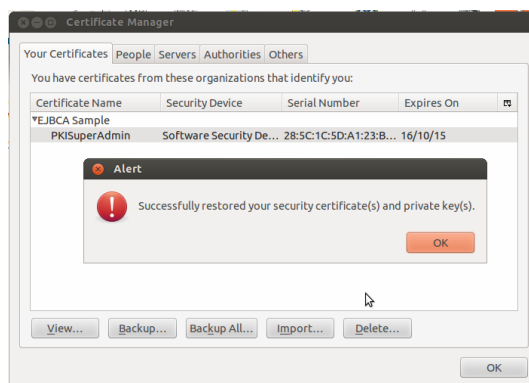


Figura E12. Importación del Certificado en el navegador

7.1. Grupos de Administradores

EJBCA es una herramienta que se basa en componentes para implantar una PKI completamente funcional, debido a esto admite distintos tipos de administradores que desempeñan actividades relacionadas con el componente PKI que se les ha delegado, de esta forma se distribuyen eficientemente las actividades de administración, y aumentan los niveles de seguridad.

Estos administradores y las actividades que realizan, son descritos y organizados de acuerdo a su importancia en la Tabla E7.

La administración de una PKI debe ser efectuada por un solo Super-administrador, pueden existir varias CAs intermedias y subordinadas dentro de la jerarquía, por lo que se debe asignar un administrador de CA independiente por cada una; cada CA dispondrá de una o

varias RAs, y de igual manera cada una de ellas debe tener un administrador de RA independiente. Los supervisores no son tan indispensables, pero debería asignarse uno por cada CA.

Tabla E7. Tipos de Administradores de EJBCA

Tipo	Actividades
Superadministrador	Este administrador tiene acceso a todo el sistema y puede: <ul style="list-style-type: none"> - Editar la configuración de todo el sistema - Crear publishers - Crear, editar, eliminar, activar y desactivar CAs - Crear superadministradores y administradores de CA
Administrador de CA	Puede administrar una CA: <ul style="list-style-type: none"> - Crear administradores de RA - Administrar perfiles de certificado y de entidad final de usuarios finales - Configurar las opciones de almacenamiento de logs de la CA Realizar tareas de administrador RA y de supervisor
Administrador de RA	Puede administrar una RA: <ul style="list-style-type: none"> - Añadir, consultar, editar y eliminar usuarios finales - Consultar, editar, eliminar y revocar certificados de usuarios finales Realizar tareas de supervisor
Supervisor	Puede supervisar CAs y RAs: <ul style="list-style-type: none"> - Ver los logs para observar quién ha hecho qué. - Consultar datos de usuarios y de sus certificados

Fuente: Creado a partir de Osorio, J. M. (s.f.). *Evaluación de la Herramienta EJBCA para un prestador de Servicios de Certificación*. (Proyecto Final de Carrera). Universidad Politécnica de Cataluña, Barcelona, España.

Todas estas consideraciones de administración pueden efectuarse en entornos PKI de gran dimensión, pero para propósitos de este proyecto, al disponer de una sola CA raíz que certificará directamente a usuarios finales, con la ayuda de una RA, es suficiente con crear un usuario Super-administrador para sobrellevar las actividades de administración de la PKI del CEE; no obstante, en etapas futuras considerando la aceptación y concientización por parte de los usuarios, referente a los beneficios y la necesidad de implementar este sistema de

seguridad, se podría complementarla con CAs y RAs adicionales, y obviamente los administradores y supervisores respectivos.

Previo a la creación de un administrador, de cualquier tipo que sea, es necesario crear un Administrator Group desde la interfaz de administración de EJBCA, en la opción Edit Administrator Privileges del apartado System Functions, presionar Add (véase Figura E13), e ingresar el nombre del grupo deseado.

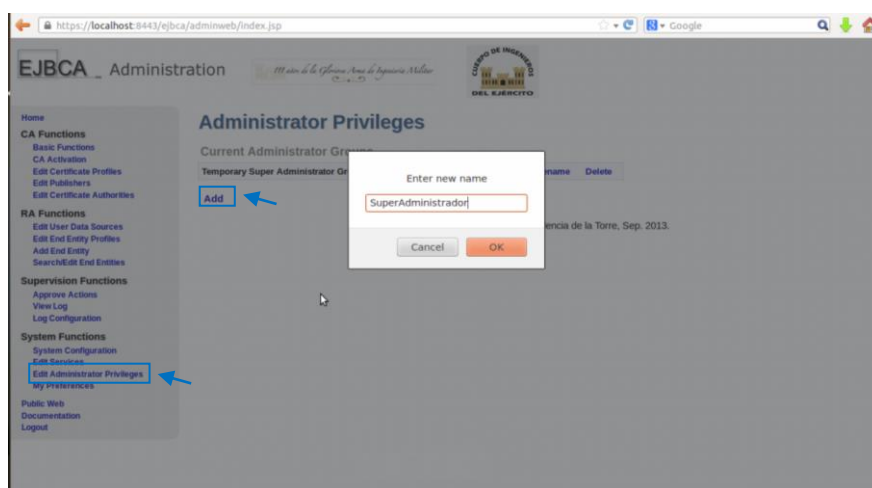


Figura E13. Crear el Administrator Group

La asignación de privilegios en esta herramienta es efectuada en base a diversos parámetros del certificado del administrador, como la organización, el Common Name, el UID, el país, entre otros; de los cuales se ha decidido establecer el número de serie como valor de comparación, por ser un parámetro que lo identifica de manera única.

Para ello, en el grupo creado acceder a la opción Administrators, completar los campos con datos del certificado de administrador que se ha emitido, y la CA desplegada (véase Tabla E8).

Tabla E8. Asignación de la CA que gestionará el Super-administrador

Parámetro	Valor
CA	Autoridad Certificadora CEE (es la CA que será gestionada por este administrador)
Match with	Certificate Serial Number (Definir el número de serie del certificado como valor de comparación para garantizar el acceso a la interfaz web de administración EJBCA)
Match Type	Equal, case sens. (valida el certificado de administrador sólo si el número de serie es el que se define en el siguiente campo)
Match Value	632D47FC7F6C88C5 (es el número de serie del certificado sin incluir los :)

Fuente: Elaborado a partir de EJBCA PKI BY PRIME KEY. (2013). *PrimeKey Support, Development and Maintenance Services – EJBCA Installation*. Recuperado de <http://www.ejbca.org/installation.html>

MAJIC.RS. (2011). *Revision of Setting-up EJBCA as Certification Authority*. Recuperado de <http://majic.rs/node/50/revisions/52/view>

Para conocer este número de serie ingresar en el administrador de certificados del navegador web en el que fue instalado (véase Figura E14).

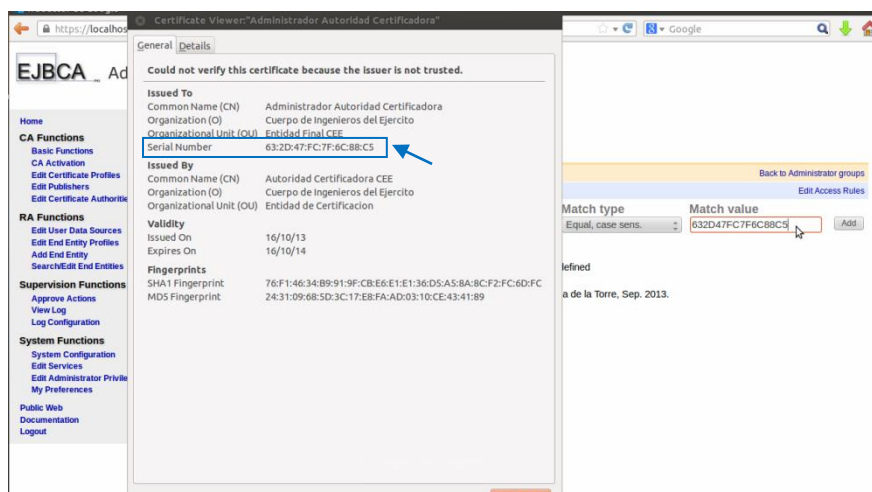


Figura E14. Número de Serie del Certificado del Administrador

Con esto se asegura que únicamente el certificado con este número de serie, esté en capacidad de acceder a la interfaz web de administración de la CA, en este caso la Autoridad

Certificadora CEE raíz, considerando que una CA no puede emitir certificados con el mismo número de serie.

Finalmente en el mismo enlace de configuración Administrators, acceder a Edit Access Rules, esta opción permite definir el rol que cumplirá este administrador dentro de la jerarquía PKI (véase Figura E15); es decir, si será Super Administrator, CA Administrator, RA Administrator o Supervisor.

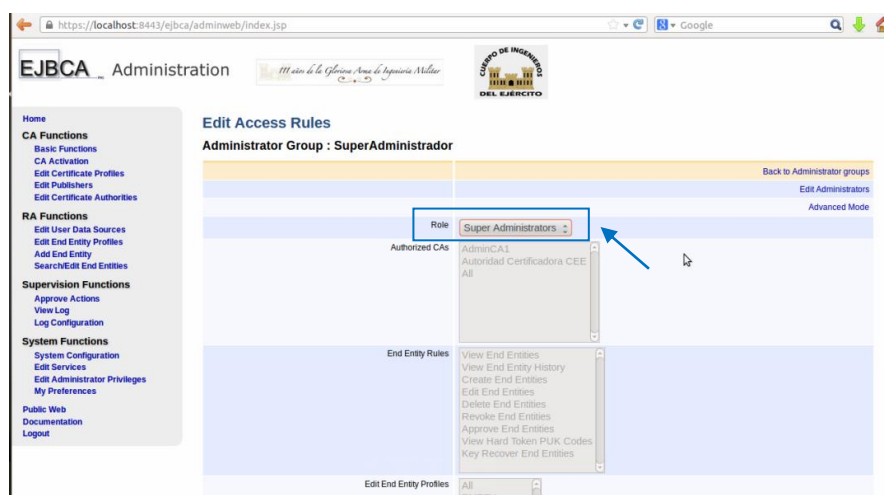


Figura E15. Asignación del rol de Super Administrador

7.2. Crear un nuevo keystore y truststore para el servidor Web EJBCA

El propósito de crear un nuevo keystore y truststore es almacenar sobre ellos los certificados y las claves de administrador, de manera que EJBCA interprete que son certificados de confianza, y permita el acceso a la interfaz web de administración.

Se necesita crearlos por el motivo de que durante la instalación de EJBCA se generaron de manera temporal una CA, un Superadministrador y un certificado de Superadministrador con su par clave, que fueron creados con parámetros predeterminados, por eso no sería viable

emplearlos en un entorno de producción real, más bien la intención es iniciar la operación de la nueva CA, el nuevo Superadministrador, y su certificado de acceso a la admin web creados, y deshabilitar todos los componentes temporales.

Esto requiere emitir un certificado para el servidor web de EJBCA desde la opción Add End Entity del apartado RA Functions de la interfaz de administración, y completar la información de registro con datos del servidor (véase Figura E16), aclarando que se debe especificar la misma contraseña que fue establecida en el campo ejbca_https_keystore_password del fichero web.properties, durante la instalación.

The screenshot shows the 'Add End Entity' form in the EJBCA Administration interface. The form is divided into several sections:

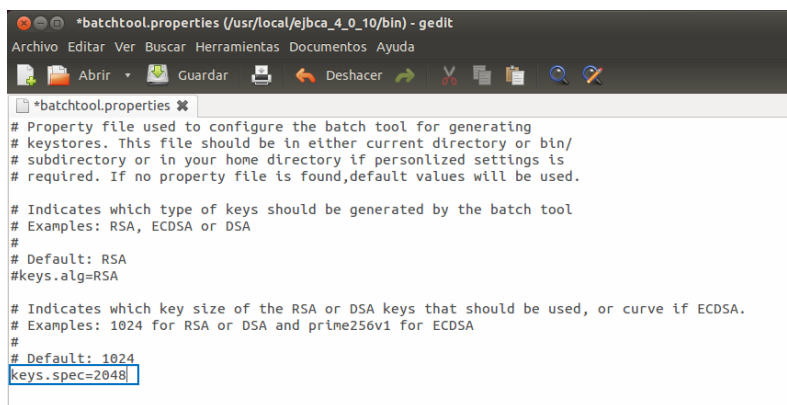
- End Entity Profile:** SERVIDORES (Required)
- Username:** pki.cee.gob.ec_ejbca (Required)
- Password:** [Redacted] (Required)
- Confirm Password:** [Redacted]
- Batch generation (clear text pwd storage):**
- E-mail address:** ejbca@cee.gob.ec
- Subject DN Attributes:**
 - CN, Common name: Autoridad Certificadora CEE (Required)
 - OU, Organizational Unit: Servidor CEE
 - O, Organization: Cuerpo de Ingenieros del Ejercito
 - C, Country (ISO 3166): EC
- Other subject attributes:**
 - RFC 822 Name (e-mail address): Use data from E-mail address field
 - DNS Name: pki.cee.gob.ec
- Main certificate data:**
 - Certificate Profile: PERFIL_SERVIDOR (Required)
 - CA: Autoridad Certificadora CEE (Required)
 - Token: JKS file (Required)

Buttons: Add, Reset

Customized by David Ricardo Valencia de la Torre, Sep. 2013.

Figura E16. Registro del Servidor Web EJBCA

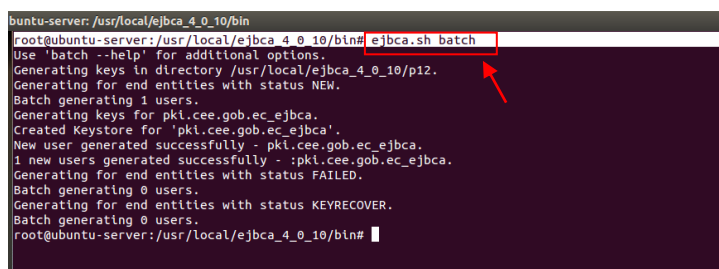
En el servidor CA modificar el fichero EJBCA_HOME/bin/batchtool.properties y agregar la longitud del par clave que va a ser creado (véase Figura E17).



```
*batchtool.properties (/usr/local/ejbca_4_0_10/bin) - gedit
Archivo Editar Ver Buscar Herramientas Documentos Ayuda
Abrir Guardar Deshacer
*batchtool.properties ✕
# Property file used to configure the batch tool for generating
# keystores. This file should be in either current directory or bin/
# subdirectory or in your home directory if personalized settings is
# required. If no property file is found, default values will be used.
# Indicates which type of keys should be generated by the batch tool
# Examples: RSA, ECDSA or DSA
#
# Default: RSA
#keys.alg=RSA
# Indicates which key size of the RSA or DSA keys that should be used, or curve if ECDSA.
# Examples: 1024 for RSA or DSA and prime256v1 for ECDSA
#
# Default: 1024
keys.spec=2048
```

Figura E17. Longitud del par clave del Servidor Web EJBCA

La generación del keystore se realiza mediante la interfaz de línea de comandos de EJBCA (CLI), desde el directorio `$EJBCA_HOME/bin` (véase Figura E18).



```
buntu-server: /usr/local/ejbca_4_0_10/bin
root@ubuntu-server: /usr/local/ejbca_4_0_10/bin# ejbca.sh batch
Use 'batch --help' for additional options.
Generating keys in directory /usr/local/ejbca_4_0_10/p12.
Generating for end entities with status NEW.
Batch generating 1 users.
Generating keys for pki.cee.gob.ec_ejbca.
Created Keystore for 'pki.cee.gob.ec_ejbca'.
New user generated successfully - pki.cee.gob.ec_ejbca.
1 new users generated successfully - :pki.cee.gob.ec_ejbca.
Generating for end entities with status FAILED.
Batch generating 0 users.
Generating for end entities with status KEYRECOVER.
Batch generating 0 users.
root@ubuntu-server: /usr/local/ejbca_4_0_10/bin#
```

Figura E18. Generación del Keystore del servidor

Adicionalmente desde esta interfaz se creará el truststore, que identifica cuales certificados son de confianza para acceder a la interfaz web de administración de la CA (véase Figura E19). Cuando solicite la contraseña del almacén de claves, se refiere a la definida en el campo `ejbca_truststore_password` del fichero de configuración `web.properties`.


```

root@ubuntu-server:/usr/local/ejbca_4_0_10/bin# ./ejbca.sh ca getrootcert 'Autoridad Certificadora CEE' rootca.der -der
Wrote Root CA certificate to 'rootca.der' using DER encoding.
root@ubuntu-server:/usr/local/ejbca_4_0_10/bin# keytool -importcert -alias autoridadcertificadorcee -file rootca.der -keystore /usr/local/ejbca_4_0_10/p12/truststore_new.jks
Escriba la contraseña del almacén de claves:
Volver a escribir la contraseña nueva:
No coinciden. Inténtelo de nuevo
Escriba la contraseña del almacén de claves:
Volver a escribir la contraseña nueva:
Propietario: ca=EC, ou=Cuerpo de Ingenieros del Ejercito, ou=Entidad de Certificacion, CN=Autoridad Certificadora CEE
Emisor: C=EC, o=Cuerpo de Ingenieros del Ejercito, ou=Entidad de Certificacion, CN=Autoridad Certificadora CEE
Número de serie: 2c6cc47f0b9d2fae
Válido desde: Wed Oct 16 16:01:03 ECT 2013 hasta: Mon Oct 16 16:01:03 ECT 2023
Huellas digitales del certificado:
MD5: 63:5A:C2:3F:BB:0E:B6:B4:48:49:9D:39:66:6C:13:59
SHA1: 01:F8:46:2D:76:ED:51:68:83:F0:F1:81:D9:7C:85:F6:92:14:8A:DB
Nombre del algoritmo de firma: SHA1withRSA
Versión: 3

Extensiones:
#1: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  DigitalSignature
  Key_CertSign
  CrL_Sign
]
#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
]
#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
  KeyIdentifier [
    0000: A6 C8 68 6A B9 D7 C0 57 D3 81 14 15 65 AC 20 71 ..hj...W....e. q
    0010: 3B 70 67 2E ;pg.
  ]
]

¿Confiar en este certificado? [no]: si
Se ha añadido el certificado al almacén de claves
root@ubuntu-server:/usr/local/ejbca_4_0_10/bin#

```

Figura E19. Generación del truststore

Antes de implementar este nuevo almacén de claves, se debe detener el servidor de aplicaciones que ejecuta EJBCA, copiar estos repositorios (keystore y truststore alojados en \$EJBCA_HOME/p12) en los directorios de JBoss (véase Figura E20), e iniciar nuevamente el servidor de aplicaciones.

```

root@ubuntu-server:/usr/local/ejbca_4_0_10/p12# ls
pkt.cee.gob.ec_ejbca.jks superadmin.p12 tomcat.jks truststore.jks truststore_new.jks
root@ubuntu-server:/usr/local/ejbca_4_0_10/p12# cp pkt.cee.gob.ec_ejbca.jks /usr/local/jboss-5.1.0.GA/server/default/conf/keystore/keystore.jks
root@ubuntu-server:/usr/local/ejbca_4_0_10/p12# cp truststore_new.jks /usr/local/jboss-5.1.0.GA/server/default/conf/keystore/truststore.jks
root@ubuntu-server:/usr/local/ejbca_4_0_10/p12#

```

Figura E20. Implementar los nuevos repositorios keystore y truststore en el servidor de aplicaciones

Ahora es posible acceder a la interfaz web de administración de la CA empleando las nuevas credenciales clave/certificado (véase Figura E21 y E22), no sin antes eliminar el historial del navegador web, con el propósito de que se supriman las credenciales anteriores, y reiniciarlo para garantizar este proceso.

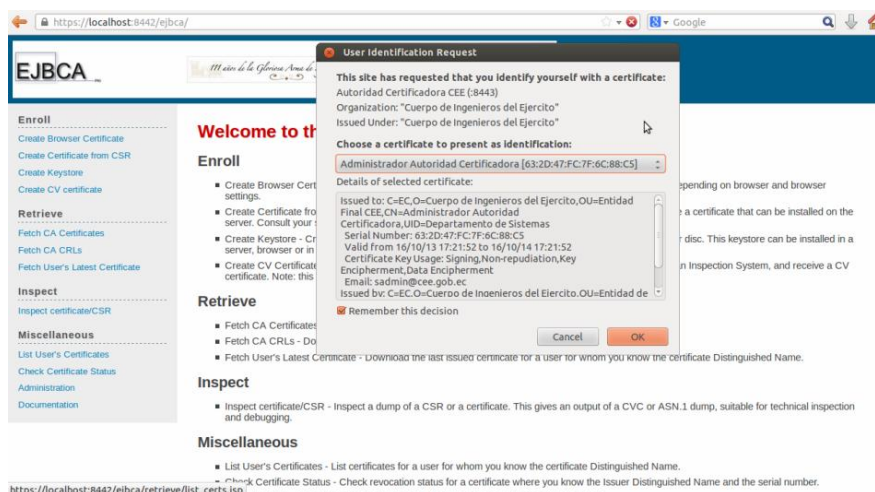


Figura E21. Certificado de Superadministrador para acceder a la admin Web

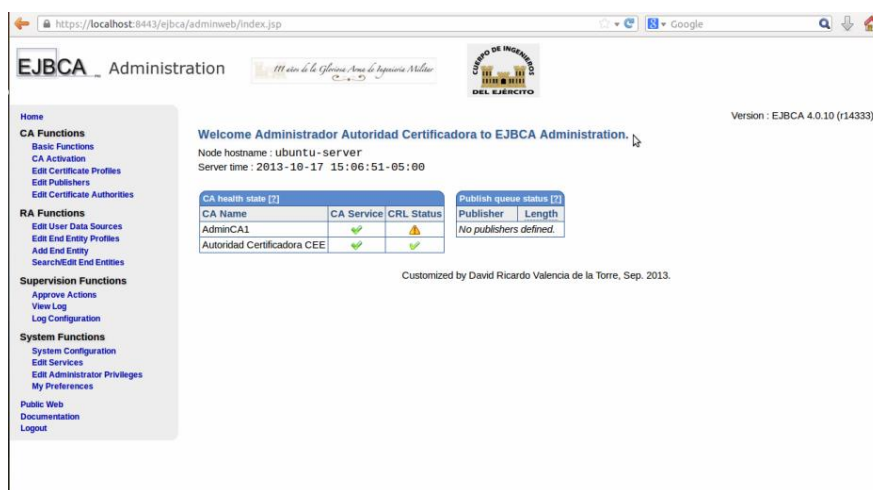


Figura E22. Interfaz Web de Administración EJBCA

Finalmente es necesario establecer como predeterminados los repositorios creados (keystore y truststore), debido a que al momento se encuentran activos los de la CA temporal creada durante la instalación, y la intención es deshabilitarla y empezar a operar la nueva CA generada (véase Figura D23).

```

root@ubuntu-server:/usr/local/ejbca_4_0_10/p12# ls
pki.cee.gob.ec_ejbca.jks  superadmin.p12  tomcat.jks  truststore.jks  truststore_new.jks
root@ubuntu-server:/usr/local/ejbca_4_0_10/p12# mv pki.cee.gob.ec_ejbca.jks tomcat.jks
root@ubuntu-server:/usr/local/ejbca_4_0_10/p12# mv truststore_new.jks truststore.jks
root@ubuntu-server:/usr/local/ejbca_4_0_10/p12# ls
superadmin.p12  tomcat.jks  truststore.jks
root@ubuntu-server:/usr/local/ejbca_4_0_10/p12#

```

Figura E23. Definir como predeterminados a los repositorios keystore y truststore

Con todo lo anterior realizado se puede deshabilitar el Grupo Superadministrador y la CA creados temporalmente durante la instalación, para el grupo desde la opción Edit Administrator Privileges de la interfaz de administración, presionar delete sobre Temporary Super Administrator Group (véase Figura E24).



Figura E24. Eliminar el Grupo d Administración Temporal

Para deshabilitar la CA temporal acceder a la opción CA Activation del apartado CA Functions, desmarcar la opción Monitored, presionar Make off-line, en este caso sobre AdminCA1 (véase Figura E25), y aplicar todos los cambios efectuados.

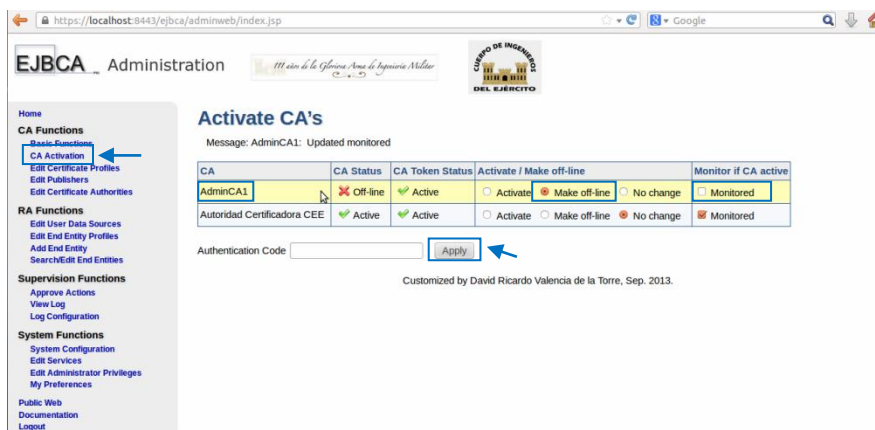


Figura E25. Deshabilitar la Autoridad Certificadora Temporal

Por seguridad es recomendable revocar los certificados temporales empleados durante la configuración inicial, para esto situarse en la opción Search/Edit End Entities del apartado RA Functions, y realizar una búsqueda Generated en el campo Search for entities with status, seleccionar los certificados de entidad final superadmin y tomcat, y clic sobre el botón Revoke And Delete (véase Figura E26).

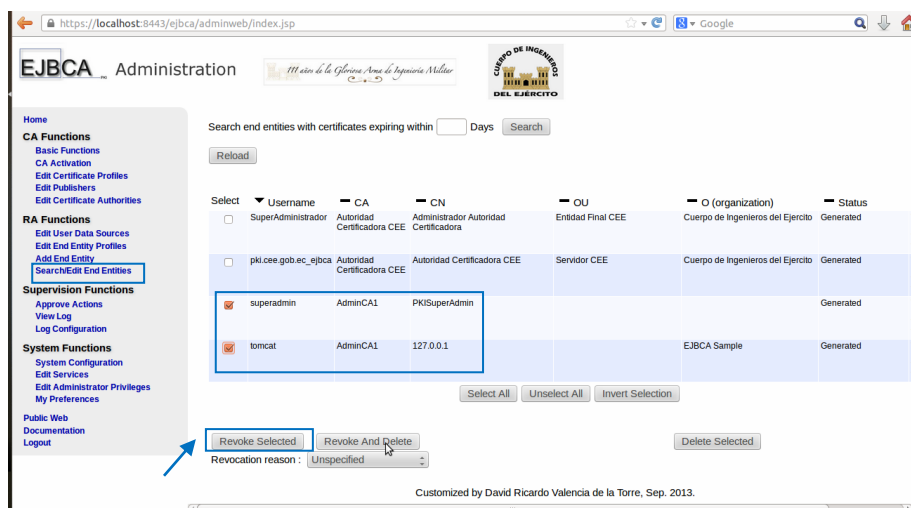


Figura E26. Revocar los certificados creados temporalmente por EJBCA

8. CONFIGURAR LA ACTUALIZACIÓN DE CRLs

La emisión de Listas de Revocación de Certificados es un requerimiento importante en entornos PKI, debido a que exponen ante los usuarios, los certificados que por determinadas razones han sido revocados, imposibilitando su uso.

La generación de estas listas es una actividad que le compete directamente a la CA, pero este es un servicio complementario que las actualiza cada cierto tiempo, para que el usuario disponga de información real.

Para generar este servicio de la PKI ingresar en la opción Edit Services del apartado System Functions , escribir el nombre de la funcionalidad, en este caso Actualización CRLs, y adicionarla (véase Figura E27).

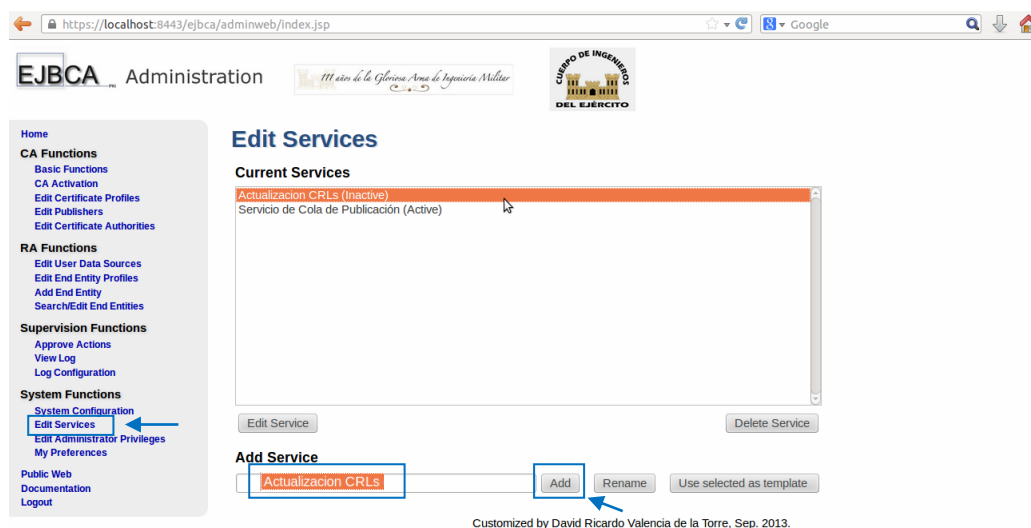


Figura E27. Servicio de actualización de CRLs

Para configurar este servicio se deben establecer parámetros referentes a la Autoridad Certificadora del CEE desplegada (véase Tabla E9).

Tabla E9. Valores establecidos para la actualización de CRLs

Parámetro	Valor
Select Worker	CRL Updater (para establecer el tipo de servicio)
CAs to Check	Autoridad Certificadora CEE (la CA de la cual actualizará la CRL)
Select Interval	Periodical Interval
Period	5 minutes
Select Action	No Action
Active	Habilitado
Pin to Specific Node(s)	pki.cee.gob.ec (es el nombre del host más el dominio de la organización)
Description	Actualización de las CRLs generadas por la CA, cada 5 minutos

Fuente: Elaborado a partir de EJBCA PKI BY PRIME KEY. (2013). *PrimeKey Support, Development and Maintenance Services – EJBCA Installation*. Recuperado de <http://www.ejbca.org/installation.html>

MAJIC.RS. (2011). *Revision of Setting-up EJBCA as Certification Authority*. Recuperado de <http://majic.rs/node/50/revisions/52/view>

ANEXO F

INSTALACIÓN DE ZIMBRA VERSIÓN 8.0.5 GA

En este anexo se presenta información relacionada con la instalación de Zimbra sobre el Sistema Operativo GNU/Linux distribución Centos 6.4 de 64 bits, como también de su configuración para cumplir con los requerimientos planteados en este proyecto, de acuerdo a un esquema que contiene todas las actividades implícitas en el proceso (véase Figura F1).

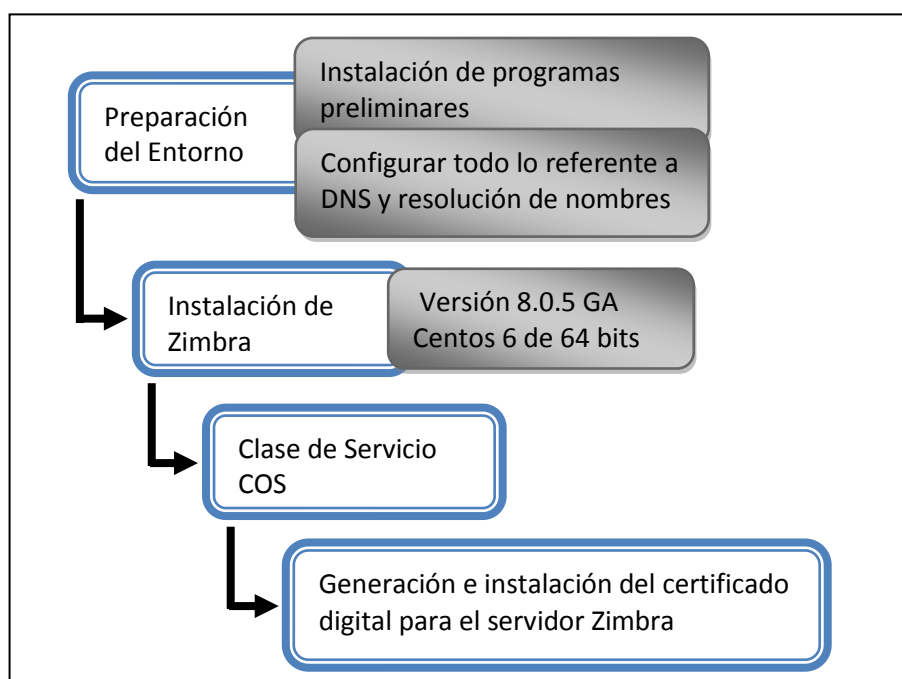


Figura F1. Etapas para la implementación del Sistema de Correo Electrónico

1. PREPARACIÓN DEL ENTORNO

De acuerdo con las pruebas de funcionamiento efectuadas, el DNS está configurado hasta este punto solo para resolver peticiones hacia el servidor de certificación `pki.cee.gob.ec`, ahora se deben incorporar ciertos parámetros del servidor de correo en los ficheros de configuración de `bind9`, para que también resuelva este tipo de peticiones.

Entonces, editar el fichero de zona directa en el directorio `/etc/bind/db.cee.gob.ec`, e incluir el nombre del host del servidor de correo y su dirección IP, en este caso el nombre es `mail` y su dirección es `192.168.0.30`, además cabe señalar que en este punto se debe establecer a este nuevo servidor como el intercambiador de correo (mail Exchange - mx) para que el DNS interprete que este servidor es el que gestionará el correo electrónico dentro del dominio (véase Figura F2).

```

db.cee.gob.ec
;
; BIND data file for local loopback interface
;
$TTL 604800
@ IN SOA cee.gob.ec. root.cee.gob.ec. (
    2013100901 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS cee.gob.ec.
@ IN A 192.168.0.20
@ IN MX 10 mail.cee.gob.ec.
cee IN A 192.168.0.20
mail IN A 192.168.0.30
pktl IN A 192.168.0.10
  
```

→ Declararlo como MX

→ Nombre del host e IP

Figura F2. Fichero de Configuración de Zona Directa

De igual manera hay que incluirlo en el fichero de configuración de zona inversa en el directorio `/etc/bind/db.192.168.0` (véase Figura F3).

```

*db.192.168.0
;
; BIND reverse data file for local loopback interface
;
$TTL 604800
@ IN SOA cee.gob.ec. root.cee.gob.ec. (
    2013100901 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS cee.gob.ec.
20 IN PTR cee.gob.ec.
30 IN PTR mail.cee.gob.ec.
10 IN PTR pktl.cee.gob.ec.
  
```

→ Indica que el host mail en el dominio cee.gob.ec tiene la dirección 192.168.0.30

Figura F3. Fichero de Configuración de Zona Inversa

Finalmente habrá que reiniciar el servicio de DNS bind9 ejecutando el comando `/etc/init.d/bind9 restart` para que se apliquen las modificaciones efectuadas.

Ahora en el host anfitrión del servidor de correo hay que fijar estos parámetros para que coincidan con los ya establecidos. Para asignarle la dirección IP editar el fichero de configuración respectivo ejecutando el comando `nano /etc/sysconfig/network-scripts/ifcfg-eth0`, y fijar los valores requeridos (véase Figura F4).



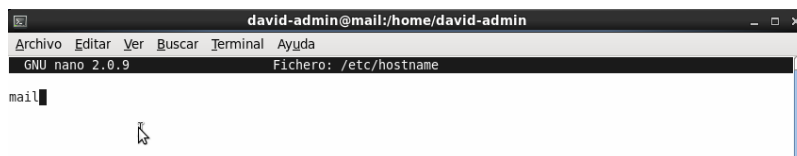
Figura F4. Fichero de Configuración del Adaptador de Red

La configuración de los servidores DNS del adaptador de red se la realiza editando el fichero mediante el comando `nano /etc/resolv.conf` para incluirlos (véase Figura F5).



Figura F5. Fichero de Configuración de los servidores DNS

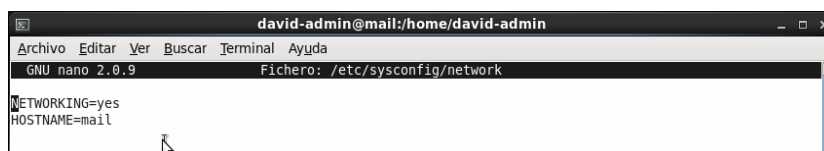
El nombre del host se lo asigna editando los ficheros `/etc/hostname` (véase Figura F6), y `/etc/sysconfig/network` (véase Figura F7), complementariamente se debe incluir el dominio al que pertenece en el fichero `/etc/hosts` (véase Figura F8).



```

david-admin@mail:/home/david-admin
GNU nano 2.0.9 Fichero: /etc/hostname
mail
  
```

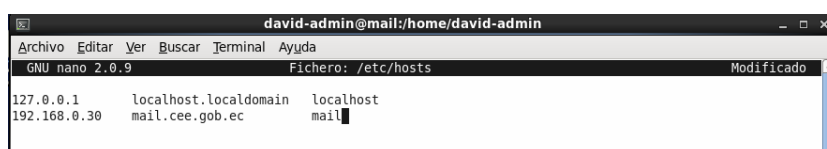
Figura F6. Fichero de Configuración del nombre del host



```

david-admin@mail:/home/david-admin
GNU nano 2.0.9 Fichero: /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=mail
  
```

Figura F7. Fichero de Configuración del nombre del host



```

david-admin@mail:/home/david-admin
GNU nano 2.0.9 Fichero: /etc/hosts Modificado
127.0.0.1    localhost.localdomain  localhost
192.168.0.30 mail.cee.gob.ec      mail
  
```

Figura F8. Fichero de Configuración del dominio al que pertenece el host

Para visualizar todos estos cambios es preciso reiniciar el ordenador, y al ejecutar el comando `hostname` deberá mostrar el nombre del host, y `hostname -f` el dominio al que pertenece (véase Figura F9).



```

david-admin@mail:/home/david-admin
[root@mail david-admin]# hostname
mail
[root@mail david-admin]# hostname -f
mail.cee.gob.ec
[root@mail david-admin]#
  
```

Figura F9. Nombre del host y dominio al que pertenece

En este punto ya es posible efectuar las pruebas de funcionamiento del DNS para identificar si es capaz de resolver el host MX del dominio cee.gob.ec, entonces desde el terminal de consola del servidor de correo ejecutar el comando nslookup para verificarlo (véase Figura F10).



```

david-admin@mail:/home/david-admin
Archivo Editar Ver Buscar Terminal Ayuda
[root@mail david-admin]# nslookup
> set q=mx
> cee.gob.ec
Server:      192.168.0.20
Address:     192.168.0.20#53

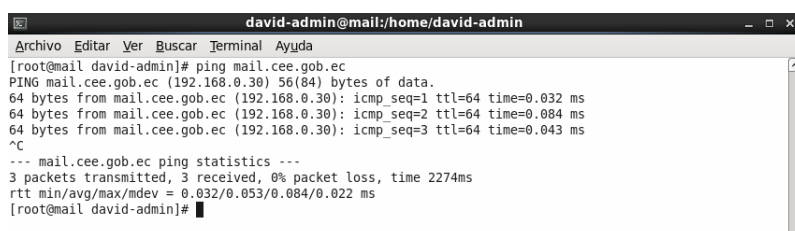
cee.gob.ec  mail exchanger = 10 mail.cee.gob.ec.
>

```

Figura F10. El DNS ha identificado al MX del dominio

Con este comando se consulta para el dominio cee.gob.ec quién es el MX, en este caso responde que el MX es el ordenador mail.cee.gob.ec con un índice de 10, con lo que se concluye que es capaz de resolverlo, pero si no es el caso la instalación de zimbra no podrá ejecutarse.

Otro aspecto importante a verificar es si es capaz de resolver la dirección IP de su propio nombre de dominio (véase Figura F11).



```

david-admin@mail:/home/david-admin
Archivo Editar Ver Buscar Terminal Ayuda
[root@mail david-admin]# ping mail.cee.gob.ec
PING mail.cee.gob.ec (192.168.0.30) 56(84) bytes of data:
64 bytes from mail.cee.gob.ec (192.168.0.30): icmp_seq=1 ttl=64 time=0.032 ms
64 bytes from mail.cee.gob.ec (192.168.0.30): icmp_seq=2 ttl=64 time=0.084 ms
64 bytes from mail.cee.gob.ec (192.168.0.30): icmp_seq=3 ttl=64 time=0.043 ms
^C
--- mail.cee.gob.ec ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2274ms
rtt min/avg/max/mdev = 0.032/0.053/0.084/0.022 ms
[root@mail david-admin]#

```

Figura F11. Resolución del nombre de dominio de zimbra

Como se observa es capaz de resolverlo y apunta de hecho a su propia dirección IP, todas estas actividades que se han llevado a cabo hasta este punto, son requerimientos que deben cumplirse antes de proceder con la instalación de zimbra.

Las herramientas preliminares que requiere zimbra para instalarse y operar, se pueden instalar en conjunto ejecutando el siguiente comando como usuario privilegiado (véase Figura F12).

```
#yum -y install nc libstdc++.i686 perl sysstat wget nano
```



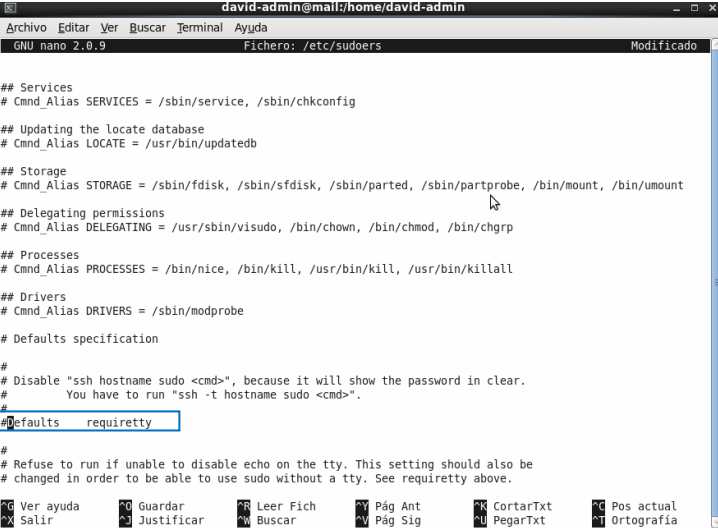
```

david-admin@mail:/home/david-admin
Archivo Editar Ver Buscar Terminal Ayuda
[root@mail david-admin]# yum -y install nc libstdc++.i686 perl sysstat wget nano
Loaded plugins: fastestmirror, refresh-packagekit, security
Loading mirror speeds from cached hostfile
 * base: mirror.edatel.net.co
 * extras: centos5.centos.org
 * updates: centosp5.centos.org
Setting up Install Process
Package 4:perl-5.10.1-131.el6 4.x86_64 already installed and latest version
Package sysstat-9.0.4-20.el6.x86_64 already installed and latest version
Package wget-1.12-1.8.el6.x86_64 already installed and latest version
Package nano-2.0.9-7.el6.x86_64 already installed and latest version
Resolving Dependencies
--> Running transaction check
--> Package libstdc++.i686 0:4.4.7-3.el6 will be installed
--> Processing Dependency: libm.so.6(GLIBC 2.0) for package: libstdc++-4.4.7-3.el6.i686
--> Processing Dependency: libm.so.6 for package: libstdc++-4.4.7-3.el6.i686
--> Processing Dependency: libgcc_s.so.1(GLIBC 2.0) for package: libstdc++-4.4.7-3.el6.i686
--> Processing Dependency: libgcc_s.so.1(GCC 4.2.0) for package: libstdc++-4.4.7-3.el6.i686
--> Processing Dependency: libgcc_s.so.1(GCC 3.3) for package: libstdc++-4.4.7-3.el6.i686
--> Processing Dependency: libgcc_s.so.1(GCC 3.0) for package: libstdc++-4.4.7-3.el6.i686
--> Processing Dependency: libgcc_s.so.1 for package: libstdc++-4.4.7-3.el6.i686
--> Processing Dependency: libc.so.6(GLIBC 2.4) for package: libstdc++-4.4.7-3.el6.i686
--> Processing Dependency: ld-linux.so.2(GLIBC 2.3) for package: libstdc++-4.4.7-3.el6.i686
--> Processing Dependency: ld-linux.so.2 for package: libstdc++-4.4.7-3.el6.i686
--> Package nc.x86_64 0:1.84-22.el6 will be installed
--> Running transaction check
--> Package glibc.i686 0:2.12-1.107.el6 4.5 will be installed
--> Processing Dependency: libfreebl3.so(NSSRAWHASH 3.12.3) for package: glibc-2.12-1.107.el6 4.5.i686
--> Processing Dependency: libfreebl3.so for package: glibc-2.12-1.107.el6 4.5.i686
--> Package libgcc.i686 0:4.4.7-3.el6 will be installed
--> Running transaction check
--> Package nss-softokn-freebl.i686 0:3.14.3-3.el6 4 will be installed
--> Finished Dependency Resolution
Dependencies Resolved

```

Figura F12. Instalación de paquetes preliminares

Editar el fichero de configuración nano `/etc/sudoers` para permitir que las tareas y procesos de zimbra se ejecuten como Superadministrador del sistema, para ello comentar la línea `Defaults requiretty` (véase Figura F13).



```

david-admin@mail:/home/david-admin
GNU nano 2.0.9 Fichero: /etc/sudoers Modificado

## Services
# Cmnnd_Alias SERVICES = /sbin/service, /sbin/chkconfig

## Updating the locate database
# Cmnnd_Alias LOCATE = /usr/bin/updatedb

## Storage
# Cmnnd_Alias STORAGE = /sbin/fdisk, /sbin/sfdisk, /sbin/parted, /sbin/partprobe, /bin/mount, /bin/umount

## Delegating permissions
# Cmnnd_Alias DELEGATING = /usr/sbin/visudo, /bin/chown, /bin/chmod, /bin/chgrp

## Processes
# Cmnnd_Alias PROCESSES = /bin/nice, /bin/kill, /usr/bin/kill, /usr/bin/killall

## Drivers
# Cmnnd_Alias DRIVERS = /sbin/modprobe

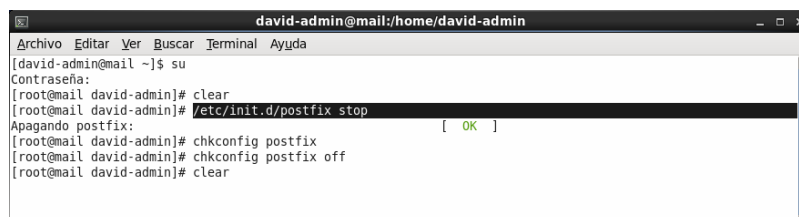
# Defaults specification
#
# Disable "ssh hostname sudo <cmd>", because it will show the password in clear.
# You have to run "ssh -t hostname sudo <cmd>".
#
Defaults requiretty
#
# Refuse to run if unable to disable echo on the tty. This setting should also be
# changed in order to be able to use sudo without a tty. See requiretty above.

Ver ayuda Guardar Leer Fich Pág Ant CortarTxt Pos actual
Salir Justificar Buscar Pág Sig PegarTxt Ortografía

```

Figura F13. Habilitar para que zimbra se ejecute como sudo

Centos incorpora de manera predeterminada el MTA postfix que en este momento se está ejecutando, entonces es preciso detenerlo (véase Figura F14) para evitar conflictos del puerto 25 al instalar zimbra.



```

david-admin@mail:/home/david-admin
Archivo Editar Ver Buscar Terminal Ayuda
[david-admin@mail ~]$ su
Contraseña:
[root@mail david-admin]# clear
[root@mail david-admin]# /etc/init.d/postfix stop
Apagando postfix: [ OK ]
[root@mail david-admin]# chkconfig postfix
[root@mail david-admin]# chkconfig postfix off
[root@mail david-admin]# clear

```

Figura F14. Detener permanentemente la ejecución de Postfix

2. INSTALACIÓN DE ZIMBRA

El instalador de Zimbra, al ser un software de código abierto, está disponible para su libre descarga en sus repositorios oficiales <http://www.zimbra.com>, para este proyecto la versión descargada fue la 8.0.5 GA para Centos 6 X86.

Es recomendable crear un directorio destinado al almacenamiento de toda la información referente a zimbra, en este caso se ha creado `/home/david-admin/ZimbraServer`, sobre el cual se ha extraído el paquete descargado de zimbra (véase Figura F15).



```

david-admin@mail:/home/david-admin/ZimbraServer
Archivo Editar Ver Buscar Terminal Ayuda
[root@mail ZimbraServer]# tar -xvf zcs-8.0.5_GA_5839.RHEL6_64.20130910123908.tgz
zcs-8.0.5_GA_5839.RHEL6_64.20130910123908/
zcs-8.0.5_GA_5839.RHEL6_64.20130910123908/packages/
zcs-8.0.5_GA_5839.RHEL6_64.20130910123908/packages/zimbra-apache-8.0.5_GA_5839.RHEL6_64-20130910123908.x86_64.rpm
zcs-8.0.5_GA_5839.RHEL6_64.20130910123908/packages/zimbra-core-8.0.5_GA_5839.RHEL6_64-20130910123908.x86_64.rpm

```

Figura F15. Descompresión del paquete zimbra

Al acceder a este directorio se observará que existen varios archivos rpm que van a ser instalados para poner en marcha el sistema de correo, pero también habrá una shell de nombre `./install.sh` que ejecuta el instalador de zimbra (véase Figura F16). Al hacerlo se realizan

una serie de comprobaciones para verificar si tiene previamente instalados varios paquetes, por eso es que inicialmente no los encuentra, también pregunta si estamos de acuerdo con los términos de la licencia, le indicamos que sí (véase Figura F16).

```

david-admin@mail:/home/david-admin/ZimbraServer/zcs-8.0.5_GA_5839.RHEL6_64.20130910123908
[root@mail zcs-8.0.5_GA_5839.RHEL6_64.20130910123908]# ls
bin  data  docs  install.sh  packages  readme_binary  en_US.txt  readme_source  en_US.txt  README.txt  util
[root@mail zcs-8.0.5_GA_5839.RHEL6_64.20130910123908]# ./install.sh --platform-override

Operations logged to /tmp/install.log.2313
Checking for existing installation...
zimbra-ldap...NOT FOUND
zimbra-logger...NOT FOUND
zimbra-mta...NOT FOUND
zimbra-snmp...NOT FOUND
zimbra-store...NOT FOUND
zimbra-apache...NOT FOUND
zimbra-spell...NOT FOUND
zimbra-convertd...NOT FOUND
zimbra-memcached...NOT FOUND
zimbra-proxy...NOT FOUND
zimbra-archiving...NOT FOUND
zimbra-cluster...NOT FOUND
zimbra-core...NOT FOUND

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE.
ZIMBRA, INC. ("ZIMBRA") WILL ONLY LICENSE THIS SOFTWARE TO YOU IF YOU
FIRST ACCEPT THE TERMS OF THIS AGREEMENT. BY DOWNLOADING OR INSTALLING
THE SOFTWARE, OR USING THE PRODUCT, YOU ARE CONSENTING TO BE BOUND BY
THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS
AGREEMENT, THEN DO NOT DOWNLOAD, INSTALL OR USE THE PRODUCT.

License Terms for the Zimbra Collaboration Suite:
http://www.zimbra.com/license/zimbra_public_eula_2.4.html

Do you agree with the terms of the software license agreement? [N]
  
```

Figura F16. Shell de instalación de zimbra

También verifica si el directorio donde está la shell contiene todos los paquetes rpm necesarios, y pregunta si queremos instalarlos paquete por paquete (véase Figura F17), después preguntará si estamos seguros de haber seleccionado los componentes que en realidad queremos instalar, obviamente le diremos que sí.

```

david-admin@mail:/home/david-admin/ZimbraServer/zcs-8.0.5_GA_5839.RHEL6_64.20130910123908
Prerequisite check complete.
Checking for installable packages
Found zimbra-core
Found zimbra-ldap
Found zimbra-logger
Found zimbra-mta
Found zimbra-snmp
Found zimbra-store
Found zimbra-apache
Found zimbra-spell
Found zimbra-memcached
Found zimbra-proxy

Select the packages to install
Install zimbra-ldap [Y] y
Install zimbra-logger [Y] y
Install zimbra-mta [Y] y
Install zimbra-snmp [Y] y
Install zimbra-store [Y] y
Install zimbra-apache [Y] y
Install zimbra-spell [Y] y
Install zimbra-memcached [N] n
Install zimbra-proxy [N] n
  
```

Figura F17. Instalación de paquetes rpm de zimbra

Habr  que dejarlo que instale todos los rpm y dependencias que necesite, al finalizar este proceso la instalaci n entra en una etapa cr tica, en la que tendr  que cuadrar todo lo referente a DNS y resoluci n de nombres, y es precisamente aqu  donde se genera el primer error, esto se debe a que zimbra interpreta que el dominio bajo el cual se est  trabajando en este caso es mail.cee.gob.ec y busca el MX para ese dominio, pero en realidad este no existe, por eso hay que especificar el dominio para el cual el host mail va a servir correo, es decir, cee.gob.ec (v ase Figura F18).

```

david-admin@mail:/home/david-admin/ZimbraServer/zcs-8.0.5_GA_5839.RHEL6_64.20130910123908
Archivo Editar Ver Buscar Terminal Ayuda
zimbra-mta
zimbra-snmpp
zimbra-store
zimbra-apache
zimbra-spell
The system will be modified. Continue? [N] y
Removing /opt/zimbra
Removing zimbra crontab entry...done.
Cleaning up zimbra init scripts...done.
Cleaning up /etc/ld.so.conf...done.
Cleaning up /etc/prelink.conf...done.
Cleaning up /etc/security/limits.conf...done.
Finished removing Zimbra Collaboration Server.
Installing packages
zimbra-core.....zimbra-core-8.0.5_GA_5839.RHEL6_64-20130910123908.x86_64.rpm...done
zimbra-ldap.....zimbra-ldap-8.0.5_GA_5839.RHEL6_64-20130910123908.x86_64.rpm...done
zimbra-logger.....zimbra-logger-8.0.5_GA_5839.RHEL6_64-20130910123908.x86_64.rpm...done
zimbra-mta.....zimbra-mta-8.0.5_GA_5839.RHEL6_64-20130910123908.x86_64.rpm...done
zimbra-snmpp.....zimbra-snmpp-8.0.5_GA_5839.RHEL6_64-20130910123908.x86_64.rpm...done
zimbra-store.....zimbra-store-8.0.5_GA_5839.RHEL6_64-20130910123908.x86_64.rpm...done
zimbra-apache.....zimbra-apache-8.0.5_GA_5839.RHEL6_64-20130910123908.x86_64.rpm...done
zimbra-spell.....zimbra-spell-8.0.5_GA_5839.RHEL6_64-20130910123908.x86_64.rpm...done
Operations logged to /tmp/zmsetup.11132013-144327.log
Installing LDAP configuration database...done.
Setting defaults...
DNS ERROR resolving MX for mail.cee.gob.ec
It is suggested that the domain name have an MX record configured in DNS
Change domain name? [Yes] yes
Create domain: [mail.cee.gob.ec] cee.gob.ec

```

Figura F18. Creaci n del Nombre del Dominio

Solventado este inconveniente la shell hace una comprobaci n e identifica al host que va a servir de correo dentro del dominio, que es lo que se necesita (v ase Figura F19).

Si todo el anterior proceso fue satisfactorio se desplegar  un men  de opciones en el que tendremos que asignar una contrase a a la cuenta de administrador creada, para ello se debe teclear dentro de este men  la opci n 3, la cual nos llevar  a un submen  en el cual

seleccionaremos la opción 4, y asignaremos la contraseña de administración (véase Figura F20).

```

david-admin@mail:/home/david-admin/ZimbraServer/zcs-8.0.5_GA_5839.RHEL6_64.20130910123908
Archivo Editar Ver Buscar Terminal Ayuda
Installing packages
zimbra-core.....zimbra-core-8.0.5_GA_5839.RHEL6_64-20130910123908.x86_64.rpm...done
zimbra-ldap.....zimbra-ldap-8.0.5_GA_5839.RHEL6_64-20130910123908.x86_64.rpm...done
zimbra-logger.....zimbra-logger-8.0.5_GA_5839.RHEL6_64-20130910123908.x86_64.rpm...done
zimbra-mta.....zimbra-mta-8.0.5_GA_5839.RHEL6_64-20130910123908.x86_64.rpm...done
zimbra-smtp.....zimbra-smtp-8.0.5_GA_5839.RHEL6_64-20130910123908.x86_64.rpm...done
zimbra-store.....zimbra-store-8.0.5_GA_5839.RHEL6_64-20130910123908.x86_64.rpm...done
zimbra-apache.....zimbra-apache-8.0.5_GA_5839.RHEL6_64-20130910123908.x86_64.rpm...done
zimbra-spell.....zimbra-spell-8.0.5_GA_5839.RHEL6_64-20130910123908.x86_64.rpm...done
Operations logged to /tmp/zmsetup.11132013-144327.log
Installing LDAP configuration database...done.
Setting defaults...

DNS ERROR resolving MX for mail.cee.gob.ec
It is suggested that the domain name have an MX record configured in DNS
Change domain name? [Yes] yes
Create domain: [mail.cee.gob.ec] cee.gob.ec
MX: mail.cee.gob.ec (192.168.0.30)

Interface: 192.168.0.30
Interface: 127.0.0.1
Interface: ::1

done.
Checking for port conflicts

Main menu
1) Common Configuration:
2) zimbra-ldap: Enabled
3) zimbra-stores: Enabled
+Create Admin User: yes
+Admin user to create: admin@cee.gob.ec
+Admin Password: UNSET
+Anti-virus quarantine user: virus-quarantine.3kgzpes_@cee.gob.ec
  
```

Figura F19. Identifica al servidor de correo dentro del dominio

```

david-admin@mail:/home/david-admin/ZimbraServer/zcs-8.0.5_GA_5839.RHEL6_64.20130910123908
Archivo Editar Ver Buscar Terminal Ayuda
q) Quit
Address unconfigured (**) items (? - help) 3

Store configuration
1) Status: Enabled
2) Create Admin User: yes
3) Admin user to create: admin@cee.gob.ec
** 4) Admin Password: UNSET
5) Anti-virus quarantine user: virus-quarantine.3kgzpes_@cee.gob.ec
6) Enable automated spam training: yes
7) Spam training user: spam_jvkbbobx7@cee.gob.ec
8) Non-spam(Ham) training user: ham.tzjbbfvc@cee.gob.ec
9) SMTP host: mail.cee.gob.ec
10) Web server HTTP port: 80
11) Web server HTTPS port: 443
12) Web server mode: https
13) IMAP server port: 143
14) IMAP server SSL port: 993
15) POP server port: 110
16) POP server SSL port: 995
17) Use spell check server: yes
18) Spell server URL: http://mail.cee.gob.ec:7780/aspell.php
19) Configure for use with mail proxy: FALSE
20) Configure for use with web proxy: FALSE
21) Enable version update checks: TRUE
22) Enable version update notifications: TRUE
23) Version update notification email: admin@cee.gob.ec
24) Version update source email: admin@cee.gob.ec

Select, or 'r' for previous menu [r] 4
Password for admin@cee.gob.ec (min 6 characters): [2hRE46JGr] ceeadmin2012
  
```

Figura F20. Definir la contraseña de administración

Para salvar los cambios teclear enter, luego presionar la tecla r para retornar al anterior menú, y solo resta continuar con la instalación, para ello teclear la letra a, y en los dos siguientes mensajes de verificación le damos yes (véase Figura F21).


```

david-admin@mail:/home/david-admin/ZimbraServer/zcs-8.0.5_GA_5839.RHEL6_64.20130910123908
Archivo Editar Ver Buscar Terminal Ayuda
14) IMAP server SSL port: 993
15) POP server port: 110
16) POP server SSL port: 995
17) Use spell check server: yes
18) Spell server URL: http://mail.cee.gob.ec:7780/aspell.php
19) Configure for use with mail proxy: FALSE
20) Configure for use with web proxy: FALSE
21) Enable version update checks: TRUE
22) Enable version update notifications: TRUE
23) Version update notification email: admin@cee.gob.ec
24) Version update source email: admin@cee.gob.ec

Select, or 'r' for previous menu [r] r

Main menu
1) Common Configuration:
2) zimbra-ldap: Enabled
3) zimbra-store: Enabled
4) zimbra-mta: Enabled
5) zimbra-snmp: Enabled
6) zimbra-logger: Enabled
7) zimbra-spell: Enabled
8) Default class of Service Configuration:
r) Start servers after configuration: yes
s) Save config to file
x) Expand menu
q) Quit

*** CONFIGURATION COMPLETE - press 'a' to apply
Select from menu, or press 'a' to apply config (? - help) a
Save configuration data to a file? [Yes] yes
Save config in file: [/opt/zimbra/config.12348]
Saving config in /opt/zimbra/config.12348...done.
The system will be modified - continue? [No] yes

```

Figura F21. Salvar los cambios y continuar con la instalación

Al finalizar estos procesos terminará la instalación, y mostrará un mensaje como el de la Figura F22.

```

david-admin@mail:/home/david-admin/ZimbraServer/zcs-8.0.5_GA_5839.RHEL6_64.20130910123908
Archivo Editar Ver Buscar Terminal Ayuda
com zimbra_url...done.
com zimbra_viewmail...done.
com zimbra_date...done.
com zimbra_proxy config...done.
com zimbra_attachmail...done.
com zimbra_email...done.
com zimbra_attachcontacts...done.
com zimbra_cert manager...done.
com zimbra_bulkprovision...done.
com zimbra_webex...done.
com zimbra_tooltip...done.
com zimbra_phone...done.
com zimbra_adminversioncheck...done.
com zimbra_clientuploader...done.
com zimbra_srchhighlighter...done.
com zimbra_ymemoticons...done.
Finished installing common zimlets.
Restarting mailboxd...done.
Creating galsync account for default domain...done.

You have the option of notifying Zimbra of your installation.
This helps us to track the uptake of the Zimbra Collaboration Server.
The only information that will be transmitted is:
  The VERSION of zcs installed (8.0.5_GA_5839_RHEL6_64)
  The ADMIN EMAIL ADDRESS created (admin@cee.gob.ec)

Notify Zimbra of your installation? [Yes] n
Notification skipped
Setting up zimbra crontab...done.

Moving /tmp/zmsetup.11132013-144327.log to /opt/zimbra/log

Configuration complete - press return to exit

```

Figura F22. Etapa de instalación de zimbra satisfactoria

Una vez hecho esto se puede comprobar el estado de zimbra para conocer si se está ejecutando, y qué servicios de los instalados están activos, para efectuarlo autenticarse como usuario zimbra mediante el comando `su zimbra`, y al ejecutar `zmcontrol status` se verifica el estado del servidor (véase Figura F23).



```

zimbra@mail:/root
Archivo Editar Ver Buscar Terminal Ayuda
[root@mail ~]# su zimbra
[zimbra@mail root]$ zmcontrol status
Host mail.cce.gob.ec
  antispam           Running
  antivirus           Running
  ldap               Running
  logger             Running
  mailbox            Running
  mta                 Running
  opendkim            Running
  snmp                Running
  spell              Running
  stats              Running
  zmconfigd          Running
[zimbra@mail root]$

```

Figura F23. Estado de los servicios de zimbra

Como se puede apreciar todos los servicios están activos, con esto se concluye la instalación de zimbra, las pruebas de funcionamiento respectivas serán tratadas en el capítulo 4 de este proyecto.

3. CLASE DE SERVICIO - COS

Este parámetro permite establecer las características y atributos que deben tener las cuentas de correo creadas en el servidor, para garantizar cierto nivel de rendimiento sobre cada una. Durante la instalación de zimbra se genera de manera predeterminada una COS con valores por defecto, pero es posible crear nuevos parámetros COS considerando los valores que se requieran habilitar o bloquear.

Es así que para crear un buzón se le debe asignar una COS dependiendo del tipo de usuario al que esté destinado, por ejemplo un administrador de red, un jefe departamental, o un usuario convencional. Esto es de gran importancia para este proyecto debido a que es posible personalizar los buzones de los funcionarios y militares tomando en cuenta el rol que desempeñan en la institución, en especial valores referentes a la capacidad permitida para el almacenamiento de mensajes en los buzones.

El servidor de correo actual del CEE de Quito (Microsoft Exchange) administra buzones con distintos tamaños, y uno de los propósitos es mantener esta configuración en el servidor zimbra empleando la COS, de acuerdo a los valores descritos en la Tabla F1.

Tabla F1. Tamaño de los buzones de usuario - Exchange

Tipo de Usuario (Perfil)	Espacio de Buzón	Tamaño de correos	
		Envío Interno	Envío Externo
Comando – Estado Mayor	Ilimitado	50 MB	50 MB
Jefes Departamentales	50 MB	50 MB	50 MB
Coordinadores	45 MB	45 MB	45 MB
Usuarios en General	30 MB	30 MB	30 MB

Fuente: Elaborado con la ayuda del Departamento de Sistemas del CEE (2013)

Entonces es claro que se necesita crear cuatro tipos de COS para cada perfil de usuario del CEE, y obviamente un perfil específico para el administrador de red; para ello desde la interfaz de administración acceder al apartado Configure, Class of Service y crear un nuevo parámetro (véase Figura F24).

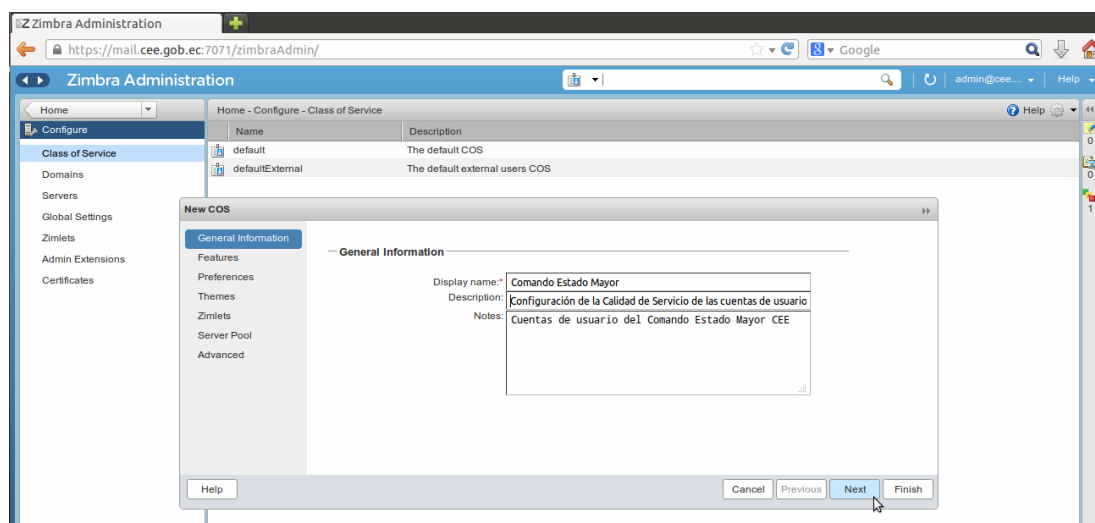


Figura F24. Creación de un parámetro de COS zimbra

Para culminar este proceso existen varios apartados que contienen parámetros que habrá que habilitar, y valores que fijar según se requiera, el primero de estos es Features y los principales valores definidos se describen en la Tabla F2.

Tabla F2. Configuraciones destacadas en el apartado Features de COS

Funcionalidad	Estado	Descripción
General Features		
Change Password	Deshabilitado	Si se encuentra habilitada obliga al usuario a cambiar su contraseña de autenticación la primera vez que accede a su cuenta.
MAPI (Microsoft Outlook Conector)	Habilitado	Los usuarios pueden usar el conector zimbra para Outlook.
Autocomplete form GAL	Habilitado	Esto ayuda a que al redactar un correo en los campos de direcciones se sugieran direcciones de los contactos para no tener que escribir toda la dirección.
Import / Export	Habilitado	Permite importar y exportar mensajería, direcciones, calendarios, para respaldar la información de sus buzones.
Dumpster Folder	Habilitado	Esta opción posibilita la recuperación de la mensajería que ha sido eliminada de la carpeta de papelera, en el caso que se requiera recobrar elementos borrados con hasta 30 días de anterioridad.
Mail Features		
Message Priority	Habilitado	Mediante esta función los usuarios pueden establecer un indicador de prioridad (normal, alta o baja) en los mensajes que envían para alertar al receptor.
POP3 access	Habilitado	Permite utilizar clientes de correo MUA como Thunderbird u Outlook para descargar la mensajería de los buzones, empleando el protocolo POP3.
External POP3 access	Habilitado	Para que la mensajería de las cuentas POP pueda recuperarse directamente desde el Cliente Web Zimbra.
Mail send later	Habilitado	Esto posibilita que un mensaje no sea enviado precisamente luego de ser creado, sino más bien definir una fecha y hora en el que debe ser enviado, mientras tanto el mensaje se almacena en los borradores.
Out of Office reply	Habilitado	Utilizado comúnmente como mensaje de vacaciones, de manera que se enviarán mensajes semanales automáticamente en respuesta a los entrantes.

S/MIME Features

Enable S/MIME	Habilitado	Los usuarios podrán enviar y recibir mensajes protegidos criptográficamente por cifrado y/o firma digital si disponen de un certificado digital y una clave privada proporcionados por una PKI.
---------------	------------	---

Fuente: Creado a partir de Zimbra Guide. (s.f.). Managing Classes of Service. Recuperado de http://zimbra.impladris.sk/download/src/HELIX-711/ZimbraWebClient/WebRoot/help/en_US/admin/html/cos/class_of_service.htm

Otro de los parámetros importantes es Advanced y los principales valores definidos se describen en la Tabla F3.

Tabla F3. Configuraciones destacadas en el apartado Advanced de COS

Funcionalidad	Estado	Descripción
Quotas		
Account quota (MB)	0	Especifica el límite de espacio en disco que un buzón puede utilizar en el servidor de correo para almacenar información de la cuenta de un usuario específico; el valor 0 MB significa que es ilimitado, y fue asignado acorde al perfil de usuario Comando – Estado Mayor de la Tabla F1.
Maximum number of contacts allowed in address book	5000	Es el número máximo de direcciones que un usuario puede almacenar en su lista de contactos.
Percentage threshold for quota warning message (%)	90	Es el umbral de porcentaje que se debe alcanzar antes de enviar un mensaje advirtiéndole que la capacidad del buzón está por saturarse.
Minimum duration of time between quota warnings	1 día	Con que frecuencia debe enviarse este mensaje de cuota.
Password		
Prevent from users changing password	Deshabilitado	Los usuarios de correo podrán cambiar la contraseña de acceso a sus buzones cuando haya expirado la vigencia de la definida inicialmente, o en caso de que se vea comprometida su privacidad; obviamente para ello deberán cumplir con todos los requerimientos de contraseña segura definidos a continuación.
Minimum password length	10	Especifica la longitud necesaria de una contraseña.
Maximum password length	64	La longitud máxima es 64 caracteres.

Minimum upper case characters	2	Cantidad mínima de caracteres letras mayúsculas (A - Z).
Minimum lower case characters	4	Cantidad mínima de caracteres letras minúsculas (a - z).
Minimum punctuation symbols	2	Cantidad mínima de caracteres símbolos de puntuación (símbolos no alfanuméricos como i, \$, #, %).
Minimum numeric characters	2	Cantidad mínima de caracteres numéricos (dígitos del 0 - 9).
Minimum y Maximum password age (Days)	365	Define el tiempo que permanecerán vigentes las contraseñas de usuario, una vez superado este intervalo los usuarios deberán cambiarlas de acuerdo a la cantidad y distintos tipos de caracteres que se han establecido.
Minimum number of unique passwords history	4	Número de nuevas contraseñas distintas que el usuario debe definir antes que pueda volver a utilizar una antigua.

Failed Login Policy

Enabled failed login lockout	Habilitado	Es para activar ciertas características de bloqueo de la cuenta.
Number of consecutive failed logins allowed	5	Cantidad de intentos de inicios de sesión fallidos permitidos antes de bloquear la cuenta.
Time to lockout the account	1 hora	El intervalo de tiempo que la cuenta deberá permanecer bloqueada.

Email Retention Policy

Email message lifetime	0	Número de días que un correo electrónico puede permanecer en cualquier carpeta antes de que sea eliminado automáticamente. El valor 0 significa que no serán eliminados automáticamente, el usuario deberá administrar su mensajería.
Trashed message lifetime	30	Número de días que un correo electrónico puede permanecer en la papelera antes de que sea eliminado automáticamente.
Spam message lifetime	5	Número de días que un correo electrónico puede permanecer en la carpeta correo no deseado antes de que sea eliminado automáticamente.

Fuente: Creado a partir de Zimbra Guide. (s.f.). Account Advanced Features. Recuperado de http://zimbra.impladris.sk/download/src/HELIX-711/ZimbraWebClient/WebRoot/help/en_US/admin/html/managing_accounts/account_advanced_features.htm

Con ello se ha creado una clase de servicio zimbra destinada para las cuentas de correo de usuarios del Comando de Estado Mayor del CEE, de igual manera se han creado el resto de COS correspondientes a los perfiles de usuario de la Tabla F1, variando fundamentalmente la capacidad de almacenamiento de mensajería en el servidor, y ciertos parámetros de acceso (véase Figura F25).

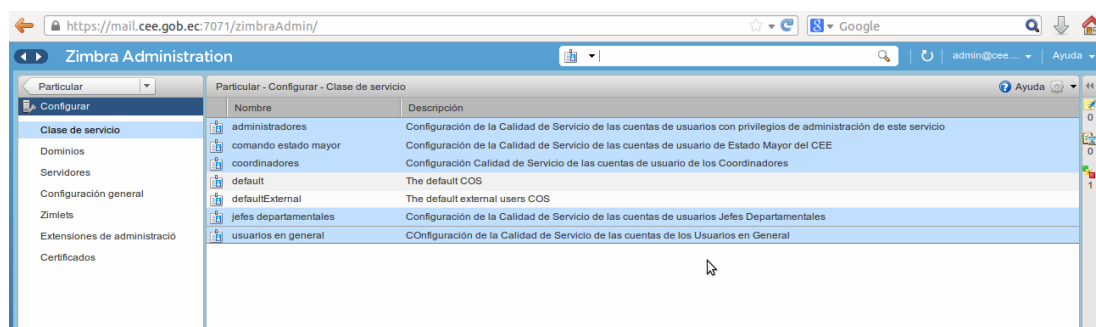


Figura F25. Parámetros de COS configurados en el servidor de correo Zimbra

De esta forma al crear una cuenta nueva de correo, o con cualquier cuenta creada anteriormente, es posible asignarle una COS dependiendo del tipo de funcionario o militar del CEE al que esté destinado.

4. GENERACIÓN E INSTALACIÓN DEL CERTIFICADO PARA EL SERVIDOR ZIMBRA

Para visualizar el certificado actual que identifica al servidor zimbra, iniciar una sesión de terminal y autenticarse como usuario privilegiado del sistema (administrador) mediante el comando `su` y la contraseña respectiva, y ejecutar el comando `/opt/zimbra/bin/zmcertmgr viewdeployedcert`, tras el cual se desplegará información acerca de este certificado (véase Figura F26).

```

[root@mail ~]# /opt/zimbra/bin/zmcertmgr viewdeployedcert
:::service mta::
notBefore=Feb 10 04:27:30 2014 GMT
notAfter=Feb 10 04:27:30 2015 GMT
subject= /C=US/ST=N/A/O=Zimbra Collaboration Server/OU=Zimbra Collaboration Server/CN=mail.cee.gob.ec
issuer= /C=US/ST=N/A/L=N/A/O=Zimbra Collaboration Server/OU=Zimbra Collaboration Server/CN=mail.cee.gob.ec
SubjectAltName=
:::service proxy::
notBefore=Feb 10 04:27:30 2014 GMT
notAfter=Feb 10 04:27:30 2015 GMT
subject= /C=US/ST=N/A/O=Zimbra Collaboration Server/OU=Zimbra Collaboration Server/CN=mail.cee.gob.ec
issuer= /C=US/ST=N/A/L=N/A/O=Zimbra Collaboration Server/OU=Zimbra Collaboration Server/CN=mail.cee.gob.ec
SubjectAltName=
:::service mailboxd::
notBefore=Feb 10 04:27:30 2014 GMT
notAfter=Feb 10 04:27:30 2015 GMT
subject= /C=US/ST=N/A/O=Zimbra Collaboration Server/OU=Zimbra Collaboration Server/CN=mail.cee.gob.ec
issuer= /C=US/ST=N/A/L=N/A/O=Zimbra Collaboration Server/OU=Zimbra Collaboration Server/CN=mail.cee.gob.ec
SubjectAltName=
:::service ldap::
notBefore=Feb 10 04:27:30 2014 GMT
notAfter=Feb 10 04:27:30 2015 GMT
subject= /C=US/ST=N/A/O=Zimbra Collaboration Server/OU=Zimbra Collaboration Server/CN=mail.cee.gob.ec
issuer= /C=US/ST=N/A/L=N/A/O=Zimbra Collaboration Server/OU=Zimbra Collaboration Server/CN=mail.cee.gob.ec
SubjectAltName=
[root@mail ~]#

```

Servicios operativos del servidor zimbra

Entidad Destino

Entidad Emisora

Figura F26. Certificado Digital predeterminado del servidor zimbra

Con esto se comprueba en efecto que todos los servicios que se están ejecutando sobre la plataforma de correo están identificados por el certificado digital predeterminado que se ha generado durante su instalación, en el que también se puede apreciar que tanto el subject o entidad hacia quien está destinado, como la entidad emisora, tienen asignado el nombre Zimbra Collaboration Server.

Ahora es necesario generar un nuevo certificado empleando la PKI del Cuerpo de Ingenieros del Ejército diseñada, que sustituya a este certificado predeterminado, el proceso de emisión es el mismo que se realizó para generar el certificado del servidor PKI, para lo cual se debe acceder a la interfaz de administración de EJBCA y en el apartado Add End Entity seleccionar el perfil de certificado SERVIDORES creado durante la configuración de EJBCA, e ingresar toda la información de registro (véase Figura F27).

La primera sección de esta plantilla de información establece el usuario y la contraseña asignados, que deberán ser ingresados desde el ordenador del cliente, en este caso el servidor

zimbra, para autenticarse y generar la solicitud de certificación, conjuntamente con toda esta información de registro.

EJBCA Administration *Misión de la Gloriosa Arma de Ingeniería Militar* **CUERPO DE INGENIEROS DEL EJERCITO**

Add End Entity **End Entity Servidor Zimbra added successfully.**

Field	Value	Required
End Entity Profile	SERVIDORES	Required
Username	Zimbra-Server	✓
Password	✓
Confirm Password	✓
Batch generation (clear text pwd storage)	<input type="checkbox"/>	
E-mail address	mail @ cee.gob.ec	<input type="checkbox"/>
Subject DN Attributes		
CN, Common name	Departamento de Sistemas - Server	✓
OU, Organizational Unit	Servidor CEE	<input type="checkbox"/>
O, Organization	Cuerpo de Ingenieros del Ejercito	<input type="checkbox"/>
C, Country (ISO 3166)	EC	<input type="checkbox"/>
Other subject attributes		
RFC 822 Name (e-mail address)	Use data from E-mail address field <input checked="" type="checkbox"/>	<input type="checkbox"/>
DNS Name	mail.cee.gob.ec	<input type="checkbox"/>
Main certificate data		
Certificate Profile	PERFIL_SERVIDOR	✓
CA	Autoridad Certificadora CEE	✓
Token	PEM file	✓

Buttons: Add, Reset

Figura F27. Parámetros de registro del certificado digital destinado al servidor zimbra

La segunda sección son los atributos del sujeto u ordenador hacia quien está destinado el certificado, que deben identificarlo de manera única ante los demás bajo el mismo dominio de certificación, lo integran parámetros como el Common Name, Organización, País y la Unidad Organizacional.

La tercera parte incluye el nombre del host y el dominio al que pertenece, y la parte final define el formato bajo el cual será emitido el certificado (token), la Autoridad Certificadora que lo emitirá y gestionará, y el perfil del certificado.

Para completar el proceso de registro y generar la solicitud de certificación, desde el servidor zimbra acceder a la interfaz pública (<https://pki.cee.gob.ec:8442/ejbca>) de la

PKI, y en el apartado Create Browser Certificate ingresar el usuario y contraseña asignados durante el registro (véase Figura F28).

Figura F28. Autenticación para generar la solicitud de certificación

Finalmente se debe definir la longitud del par clave criptográfico para completar la solicitud y recibir el certificado solicitado (véase Figura F29).

Figura F29. Establecer la longitud del par clave criptográfico y obtener el certificado

Este es el proceso que realizará el administrador de red del Cuerpo de Ingenieros del Ejército, pero la interacción de los componentes PKI luego de haber definido la longitud del par clave criptográfico, es generarlo y enviar la solicitud en el formato PKCS#10 al componente RA para que la verifique, la transfiera hacia la CA que responderá generando el certificado solicitado.

Al ser un certificado destinado para un servidor, el formato con el que fue emitido no es el convencional PKCS#12 (.p12) empleado para identificar los ordenadores cliente, el formato en este caso es .pem que a diferencia del anterior no se instala almacenándose automáticamente en el repositorio de certificados del sistema operativo, luego de ejecutarlo, el proceso difiere de cierta forma debido a que habrá que alojarlo en un directorio específico del servidor.

Este fichero está estructurado por tres secciones, la clave privada y el certificado de entidad final (Servidor de Correo), y el certificado de Autoridad Certificadora Raíz (Autoridad Certificadora CEE) (véase Figura F30), de manera que el propósito es dividirlo en tres ficheros distintos para almacenarlos e instalarlos en el servidor.

El proceso es sencillo, se accede al fichero Zimbra-Server.pem descargado y se copia el contenido de cada sección a un nuevo fichero pero con una extensión diferente, en el caso de la clave privada debe tener una extensión .key (Zimbra-Server.key), el certificado de servidor .crt (Zimbra-Server.crt), y el de Autoridad Certificadora .crt (AutoridadCertificadoraCEE.crt) (véase Figura F31).



Figura F30. Contenido del archivo Zimbra-Server.pem emitido por la Autoridad Certificadora del CEE

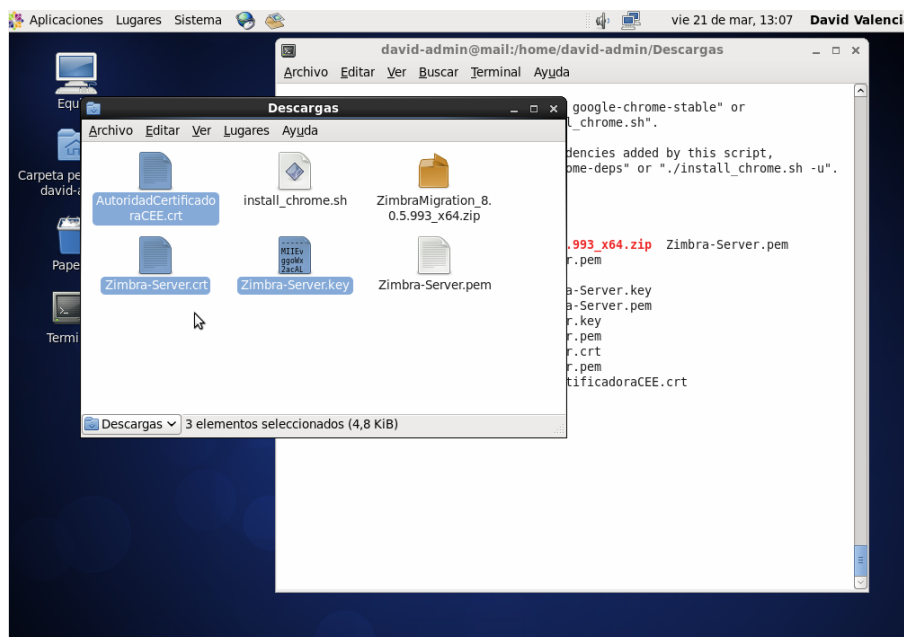


Figura F31. Archivos creados para separar cada sección del archivo Zimbra-Server .pem

En este punto vale la pena definir que lo se pretende realizar con este proceso es securizar la conexión cliente/servidor de zimbra mediante el protocolo SSL/TLS, con un certificado digital generado por la PKI del CEE, para ello se debe conocer que zimbra posee tres ficheros que definen su certificado (`comercial.crt`) y clave privada respectiva (`comercial.key`), como también el certificado de Autoridad Certificadora (`comercial_ca.crt`), empleados durante una conexión SSL/TLS.

Entonces los tres ficheros creados anteriormente, mostrados en la Figura F31, deben ser renombrados para que coincidan con los que están definidos en el servidor, obviamente sin alterar su contenido, de acuerdo a como se muestra en la Figura F32.

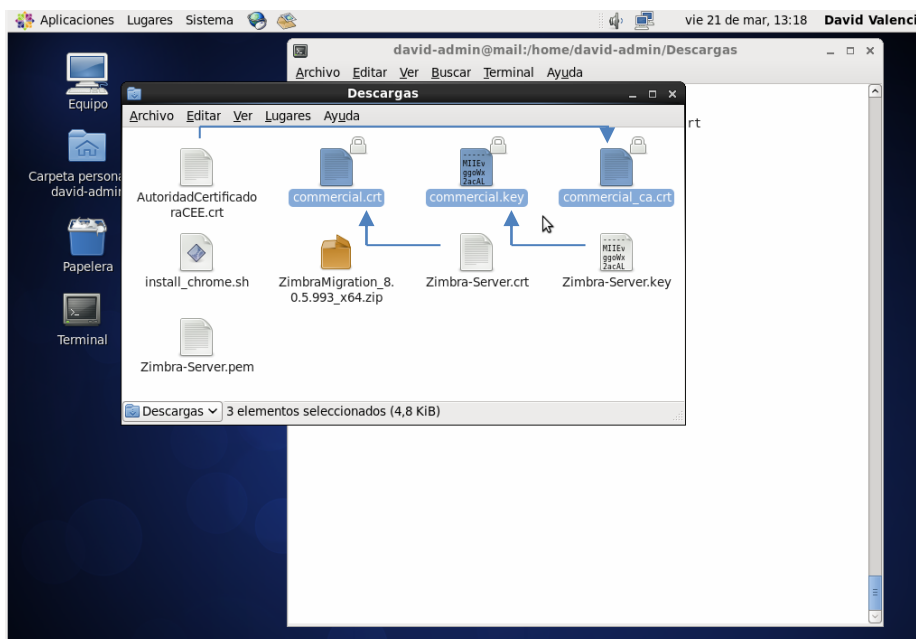


Figura F32. Renombrar los ficheros que contienen los certificados y la clave privada del Servidor Zimbra y la Autoridad Certificadora CEE

Si se tiene a disposición estos tres ficheros, como se ha indicado, es necesario mover `commercial.key` hacia un directorio específico de zimbra (`/opt/zimbra/ssl/comercial/`), debido a que el servidor debe disponer de la clave privada previo a la instalación del certificado (véase Figura F33), caso contrario se generarán errores que no permitirán su ejecución.

```

david-admin@mail:/opt/zimbra/ssl/zimbra/comercial
Archivo Editar Ver Buscar Terminal Ayuda
[david-admin@mail ~]$ su
Contraseña:
[root@mail david-admin]# cd Descargas/
[root@mail Descargas]# ls
AutoridadCertificadoraCEE.crt  commercial.key  Zimbra-Server.crt
commercial_ca.crt             install_chrome.sh  Zimbra-Server.key
                                ZimbraMigration_8.0.5.993_x64.zip  Zimbra-Server.pem
[root@mail Descargas]# cp commercial.key /opt/zimbra/ssl/zimbra/comercial/
[root@mail Descargas]# cd /opt/zimbra/ssl/zimbra/comercial/
[root@mail comercial]# ls
commercial_ca.crt  commercial.key
[root@mail comercial]#

```

Figura F33. Almacenamiento de la clave privada generada para zimbra

De este modo ya es posible efectuar la instalación tanto del certificado del servidor, como de la Autoridad Certificadora, ejecutando el comando `/opt/zimbra/bin/zmcertmgr deploycrt comm comercial.crt comercial_ca.crt` (véase Figura F34).

Zimbra Autoridad Certificadora

```

[root@mail Descargas]# /opt/zimbra/bin/zmcertmgr deploycrt comm comercial.crt comercial_ca.crt
** Verifying comercial.crt against /opt/zimbra/ssl/zimbra/commercial/commercial.key
Certificate (comercial.crt) and private key (/opt/zimbra/ssl/zimbra/commercial/commercial.key) match
.
Valid certificate: comercial.crt: OK
** Copying comercial.crt to /opt/zimbra/ssl/zimbra/commercial/commercial.crt
** Appending ca chain comercial_ca.crt to /opt/zimbra/ssl/zimbra/commercial/commercial.crt
** Importing certificate /opt/zimbra/ssl/zimbra/commercial/commercial_ca.crt to CACERTS as zcs-user-c
ommercial_ca...done.
** NOTE: mailboxd must be restarted in order to use the imported certificate.
** Saving server config key zimbraSSLCertificate...done.
** Saving server config key zimbraSSLPrivateKey...done.
** Installing mta certificate and key...done.
** Installing slapd certificate and key...done.
** Installing proxy certificate and key...done.
** Creating pkcs12 file /opt/zimbra/ssl/zimbra/jetty.pkcs12...done.
** Creating keystore file /opt/zimbra/mailboxd/etc/keystore...done.
** Installing CA to /opt/zimbra/conf/ca...done.
[root@mail Descargas]#

```

Figura F34 Instalación del certificado de zimbra y de la CA

Este comando comprueba que la clave privada almacenada con anterioridad sea la correspondiente a su par clave pública almacenada en el certificado del servidor, y finalmente algunas operaciones de almacenamiento e instalación de los certificados y la clave privada en cada uno de los servicios que se están ejecutando sobre la plataforma de correo zimbra.

Si todo este proceso se ha realizado sin ningún inconveniente, se pueden efectuar pruebas para cerciorarse de que en realidad los certificados generados sustituyeron a los predeterminados, ejecutando el comando `/opt/zimbra/bin/zmcertmgr viewdeployedcrt` (véase Figura F35).

Como se puede apreciar el certificado que identifica cada uno de los servicios del servidor zimbra ha sido sustituido por que fue generado en la PKI del CEE, con esto se garantiza que este certificado sea validado en el entorno de los ordenadores de esta entidad que formen parte de este proceso de certificación, cada vez que establezcan conexión con el servidor de correo zimbra.

```

david-admin@mail:/home/david-admin/Descargas
Archivo Editar Ver Buscar Terminal Ayuda
[root@mail Descargas]# /opt/zimbra/bin/zncertmgr viewdeployedcert
::service mta:
notBefore=Mar 21 17:39:59 2014 GMT
notAfter=Mar 21 17:39:59 2015 GMT
subject= /CN=Servidor de Correo/OU=Servidor CEE/O=Cuerpo de Ingenieros del Ejercito/C=EC
issuer= /CN=Autoridad Certificadora CEE/OU=Entidad de Certificacion/O=Cuerpo de Ingenieros del Ejercito/C=EC
SubjectAltName= email:mail@cee.gob.ec, mail.cee.gob.ec
← Entidad Destino
← Entidad Certificadora
::service proxy:
notBefore=Mar 21 17:39:59 2014 GMT
notAfter=Mar 21 17:39:59 2015 GMT
subject= /CN=Servidor de Correo/OU=Servidor CEE/O=Cuerpo de Ingenieros del Ejercito/C=EC
issuer= /CN=Autoridad Certificadora CEE/OU=Entidad de Certificacion/O=Cuerpo de Ingenieros del Ejercito/C=EC
SubjectAltName= email:mail@cee.gob.ec, mail.cee.gob.ec
::service ldap:
notBefore=Mar 21 17:39:59 2014 GMT
notAfter=Mar 21 17:39:59 2015 GMT
subject= /CN=Servidor de Correo/OU=Servidor CEE/O=Cuerpo de Ingenieros del Ejercito/C=EC
issuer= /CN=Autoridad Certificadora CEE/OU=Entidad de Certificacion/O=Cuerpo de Ingenieros del Ejercito/C=EC
SubjectAltName= email:mail@cee.gob.ec, mail.cee.gob.ec
[root@mail Descargas]#

```

Servicios que se ejecutan sobre Zimbra

Figura F35. Certificado Digital generado para zimbra

Finalmente para complementar este proceso en el servidor zimbra, es necesario garantizar que el certificado que ha sido instalado pueda ser validado por la seguridad de Java, debido a que es un lenguaje que opera independiente de la plataforma ejecutando una máquina virtual, por lo que no utiliza la información de los repositorios de certificados del sistema operativo anfitrión.

Entonces empleando la herramienta de línea de comandos keytool que incorpora Java para gestionar sus almacenes de claves (keystores), se debe importar el certificado que identifica el servidor zimbra, para que sea reconocido como fiable (véase Figura F36).

```

david-admin@mail:/home/david-admin/Descargas
Archivo Editar Ver Buscar Terminal Ayuda
[root@mail Descargas]# /opt/zimbra/java/bin/keytool -import -alias new -keystore /opt/zimbra/java/jre^
/lib/security/cacerts -storepass changeit -file /opt/zimbra/ssl/zimbra/commercial/commercial.crt
Se ha agregado el certificado al almacén de claves
[root@mail Descargas]#

```

El certificado es fiable

Figura F36. Incluir el Certificado Digital de zimbra en el keystore de Java

Lo que queda es reiniciar el servidor zimbra y esperar a que se ejecuten con normalidad todos sus servicios para visualizar el certificado instalado mediante su interfaz de administración desde un navegador web (véase Figura F37 y F38).

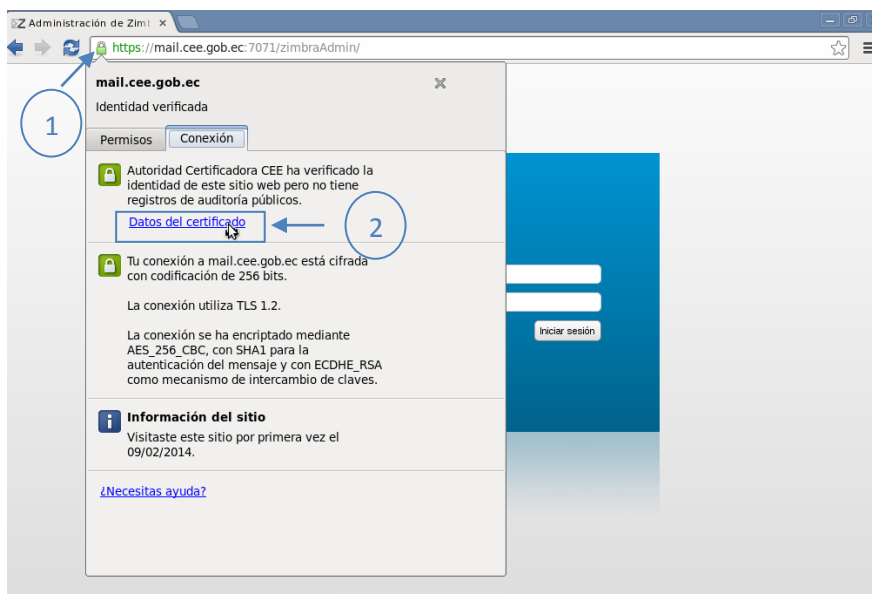


Figura F37. Pantalla del navegador web para acceder al certificado

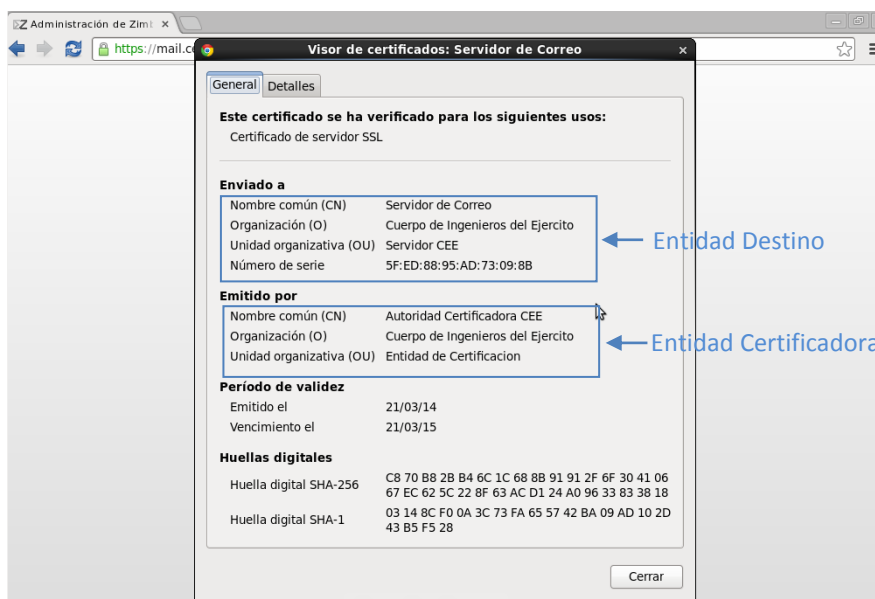


Figura F38. Certificado Digital que identifica al servidor de correo zimbra durante una conexión SSL

ANEXO G

MIGRACIÓN DE LAS CUENTAS DE CORREO ACTUAL EXCHANGE A ZIMBRA SERVER

En este anexo se presenta información relacionada con la instalación de Microsoft Exchange 2010, sobre el sistema operativo Windows Server 2008 de 64 bits, la creación de la base de datos Active Directory y las cuentas de correo de usuario, el envío y recepción de mensajes, agregar contactos, y finalmente la migración de toda esta información hacia la nueva plataforma de correo Zimbra desarrollada.

1. SISTEMA OPERATIVO DEL SERVIDOR EXCHANGE

Se ha decidido utilizar Windows Server 2008 debido a que el servidor real del CEE ha sido implementado sobre este sistema, el paquete de instalación obtenido desde los repositorios oficiales de Microsoft <http://www.microsoft.com/es-es/download/details.aspx?id=11093> proporciona una versión de Evaluación de este sistema operativo que dura 180 días, los cuales son suficientes para realizar las configuraciones y pruebas necesarias para este proyecto.

De igual forma que el servidor zimbra y el DNS, este servidor será virtualizado de acuerdo a los parámetros de hardware recomendados por la página oficial de Microsoft (véase Tabla G1) para instalar la edición Standard, considerando que es una simulación que no almacenará demasiada información o ejecutará excesivos procesos.

Tabla G1. Principales requerimientos de Hardware para la instalación de Windows Server 2008 Standard

Componente	Requerimiento
Procesador	Mínimo: 1 GHz (procesador x86) o 1.4 GHz (procesador x64) Recomendado: 2 GHz o superior Nota: Se requiere un procesador Intel Itanium 2 para Windows Server 2008 para Sistemas basados en Itanium
Memoria	Mínimo: 512 MB RAM Recomendado: 2 GB RAM o mayor Máximo (sistemas de 32 bits): 4 GB (Edición Standard) o 64 GB (Ediciones Enterprise and Datacenter) Máximo (sistemas de 64 bits): 32 GB (Edición Standard) o 1 TB (Ediciones Enterprise and Datacenter) o 2 TB (Sistemas Basados en Itanium)
Espacio disponible en Disco	Mínimo: 10 GB Recomendado: 40 GB o mayor Nota: Computadores con más de 16 GB de RAM requerirán mayor espacio de disco para paginación, hibernación y volcado de archivos

Fuente: Traducido y adaptado a partir de Microsoft Corporation. (2014). Windows Server 2008 System Requirements. Recuperado de <http://technet.microsoft.com/enus/windowsserver/bb414778>

La instalación de este sistema operativo es relativamente sencilla, es posible compararla con una instalación tradicional de Windows XP sobre un ordenador de escritorio, en la que las cosas se facilitan con la ayuda del asistente para cada etapa de este proceso; de todas formas el punto de enfoque de este anexo no es mostrar la instalación de este sistema, sino más bien la de Microsoft Exchange y la vinculación con zimbra para la transferencia de información.

No obstante, es necesario realizar ciertas configuraciones previas a la instalación de Exchange para personalizar al servidor, como definir el nombre del equipo y una dirección IP estática de la red de servidores en desarrollo que permita el acceso a internet, y actualizar el sistema para garantizar la ejecución de procesos posteriores (véase Figura G1, G2 y G3).

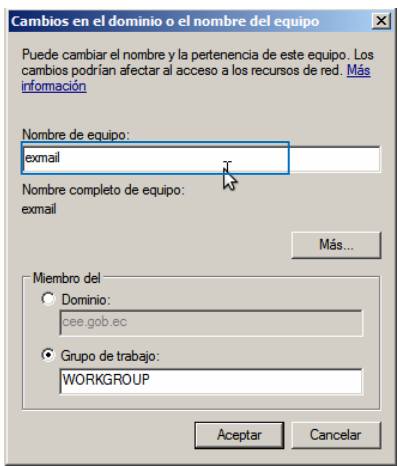


Figura G1. Definir el nombre del Servidor

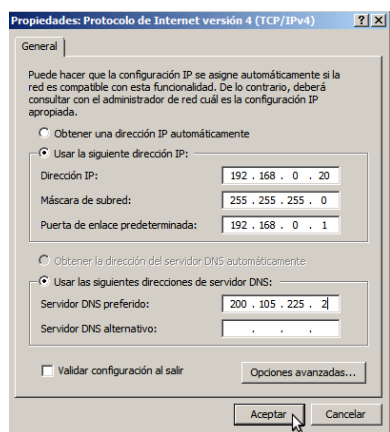


Figura G2. Establecer una Dirección IP Estática



Figura G3. Actualización del Sistema

2. REQUERIMIENTOS PREVIOS

Análogamente a zimbra para ejecutar el asistente de instalación de Exchange, es necesario tener resuelto todo el tema referente a controlador de dominio Active Directory, y resolución de nombres DNS, esto permite identificar el dominio al que este servidor va servir de MX o intercambiador de correo.

Entonces desde la pantalla del asistente de Tareas de Configuración Inicial de Windows Server 2008, acceder al apartado Agregar Roles, cerciorarse de haber cumplido con las recomendaciones que se muestran (véase Figura G4), y hacer clic en **Siguiente**.

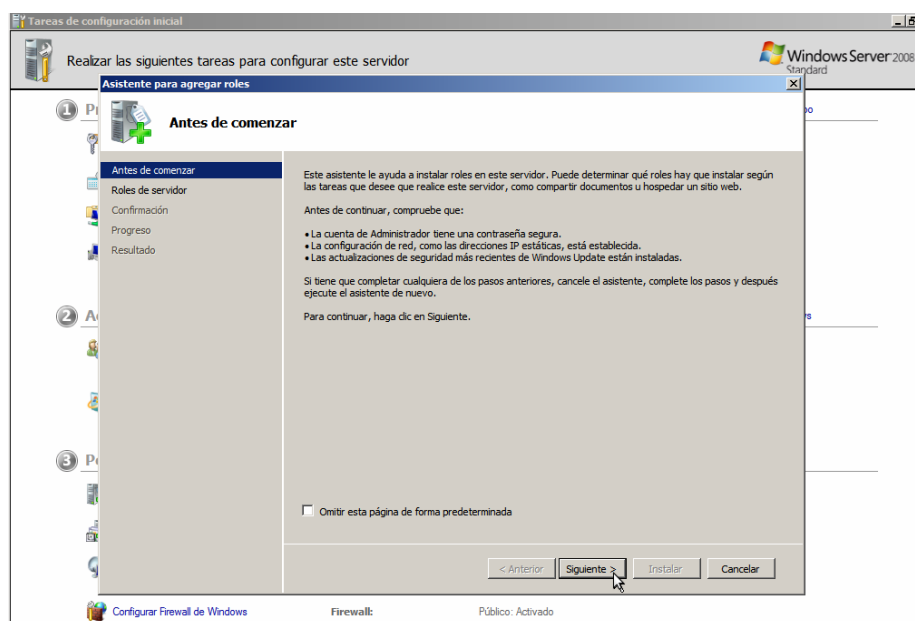


Figura G4. Asistente para agregar roles al Sistema

Un rol es el trabajo o la función que va a desempeñar un servidor sobre la infraestructura de red, en este caso lo que se requiere es agregar el rol de Active Directory (AD) (véase Figura G5).

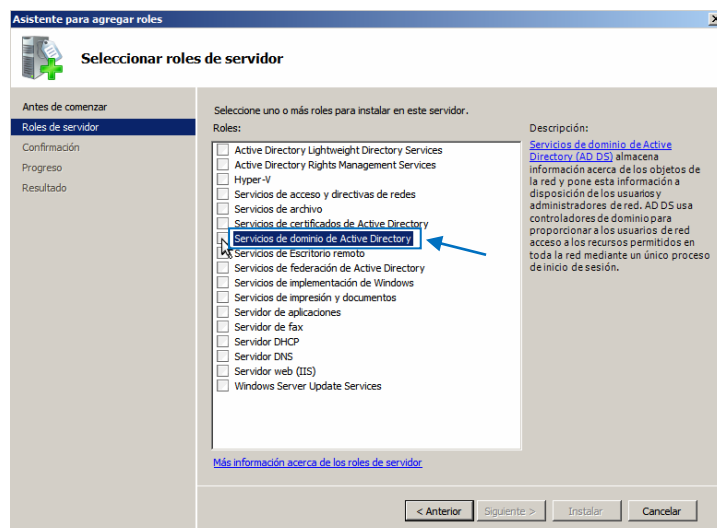


Figura G5. Agregar este rol al Sistema

AD es un controlador de dominio con una base de datos que almacena objetos como Usuarios, Grupos, Unidades Organizacionales, Recursos Compartidos, Servicios, Dominios y Subdominios, con el propósito de centralizar su administración, y mediante mecanismos de autenticación y políticas de seguridad permitir o denegar el acceso hacia estos recursos o servicios; esto de forma general, debido a que proporciona otras funcionalidades adicionales que contribuyen a la administración de los sistemas y usuarios.

Sin embargo, lo que se necesita para efectuar la simulación de una plataforma de correo Exchange completamente operativa, es implementar AD en primera instancia para generar una base de datos de usuarios, con direcciones de correo electrónico vinculadas para cada uno, y también para suministrar el servicio de DNS, de manera que la autenticación para cada buzón de usuario, sea efectuada con los datos (contraseñas) almacenados en AD, y el servidor sea identificado en el entorno de la red del CEE.

Para agregar este rol el sistema requiere ciertas características adicionales que permitan su ejecución (véase Figura G6).

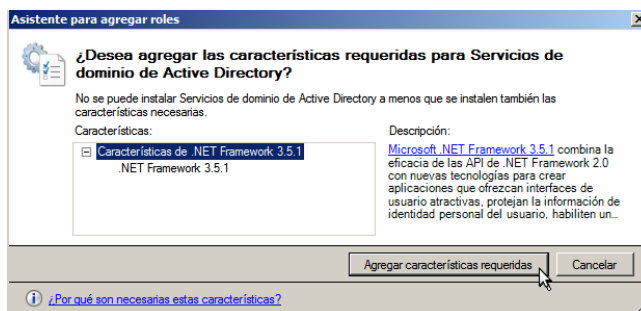


Figura G6. Agregar características necesarias al Sistema

Al instalar estas características se activa la casilla de selección del rol mostrada en la Figura G5, con ello es posible continuar y en el siguiente paso el asistente muestra una pantalla informativa (véase Figura G7).

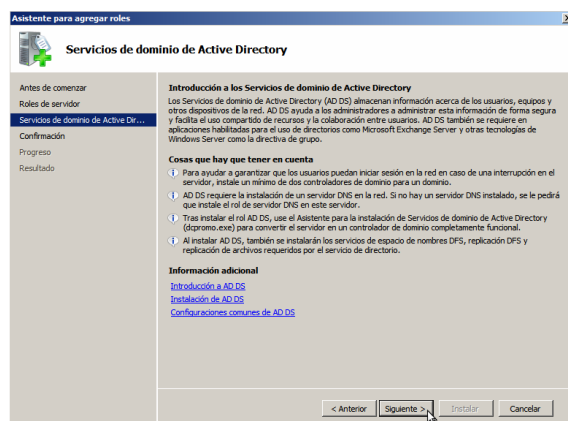


Figura G7. Pantalla informativa del asistente de instalación referente a AD

Nos da la opción de confirmar los cambios a realizarse en el sistema, por cuestiones de seguridad en el caso de no tener la certeza de lo que se ha seleccionado, y también muestra cual es el siguiente paso a realizar para la instalación y configuración del servicio de control de dominio (véase Figura G8).

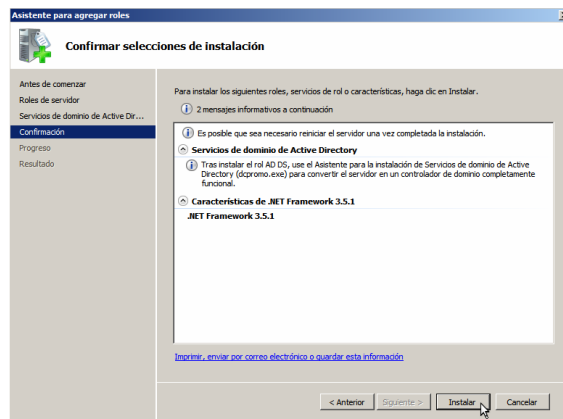


Figura G8. Pantalla de confirmación de los cambios a efectuarse

Si todo este proceso se ha ejecutado con normalidad la instalación del rol ha terminado (véase Figura G9), dando paso a la instalación y configuración de este servicio.

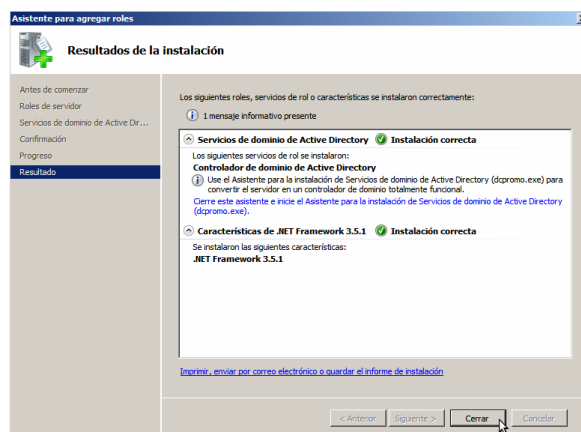


Figura G9. Instalación exitosa del Rol de Servidor de Dominio

Se debe configurar el adaptador de red para definir la propia dirección IP como servidor DNS, esto debido a que el mismo servidor proveerá la resolución de nombres del dominio (véase Figura G10).

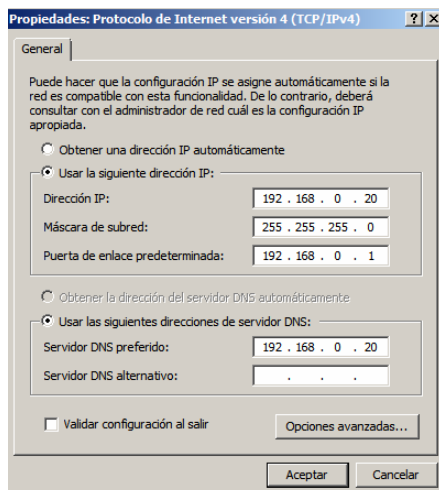


Figura G10. Establecer la propia dirección IP como servidor DNS

Para ejecutar el asistente de instalación del servicio desde la barra de tareas en el menú Inicio escribir dcpromo y ejecutar el programa que se muestra (véase Figura G11).

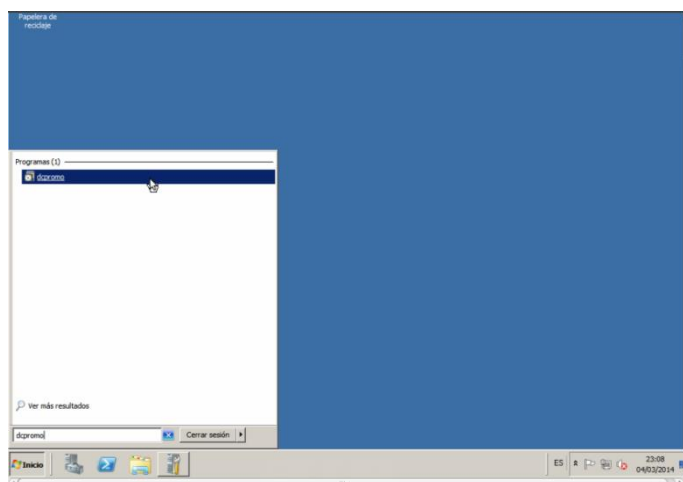


Figura G11. Ejecutar el asistente de instalación del controlador de dominio

Es de suma importancia marcar la casilla de instalación en modo avanzado, pues de esta manera se garantiza que todas las opciones de instalación y configuración del servicio de Directorio Activo permanezcan habilitadas (véase Figura G12).

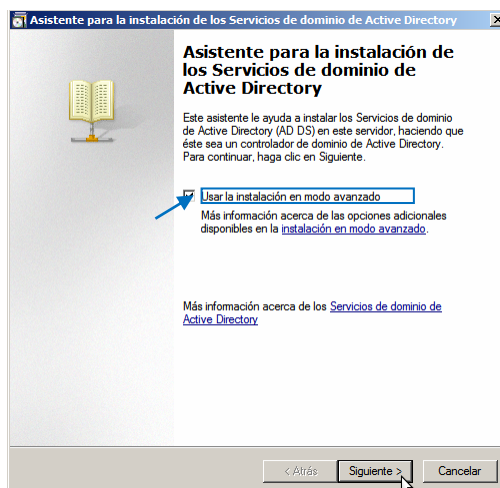


Figura G12. Habilitar el modo avanzado de instalación

AD mantiene un esquema de organización jerárquica en la que el punto de partida es el objeto, que lo integran los usuarios, grupos, recursos compartidos y servicios, a los que Microsoft los identifica como frutos; cada fruto está dispuesto para pertenecer a una Unidad Organizativa, que representaría en el entorno del CEE a cada Departamento, y toda esta organización jerárquica integra un dominio o árbol (véase Figura G13).

Dependiendo de la dimensión de las empresas en ocasiones es necesario crear subdominios o implementar varios dominios para administrar de mejor manera sus dependencias, o puede suceder que se vinculen dominios pertenecientes a empresas diferentes que necesiten trabajar en conjunto; en cualquier situación lo que se pretende puntualizar es que dentro de la jerarquía AD existe un elemento denominado bosque, que hace referencia al conjunto de dominios y subdominios administrados bajo el mismo controlador.

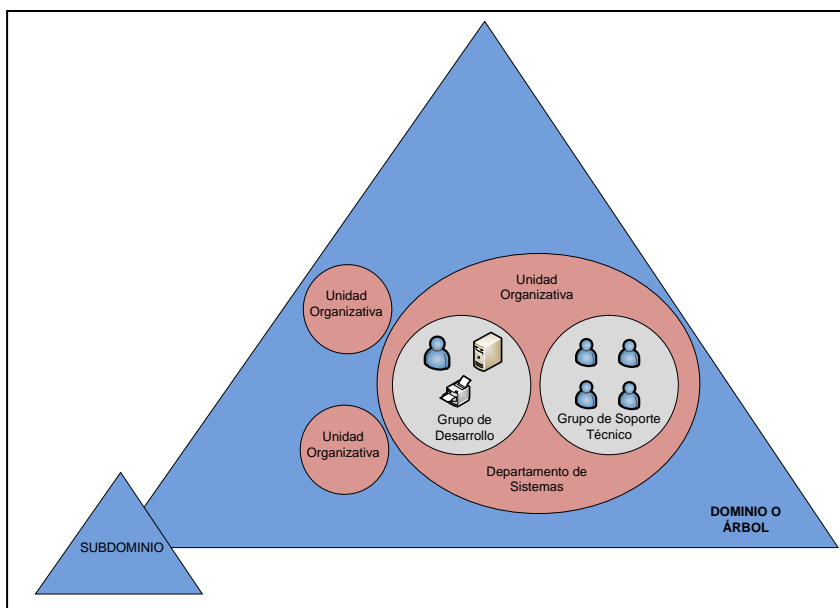


Figura G13. Estructura Jerárquica de Active Directory

Fuente: Elaborado a partir de Morales, S. Configuración del Active Directory Domain Services a nivel Básico – Módulo 5. Recuperado de https://www.youtube.com/watch?v=sgOz_v5rJpQ

Teniendo claro los elementos de esta jerarquía se puede retomar la instalación, y en esta parte el asistente pregunta si se quiere crear un nuevo bosque, o si se dispone de uno creado previamente (véase Figura G14).

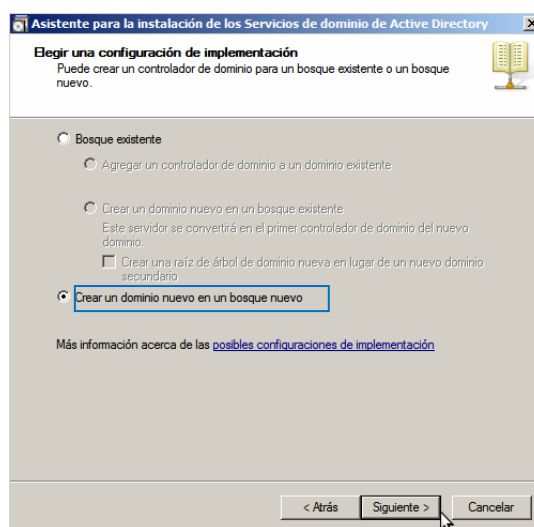


Figura G14. Generar un nuevo bosque

Especificar el nombre del dominio de la organización, tal como se lo ha venido manejando durante todo el proyecto se utilizará el dominio real del CEE (cee.gob.ec) para desarrollar este controlador de dominio local (véase Figura G15).

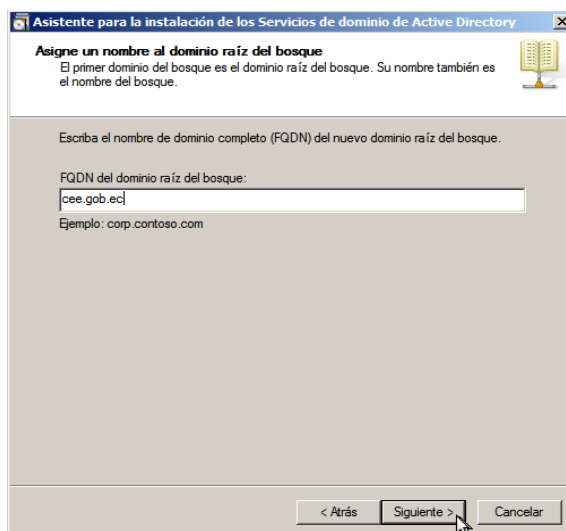


Figura G15. Definir el dominio del Bosque

El NetBIOS es el nombre con el cual los ordenadores identifican al dominio, y durante la instalación este asistente sugiere un nombre NetBIOS (CEE) derivado del dominio definido anteriormente (cee.gob.ec) (véase Figura G16).

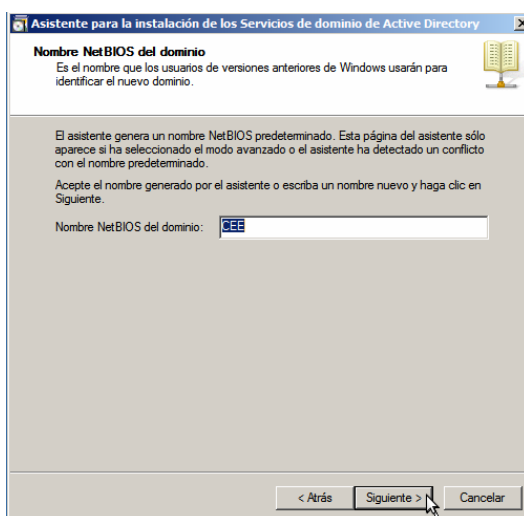


Figura G16. Definir el nombre del NetBIOS

Luego existe la posibilidad de definir el nivel funcional tanto del bosque como del dominio, entre Windows 2000 y 2003, esto se refiere a la gama de funciones que el servidor está destinado a suministrar, y es recomendable elegir Windows 2003 debido a que además de contener las características de Windows 2000, incluye otras adicionales (véase Figuras G17 y G18).

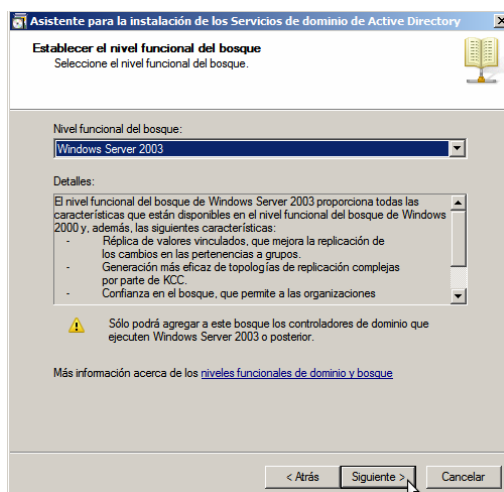


Figura G17. Definir el nivel funcional del bosque

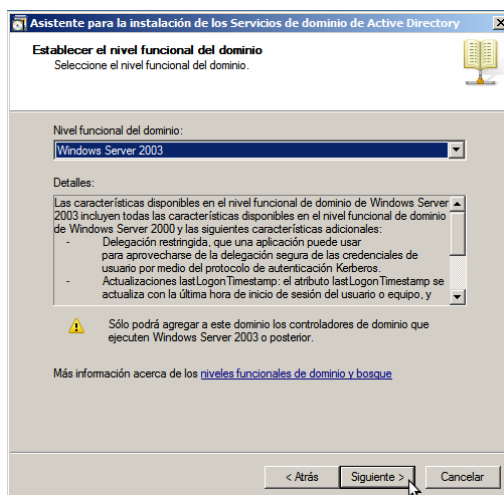


Figura G18. Definir el nivel funcional del dominio

Marcar la casilla de DNS para que instale también esta opción de servicio adicional, para que este mismo servidor ejecute la resolución de nombres (véase Figura G19).

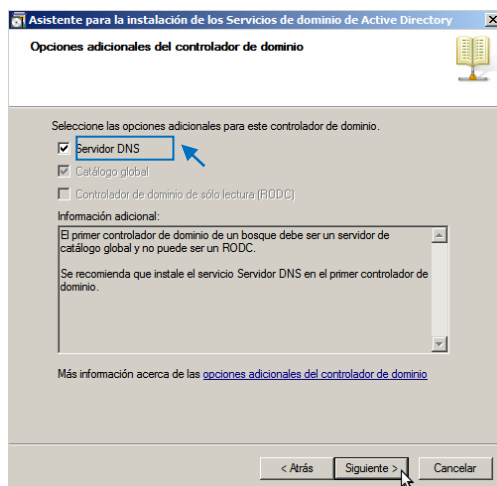


Figura G19. Incluir el servicio de DNS

Especificar el directorio en el que se almacenará la información de la base de datos y los archivos de registro del servicio, por defecto el asistente sugiere una ubicación adecuada para ello, por ese motivo no ha sido necesario modificarlo (véase Figura G20).

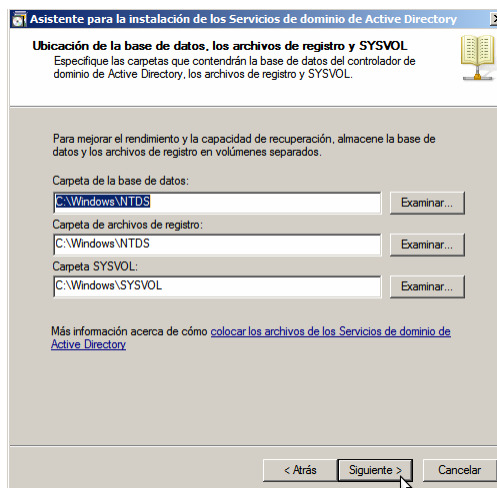


Figura G20. Ubicación de la base de datos de AD y los archivos de registro del servicio

Ingresar la contraseña de la cuenta de Administrador del modo de restauración de servicios de directorio, que deberá estar integrada por letras mayúsculas, minúsculas y números, con una longitud de 12 caracteres, si no se cumple con estas políticas de contraseña segura el asistente de instalación la reconocerá como insegura e inválida (véase Figura G21).

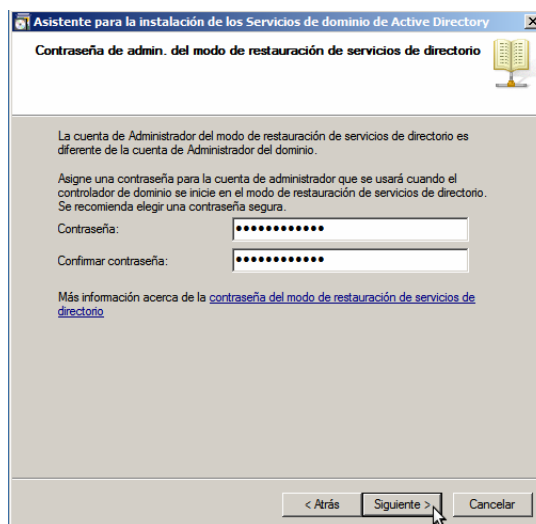


Figura G21. Contraseña del modo restauración del servicio de directorio

La cuenta de Administrador del modo de restauración de servicios de directorio permite únicamente la validación local ante el equipo servidor, no ante el dominio, y es utilizada para acceder a este equipo en modo seguro y ejecutar una copia de seguridad del sistema para recuperarlo a un estado anterior de funcionamiento.

Las credenciales que se deben suministrar para validarse ante el dominio, son las de la cuenta de usuario Administrador del Dominio; ambas cuentas serán creadas automáticamente durante este proceso instalación, pero aunque son cuentas de administración diferentes, el asistente de instalación emplea la contraseña definida en la Figura G21 como credencial para ambas.

Finalmente aparecerá una pantalla de resumen que contiene todas las operaciones que se van a efectuar sobre el sistema (véase Figura G22).

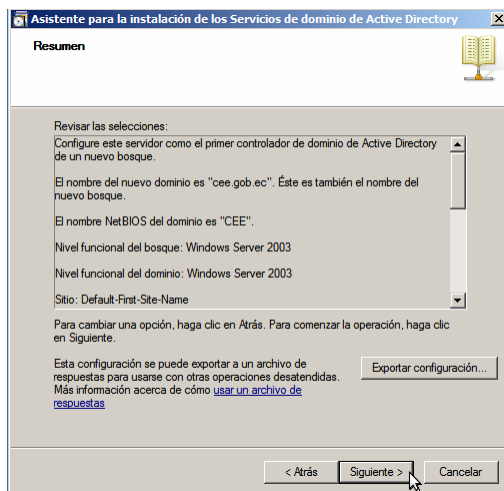


Figura G22. Operaciones que serán ejecutadas sobre el sistema

Al culminar la instalación el sistema se reiniciará automáticamente y después de cargar todos los servicios para iniciarlo aparecerá la pantalla de validación con el nombre del controlador de dominio (véase Figura G23). Acceder al sistema autenticándose con la contraseña de usuario Administrador definida.

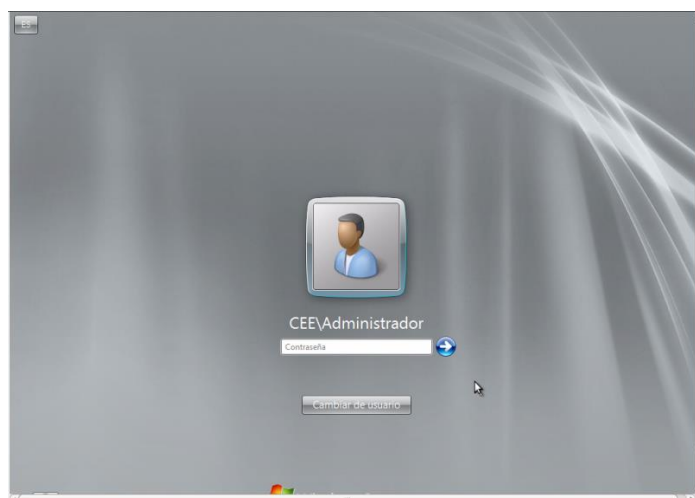


Figura G23. Inicio del Sistema Controlador de Dominio

Durante la instalación del controlador de dominio sucede que la dirección IP del DNS del adaptador de red será modificada y reemplazada por la de loopback 127.0.0.1, entonces se debe deshacer ese cambio utilizando la propia IP del servidor (véase Figura G24).

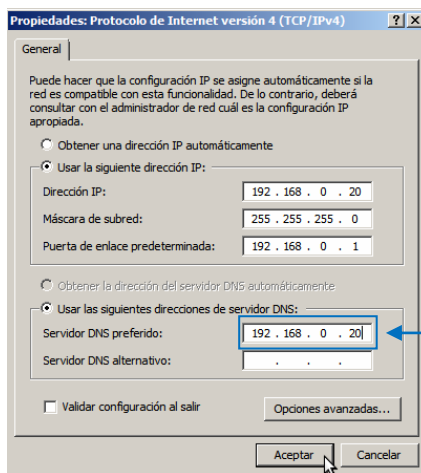


Figura G24. Configurar la dirección IP del DNS del servidor

Verificar que el sufijo DNS para esta conexión se haya agregado, si no es el caso se debe agregarlo (véase Figura G25).

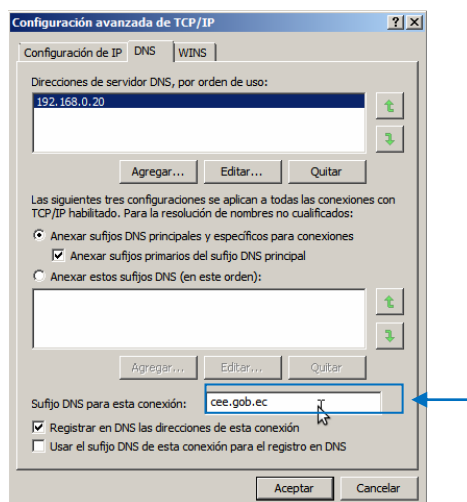


Figura G25. Configurar el sufijo del DNS del servidor

Entonces es posible visualizar el nombre completo del equipo servidor (FQDN⁵⁴) y el dominio al que está vinculado (véase Figura G26).

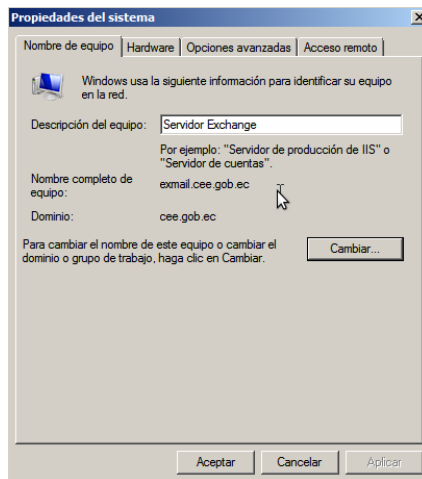


Figura G26. Propiedades del equipo servidor

Para complementar la fase de preparación de este servidor es necesario crear la zona inversa del servicio de DNS, debido a que la zona directa la crea Active Directory automáticamente; para ello acceder a la Consola de Administración del DNS como se muestra en la Figura G27.

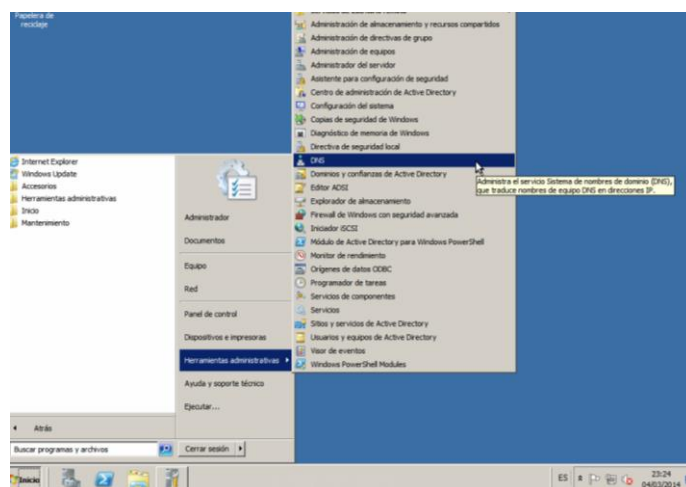


Figura G27. Procedimiento para ingresar a la Administración del DNS

⁵⁴ Fully Qualified Domain Name

Seleccionar la opción Zonas de búsqueda inversa con clic derecho y en Zona nueva (véase Figura G28), esto ejecutará el asistente que guiará paso a paso.

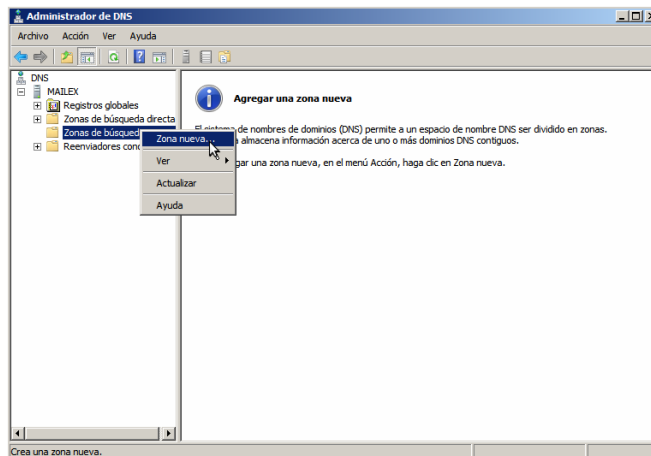


Figura G28. Creación de la Zona Inversa

La zona que se requiere crear es una zona principal (véase Figura G29).

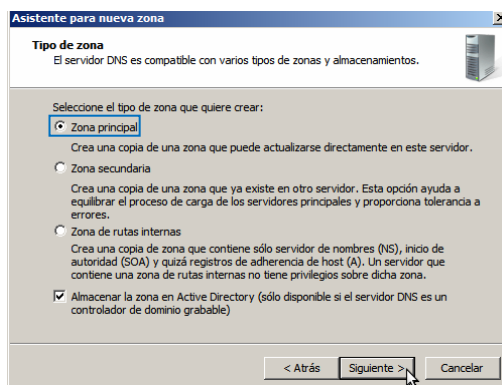


Figura G29. Especificar el tipo de Zona

A esta altura del desarrollo de este anexo se tiene claro que un bosque puede estar integrado por uno o varios dominios y subdominios, entonces habrá que especificar cuál es el alcance en el que esta zona del DNS será válida, para todo el bosque o sólo para algún dominio en especial, en este caso la opción más adecuada es que sea válida para el dominio configurado cee.gob.ec (véase Figura G30).

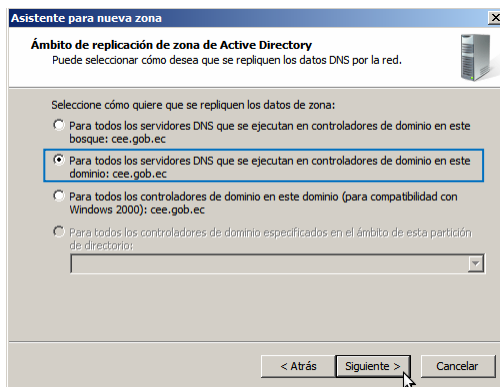


Figura G30. Especificar el alcance que tendrá la zona a crearse

Definir el tipo de direccionamiento IP que esta zona del DNS deberá resolver (véase Figura G31).

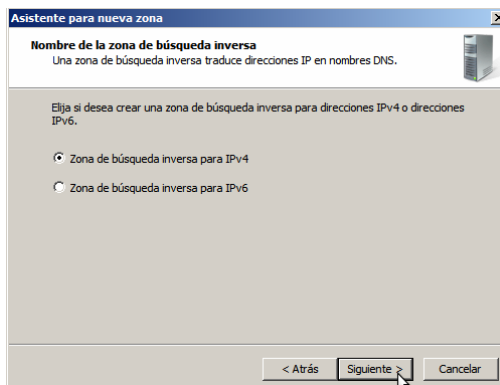


Figura G31. Tipo de Direccionamiento IP que esta zona traducirá

Ingresar los tres primeros octetos que identifican a la red sobre la que se va a implementar el servicio de resolución de nombres (véase Figura G32).

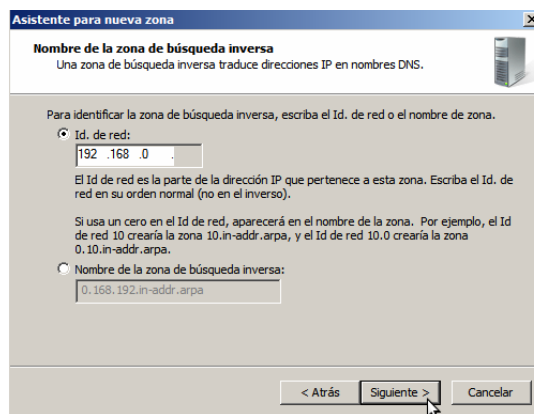


Figura G32. Dirección IP de Red de la zona inversa a crearse

Con esto se concluye y la zona inversa ha sido creada (véase Figura G33).

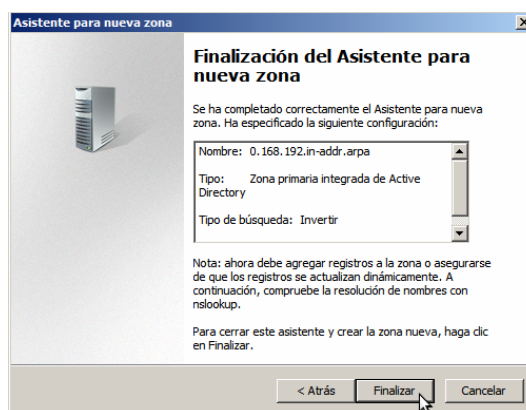


Figura G33. La zona inversa ha sido creada

Ahora lo que se requiere es agregar un nuevo host en esta zona, que va a representar a este servidor, para que mediante la resolución de nombres sea identificado en el entorno de la red del CEE, cuando se realicen peticiones de búsqueda empleando su dirección IP. Entonces se agrega un nuevo puntero (véase Figura G34).

Ingresar la dirección de red a la que pertenece el servidor, en este caso a la red 192.168.0, y pulsar Examinar para encontrar el registro correspondiente a este servidor (192.168.0.20) definido en la zona directa (véase Figura G35).

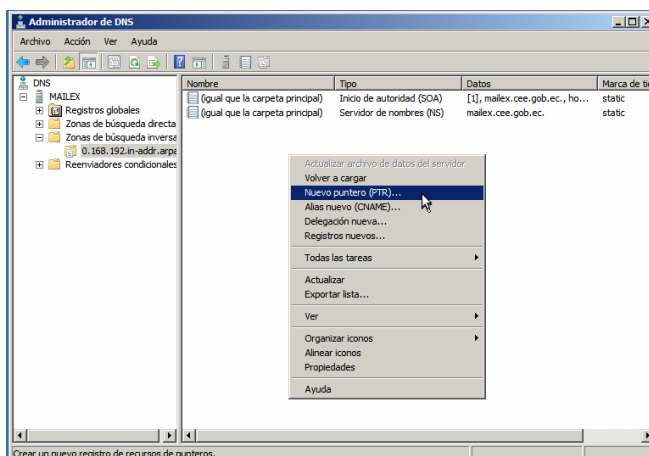


Figura G34. Agregar un nuevo host en la zona inversa

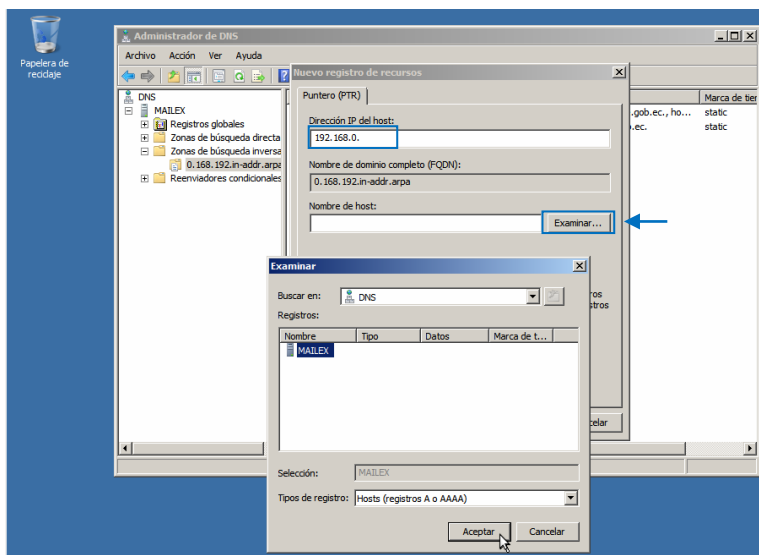


Figura G35. Búsqueda del registro correspondiente

Para que un host configurado en los registros del DNS sea identificado en la red, debe haber sido definido tanto de la zona directa como en la inversa, de manera que las peticiones de búsqueda hacia el host mailex.cee.gob.ec por ejemplo, puedan ser efectuadas también empleando su dirección IP 192.168.0.20.

Ingresar a la zona de búsqueda directa del DNS (véase Figura G36).

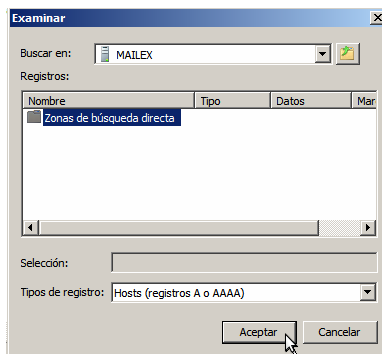


Figura G36. Zona Directa

Seleccionar el dominio configurado (véase Figura G37).

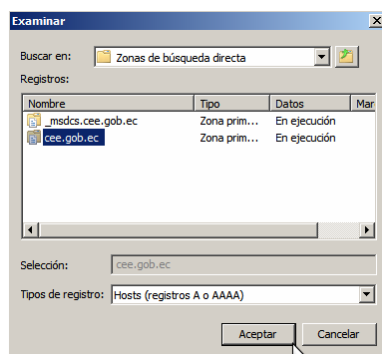


Figura G37. Dominio del CEE

Elegir el registro del host que identifica al servidor (véase Figura G38).

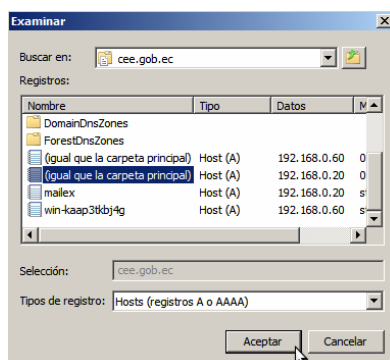


Figura G38. Registro definido para el servidor

Con ello se crea el puntero para que este servidor sea accesible desde la red (véase Figura G39).

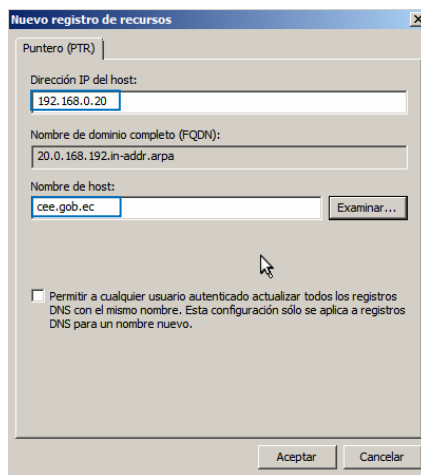


Figura G39. Dirección IP y dominio al que pertenece el servidor

Un factor importante en un DNS es la capacidad que tiene para resolver consultas DNS de registros que no se encuentran en el servidor, como es el caso más común de una página web de internet, para ello los DNS utilizan otros servidores DNS externos denominados reenviadores (forwarders) y proporcionar de esta forma acceso a este tipo de registros.

La configuración de estos reenviadores se efectúa accediendo a las propiedades del servidor DNS en desarrollo, en la pestaña llamada precisamente Reenviadores (véase Figura G40).

Los reenviadores DNS que se deben ingresar son los que proporciona el proveedor del servicio de internet, sea el caso de un servicio residencial o empresarial (véase Figura G41), y finalmente aceptar y aplicar para que se conserven los cambios.

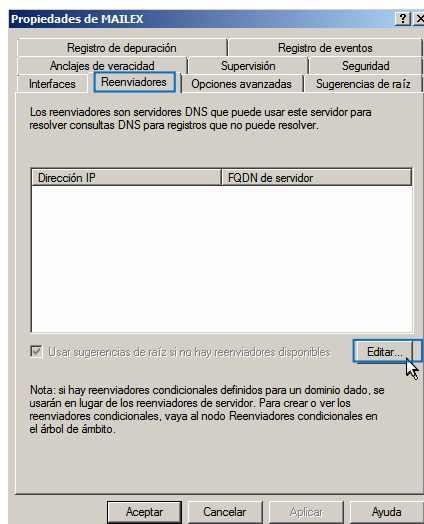


Figura G40. Parámetros de configuración DNS

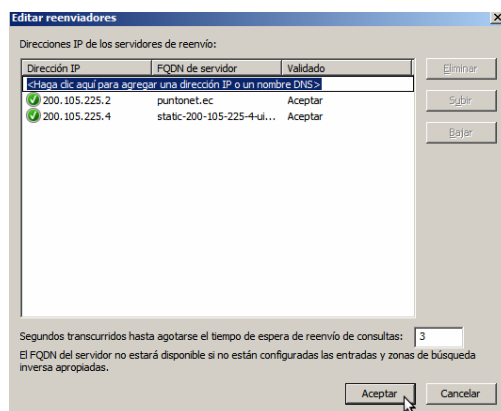


Figura G41. Agregar los DNS del proveedor de internet

Para esta simulación también se necesita agregar en los registros del DNS un host nuevo con su respectiva zona inversa, que identifique al servidor de correo zimbra (mail.cee.gob.ec), con su dirección 192.168.0.30; entonces agregarlo desde la consola de administración DNS (véase Figura G42).

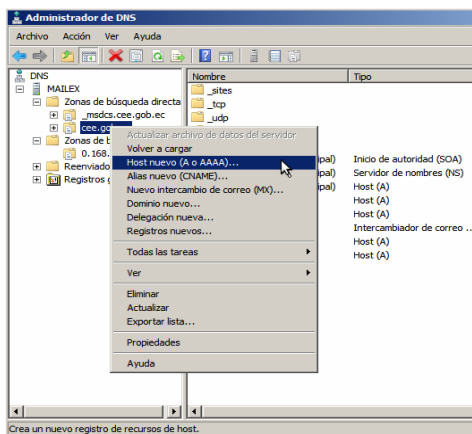


Figura G42. Agregar al servidor Zimbra

Definir el nombre del servidor zimbra y su dirección IP, percatándose de marcar la casilla de creación del puntero PTR en la zona inversa, y agregamos al host (véase Figura G43).

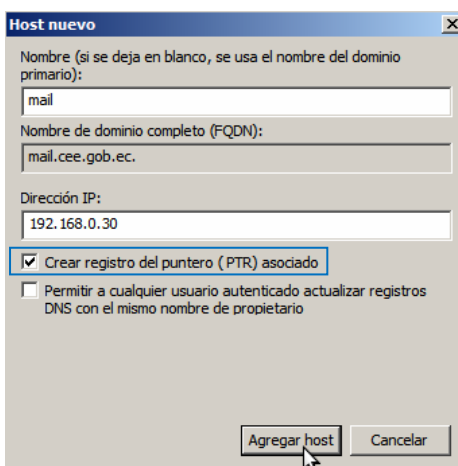


Figura G43. Parámetros que identifican al servidor Zimbra

Desde una consola de terminal del servidor ejecutar el comando `nslookup` para verificar el funcionamiento del DNS (véase Figura G44).

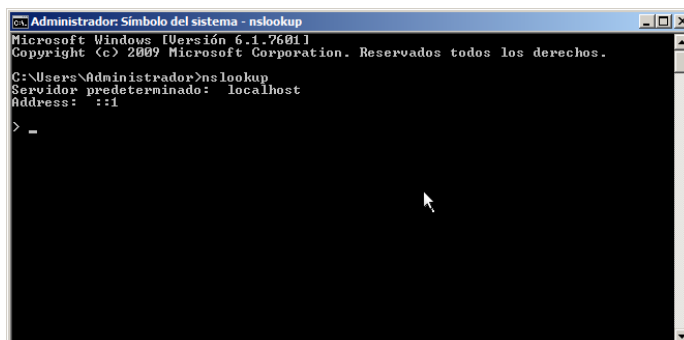


Figura G44. Prueba de funcionamiento del DNS

Normalmente en Servidor predeterminado debería mostrar el dominio al que está vinculado el servidor, y en Address su dirección IP, pero en este caso está mostrando el DNS definido para IPv6, habrá que acceder a la configuración del adaptador de red y modificarla (véase Figura G45).

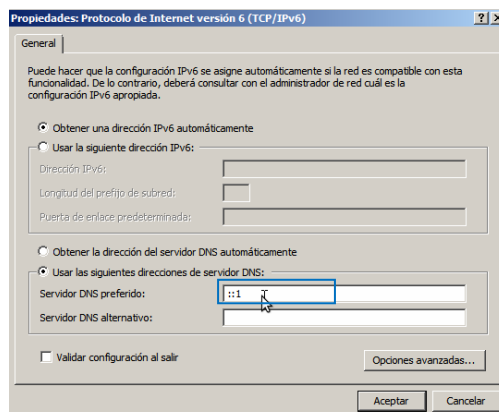
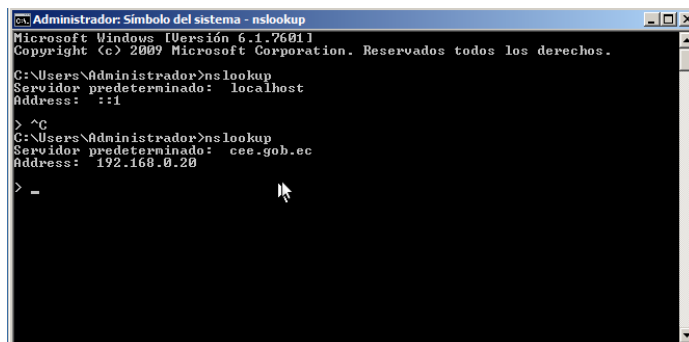


Figura G45. Configuración de TCP/IP v6

Como se había mencionado este era el problema, cambiarlo a la opción Obtener la dirección del servidor DNS automáticamente y guardar los cambios para solucionarlo. Ejecutar nuevamente el comando nslookup para verificarlo (véase Figura G46).



```

Administrador: Símbolo del sistema - nslookup
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\Administrador>nslookup
Servidor predeterminado: localhost
Address: ::1

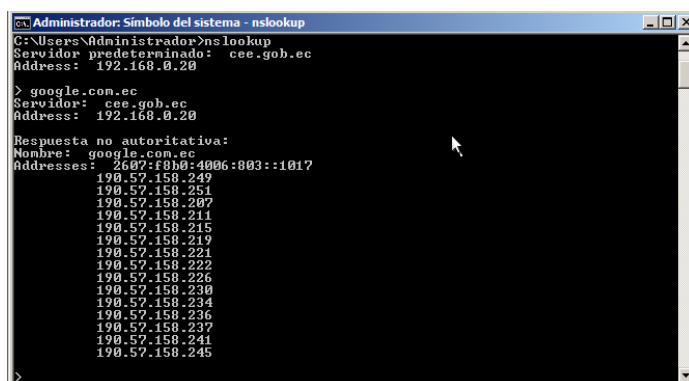
> ^C
C:\Users\Administrador>nslookup
Servidor predeterminado: cee.gob.ec
Address: 192.168.0.20

> =

```

Figura G46. Prueba de funcionamiento del DNS

Efectivamente el problema se solventó y ahora hay que hacer una solicitud de búsqueda de DNS para el sitio www.google.com.ec y esperar a que lo resuelva (véase Figura 47).



```

Administrador: Símbolo del sistema - nslookup
C:\Users\Administrador>nslookup
Servidor predeterminado: cee.gob.ec
Address: 192.168.0.20

> google.com.ec
Servidor: cee.gob.ec
Address: 192.168.0.20

Respuesta no autoritativa:
Nombre: google.com.ec
Addresses: 2607:F80:406:803::1017
          190.57.158.249
          190.57.158.251
          190.57.158.207
          190.57.158.211
          190.57.158.215
          190.57.158.219
          190.57.158.221
          190.57.158.222
          190.57.158.226
          190.57.158.230
          190.57.158.234
          190.57.158.236
          190.57.158.237
          190.57.158.241
          190.57.158.245

```

Figura G47. Solicitud DNS de búsqueda de google

En tal virtud, ya se tienen los preparativos para la instalación de Microsoft Exchange, al disponer de un Controlador de Dominio y un DNS en operación.

3. INSTALACIÓN DE MICROSOFT EXCHANGE 2010

De acuerdo a la guía de requisitos publicada en los repositorios oficiales de Microsoft [http://technet.microsoft.com/es-es/library/bb691354\(v=exchg.140\).aspx](http://technet.microsoft.com/es-es/library/bb691354(v=exchg.140).aspx), la

instalación de este sistema de correo requiere ciertos paquetes y configuraciones previas a la ejecución de Exchange.

Lo primero que se debe hacer es descargar el paquete Microsoft Filter Pack desde la dirección <http://www.microsoft.com/es-es/download/details.aspx?id=20109> que sugiere esta guía, dependiendo del sistema operativo del servidor, en este caso 64 bits (véase Figura G48).

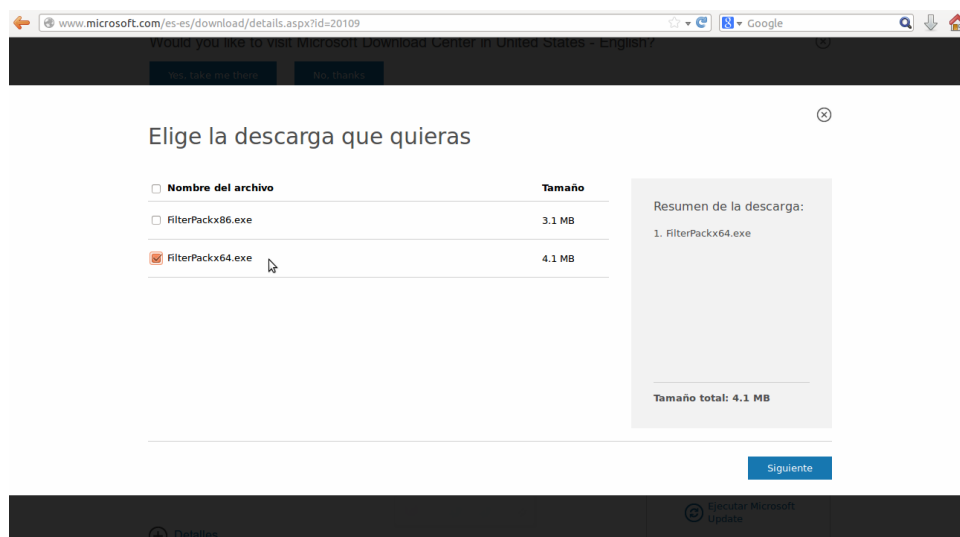


Figura G48. Descarga de Microsoft Filter Pack x64

La instalación de este paquete mejora el servicio de búsqueda de Windows, al proveer filtros (IFiltres) que admiten diversos escenarios de búsqueda sobre varios productos de Microsoft, por ejemplo metro (.docx, .docm, .pptx, .pptm, .xlsx, .xlsm, .xlsb), visio (.vdx, .vss, .vst, .vdx, .vsx, .vtx), OneNote (.one), zip (.zip), entre otros, esto mejorará el motor de búsqueda de Exchange.

Ejecutar este paquete cuya instalación es relativamente sencilla, percatarse de revisar el mensaje de propiedad intelectual y presionar **Siguiente** (véase Figura G49).



Figura G49. Instalación de Filter Pack x64

Examinar los términos de licencia de software para aceptarlos (véase Figura G50), y esperar un momento a que culmine la instalación.

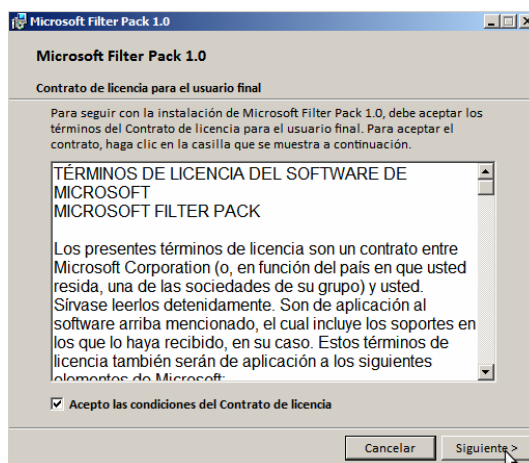


Figura G50. Acuerdos de Licencia de Software

Acceder como administrador a una consola de Windows PowerShell (véase Figura G51).

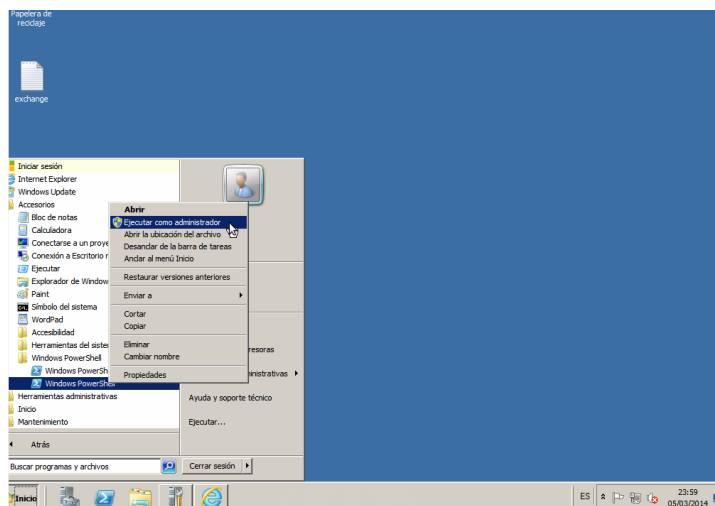


Figura G51. Ejecución de Windows PowerShell

Cargar el Módulo de Administración de Servicios para agregar los roles necesarios de este servidor, ejecutando el comando `Import-Module ServerManager` (véase Figura G52).



Figura G52. Ejecución de Windows PowerShell

Elegir la opción 3a de esta guía de requisitos, que describe la preparación para un servidor destinado a desempeñar roles de Acceso de clientes, Transporte de Concentradores y Buzón de Correo, que es una instalación de roles típica para Exchange.

Entonces ejecutar el comando `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`, para instalar los componentes necesarios del sistema operativo (véase Figura G53).

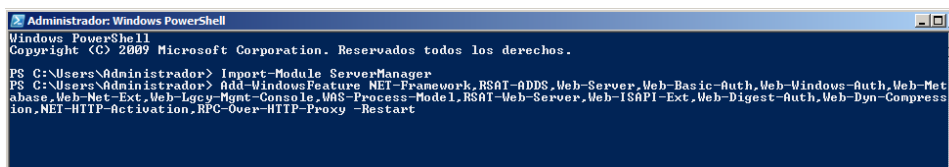


Figura G53. Instalar los componentes necesarios del sistema operativo para Exchange 2010

Al finalizar la instalación el sistema se reiniciará, y es necesario acceder a la configuración de los Servicios del sistema (véase Figura G54), mediante Inicio + Herramientas Administrativas + Servicios.

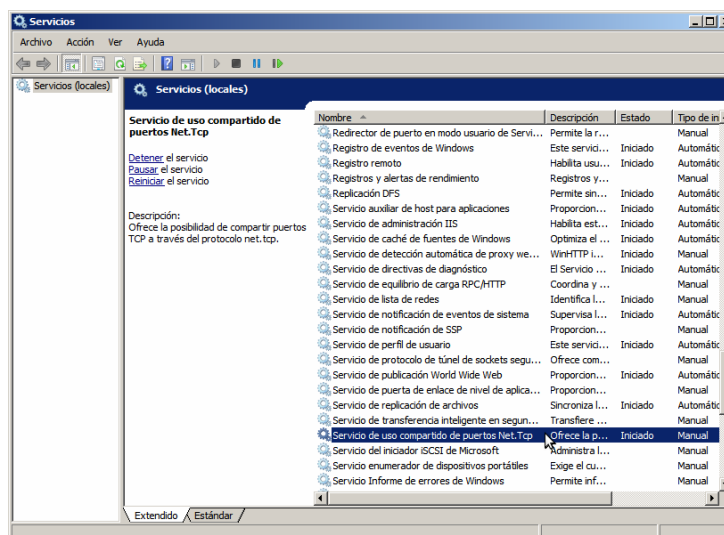


Figura G54. Ejecución del Administrador de Servicios

Este servidor desempeñará el rol de Acceso de Cliente, en tal virtud, el Servicio de uso compartido de puertos Net.Tcp debe estar configurado para ejecutarse automáticamente (véase Figura G55).

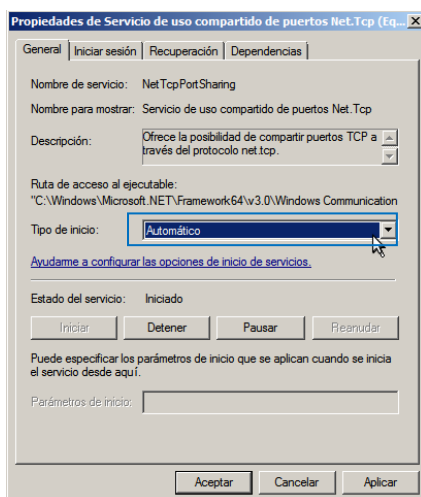


Figura G55. Tipo de ejecución de este Servicio

La descarga del paquete de instalación de Exchange Server 2010 se la realizó desde los repositorios oficiales de Microsoft <http://www.microsoft.com/eses/download/details.aspx?id=21308>, siendo un proceso muy sencillo y que no tiene costo. Acceder a los ficheros del paquete descargado y ejecutar el instalador (véase Figura G56).

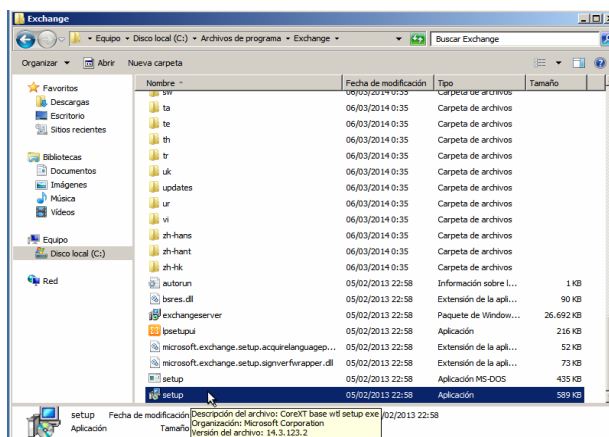


Figura G56. Ejecución del Asistente de instalación de Exchange

Este asistente inicia comprobando si varios de los requisitos previos han sido instalados en el sistema operativo, y al finalizar este proceso activa la opción de instalación de Exchange (véase Figura G57).

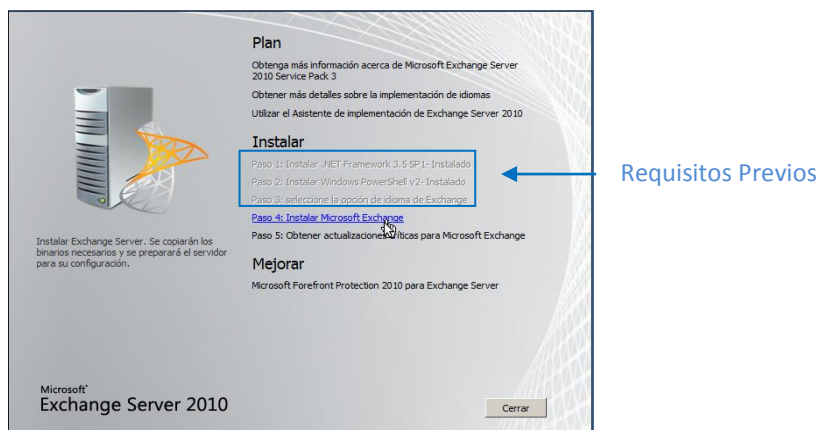


Figura G57. Instalación de Exchange Server

Inmediatamente se muestra una pantalla informativa de sus funcionalidades y beneficios, y tras analizar los Términos de Licencia de este software deberemos aceptarlos (véase Figura G58).

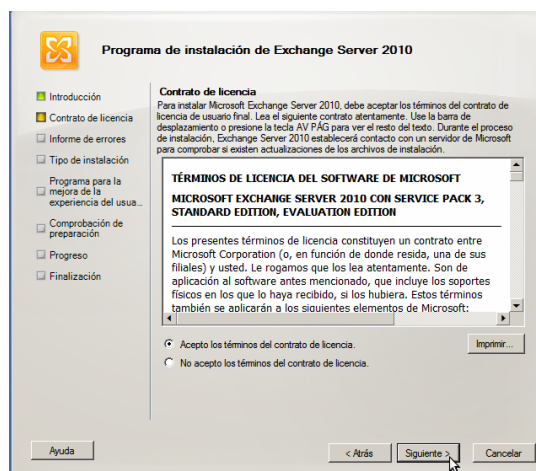


Figura G58. Términos de Licencia de Exchange

Es preferible habilitar la opción informe de errores para permitir que en caso de suscitarse eventos inesperados en este servicio, enviarlos a Microsoft para que los analice y ayude a solucionarlos (véase Figura G59).

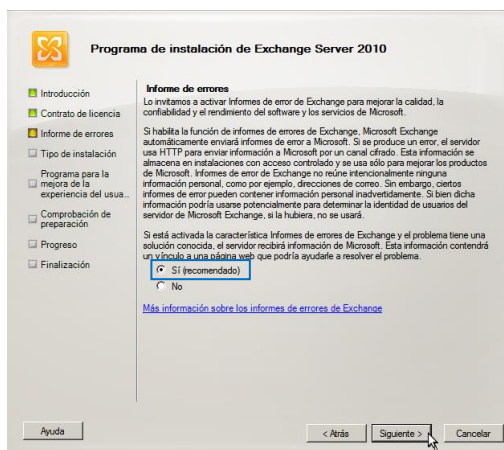


Figura G59. Habilitar el envío de Informes de error

Elegir la instalación típica de Exchange (véase Figura G60).



Figura G60. Tipo de Instalación

Ingresar el nombre de la organización sobre la que se prestará el servicio de correo Exchange, en este caso es el Cuerpo de Ingenieros del Ejército - CEE (véase Figura G61).

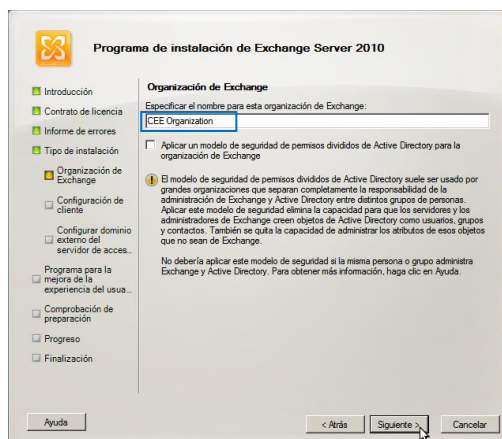


Figura G61. Definir el nombre de la Organización

Si en la organización sobre la que se implementará este servicio de correo existen clientes Outlook 2003, éstos necesitarán una base de datos de carpetas públicas para establecer conexión con el servidor Exchange, pero en el caso de este proyecto el CEE no dispone de este tipo de usuarios, por lo que no es necesario habilitar esta opción en el asistente (véase Figura G62); sin embargo, es posible habilitar esta conectividad más adelante, si resulta necesaria.

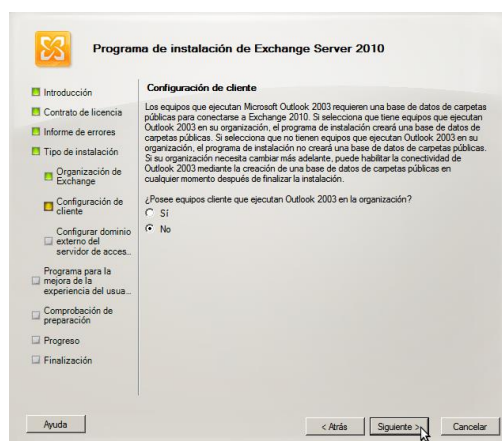


Figura G62. Conectividad con Outlook 2003

Se llevará a cabo un análisis del sistema operativo para verificar si los requisitos y configuraciones previas a la instalación hayan sido efectuadas (véase Figura G63).



Figura G63. Requisitos y Configuraciones previas

Al finalizar este análisis se activará la opción Instalar para iniciar la instalación de Exchange (véase Figura G64).



Figura G64. Instalación de Exchange

Finalmente la instalación se completará cuando todos los ítems se encuentren marcados con un visto verde (véase Figura G65).



Figura G65. Instalación de Exchange

Ahora lo que se debe hacer es crear una Unidad Organizativa y agregar usuarios a la base de datos de Active Directory, cada uno estará vinculado a una dirección de correo electrónico administrada por Exchange. Para ello acceder a la consola de administración del controlador de dominio (véase Figura G66) pulsando Inicio + Herramientas Administrativas + Usuarios y Grupos de Active Directory.

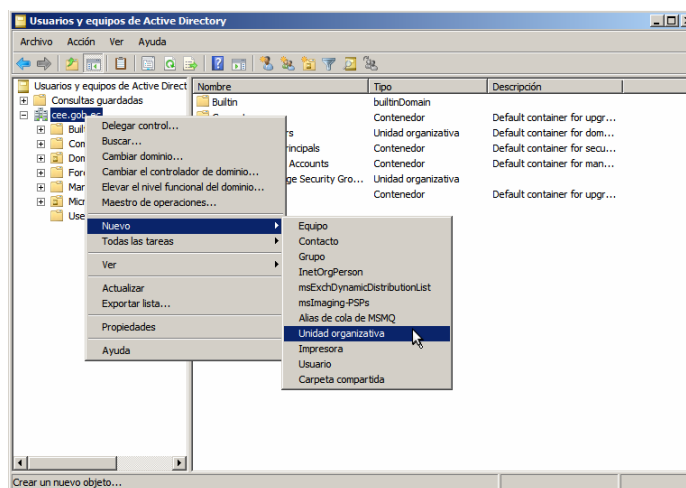


Figura G66. Creación de una Unidad Organizativa

Definir el nombre de la Unidad Organizativa (véase Figura G67).

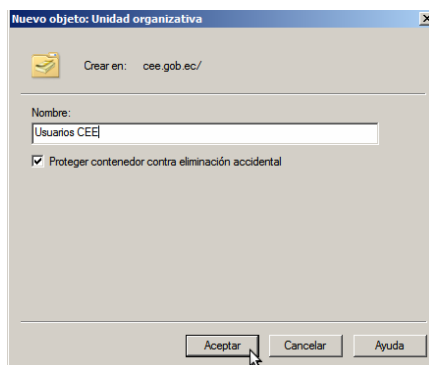


Figura G67. Nombre de la Unidad Organizativa

Desde esta consola se pueden crear varios objetos y organizarlos en grupos o unidades organizativas, bajo la administración de Active Directory, pero en este caso se realizará un solo proceso de creación de los usuarios y sus cuentas de correo desde la consola de administración de Exchange, en el apartado Configuración de Destinatarios, utilizando la Unidad Organizativa creada (véase Figura G68). Para acceder a esta consola pulsar Inicio + Microsoft Exchange Server 2010 + Exchange Management Console.

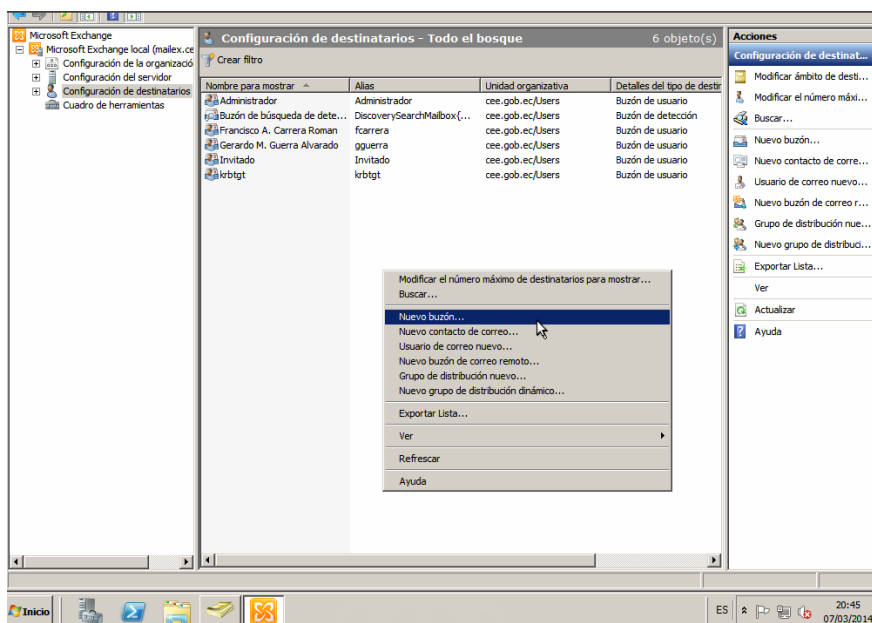


Figura G68. Creación de un nuevo buzón de usuario

Seleccionar la alternativa buzón de usuario (véase Figura G69).

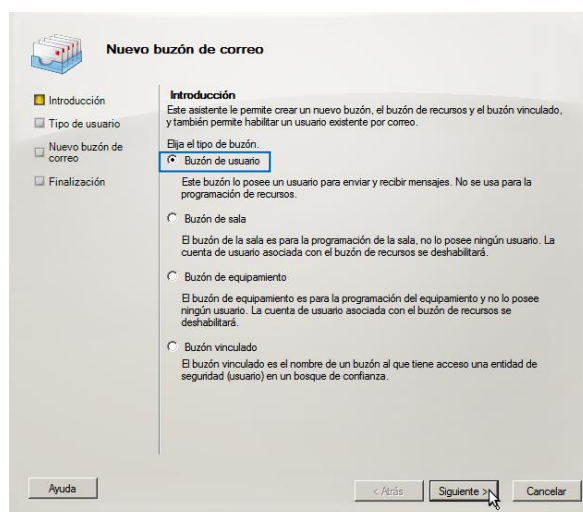


Figura G69. Definir el tipo de buzón

Existe la posibilidad de crear buzones para nuevos usuarios, es decir que se generará el buzón en Exchange y el usuario respectivo en la base de datos de Active Directory, o también buzones para usuarios existentes en Active Directory, en este caso crearemos el usuario y su buzón (véase Figura G70).

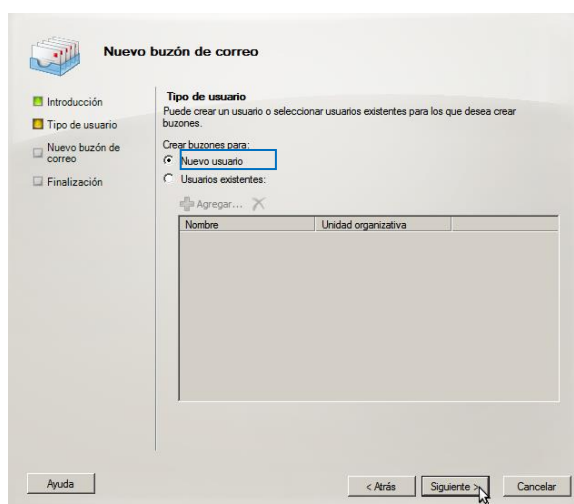


Figura G70. Buzón para un nuevo usuario

Seleccionar la Unidad Organizativa a la que pertenecerá el usuario (véase Figura G71).

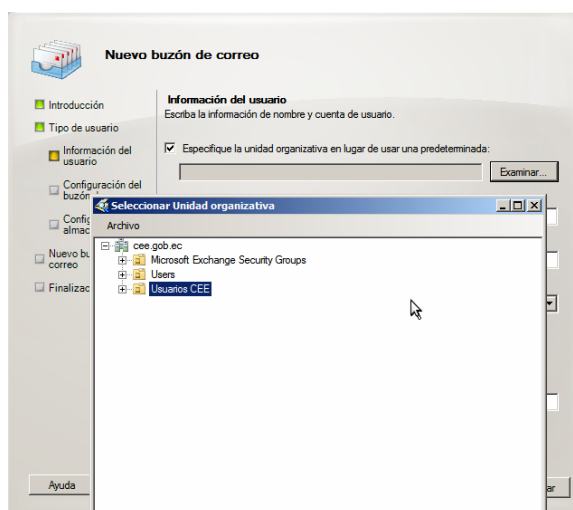


Figura G71. Unidad Organizativa del nuevo usuario

Ingresar la información del usuario (Ramiro Buchelli), en esta caso se ha mantenido el estándar del CEE para definir las direcciones de correo, es decir la primera letra del nombre y el primer apellido completo (rbuchelli) (véase Figura G72).

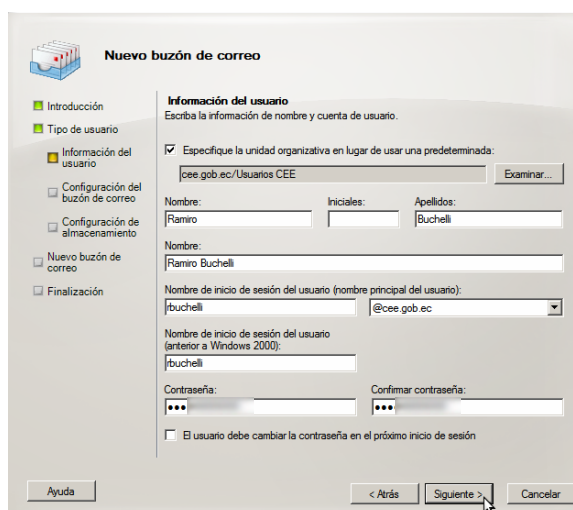


Figura G72. Datos del usuario

Establecer la base de datos de buzones del sistema de correo MAILEX configurado, en lugar de emplear una definida automáticamente (véase Figura G73).

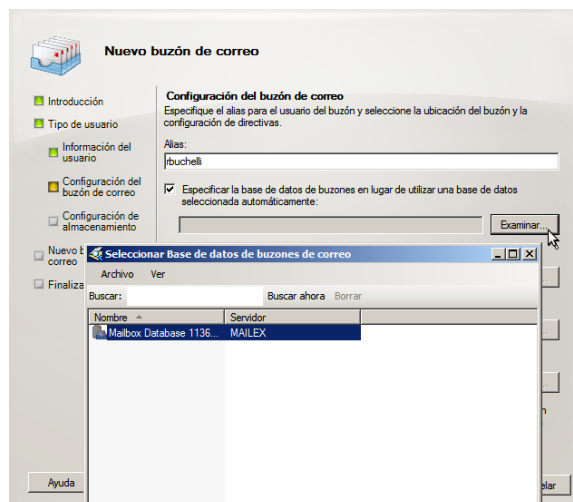


Figura G73. Base de Datos de buzones

Con ello el proceso de creación del buzón y el usuario iniciará y si todo se ha efectuado con normalidad debería mostrar una pantalla como la de la Figura G74.

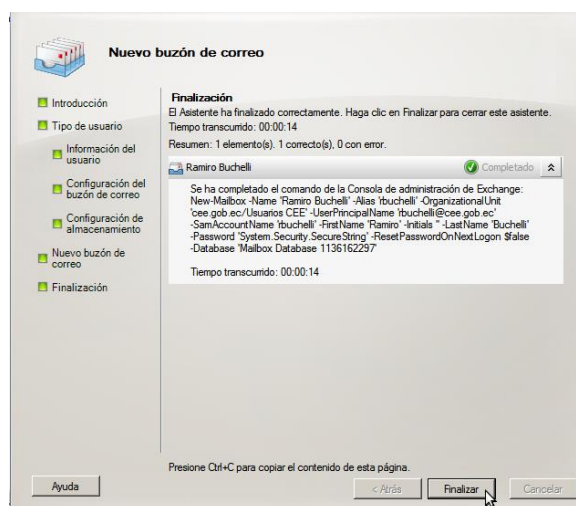


Figura G74. La creación ha sido exitosa

De esta forma se puede verificar en la consola de administración de Exchange el nuevo usuario creado (véase Figura G75). Se puede apreciar el usuario, el alias, la Unidad

Organizativa a la que pertenece y otros detalles adicionales, pero también se destaca que se han creado previamente tres usuarios adicionales a este, utilizando el mismo procedimiento, aunque dos de ellos pertenezcan a una Unidad Organizativa diferente, y también el usuario administrador del sistema que se crea por defecto durante la instalación.

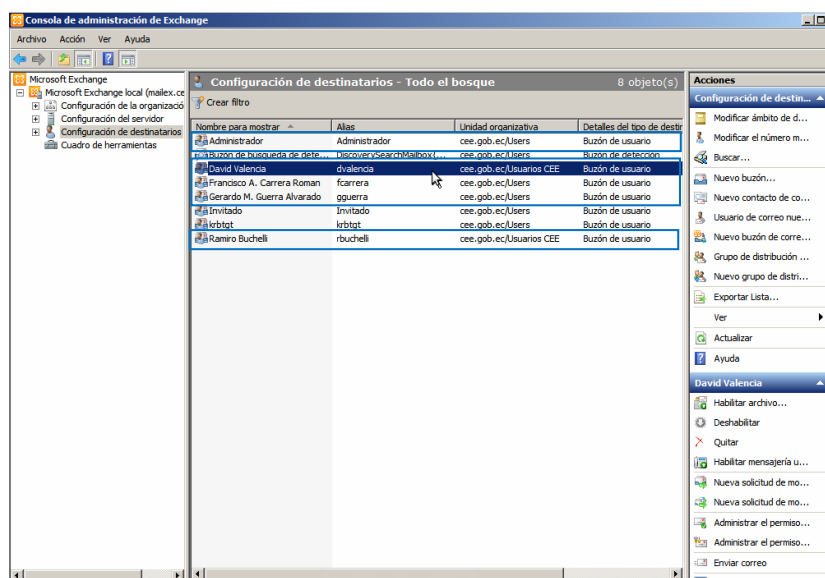


Figura G75. Usuarios creados en Exchange Server

De igual manera se puede verificar que se han agregado estos usuarios en la base de datos de Active Directory, en la Unidad Organizativa respectiva (véase Figura G76).

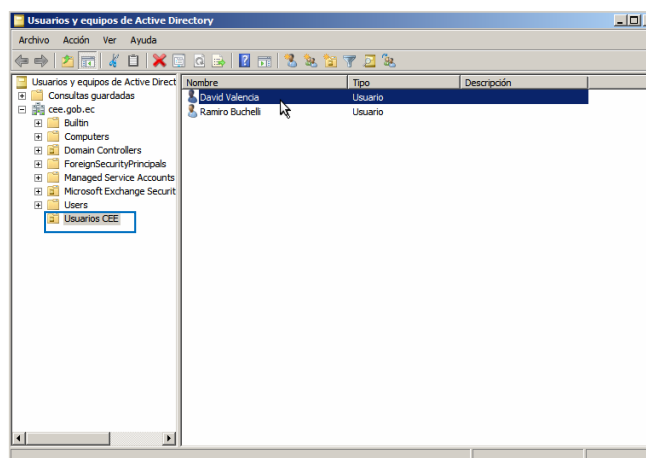


Figura G76. Usuarios creados en Active Directory

Se realizará una prueba simple de funcionalidad de Exchange Server 2010, accediendo a través de la interfaz webmail a los buzones de usuario, y efectuando el envío de mensajes. La dirección para acceder a esta interfaz es <https://cee.gob.ec/owa> (véase Figura G77).

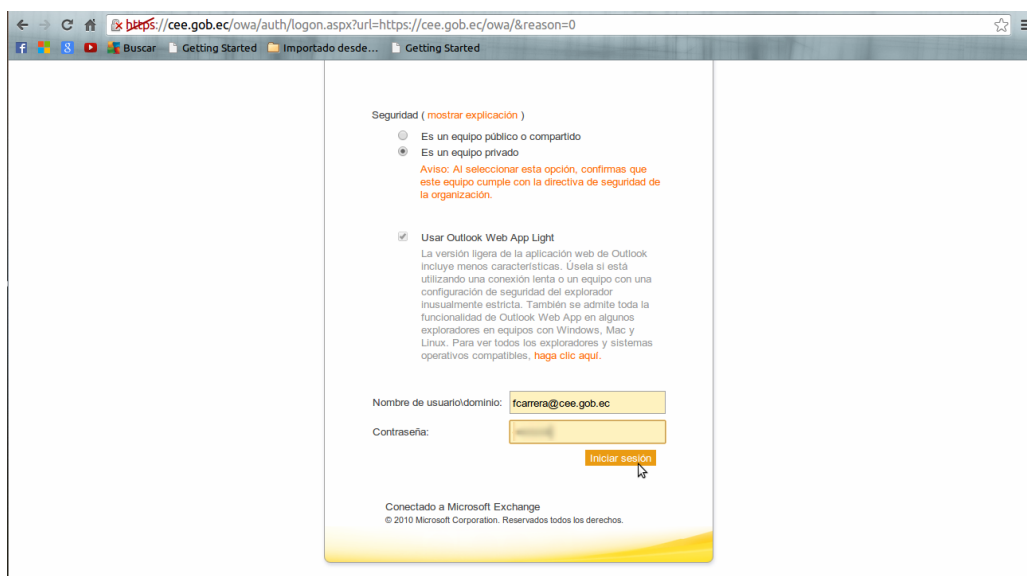


Figura G77. Interfaz webmail de Exchange Server 2010

Tras ingresar las credenciales de autenticación (por ejemplo de Francisco Carrera) se tendrá acceso a su buzón para editar un mensaje y enviarlo (véase Figura G78).

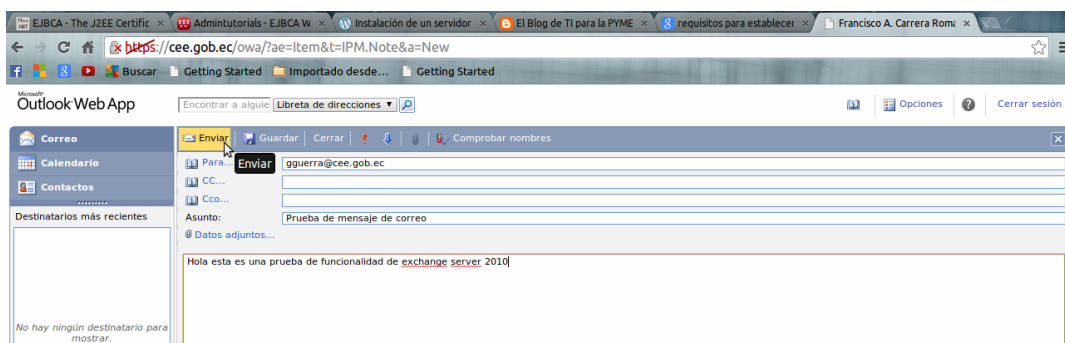


Figura G78. Generación y envío de un mensaje de correo electrónico

Desde el extremo del receptor de este mensaje (Gerardo Guerra) accedemos de igual manera a su buzón y verificamos su bandeja de entrada (véase Figura G79).

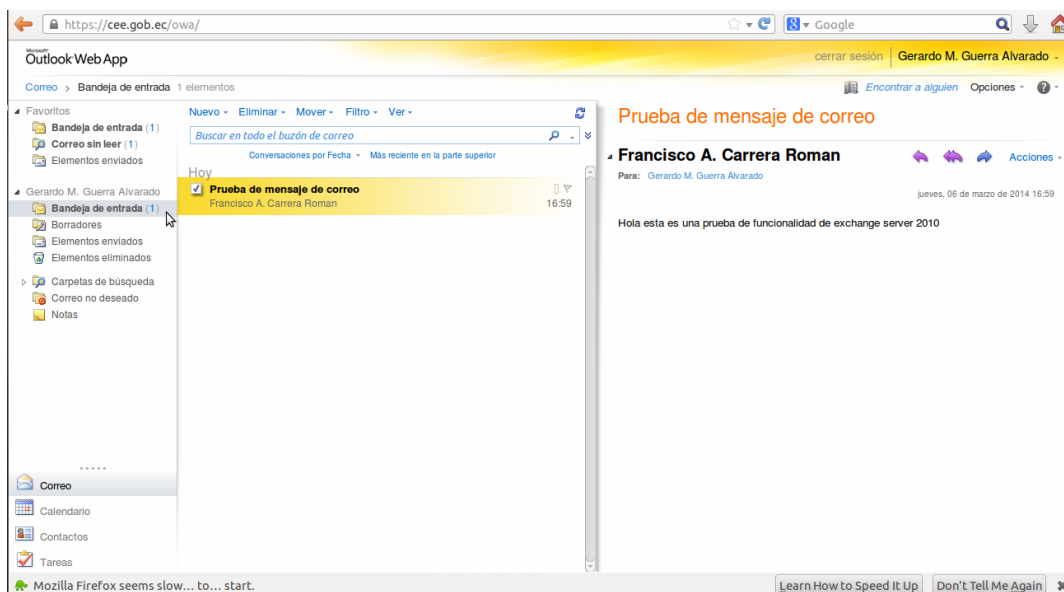


Figura G79. Recepción de un mensaje de correo electrónico

Como se suponía el mensaje ha sido entregado, con lo que se puede concluir que actualmente la plataforma de correo electrónico Exchange está operativa, más adelante se realizarán pruebas más complejas como la conexión con Microsoft Outlook, o la vinculación de usuarios al dominio.

4. MIGRACIÓN DE EXCHANGE A ZIMBRA

Zimbra Server provee una funcionalidad denominada ZCS Migration Wizard for Exchange que permite migrar los buzones de usuario de correo, la mensajería, los contactos, entre otros datos, desde una plataforma de correo operativa basada en Exchange.

Para el efecto utiliza interfaces MAPI⁵⁵ que posibilitan la conexión entre diversas aplicaciones de mensajería que las soporten, como Microsoft Exchange Server y Microsoft Outlook, que es el caso de interés para este proyecto.

⁵⁵ **Messaging Application Programming Interface** – Interfaz de Programación de Aplicaciones de Mensajería

MFCMAPI es una de las aplicaciones desarrolladas en base a interfaces MAPI, que utiliza un perfil de Outlook para conectarse con Exchange y acceder al contenido de los buzones del perfil, por ello es considerado un componente fundamental del conjunto de herramientas de administración de Exchange.

En tal virtud, se requiere inicialmente vincular un ordenador de usuario al dominio Active Directory configurado, para luego acceder al mismo empleando las credenciales de un usuario existente en su base de datos. Ingresar a las Propiedades del Sistema (véase Figura G80) pulsando Inicio + clic derecho en Equipo + Propiedades + Cambiar Configuración.

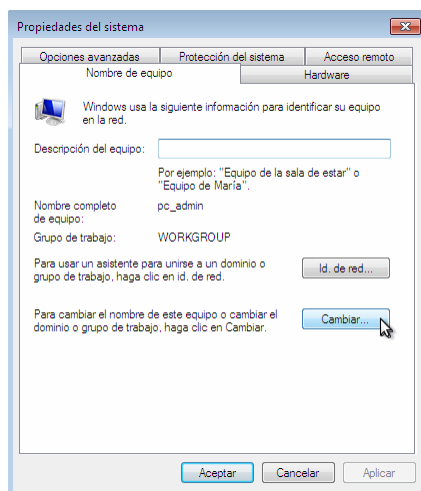


Figura G80. Propiedades del Sistema

Aquí se puede apreciar que este equipo no está vinculado a ningún dominio solo pertenece al grupo de trabajo por defecto de Windows, seleccionar Cambiar para ingresar el dominio del CEE al que pertenecerá (véase Figura G81).

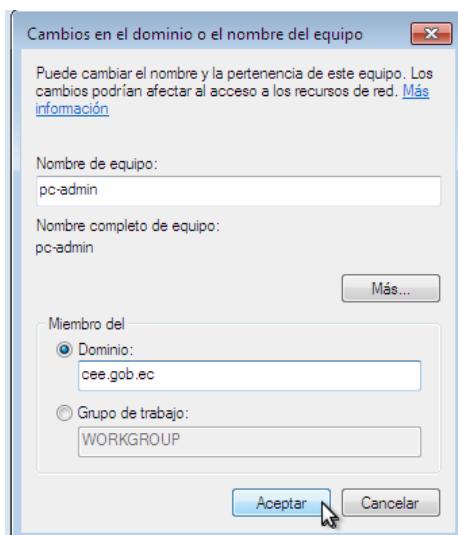


Figura G81. Definir el dominio del CEE

Configurar en el adaptador de red la dirección IP del DNS desarrollado 192.168.0.20 (véase Figura G82).

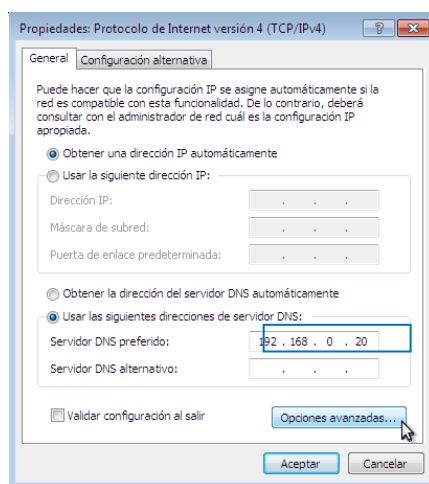


Figura G82. Definir el DNS

En Opciones avanzadas ingresar el sufijo del dominio para esta conexión (véase Figura G83).

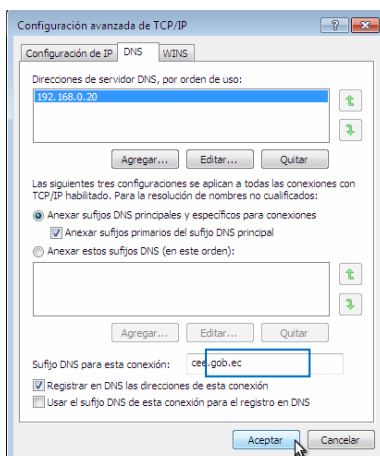


Figura G83. Definir el sufijo DNS

Al realizar todos estos cambios el sistema solicitará las credenciales del usuario que ingresará frecuentemente al dominio desde este ordenador (véase Figura G84).

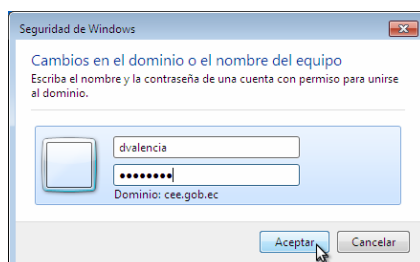


Figura G84. Asignar las credenciales de usuario

Tras ingresar las credenciales correctas mostrará un mensaje indicando que la vinculación con el dominio ha sido exitosa, se reiniciará el sistema, y se mostrará una nueva pantalla de acceso (véase Figura G85).



Figura G85. Inicio de sesión para vincularse al dominio

Desde la consola de administración de Active Directory se puede verificar que este equipo ha sido agregado a su base de datos (véase Figura G86).

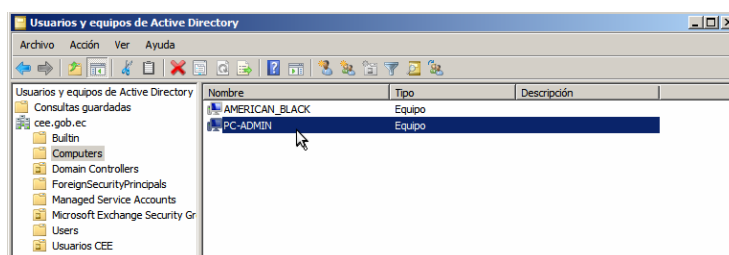


Figura G86. Consola de Administración de Active Directory

El requerimiento para ejecutar las interfaces MAPI es disponer en el sistema de dominio de un usuario con derechos administrativos, que también disponga de estos privilegios sobre Exchange, este usuario puede ser el que se crea por defecto durante la instalación de Exchange y Active Directory, o puede ser creado para administrar estos sistemas.

El propósito es acceder al dominio desde este ordenador empleando las credenciales de usuario administrador, para configurar su cuenta de correo en Outlook que permita ejecutar MFCMAPI, y finalmente el asistente de migración de datos hacia zimbra.

Existe otra alternativa para ejecutar MFCMAPI desde el propio servidor, es mucho más sencilla debido a que no se debe vincular al dominio a ningún ordenador específicamente para esto, ni tampoco la configuración del cliente de correo Outlook, sólo es necesario instalar MAPI Collaboration Data Objects (MAPIDCO) en el servidor, y luego ejecutar MFCMAPI.

Sin embargo, optar por esta alternativa para este proyecto no es muy conveniente, considerando que no se admitiría, por parte de las autoridades, el acceso y la manipulación del servidor Exchange operativo del CEE; por tal motivo se ha decidido utilizar la primera alternativa que resulta mucho más factible, lo único que se requiere es que el administrador de red genere un usuario con acceso privilegiado al sistema controlador de dominio.

Hecha esta aclaración acceder desde el ordenador vinculado y como administrador al sistema (véase Figura G87), esto se hace cuando la sesión está iniciándose al presionar la opción Cambiar de Usuario (véase Figura G85).

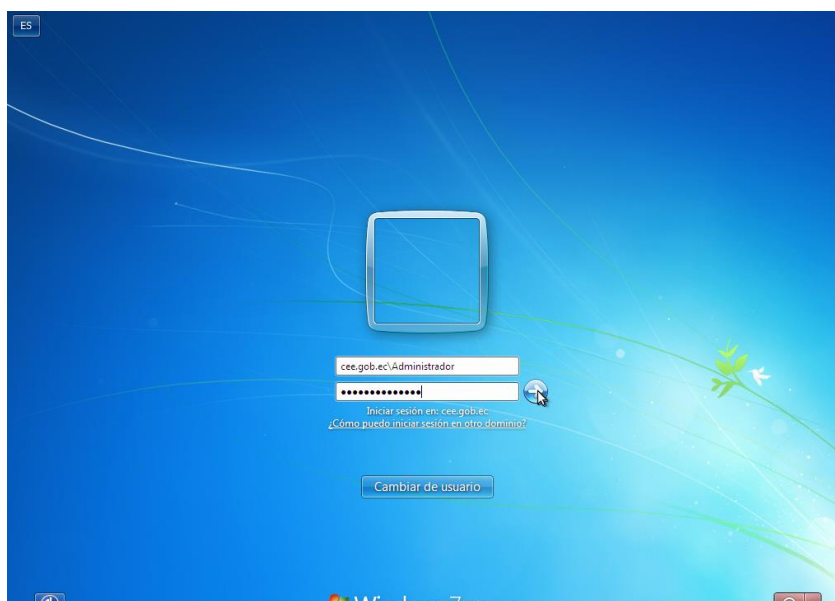


Figura G87. Inicio de sesión como Administrador

Al configurar una cuenta de correo empleando Outlook, ésta se almacena en un perfil que generalmente se genera por defecto, o puede ser creado por el usuario, este perfil es el que utiliza MFCMAPI para conectarse con Exchange y acceder al buzón respectivo. Para crear este buzón dirigirse a Inicio + Panel de Control + Cuentas de Usuario + Correo + Agregar, y definir el nombre del perfil (véase Figura G88).

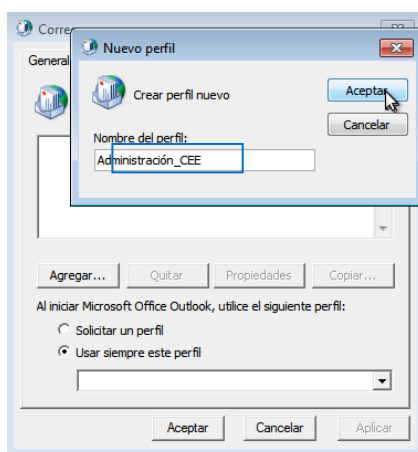


Figura G88. Perfil de Correo Outlook

Al crearlo inmediatamente se desplegará una ventana del asistente de configuración de la cuenta de correo para este perfil y se debe seleccionar la opción de configuración manual (véase Figura G89).

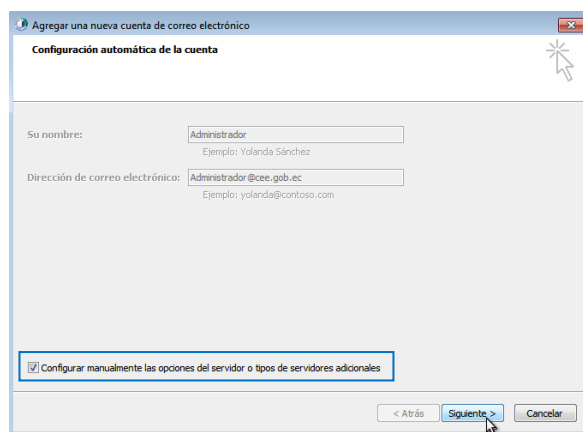


Figura G89. Creación de la cuenta de correo

Definir el tipo de servicio de correo (véase Figura G90).

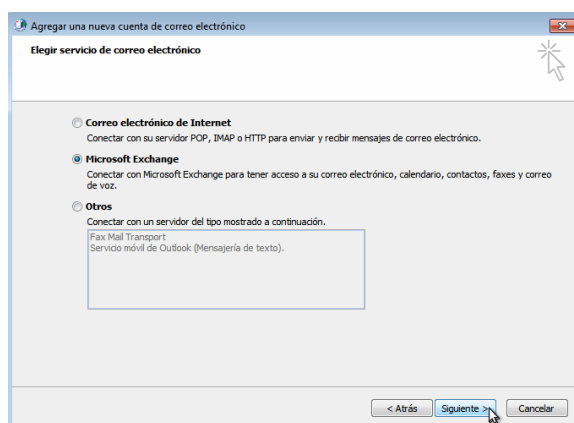


Figura G90. Tipo de servicio que aloja esta cuenta

Ingresar el nombre del servidor Exchange conjuntamente con el dominio al que pertenece (mailex.cee.gob.ec), y el nombre del usuario de la cuenta (véase Figura G91).

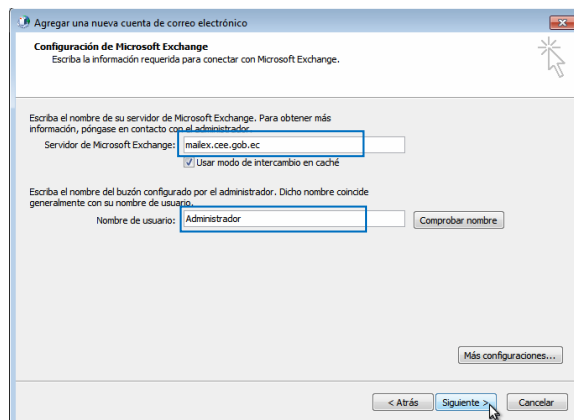


Figura G91. Definición del servidor y usuario de la cuenta

Con ello se concluye la configuración del agente MUA para esta cuenta de Administrador (véase Figura G92).

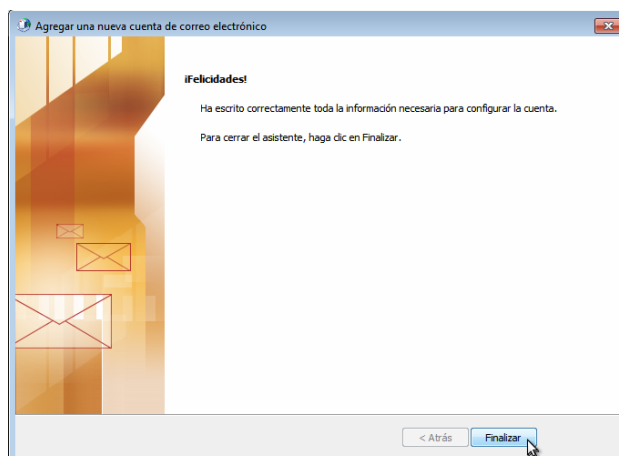


Figura G92. Configuración exitosa de esta cuenta

Este procedimiento fue realizado para cada usuario creado en el controlador de dominio y se realizaron pruebas de envío y recepción de mensajes, y agregar contactos para cada cuenta; toda esta información podrá ser verificada cuando se efectúe la migración hacia zimbra, por el momento se empleará MFCMAPI para cerciorarse de que se tiene acceso al buzón del Administrador.

Descargar el paquete de MFCMAPI desde el sitio <http://mfcmapl.codeplex.com/> (véase Figura G93).

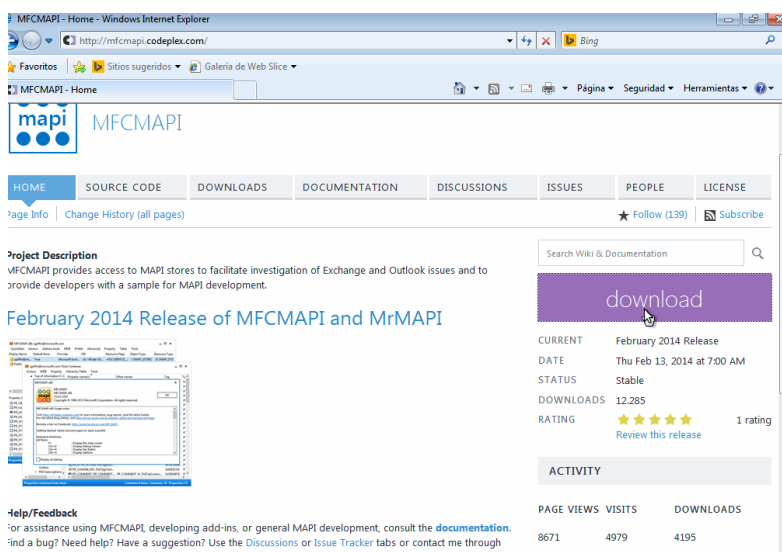


Figura G93. Sitio de descarga de MFCMAPI

Este paquete no se debe instalarlo, únicamente ejecutarlo e iniciar la autenticación (véase Figura G94).

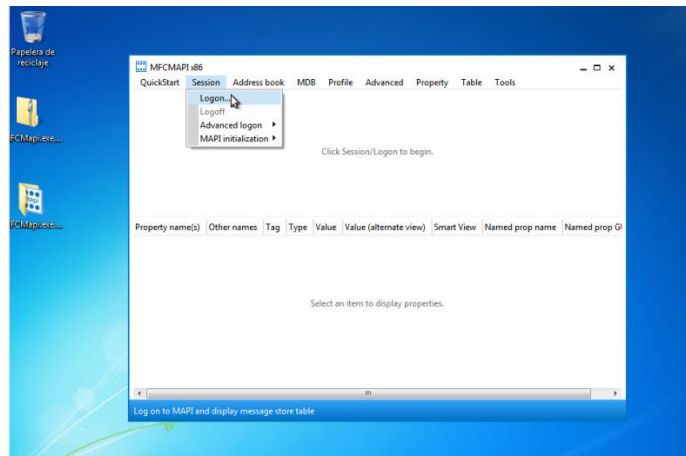


Figura G94. Ejecución de MFCMAPI

Establecer el perfil de la cuenta Outlook de administrador creado (véase Figura G95).

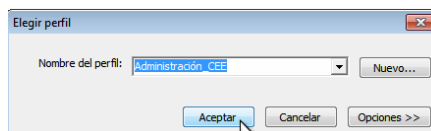


Figura G95. Perfil de Administrador

Se ha conseguido el acceso al buzón de Administrador (véase Figura G96).

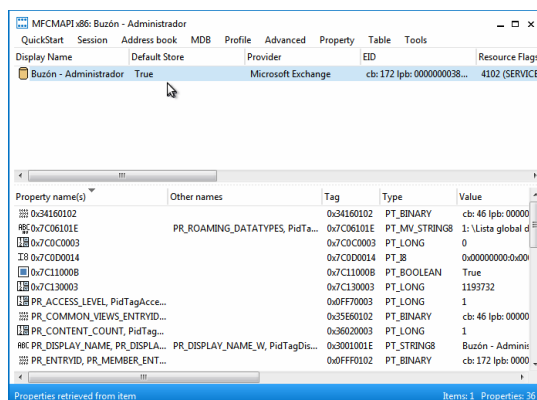


Figura G96. Buzón de Administrador

Ahora se puede acceder a toda la información que contiene este buzón (véase Figuras G97, G98 y G99).

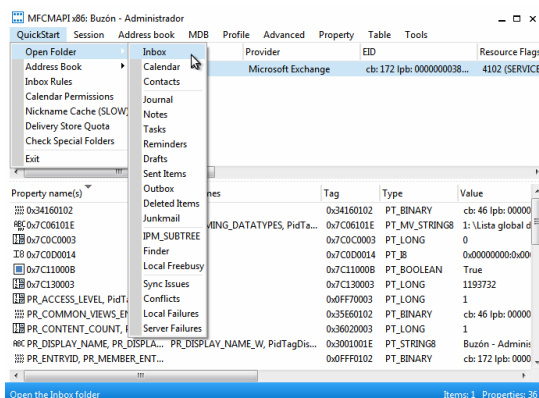


Figura G97. Información del Buzón

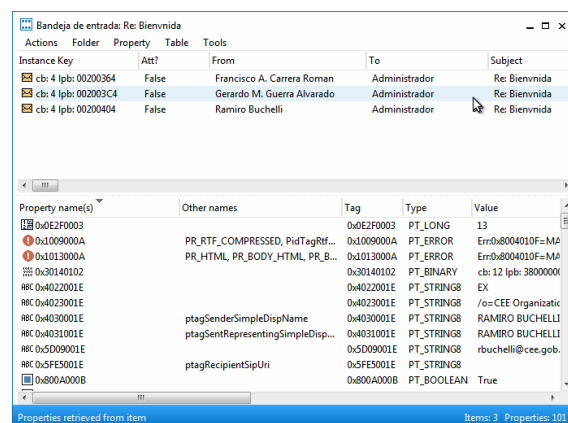


Figura G98. Bandeja de Entrada

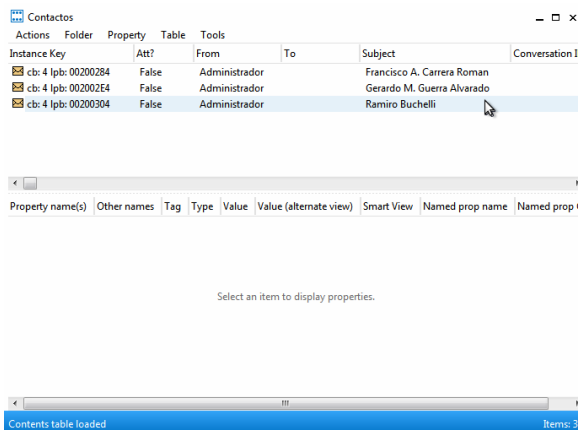


Figura G99. Contactos

En tal virtud, se concluye que este perfil MAPI configurado funciona y que puede ser utilizado por el asistente de migración zimbra. Este asistente puede descargarse directamente desde la consola de Administración de Zimbra <https://mail.cee.gob.ec:7071> en el apartado Tools and Migration (véase Figura G100).

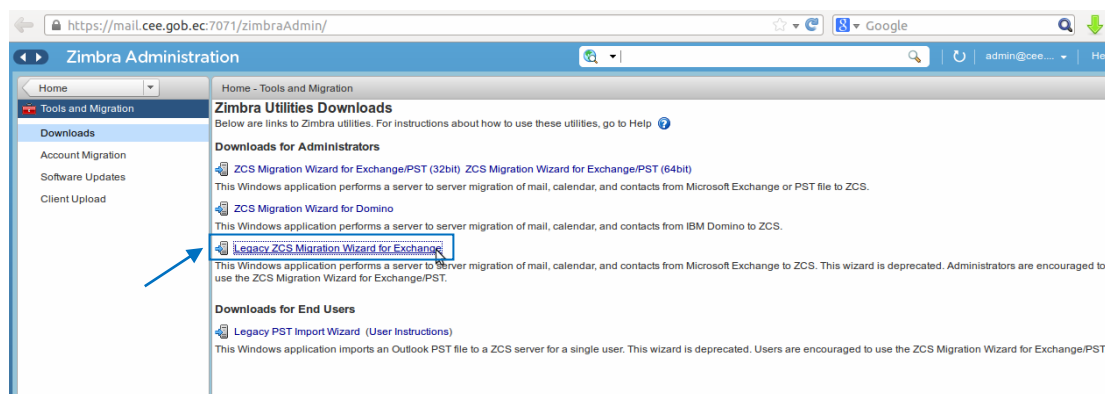


Figura G100. Descarga del Asistente de Migración

Al ejecutarlo aparecerá una pantalla informativa y después se deberá ingresar información del servidor zimbra (véase Figura G101).

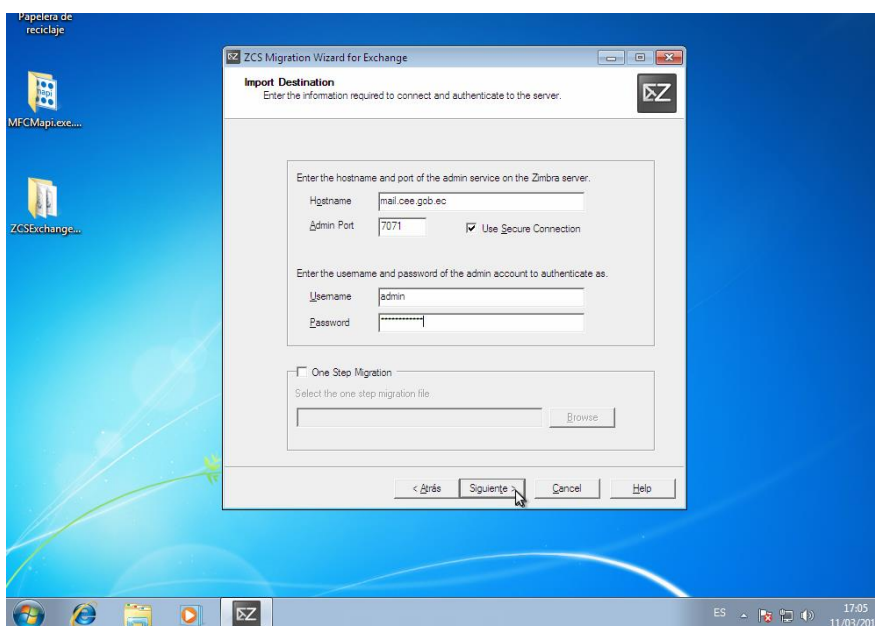


Figura G101. FQDN de zimbra y credenciales de la cuenta de administración

Confirmar el dominio al que pertenece zimbra (véase Figura G102).

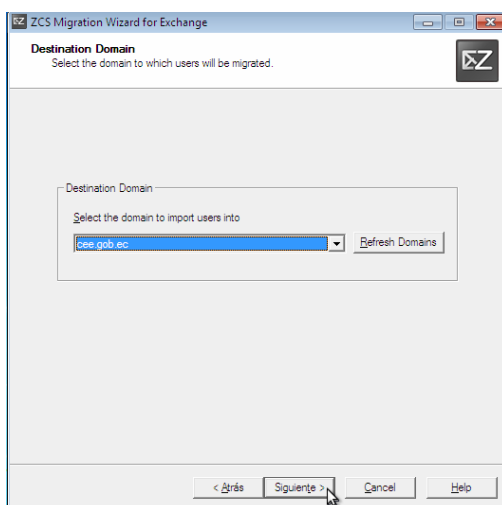


Figura G102. Dominio de Zimbra

Elegir el perfil MAPI de la cuenta de Administrador (véase Figura G103).

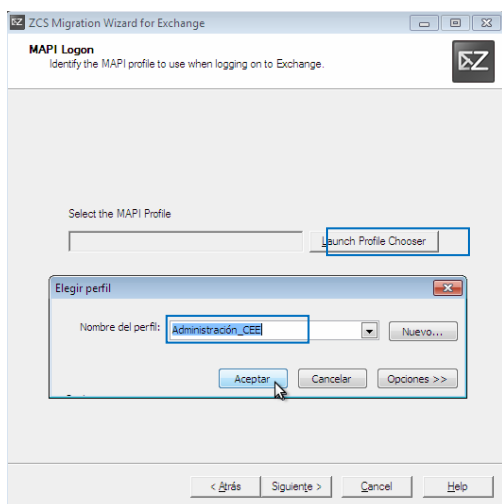


Figura G103. Perfil MAPI configurado

En esta parte del proceso se especificará las cuentas de usuario de correo a ser migradas, existen dos opciones, Object Picker permite especificar usuarios individuales, y Query Builder para especificar grupos de usuarios. Seleccionar la primera opción y definir las cuentas de usuario (véase Figura G104).

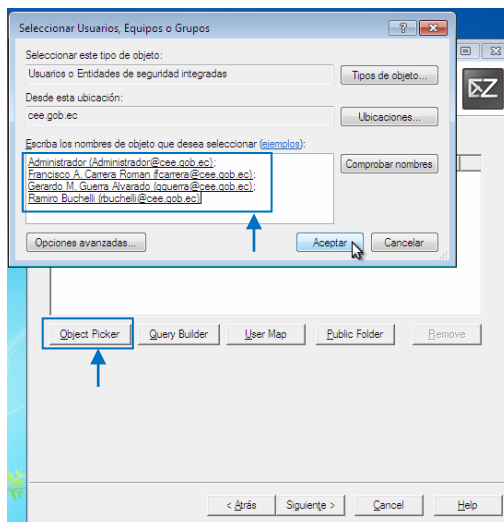


Figura G104. Cuentas de usuario a migrarse

Definidas las cuentas pulsar **Siguiete** (véase Figura G105).

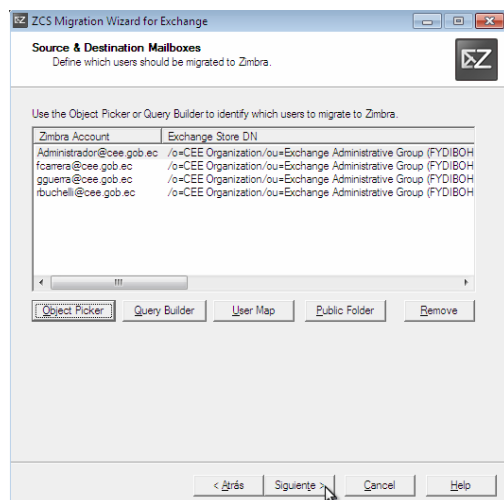


Figura G105. Cuentas de usuario a migrarse

Este asistente verifica si estas cuentas existen en zimbra server, si es el caso únicamente importará la información correspondiente, de lo contrario creará estas cuentas y luego importará su información (véase Figura G106).

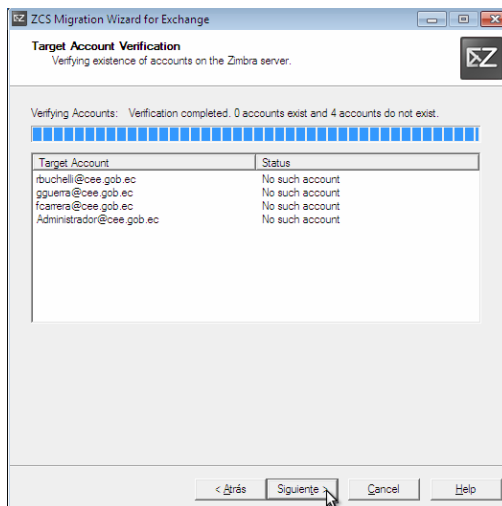


Figura G106. Verificación de la existencia de estas cuentas

La pantalla de aprovisionamiento de cuentas permite identificar las cuentas que no existen en zimbra y deben ser creadas (Unprovisioned Accounts), definir la clase de servicio COS y la contraseña predeterminada que se asignará a cada una (véase Figura G107).

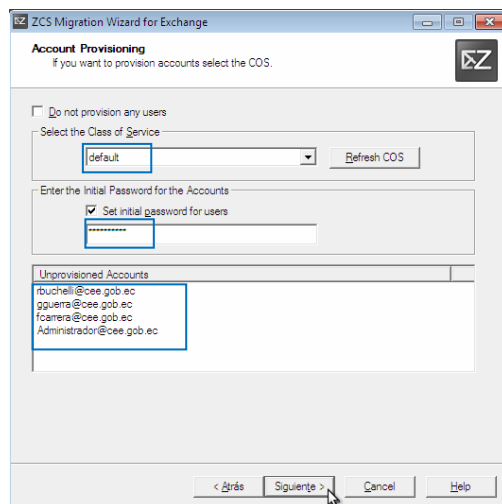


Figura G107. Características y contraseña de las cuentas

La COS establece las características y preferencias de la cuenta, al elegir default hacemos referencia a la COS que se genera automáticamente al instalar zimbra; la contraseña

que se define es de carácter temporal, y para todas las cuentas migradas, posteriormente será necesario restablecerlas manualmente desde la consola de administración de zimbra, o configurar zimbra para que la autenticación se lleve a cabo desde directorios LDAP externos como OpenLDAP o Active Directory.

Con toda esta información las cuentas serán creadas en zimbra y se mostrará una pantalla para seleccionar la información que se desea importar para cada cuenta (véase Figura G108).

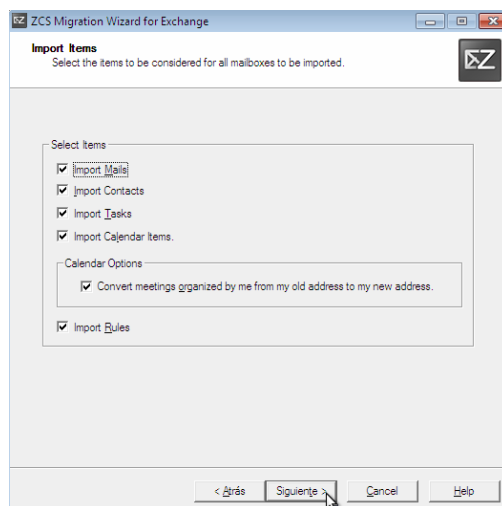


Figura G108. Tipo de información a ser importada

Existe la posibilidad de importar datos desde otro tipo de bandejas, como correo basura, correos eliminados, y correos enviados, e inclusive se puede establecer una fecha desde la cual realizar la migración de datos, para evitar importar datos muy antiguos (véase Figura G109).

Es recomendable importar buzón a buzón y no tratar de hacerlo con varios simultáneamente, aunque tome mucho más tiempo realizarlo, para garantizar este proceso.

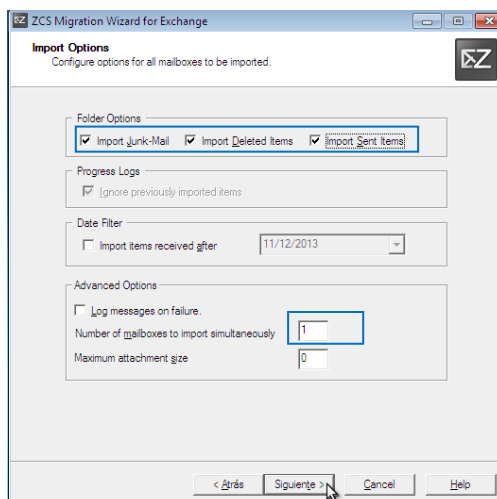


Figura G109. Bandejas de mensajería opcionales a importar

Con esto iniciará la importación (véase Figura G110).

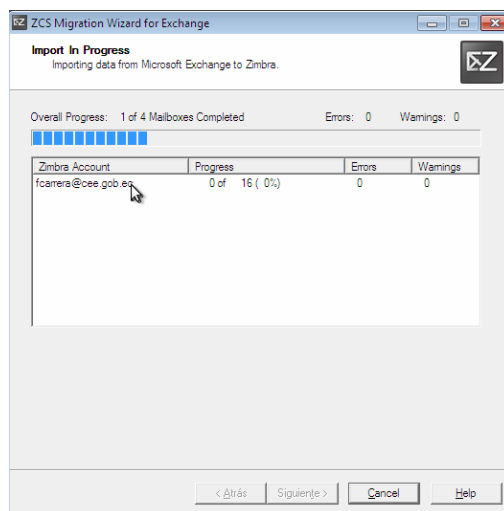


Figura G110. Progreso de la importación

Si todo ha sido llevado a cabo sin novedades la importación se completará (véase Figura G111).

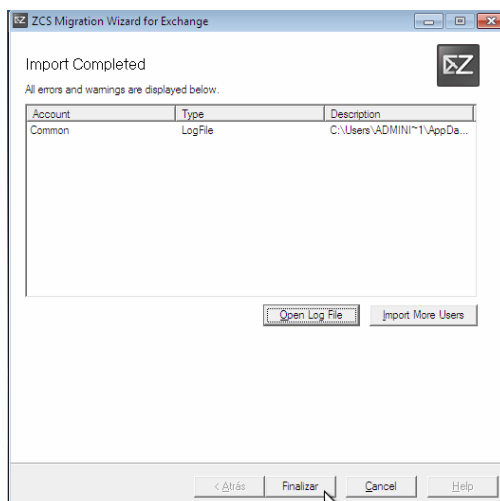


Figura G111. Importación exitosa

Para verificar que todo este proceso en realidad se ha efectuado, acceder a la interfaz de administración de zimbra y se apreciarán las nuevas cuentas creadas (véase Figura G112).

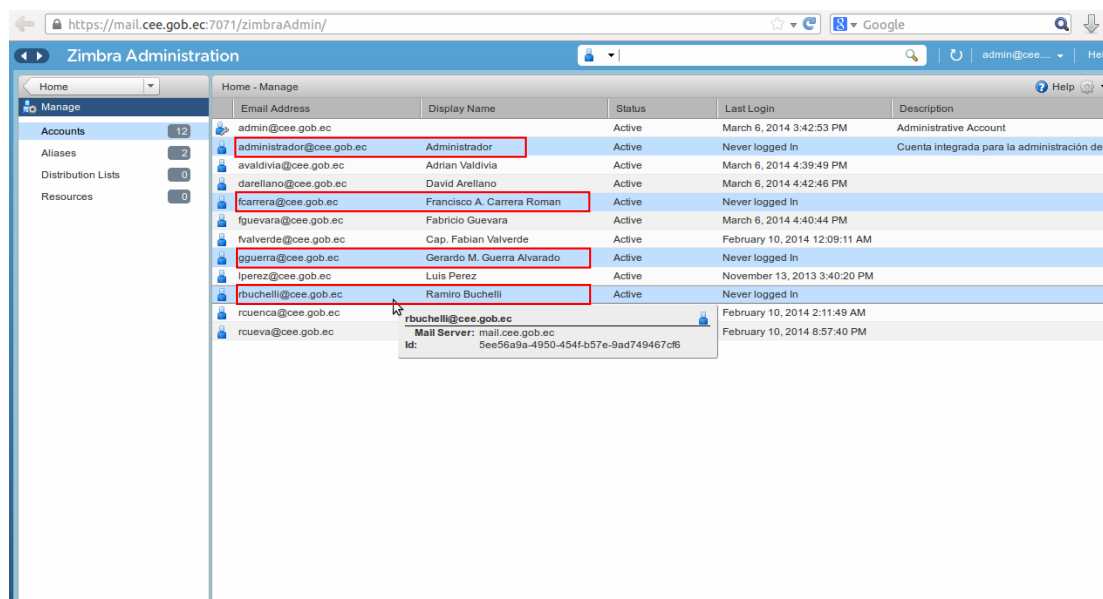


Figura G112. Cuentas de correo importadas

Finalmente se inspeccionará un mensaje del buzón de entrada y los contactos de la cuenta de administrador, desde la interfaz webmail de Zimbra, como de Exchange, para demostrar que son legítimos (véase Figuras G113, G114, G115 y G116).

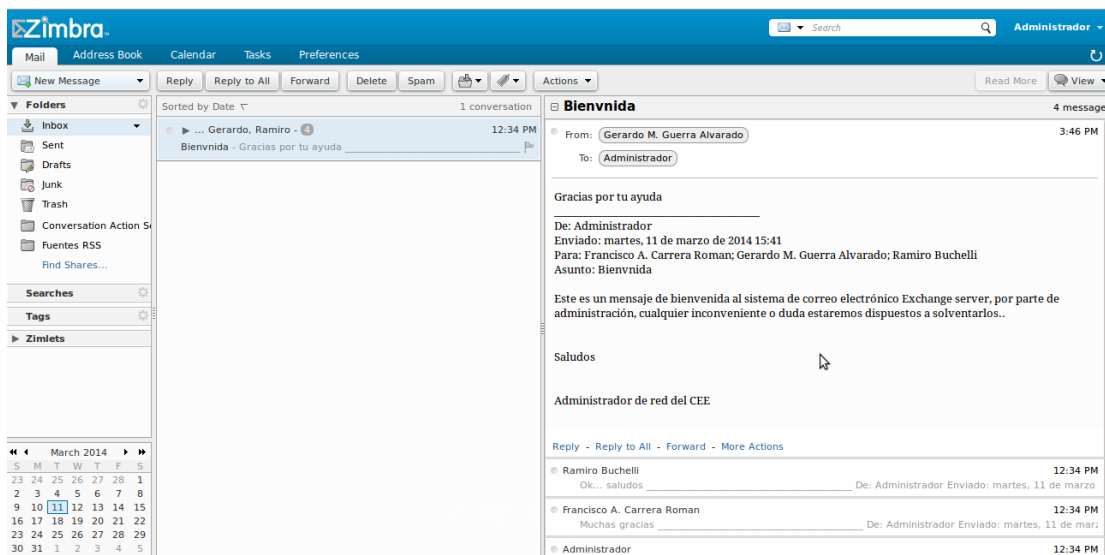


Figura G113. Interfaz webmail de Zimbra – Mensaje de Correo

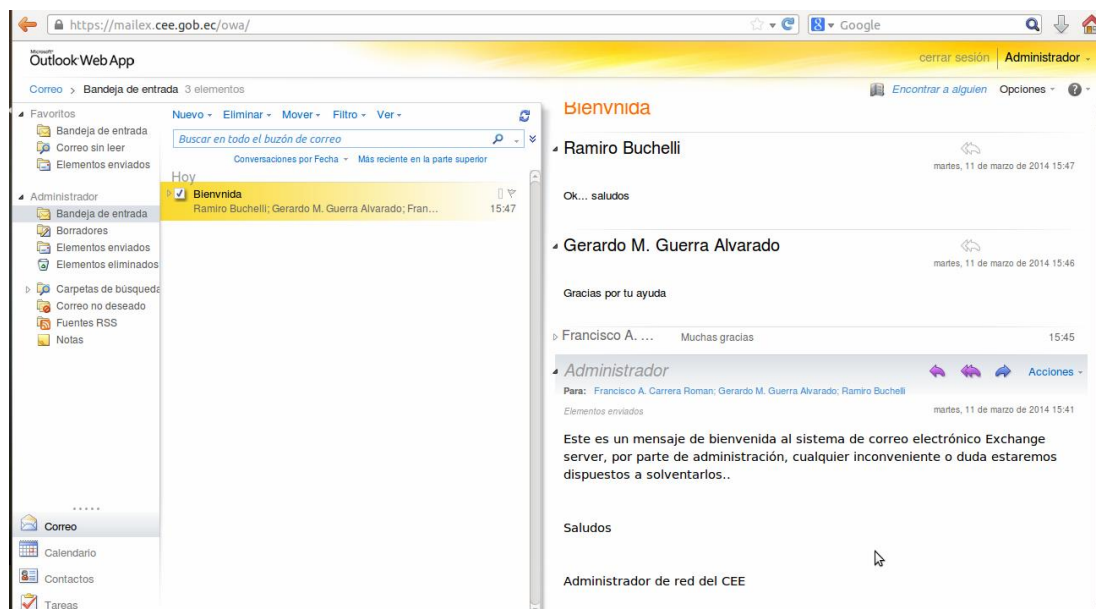


Figura G114. Interfaz webmail de Exchange - Mensaje de Correo

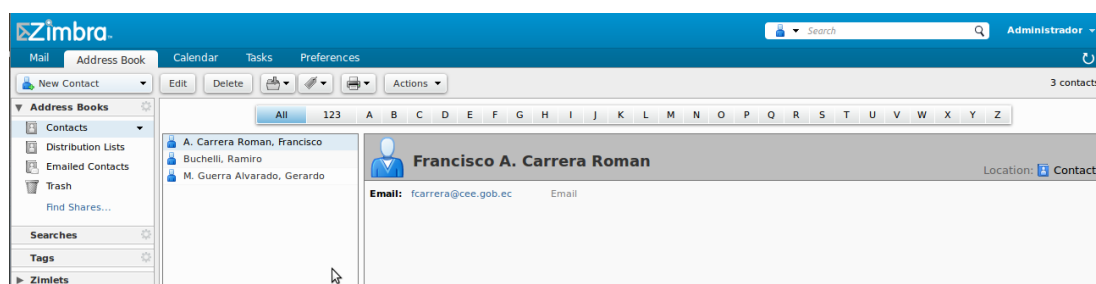


Figura G115. Interfaz webmail de Zimbra – Contactos

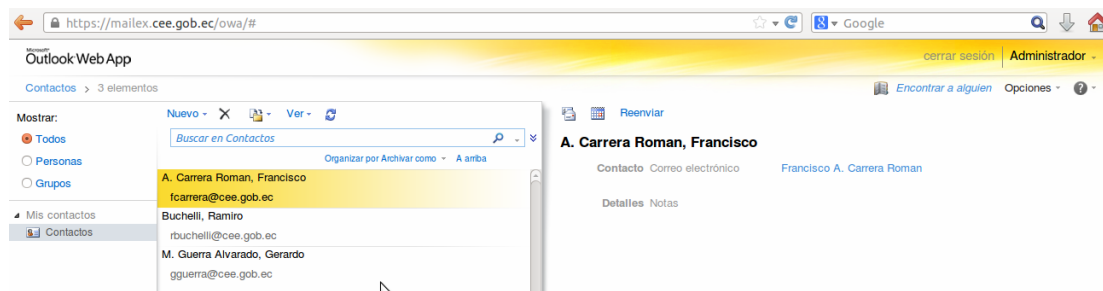


Figura G116. Interfaz webmail de Exchange – Contactos

ANEXO H

UNIVERSIDAD TÉCNICA DEL NORTE

2014

**MANUAL DE
ADMINISTRACIÓN**

**INFRAESTRUCTURA DE
CLAVE PÚBLICA**

Autor: David R. Valencia

1.INTRODUCCIÓN

Este manual de administración proporciona información detallada sobre los procedimientos necesarios para gestionar la Infraestructura de Clave Pública, y la Plataforma de Correo Electrónico Seguro, diseñados para el entorno del Cuerpo de Ingenieros del Ejército de Quito.

Se exponen los procesos de registro, solicitud, emisión e instalación de los certificados digitales destinados a los funcionarios y militares del CEE; y su integración con el sistema de correo electrónico institucional diseñado en este proyecto, para proteger la mensajería transferida por este medio.

2.PKI - INTERFAZ WEB DE ADMINISTRACIÓN EJBCA

Todas las actividades de gestión de la PKI se realizan a través de esta interfaz, pero el proceso de certificación también involucra el acceso desde los ordenadores de los usuarios solicitantes, hacia la interfaz web pública de EJBCA (<http://pki.cee.gob.ec:8080/ejbca> - véase Figura H1), para obtener los certificados solicitados e instalarlos para su posterior aplicación.

Esta interfaz pública contiene la opción Administration en el apartado Miscellaneous que es un enlace de acceso hacia la interfaz privada de administración (admin web), pero debido a que este sistema está diseñado con un mecanismo de autenticación basado en certificados digitales, únicamente podrá acceder el usuario cuyo certificado esté autorizado para ello, en este caso el certificado destinado al administrador de red del Cuerpo de Ingenieros del Ejército - CEE, tendrá todos los privilegios de administración.



Figura H1. Interfaz Web Pública EJBCA

2.1. PROCESO DE CERTIFICACIÓN

Todas las actividades que involucra este proceso las efectuará el administrador de red del CEE, con el apoyo de personal capacitado; los funcionarios y militares de esta institución, que son las entidades para quienes se emitirán los certificados digitales X.509, únicamente serán instruidos para utilizar sus buzones de correo y generar mensajes protegidos por técnicas de cifrado y firma digital.

2.1.1. REGISTRO

Este es el proceso en el cual el administrador registra en el componente RA de la PKI, la información del usuario hacia quien está destinada la certificación, después de haber constatado su legitimidad; aunque en este caso, al tratarse de solicitantes que laboran en la misma entidad, este proceso resulta sencillo.

Acceder al apartado RA Functions de la admin web, elegir Add End Entity, seleccionar en el campo End Entity Profile el valor PERSONAS, e ingresar los datos del solicitante (véase Figura H2).

EJBCA Administration *111 años de la Gloriosa Arma de Ingeniería Militar* **CUERPO DE INGENIEROS DEL EJERCITO**

Add End Entity

Field	Value	Required
End Entity Profile	PERSONAS	Required
Username	Fabian Pazmiño	✓
Password	✓
Confirm Password	✓
E-mail address	fpazmino @ cee.gob.ec	☐
Subject DN Attributes		
CN, Common name	Mayor Fabián Pazmiño	✓
UID, Unique Identifier	Departamento de Sietemas	✓
O, Organization	Cuerpo de Ingenieros del Ejercito	☐
OU, Organizational Unit	Entidad Final CEE	☐
C, Country (ISO 3166)	EC	☐
Other subject attributes		
Subject Alternative Name		
RFC 822 Name (e-mail address)	Use data from E-mail address field	☐
Main certificate data		
Certificate Profile	PERFIL_ENTIDAD_FINAL	✓
CA	Autoridad Certificadora CEE	✓
Token	P12 file	✓
Other data		
Key Recoverable	<input checked="" type="checkbox"/>	
Add Reset		

Customized by David Ricardo Valencia de la Torre, Sep. 2013.

Figura H2. Proceso de registro del usuario solicitante

El campo Username corresponde a la asignación de un nombre de usuario para esta persona, y la contraseña por motivos de seguridad debe ser definida por este usuario solicitante de acuerdo a ciertas recomendaciones establecidas en el Anexo A de este proyecto; esto garantiza mayor facilidad para memorizarla, tratando evitar al máximo que tengan la necesidad de apuntarla en cualquier lugar para recordarla. Con esto clic en Add y se obtendrá un mensaje confirmando que se ha registrado exitosamente a este usuario en el sistema.

2.1.2. CONFIAR EN LA CA RAÍZ DE LA PKI

En un ambiente de certificación se debe considerar que la fiabilidad de todas las entidades certificadas, bajo la misma administración, radica en la Autoridad Certificadora Raíz; de manera que previamente a instalar un certificado personal, es necesario establecerla como una entidad fiable, para garantizar la interacción con cualquier certificado que ésta gestione.

Para ello se debe instalar el certificado auto-firmado de la CA Raíz del CEE, en cada uno de los ordenadores de usuario que requieran utilizar este sistema de seguridad.

2.1.2.1. INSTALACIÓN DEL CERTIFICADO CA RAÍZ

Acceder a la interfaz web pública de EJBCA, seleccionar la opción Fetch CA & OCSP Certificates y pulsar en Download to Internet Explorer para obtenerlo (véase Figura H3).

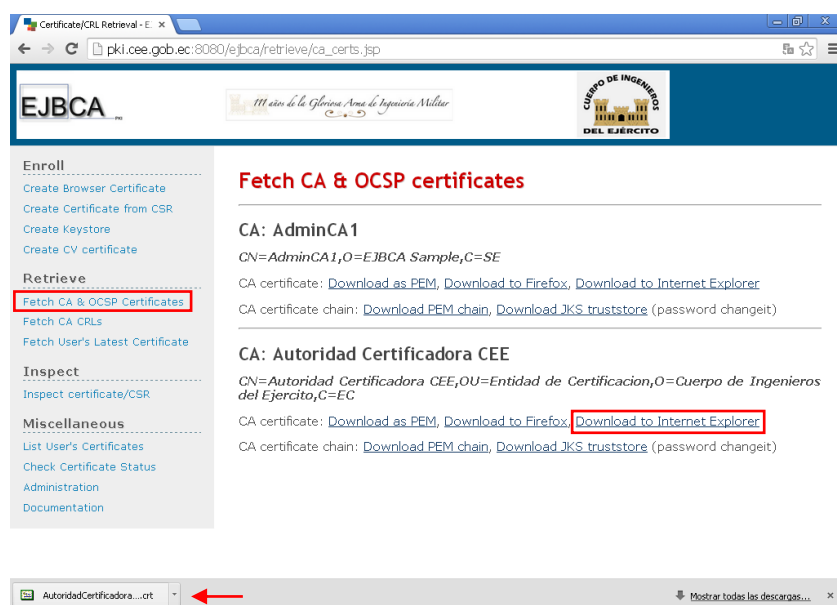


Figura H3. Descarga de Certificado de la CA Raíz

Mozilla Firefox utiliza su propio almacén de certificados, a diferencia de Internet Explorer o Google Chrome que emplean el almacén de Windows, por ello es recomendable descargar el certificado de la CA para este tipo de navegador web.

Ejecutar el archivo descargado para iniciar el asistente de importación de certificados de Windows (véase Figuras H4 y H5).

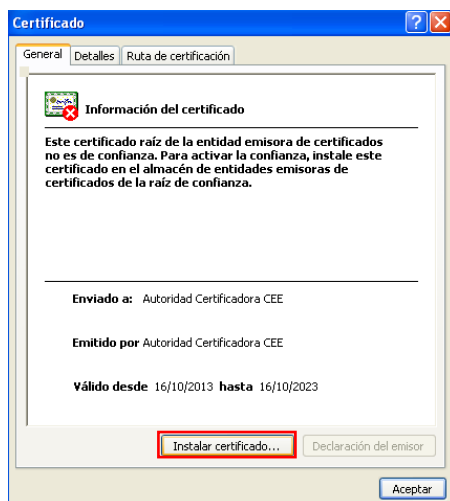


Figura H4. Certificado de la CA Raíz

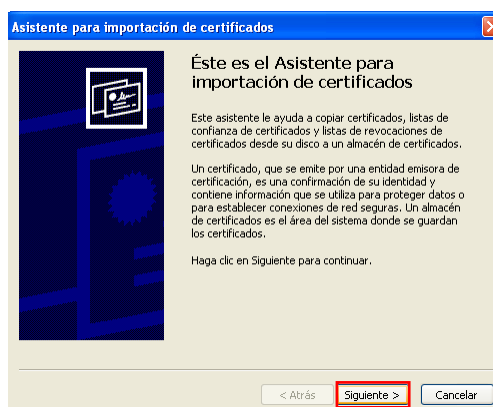


Figura H5. Asistente de Importación de Certificados de Windows

Elegir el repositorio de certificados de Windows donde se almacenará este certificado, es preferible que el asistente lo elija automáticamente (véase Figura H6).

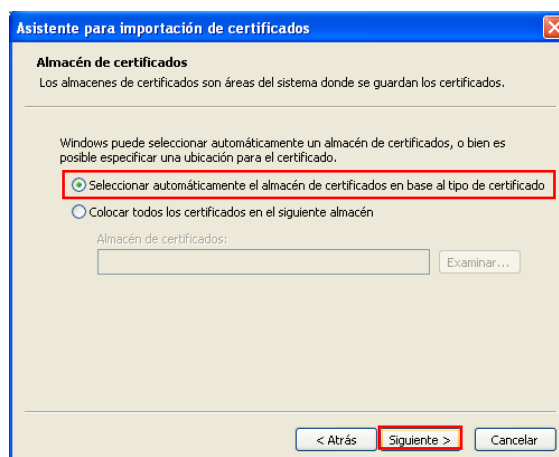


Figura H6. Almacén de Certificados de Windows

Luego se mostrará una alerta indicando que se instalará un certificado que identifica a una Autoridad Certificadora, y que desde este momento se confiará en cualquier certificado emitido por esta entidad (véase Figura H7).

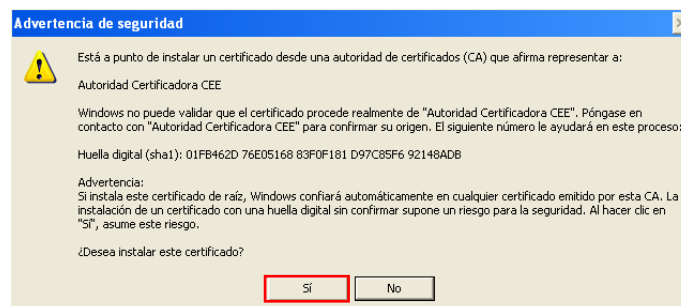


Figura H7. Confiar en el certificado de la CA Raíz del CEE

Al finalizar este proceso se puede comprobar que este certificado se ha importado en el almacén Entidades emisoras raíz de confianza, empleando el administrador de certificados de un navegador web (véase Figura H8).

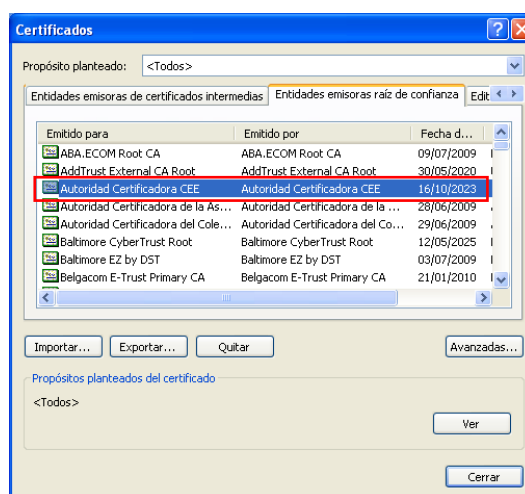


Figura H8. Administrador de Certificados de Google Chrome

2.1.3. EMISIÓN E INSTALACIÓN

Para obtener el certificado del usuario solicitante, previamente registrado, acceder a la opción Create Browser Certificate de la interfaz web pública, y autenticarse con el usuario y la contraseña acordados durante el registro (véase Figura H9).

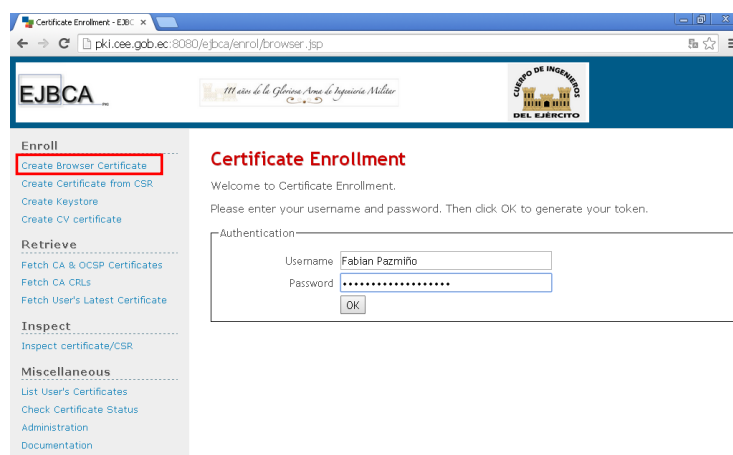


Figura H9. Usuario y contraseña del solicitante

Si la autenticación ha sido exitosa se procede a definir la longitud del par clave criptográfico RSA a ser creado, para generar la solicitud de certificación, y obtener el certificado (véase Figura H10). Es necesario establecer un tamaño estándar de 2048 bits para este par clave criptográfico.

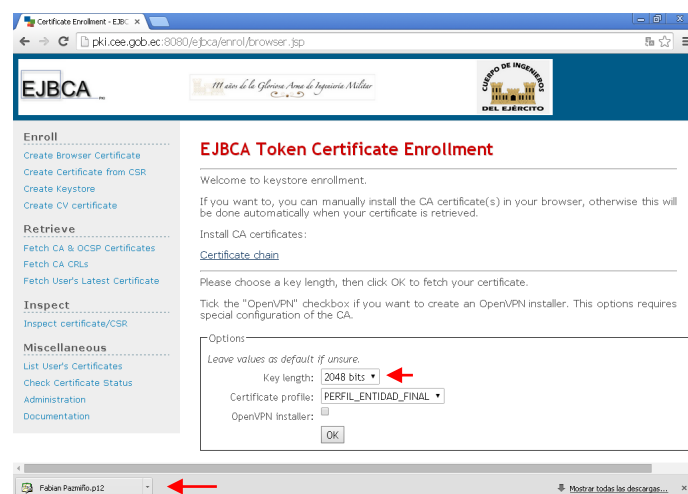


Figura H10. Establecer la longitud del par clave

Se obtendrá un archivo de extensión .p12 que contiene la clave pública de este usuario, alojada en su certificado, y la clave privada que por seguridad ha sido cifrada con la contraseña de autenticación del registro; al ejecutarlo activará el asistente de importación de certificados de Windows, similar al proceso anterior, pero en este caso al tratarse de un

certificado personal solicitará esta contraseña de registro para descifrar la clave criptográfica privada, y continuar con su importación (véase Figura H11).

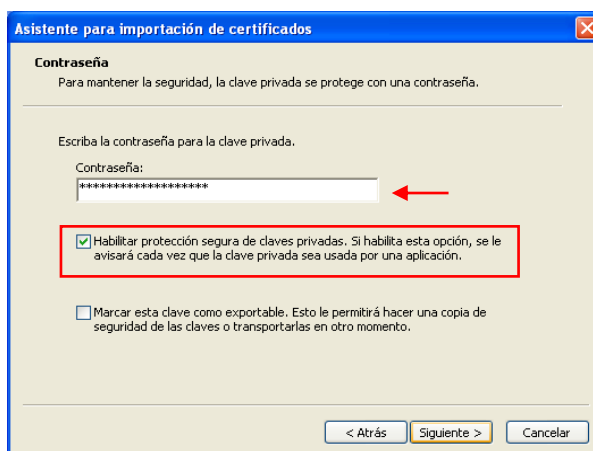


Figura H11. Descifrar la clave criptográfica privada

Por seguridad no será necesario exportar posteriormente la clave criptográfica privada de este usuario, esto impide que se genere una copia de la misma para que únicamente sea utilizada en el ordenador sobre el que ha sido instalada inicialmente, garantizando su protección.

Al finalizar este proceso iniciará una aplicación para proteger la clave privada durante su almacenamiento en el sistema operativo del ordenador cliente (véase Figura H12).



Figura H12. Protección de la clave privada

Se debe seleccionar Nivel de seguridad y fijar la opción Alto, esto hace que cada vez que se requiera emplear esta clave criptográfica privada sea necesario ingresar una contraseña de protección que deberá ser establecida (véase Figura H13).

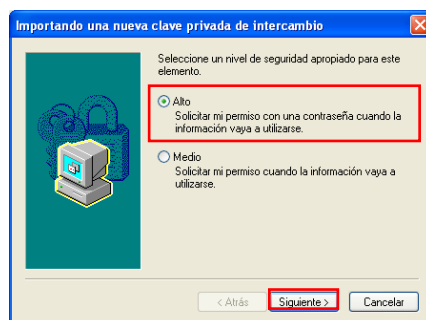


Figura H13. Nivel de Protección

Esta podría ser cualquier contraseña, pero en este caso se ha considerado adecuado emplear la misma contraseña que cada usuario debe definir para efectuar el proceso de registro durante la solicitud de certificación; esto garantiza que se utilicen contraseñas robustas en este proceso (véase Figura H14).



Figura H14. Contraseña de protección de la clave privada

Con esto se ha completado la solicitud, emisión e instalación del certificado personal, disponiendo desde este momento de un mecanismo de seguridad fiable, que puede ser empleado para diversos propósitos (véase Figura H15), pero en lo que se refiere a este proyecto será empleado específicamente para la seguridad del correo institucional.

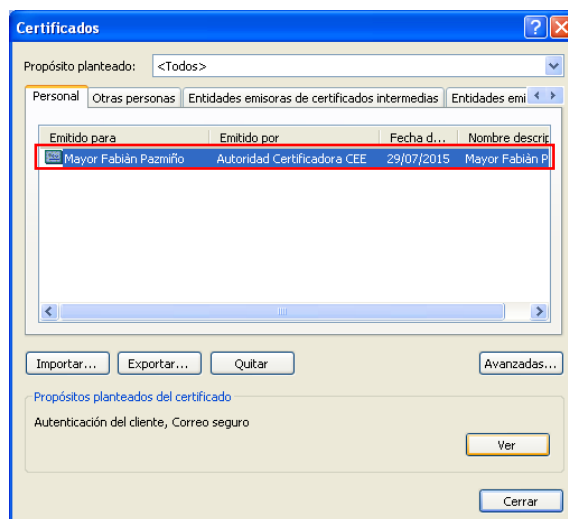


Figura H15. Certificado Personal instalado en el repositorio Windows visualizado empleando Google Chrome

2.2. GESTIÓN DEL CICLO DE VIDA DE LOS CERTIFICADOS

La interacción de las aplicaciones que implementan seguridad basada en certificados digitales, generalmente es verificar si el certificado (empleado, o que va a ser empleado) proviene de una Autoridad Certificadora de confianza, acceder a la URL del certificado que contiene la publicación de CRLs emitidas por esta entidad para verificar su validez, y comprobar su fecha de vigencia; si falla alguna de estas pruebas mostrarán alertas que lo identifiquen como no fiable.

La Infraestructura de Clave Pública diseñada no solo está destinada a la emisión de certificados digitales, está en capacidad de gestionarlos controlando las actividades de sus titulares; es decir, que un certificado no sólo dejará de ser válido por haber expirado, también pueden existir otras circunstancias que los invaliden contribuyendo para su revocación, administrando de esta forma su ciclo de vida.

2.2.1. RENOVACIÓN DE CERTIFICADOS CADUCADOS

Este es el estado de un certificado luego de haber completado su ciclo de vida útil, sin haber presentado ningún percance de por medio (véase Figura H16).

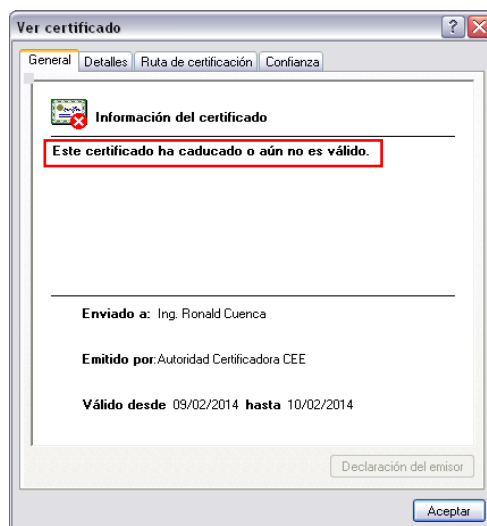


Figura H16. Certificado Digital caducado

Desde este momento este certificado no tendrá validez, pero su titular puede solicitar una renovación a la administración de la PKI del CEE, para mantener la misma clave criptográfica privada que le permitan firmar nuevos mensajes de correo, y descifrar los anteriores; y ser identificado ante los demás por un certificado renovado que contenga la misma clave pública.

Este proceso se lo realiza desde la admin web, la opción Search/Edit End Entities del apartado RA Functions, buscando el nombre del usuario en cuestión (véase Figura H17). Al encontrarlo se presentarán detalles del Distinguished Name que identifican a esta persona, como el nombre de usuario, de la Entidad Certificadora, el Common Name, la Unidad Organizativa, la Organización, y el estado del certificado, en este caso es un certificado válido pero se supondrá que ya caducó para efectuar su renovación.

The screenshot shows the EJBCA Administration web interface. The search criteria 'Fabian Pazmiño' is entered in the search field. The results table shows one entry for 'Fabian Pazmiño' with various attributes like CA, CN, OU, and Status. A red arrow points to the search button, and another red arrow points to the 'View End Entity' link in the results table.

Figura H17. Búsqueda de entidades certificadas en la admin web

Al acceder a la opción View Certificates se pueden apreciar las características del certificado operativo (véase Figura H18).

The screenshot shows the 'View Certificate' page in the EJBCA Administration web interface. The page displays detailed information about a certificate for 'Fabian Pazmiño', including the certificate number, type, serial number, issuer DN, subject DN, and public key. A red box highlights the public key field.

Username	Fabian Pazmiño
Certificate number	2 of 2
Certificate Type/Version	X.509 v.3
Certificate Serial Number	SBOE155CC011EB3B
Issuer DN	CN=Autoridad Certificadora CEE,OU=Entidad de Certificacion,O=Cuerpo de Ingenieros del Ejercito,C=EC
Valid from	2014-07-29 16:19:15-05:00
Valid to	2015-07-29 16:19:15-05:00
Subject DN	UID=Departamento de Sietemas,CN=Mayor Fabiàn Pazmiño,OU=Entidad Final CEE,O=Cuerpo de Ingenieros del Ejercito,C=EC
Subject Alternative Name	rfc822name=fpazmino@cee.gob.ec
Subject Directory Attributes	None
Public key	RSA (2048 bits): 8428621DD95A654A1BAE0F06702504EB82F35C9F5976FD6...
Basic constraints	End Entity
Key usage	Digital Signature, Non-repudiation, Key encipherment, Data encipherment
Extended key usage	Client Authentication, Email Protection
Qualified Certificates Statements	No
Signature Algorithm	SHA1WithRSAEncryption
Fingerprint SHA-1	BA927A9FCC2CBFCDF8D2F56917FD099B412E093E
Fingerprint MD5	297F484E6E16DE99F74CA420FE6B2DBE
Revoked	No
Recover Key	Republish
Download binary to IE	Download to Firefox
Download PEM file	

Figura H18. Parámetros de un certificado de entidad final

Es importante distinguir el número de serie y la clave pública que contiene este certificado, debido a que son parámetros que identifican exclusivamente a cada titular, y que son únicos para cada certificado.

En este caso lo que se requiere es su renovación para conservar el mismo par clave criptográfico, entonces presionar Recover Key para efectuar este proceso (véase Figura H18). Esto cambiará el estado del certificado de Generated a Key Recovery, y será necesario establecer nuevamente el usuario y la contraseña de registro (véase Figura H20) para autenticarse desde el ordenador cliente, descargar e instalar el certificado renovado, tal como se realizó en procedimientos preliminares de este manual.

End Entity Profile		PERSONAS	Required
Status	Key Recovery	Save	
Username	Fabian Pazmiño		<input checked="" type="checkbox"/>
Password		<input checked="" type="checkbox"/>
Confirm Password		<input checked="" type="checkbox"/>
Maximum number of failed login attempts	<input type="radio"/> [] <input checked="" type="radio"/> Unlimited		
Remaining login attempts	<input type="text"/> <input type="checkbox"/> Reset login attempts		
E-mail address	fpazmino@cee.gob.ec		<input type="checkbox"/>
Subject DN			
CN, Common name	Mayor Fabián Pazmiño		<input checked="" type="checkbox"/>
UID, Unique Identifier	Departamento de Sietemas		<input checked="" type="checkbox"/>
O, Organization	Cuerpo de Ingenieros del Ejercito		<input type="checkbox"/>
OU, Organizational Unit	Entidad Final CEE		<input type="checkbox"/>
C, Country (ISO 3166)	EC		<input type="checkbox"/>
Other subject attributes			
Subject Alternative Name			
RFC 822 Name (e-mail address)	Use data from E-mail address field : <input checked="" type="checkbox"/>		<input type="checkbox"/>
Main certificate data			
Certificate Profile	PERFIL_ENTIDAD_FINAL		<input checked="" type="checkbox"/>
CA	Autoridad Certificadora CEE		<input checked="" type="checkbox"/>
Token	P12 file		<input checked="" type="checkbox"/>

Figura H19. Credenciales de autenticación del solicitante

Tras este proceso este certificado regresará a su estado Generated y se podrán observar las propiedades que lo caracterizan (véase Figura H20).

Se puede apreciar que en efecto el número de serie ha cambiado, debido a que una PKI no puede gestionar dos certificados distintos que contengan el mismo número de serie, aunque estén destinados para el mismo titular; pero se ha conservado la misma clave pública en el certificado, y al momento de instalarlo en el ordenador cliente se almacenará la clave privada anterior.

View Certificate	
Username	Fabian Pazmiño
Certificate number	1 of 2
< View Older	
Certificate Type/Version	X.509 v.3
Certificate Serial Number	7A0D0D570314514A
Issuer DN	CN=Autoridad Certificadora CEE,OU=Entidad de Certificacion,O=Cuerpo de Ingenieros del Ejercito,C=EC
Valid from	2014-08-12 01:20:03-05:00
Valid to	2015-08-12 01:20:03-05:00
Subject DN	UID=Departamento de Sietemas,CN=Mayor Fabiàn Pazmiño,OU=Entidad Final CEE,O=Cuerpo de Ingenieros del Ejercito,C=EC
Subject Alternative Name	rfc822name=fpazmino@cee.gob.ec
Subject Directory Attributes	None
Public key	RSA (2048 bits): 8428621DD95A654A1BAE0F06702504EB82F35C9F5976FD6
Basic constraints	End Entity
Key usage	Digital Signature, Non-repudiation, Key encipherment, Data encipherment
Extended key usage	Client Authentication, Email Protection
Qualified Certificates Statements	No
Signature Algorithm	SHA1WithRSAEncryption
Fingerprint SHA-1	C123B346A624E42501A4468479BD91E3CAA1FB83
Fingerprint MD5	4EC3A994636428ABF0887C102F419382
Revoked	No
<input type="button" value="Republish"/>	Unspecified <input type="button" value="Revoke"/>
Download binary/to IE Download to Firefox Download PEM file	<input type="button" value="Close"/>

Figura H20. Parámetros de un certificado de entidad final - Renovado

Con esto se garantiza que después de que un certificado cumpla con su tiempo de vigencia, en este caso de 1 año, es posible renovarlo para continuar utilizando este sistema de seguridad destinado para el entorno de esta institución.

2.2.2.REVOCACIÓN DE CERTIFICADOS

El estado de revocación invalida a un certificado para que el resto de entidades certificadas lo reconozcan como no fiable y les impida establecer comunicación con su titular. Pueden existir muchas razones por las que un certificado puede ser invalidado, sin posibilidad de que la administración de la PKI pueda establecerlo como válido nuevamente y lo habiliten para retomar su operación.

Las situaciones que justifiquen la revocación de un certificado en lo referente a este proyecto pueden ser: la pérdida del par clave privada o el certificado en el caso de formateo inadecuado, o desperfecto del ordenador que provoque la pérdida de información, el compromiso del par clave privada del usuario, o peor aún de la entidad certificadora, un cambio de afiliación que amerite modificar los datos del usuario, la sustitución de éste

certificado actualizado por el anterior, el cese de la actividad laboral del titular en la institución, o por exceptuar los privilegios de administración de un usuario autorizado sobre algún componente de la PKI.

La revocación se la realiza desde la admin web la opción Search/Edit End Entities del apartado RA Functions, buscando el nombre del usuario en cuestión (véase Figura H17), y accediendo al vínculo View Certificates (véase Figura H21).

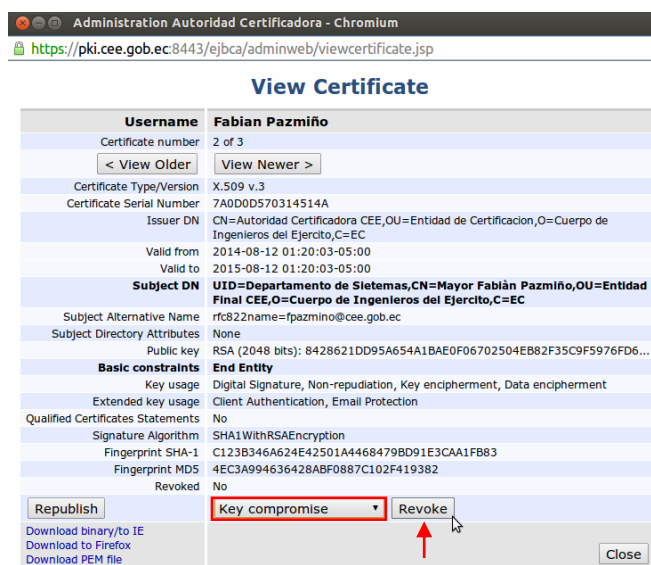


Figura H21. Procedimiento de Revocación

Elegir el motivo por el cual se llevará a cabo la anulación de este certificado de acuerdo a los que se adapten de mejor manera a los descritos anteriormente, las opciones disponibles son: Key compromise, CA compromise, Afiliation Changed, Superseded (sustitución), Cessation of Operation, Certificate hold (certificado retenido), Remove from CRL, Privileges Withdrawn (exceptuar privilegios), AA compromise, y Unspecified por razones distintas.

Finalmente clicar en Revoke y el proceso ha sido completado; con esto se observará en las características de éste certificado que ha sido invalidado, y los motivos de su revocación (véase Figura H22).

Administration Autoridad Certificadora - Chromium
 https://pki.cee.gob.ec:8443/ejbca/adminweb/viewcertificate.jsp

View Certificate

Username	Fabian Pazmiño
Certificate number	2 of 3
< View Older	View Newer >
Certificate Type/Version	X.509 v.3
Certificate Serial Number	7A0D0D570314514A
Issuer DN	CN=Autoridad Certificadora CEE,OU=Entidad de Certificacion,O=Cuerpo de Ingenieros del Ejercito,C=EC
Valid from	2014-08-12 01:20:03-05:00
Valid to	2015-08-12 01:20:03-05:00
Subject DN	UID=Departamento de Sietemas,CN=Mayor Fabiàn Pazmiño,OU=Entidad Final CEE,O=Cuerpo de Ingenieros del Ejercito,C=EC
Subject Alternative Name	rfo822name=fpazmino@cee.gob.ec
Subject Directory Attributes	None
Public key	RSA (2048 bits): 8428621DD95A654A1BAE0F06702504EB82F35C9F5976FD6...
Basic constraints	End Entity
Key usage	Digital Signature, Non-repudiation, Key encipherment, Data encipherment
Extended key usage	Client Authentication, Email Protection
Qualified Certificates Statements	No
Signature Algorithm	SHA1WithRSAEncryption
Fingerprint SHA-1	C123B346A624E42501A4468479BD91E3CAA1FB83
Fingerprint MD5	4EC3A994636428ABF0887C102F419382
Revoked	Yes Revocation date : 2014-08-12 01:48:15-05:00 Revocation reasons : Key compromise
Republish	
Download binary/to IE Download to Firefox Download PEM file	Close

Figura H22. Parámetros de un certificado de entidad final revocado

Las listas de Revocación de Certificados (CRLs), que son archivos que contienen las publicaciones de los certificados que han sido invalidados por la CA, están configuradas para generarse diariamente de manera automática, pero existe la posibilidad hacer que este proceso sea más eficiente al generarla manualmente después de efectuar alguna invalidación.

Esto desde la admin web la opción Basic Functions del apartado CA Functions, y clicar en Create CRL (véase Figura H23).

https://pki.cee.gob.ec:8443/ejbca/adminweb/index.jsp

EJBCA Administration *Misión de la Gloriosa Arma de Ingeniería Militar* CUERPO DE INGENIEROS DEL EJERCITO

CA Functions

CA Functions
 Basic Functions
 CA Activation
 Edit Certificate Profiles
 Edit Publishers
 Edit Certificate Authorities

RA Functions
 Edit User Data Sources
 Edit End Entity Profiles
 Add End Entity
 Search/Edit End Entities

Supervision Functions
 Approve Actions
 View Log
 Log Configuration

System Functions
 System Configuration
 Edit Services
 Edit Administrator Privileges
 My Preferences

Public Web
 Documentation
 Logout

Basic Functions for CA : AdminCA1 View Certificate View Information

Root CA : CN=AdminCA1,O=EJBCA Sample,C=SE
 Download binary/to IE Download to Firefox Download PEM file Download JKS file

Latest CRL: Created 2013-10-16 15:06:07-05:00, Expired 2013-10-17 15:06:07-05:00, number 1 [Get CRL](#)
 Delta CRLs are not enabled.

Create a new updated CRL : CA Is not active

Basic Functions for CA : Autoridad Certificadora CEE View Certificate View Information

Root CA : CN=Autoridad Certificadora CEE,OU=Entidad de Certificacion,O=Cuerpo de Ingenieros del Ejercito,C=EC
 Download binary/to IE Download to Firefox Download PEM file Download JKS file

Latest CRL: Created 2014-08-12 01:10:39-05:00, Expires 2014-08-13 01:10:39-05:00, number 31 [Get CRL](#)
 Delta CRLs are not enabled.

Create a new updated CRL : [Create CRL](#)

Figura H23. Generación manual de CRLs

Sólo con propósitos de verificar este proceso descargar la CRL actualizada de la PKI desde la interfaz web pública de EJBCA (véase Figura H24).

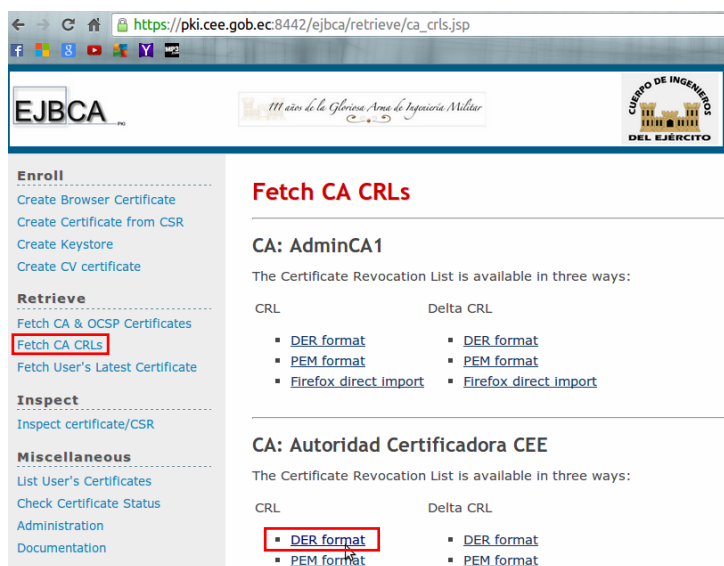


Figura H24. Descarga de la CRL actualizada

Finalmente se puede constatar que en realidad el número de serie del certificado revocado consta en esta lista (véase Figura H25), por lo que no podrá ser utilizado desde este momento para securizar los mensajes transferidos por el correo electrónico institucional.

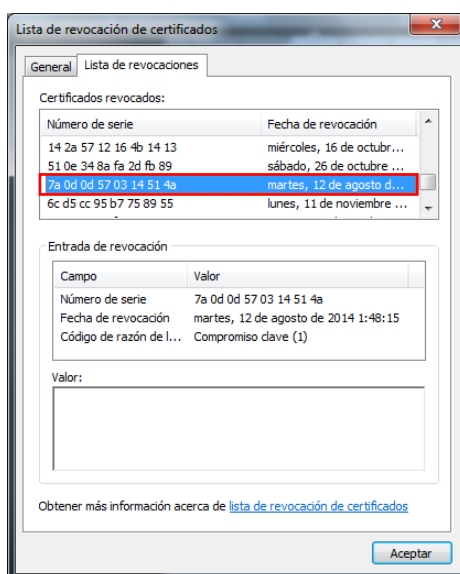


Figura H25. CRL actualizada PKI CEE

De esta forma se cumple con la emisión y gestión de los certificados digitales destinados a los funcionarios y militares en el entorno del CEE.

3.SISTEMA DE CORREO ZIMBRA

Crear o eliminar cuentas de usuario en el servidor de correo serán actividades cotidianas que deberá efectuar el administrador de red del CEE, para ello desde la interfaz web de administración zimbra (<https://mail.cee.gob.ec:7071>) acceder al apartado Administrar y a la sección Cuentas, lugar desde el cual se pueden gestionar los buzones de usuario; en este caso, se mostrará el proceso para crear uno nuevo (véase Figura H26).

Dirección de correo	Nombre mostrado	Estado	Último inicio de sesión	Descripción
admin@cee.gob.ec		Activo	13 de Octubre 2014 10:25:56	Administrative Account
avaldivia@cee.gob.ec	Adrian Valdivia	Activo	29 de Julio 2014 17:17:06	
darellano@cee.gob.ec	David Arellano	Activo	6 de Marzo 2014 16:42:46	
fguevara@cee.gob.ec	Fabrizio Guevara	Activo	8 de Julio 2014 0:29:00	

Nueva cuenta

Información de contacto

Alias

Miembro de

Reenvío

Funciones

Preferencias

Temas

Zimlets

Avanzado

Nombre de cuenta: fpazmino@cee.gob.ec

Nombre: Mayor Fabián

Inicial 2º nombre:

Apellido: Pazmiño

Nombre mostrado: Mayor Fabián Pazmiño auto

Ocultar en GAL:

Estado: Activo

Clase de servicio: **jefes departamentales** auto

Administrador global

Servidor: mail.cee.gob.ec auto

Ayuda Cancelar Anterior Siguiente Finalizar

Figura H26. Creación de una cuenta de correo en el servidor zimbra del CEE

Como se puede apreciar este procedimiento resulta sencillo e involucra ingresar ciertos datos del usuario solicitante, pero uno de los parámetros a definirse es la Clase de Servicio dependiendo del tipo de usuario al que esté destinado; en este caso al usuario de la Figura H26 se le ha asignado el parámetro Jefes Departamentales.

Este servidor tiene configurado varios parámetros de clase de servicio: Comando - Estado Mayor, Jefes Departamentales, Coordinadores, Administrador de Red y Usuarios en General; cada uno de ellos tiene habilitadas distintas características y atributos que

determinan el nivel de funcionamiento de las cuentas de correo, especialmente referentes a la capacidad de almacenamiento de mensajería en los buzones; es así que a cada cuenta creada se le debe asignar un parámetro de Calidad de Servicio acorde al solicitante.

Además se deberá establecer una contraseña de acceso al buzón, números de teléfono y el rol que desempeña el funcionario o militar solicitante en la institución, el resto de parámetros en los apartados Funciones, Preferencias y Avanzado, están predefinidas con la Clase de Servicio asignada (véase Figura H27 y H28).



Figura H27. Funcionalidades de la cuenta

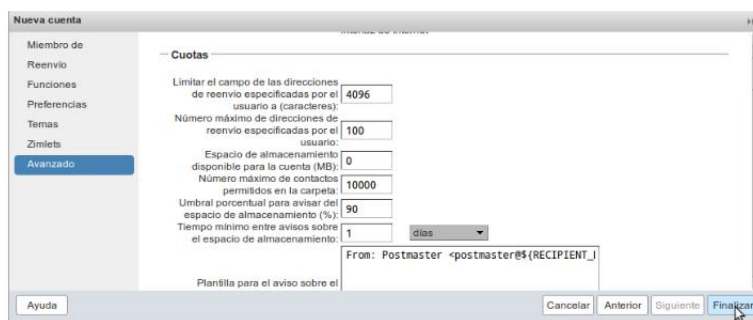


Figura H28. Parámetros del apartado Avanzado

Para complementar este proceso desde el ordenador del usuario solicitante es necesario configurar el cliente de correo (MUA) Outlook que le permita descargar y revisar su mensajería, esta es la forma como los funcionarios y militares del CEE emplean actualmente sus buzones; para ello clic en Inicio, ejecutar Microsoft Office Outlook, elegir la opción Configurar manualmente las opciones del servidor o tipos de servidores

adicionales, acceder al servicio Correo electrónico de Internet, e ingresar los datos del usuario y del servidor de correo (véase Figura H29).

Figura H29. Parámetros de configuración del cliente Outlook

Previo a probar la configuración acceder a la opción Más configuraciones y establecer las seguridades del servidor entrante y de salida (véase Figura H30).

Figura H30. Seguridades para los puertos SMTP y POP3

El servidor zimbra está configurado para proteger la información de usuario de modo que al emplear el puerto SMTP utilizará una conexión cifrada TLS, y al emplear el puerto POP3 para la entrega de mensajería utilizará una conexión cifrada SSL con el cliente.

Con esto es posible verificar y finalizar la configuración de la cuenta, ahora es necesario configurar el cliente Outlook para activar el mecanismo de seguridad S/MIME y cargar el certificado digital con el cual el usuario podrá generar mensajes firmados digitalmente.

Entonces desde el panel Herramientas de Outlook seleccionar Centro de Confianza, en él dirigirse a Seguridad del Correo Electrónico y habilitar las tres primeras casillas (véase Figura H31), esto activará las técnicas de cifrado y firma digital.

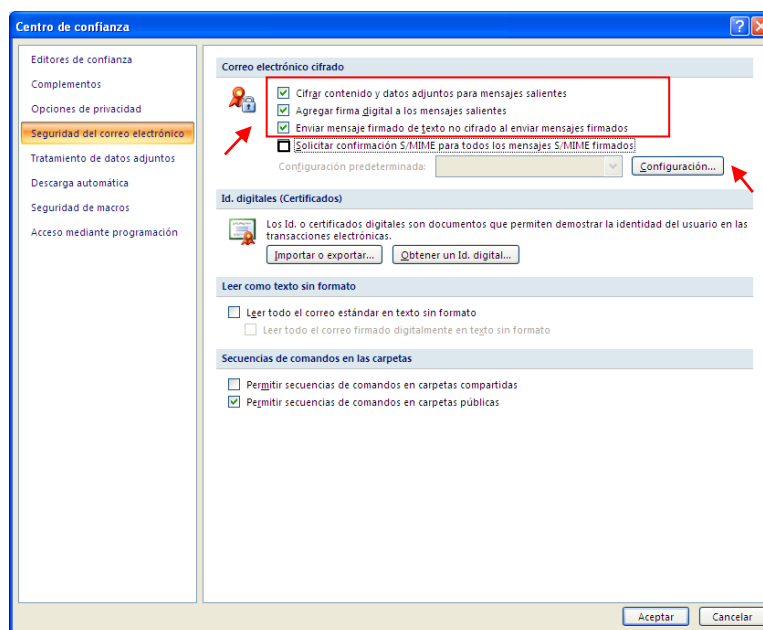


Figura H31. Habilitar técnicas S/MIME de cifrado y firma digital

La cuarta casilla habilita una respuesta de confirmación S/MIME, eso significa que cada vez que un funcionario envíe un mensaje con su firma digital, recibirá un mensaje notificando que éste ha sido revisado por el receptor; pero se ha considerado que al enviar mensajes a una lista de destinatarios simultáneamente, esto generaría demasiadas respuestas e incrementaría el flujo de tráfico innecesario en la red, por ello no ha sido habilitada esta opción.

Sobre la misma pantalla Seguridad del Correo Electrónico (Figura H31) seleccionar Configuración y elegir el certificado de usuario que se va a utilizar desde este momento para firmar digitalmente los mensajes que se originen en esta cuenta de correo, y también los algoritmos criptográficos tanto de firma, como de cifrado (véase Figura H32).

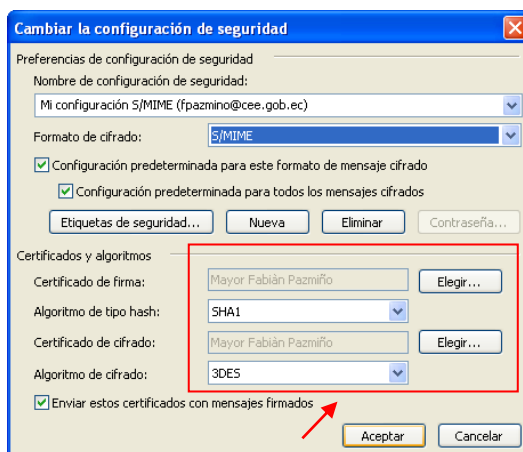


Figura H32. Certificado de firma digital

Todas estas actividades y procedimientos los efectuará el administrador de red del CEE de Quito para implementar una plataforma de correo electrónico segura bajo la administración de una Infraestructura de Clave Pública que avale la legitimidad de los certificados emitidos en esta entidad.

ANEXO I

2014

UNIVERSIDAD TÉCNICA DEL NORTE

MANUAL DE

USUARIO

Autor: David R. Valencia

1.INTRODUCCIÓN

Este manual contiene información relacionada con las actividades que tendrán que efectuar los militares y funcionarios que laboran en el CEE, para proteger la información transferida a través del sistema de correo electrónico institucional.

1.1. MENSAJES DE CORREO CON FIRMA DIGITAL

Para enviar este tipo de mensajes el proceso es el mismo que se realiza con un mensaje convencional, pero antes de transferirlo cerciorarse de que el ícono del sobre con un sello rojo esté activado (véase Figura I1).

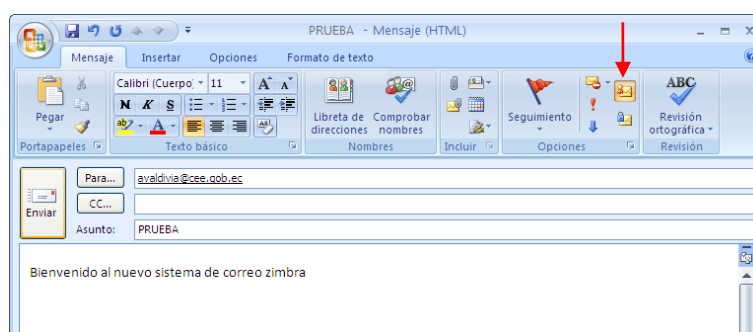


Figura I1. Enviar un mensaje firmado digitalmente

Para generar la firma de este mensaje, de acuerdo a las configuraciones realizadas, es necesario ingresar la contraseña de protección del par clave privada acordada con el administrador de red (véase Figura I2).

En el extremo del destinatario se visualiza el contenido del mensaje, y para verificar la firma digital basta con acceder al botón rojo a la derecha de la bandeja de entrada (véase Figura I3).

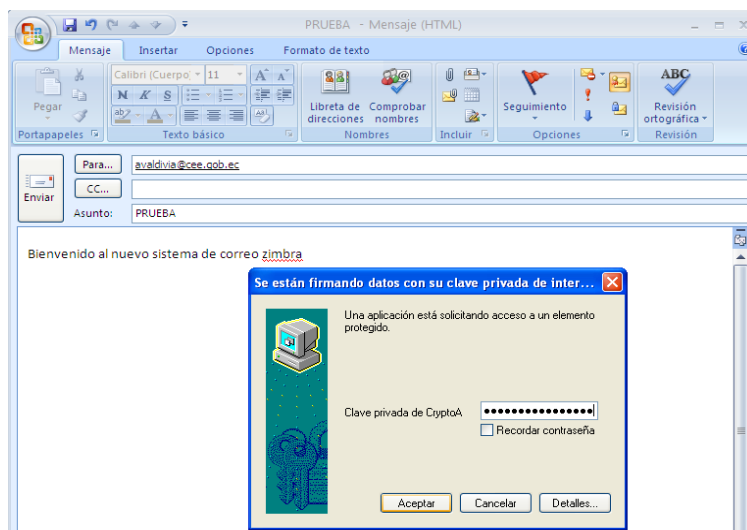


Figura I2. Contraseña de protección de la clave privada - emisor

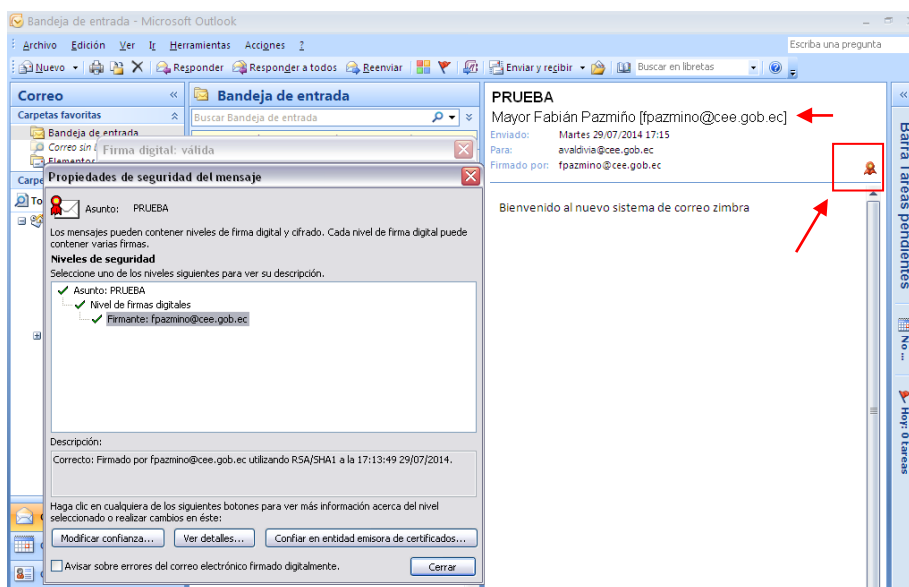


Figura I3. Comprobación de la firma del mensaje

En este caso la firma ha sido validada y se puede considerar que este mensaje no ha sufrido ningún tipo de modificación desde que fue creado, garantizando su integridad, y el no repudio por parte del emisor responsabilizándolo por el contenido del mensaje que ha generado.

1.2. OBTENCIÓN DE LOS CERTIFICADOS DE OTROS USUARIOS

Es necesario disponer de los certificados de los destinatarios con quienes se requiera establecer comunicaciones seguras a través del correo, para cifrar los mensajes dirigidos hacia ellos y que puedan revisarlos únicamente empleando su par clave privada respectiva.

La manera más sencilla de hacerlo es enviando un mensaje firmado digitalmente, como se ha indicado en el proceso anterior, para que el destinatario agregue a sus contactos de correo al funcionario emisor, e implícitamente importe su certificado en el repositorio de Windows.

Entonces al recibir un mensaje con firma digital dar clic derecho sobre la dirección de correo electrónico del emisor (Mayor Fabián Pazmiño [fpazmino@cee.gob.ec]) y agregarla a la lista de contactos personales, en el caso que este usuario ya exista habrá que reemplazarlo, con ello se almacenará el contacto incorporando su certificado (véase Figura I4).

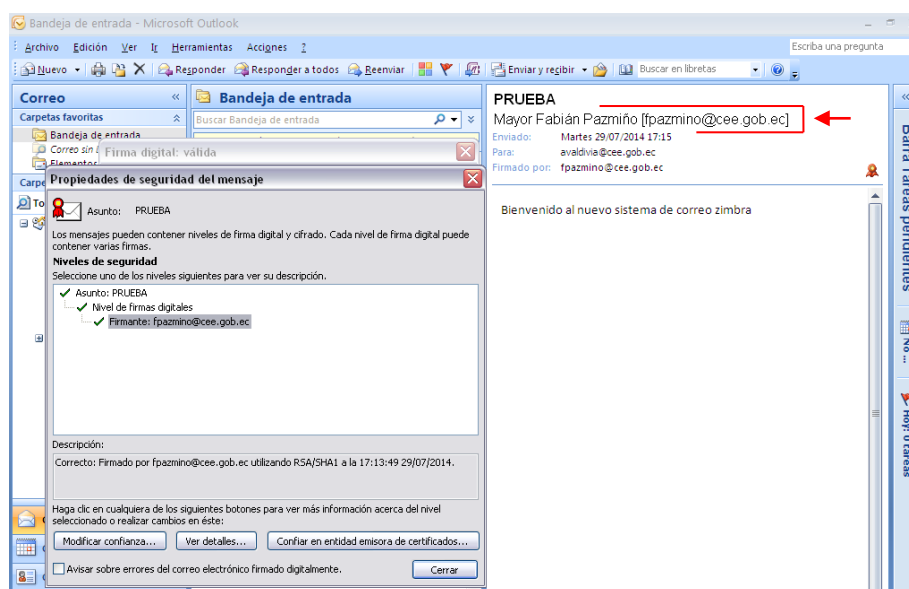


Figura I4. Obtener el certificado digital desde un e-mail firmado digitalmente

Al disponer del certificado de este funcionario es posible enviarle desde este momento mensajes cifrados.

1.3. MENSAJES DE CORREO CIFRADOS

Previo a generar un mensaje que será cifrado para protegerlo de lecturas no autorizadas y garantizar que únicamente su destinatario pueda hacerlo, es necesario contar con su certificado; esto se puede verificar accediendo a los detalles del contacto y al ícono de los certificados para saber si se ha importado el certificado de este usuario (véase Figura I5).

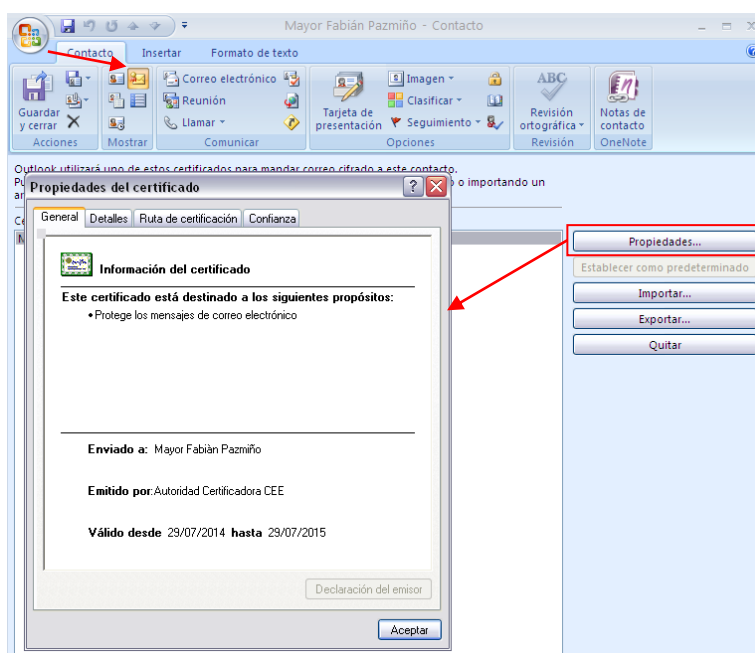


Figura I5. Agregar un contacto incluyendo su certificado

Para enviar este tipo de mensajes el proceso es el mismo que se realiza con un mensaje convencional, pero antes de transferirlo cerciorarse de que el ícono del sobre con un candado azul esté activado (véase Figura I6).

En el extremo del destinatario se puede apreciar que no se muestra ningún elemento en el panel de lectura, de manera que si no se ingresa la contraseña que protege el par clave privada acordada con el administrador de red del CEE, que va a ser empleada para descifrar este mensaje, no se tendrá acceso éste (véase Figura I7).

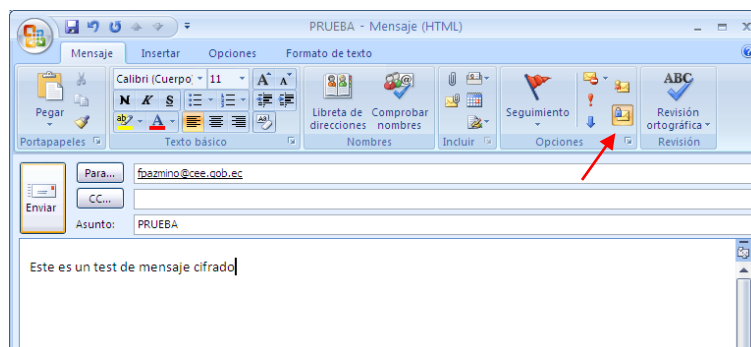


Figura I6. Envío de un mensaje cifrado

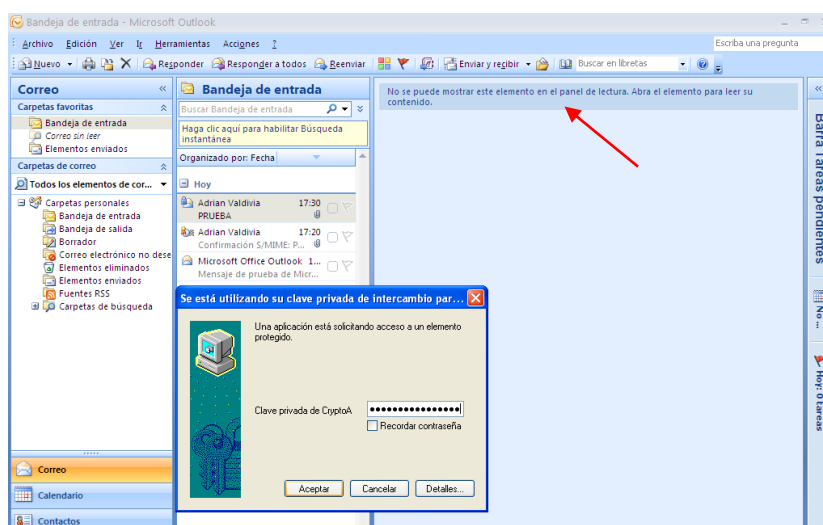


Figura I7. Contraseña para utilizar la clave privada

Al ingresarla se desplegará este panel para visualizar el mensaje, y al presionar sobre el símbolo del candado azul, se verificará el algoritmo de cifrado y hacia quién está dirigido (véase Figura I8).

Con esto se garantiza la confidencialidad del mensaje, y la autenticación del destinatario. En el caso de recibir mensajes cifrados con documentos adjuntos, de igual forma no se muestra ningún elemento en el panel de lectura (véase Figura I9).

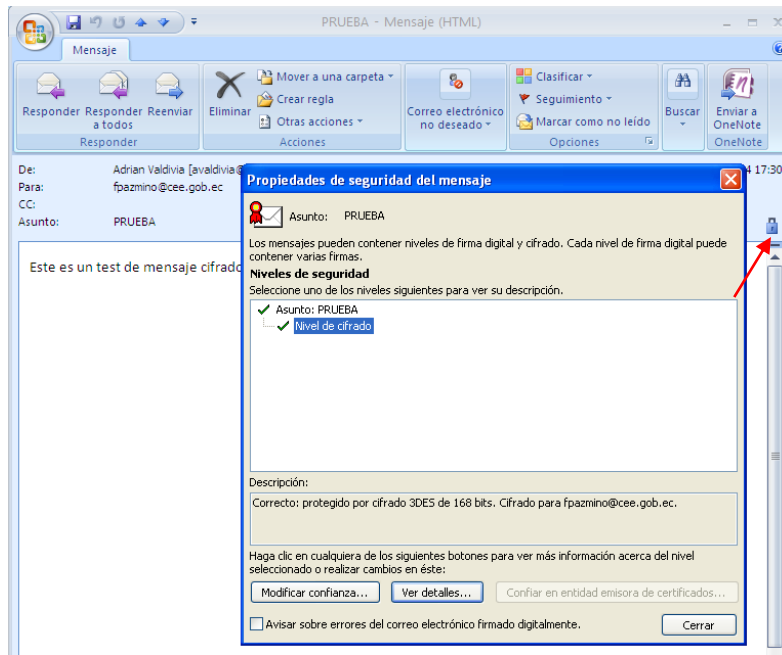


Figura I8. Visualizar el mensaje cifrado

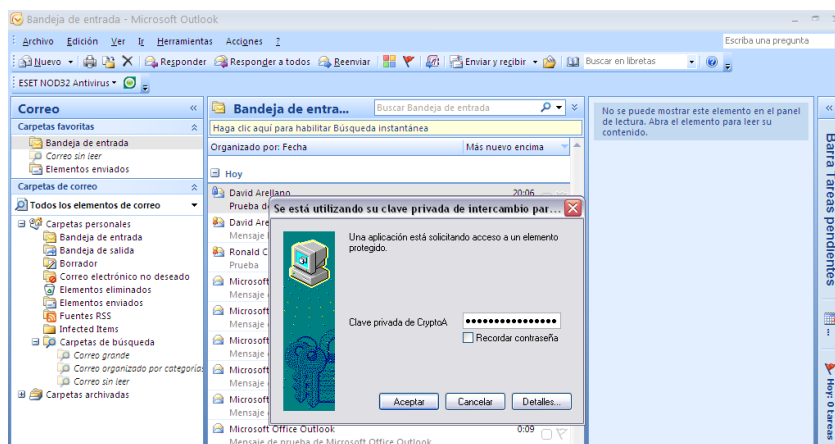


Figura I9. Mensaje cifrado que contiene documentos adjuntos

Sólo al ingresar la contraseña que protege el par clave privada se podrá revisar su contenido (véase Figura I10).

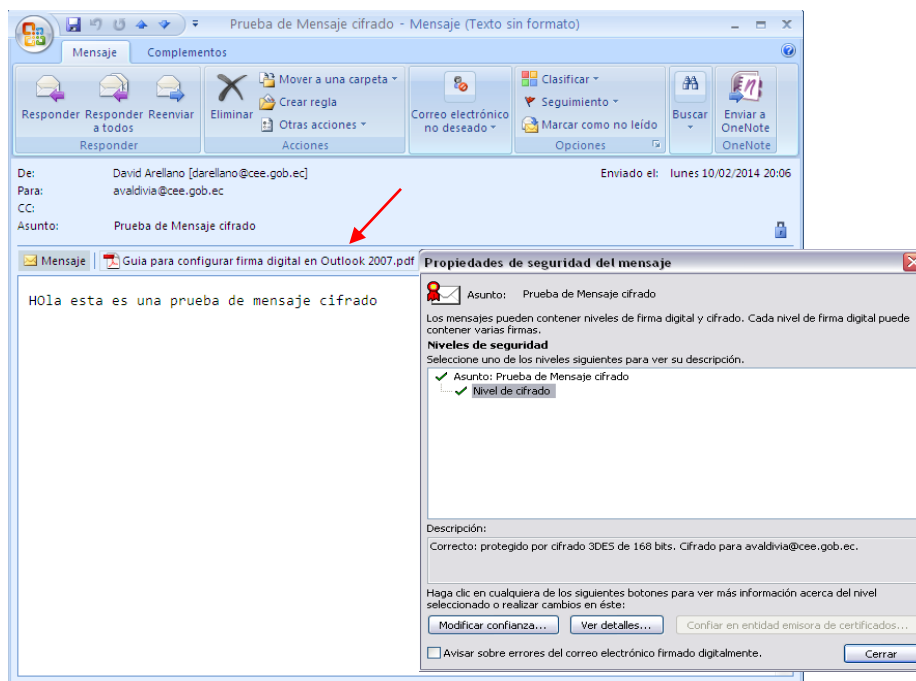


Figura I10. Visualizar un mensaje cifrado con documentos adjuntos

1.4. MENSAJES DE CORREO FIRMADOS Y CIFRADOS

El propósito de este manual es capacitar a los funcionarios y militares del CEE de Quito para que generen mensajes de correo electrónico utilizando estos dos tipos de protecciones criptográficas.

Entonces, análogamente a los anteriores proceso descritos, al recibir un mensaje que ha sido firmado y cifrado, el proceso es el mismo, pero al visualizarlo se apreciará que existen los dos símbolos, el candado y el botón rojo, al acceder a cada uno se verifica tanto el nivel de firma, como el de cifrado (véase Figura I11).

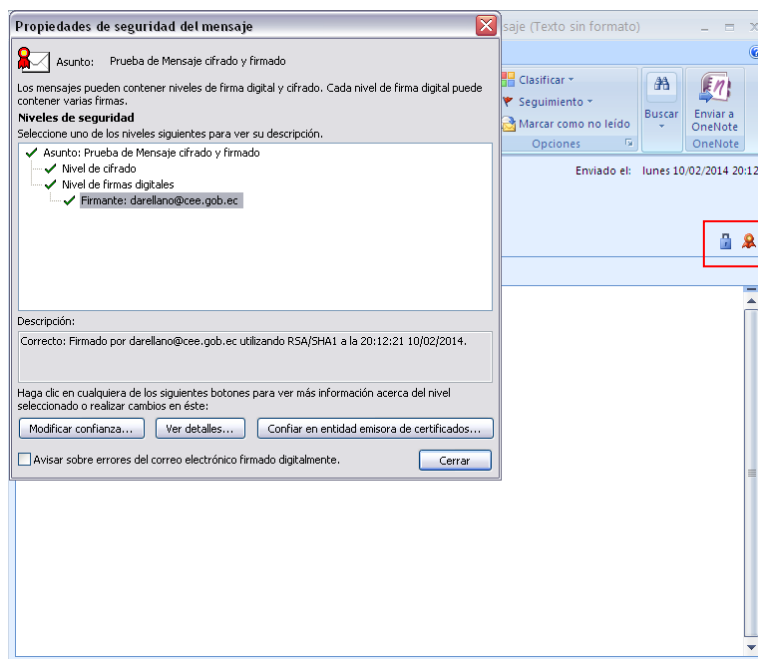


Figura I11. Visualizar un mensaje firmado y cifrado

Si la firma digital es validada se garantiza la integridad del mensaje, y el no repudio del emisor; y si el nivel de cifrado es válido se garantiza la confidencialidad del mensaje, y la autenticación del destinatario, logrando de esta manera implantar cuatro dimensiones de seguridad por cada mensaje transferido sobre esta plataforma de correo institucional.