ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMATICA Y ELECTRONICA

ESCUELA DE INGENIERIA EN SISTEMAS

"IMPLEMENTACIÓN DE FIRMAS DIGITALES PARA MENSAJERÍA DE DATOS MEDIANTE LA UTILIZACIÓN DE DISPOSITIVOS TOKEN, CASO PRÁCTICO: PROTOTIPO DE FIRMAS DIGITALES PARA EL HOSPITAL DE BRIGADA No. 11 GALÁPAGOS"

TESIS DE GRADO

Previa la obtención del título de:

INGENIERO EN SISTEMAS INFORMATICOS

Presentado por:

PILAR DE LOURDES GAIBOR NARANJO

RIOBAMBA – ECUADOR

2010

AL ING. PATRICIO MORENO

Colaborador de Tesis, por su valioso aporte de experiencia y conocimientos para la realización de este trabajo.

Este trabajo se lo dedico primeramente a Dios, ya que sin él nada podemos hacer. Dios es quien nos concede el privilegio de la vida y nos ofrece lo necesario para lograr nuestras metas.

A mi esposo Angel y a mis hijos Melanie y Daniel, por su amor y apoyo permanente.

FIRMAS DE RESPONSABILIDADES

NOMBRE	**FIRMA**	**FECHA**
Ing. Iván Menes **DECANO DE LA FACULTAD DE INFORMATICA Y ELECTONICA**	_____	_____
Ing. Raúl Rosero **DIRECTOR DE LA ESCUELA DE INGENIERÍA EN SISTEMAS**	_____	_____
Ing. Patricio Moreno **DIRECTOR DE TESIS**	_____	_____
Ing. Diego Ávila **MIEMBRO TRIBUNAL**	_____	_____
Tlgo. Carlos Rodríguez **DIRECTOR CENTRO DE DOCUMENTACIÓN**	_____	_____

NOTA _____

"Yo, PILAR DE LOUDES GAIBOR NARANJO soy responsable de las ideas, doctrinas, resultados, expuestos en la presente investigación, y el patrimonio intelectual del mismo, pertenece a la ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO"

_____

Pilar de Lourdes Gaibor Naranjo

INDICE

INDICE DE ABREVIATURAS

AC	Autoridad Certificadora
AR	Autoridad de Registro
BCE	Banco Central del Ecuador
CP	Políticas de Certificación
CPS	Declaración de Prácticas de Certificación
CRL	Lista de Certificados Revocados
ECIBCE	Entidad de Información del Banco Central del Ecuador
FIPS	Federal Information Processing Standard (Estándares del Gobierno Norteamericano para el procesamiento de la información)
LDAP	Protocolo de acceso a servicios de directorio
MD5	Algoritmo de Resumen de Mensaje
NDS	Novell directory Services.
OCSP	Online Certificate Status Protocol. Este protocolo permite comprobar en línea la vigencia de un certificado electrónico.
PC	Políticas de Certificados
PIN	Número de Identificación Personal o contraseña
PKI	Infraestructura de Clave Pública
RSA	Rivest, Shamir and Adelman
SHA	Algoritmo Hash Seguro

INDICE DE TABLAS

INDICE DE FIGURAS

INTRODUCCIÓN

La firma digital tiene muy poco tiempo de haber surgido, debido a la necesidad de un mundo globalizado en donde las transacciones y la interacción entre individuos son interpersonales y sin vínculos físicos, haciendo de la identificación un problema y un requerimiento de primera necesidad, es por eso que se ha decidido realizar un prototipo de firmas digitales utilizando el dispositivo Token usb, en el Hospital de Brigada N° 11 "Galápagos", el mismo que permite realizar firmas digitales en los diferentes tramites como lo son oficios, memorándum, telegramas que se realiza dentro y fuera de la institución, lo que garantiza que sean enviados con total seguridad.

El objetivo de esta Tesis es realizar una implementación de firmas digitales para mensajería de datos mediante la utilización de dispositivos token, para lograr esto se ha realizado una investigación y se ha adquirido el dispositivo Token usb para firmas digitales en la entidad certificadora en el Banco Central del Ecuador que permite el desarrollo de este prototipo, así como también la comparación del funcionamiento del dispositivo Token para firmas digitales entre las plataformas Windows XP y Linux Ubuntu 8.04 en la cual se ha seleccionado la más optima.

El Capitulo I presenta para un mejor entendimiento acerca de los fundamentos generales de criptografía, firma digital, certificado digital posterior a esto en el capitulo II se trata los conceptos de una Infraestructura de clave publica además la infraestructura de clave pública del Banco Central del Ecuador.

En el capitulo III se realizó una comparación del funcionamiento del dispositivo Token para firma digital entre las plataformas Windows XP y Linux Ubuntu 8.04, en la que se establece cual de ellas posee mayores ventajas, para el desarrollo del prototipo de

firmas digitales. Finalmente en el capitulo IV se muestra el proceso de construcción de un prototipo de firmas digitales utilizando el dispositivo Token usb para el Hospital de Brigada N° 11 “Galápagos”.

CAPÍTULO I. FUNDAMENTOS GENERALES

En este capítulo se presenta la definición, objetivo, tipos de criptografía , criptografía simétrica y criptografía asimétrica, ventajas y desventajas de los tipos de criptografía, algoritmos asimétricos, sobre el concepto de funciones hash, integridad de los datos, principales funciones hash, conceptos, proceso, características acerca de la firma digital y finalmente concepto de certificado digital dentro del cual se encuentran formatos, campos predeterminados, versión, Número de serie, firma, expedidor, periodo de validez, Propietario, Información de la Clave Pública del Propietario, Identificador del Expedidor, Extensiones.

1.1. Criptografía

1.1.1. Definición

La palabra criptografía proviene del griego “kryptos” que significa ocultar y “grafos” que significa escribir, literalmente sería “escritura oculta”.

La criptografía es la ciencia que utilizando matemáticas complejas, desarrolla algoritmos criptográficos que permiten modificar (cifrar) un mensaje legible con el uso de una clave; después de la modificación, dicho mensaje es ilegible para todo aquel que no posea la clave. Lo que hace posible que la transferencia de información sea segura y que solo pueda ser leída por las personas a quienes va dirigida.

1.1.2. Objetivo

La finalidad de la criptografía es, en primer lugar, garantizar el secreto en la comunicación entre dos entidades (personas, organizaciones, etc.) y, en segundo lugar, asegurar que la información que se envía es auténtica en un doble sentido: que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado, habitualmente denominado criptograma, no haya sido modificado en su tránsito.

1.1.3. Tipos

Se puede distinguir principalmente dos tipos de criptografía: la simétrica y la asimétrica

1.1.3.1. Criptografía simétrica

Los sistemas de criptografía simétrica son aquellos que utilizan la misma clave para cifrar y descifrar un documento. Este tipo de sistema tiene un problema de seguridad y reside en el intercambio de claves entre el emisor y el receptor ya que ambos deben usar la misma clave. Para evitar este problema ambas partes deben formalizar una cita para el intercambio de claves.

Este tipo de criptografía se usa para cifrar y descifrar mensajes, se basa en el uso de una única clave conocida de antemano por ambas partes.

La seguridad de este tipo de criptografía radica principalmente en mantener en secreto la clave y no se preocupa necesariamente por el algoritmo de cifrado, es decir, que no es de mucha ayuda conocer el algoritmo que se utilizó.

Dado que toda la seguridad se centra en la clave, esta tiene que ser difícil de adivinar. Esto quiere decir que el abanico de claves posibles, es decir, el espacio de posibilidades de claves, debe ser amplio. Algunos ejemplos de algoritmos simétricos son 3DES, AES, e IDEA.

Uno de los principales inconvenientes con este tipo de sistema no está ligado a su seguridad, sino al intercambio de claves. El canal utilizado para el intercambio debe ser lo suficientemente seguro. Una vez que el remitente y el destinatario hayan intercambiado las claves pueden usarlas para comunicarse con seguridad. Otro problema es el número de claves que se necesitan. Si tenemos un número n de personas que necesitan comunicarse entre sí, se necesitan n/2 claves para cada pareja de personas que tengan que comunicarse de modo privado. Esto puede funcionar con un grupo reducido de personas, pero sería imposible llevarlo a cabo con grupos más grandes.

La criptografía simétrica utiliza algoritmos criptográficos que permiten cifrar y descifrar un texto con la misma clave. Esta clave toma por ese motivo el nombre de clave simétrica.

La Figura I-I. muestra el proceso de criptografía simétrica; en este proceso se maneja una clave simétrica y un algoritmo para cifrar y descifrar un mensaje. Un texto cifrado con una clave simétrica sólo puede ser descifrado utilizando la misma clave.

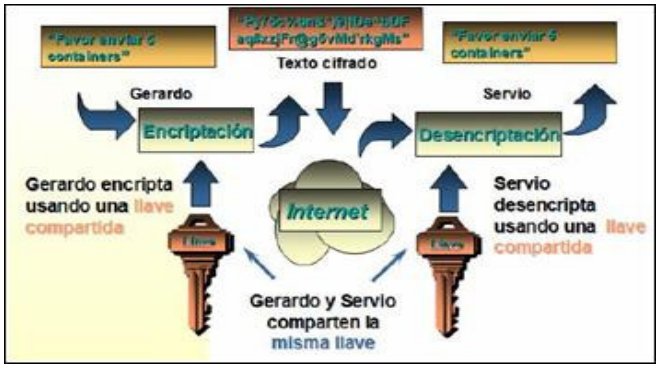


FIGURA I-I. Criptografía simétrica

La criptografía simétrica garantiza el servicio de confidencialidad. Para cumplir con este servicio, la clave debe ser conocida solamente por el emisor y el receptor de un mensaje; así solo los dos pueden descifrarlo. El secreto de la clave es lo único que garantiza que la información está protegida.

Puede utilizarse una clave por cada comunicación que se inicie con cada receptor; de esta manera, si un atacante logra encontrar una clave y descifrar cierto mensaje, no podrá descifrar el siguiente utilizando la clave encontrada, incluso si la comunicación se lleva a cabo con el mismo receptor.

1.1.3.1.1 Ventajas y Desventajas

a. Ventajas

Entre las principales ventajas de la criptografía simétrica, con respecto a la criptografía asimétrica se pueden mencionar:

- El mensaje en texto cifrado mantiene un tamaño igual o menor al mensaje en texto plano.
- Una clave simétrica con menor tamaño entrega el mismo nivel de resistencia a un ataque que una clave asimétrica de mayor tamaño.
- La criptografía simétrica garantiza la confidencialidad de la información.

b. Desventajas

Entre las principales desventajas de la criptografía simétrica, con respecto a la criptografía asimétrica se tiene:

- La administración de claves simétricas es compleja.
- El intercambio de claves es susceptible a interceptación.
- Para que el intercambio se lleve a cabo, el emisor y el receptor deben establecer una comunicación previamente.
- El número de claves involucradas en un sistema que utiliza criptografía simétrica es aproximadamente el cuadrado del número de participantes.
- Debido a que se utiliza la misma clave para cifrar y descifrar, la criptografía simétrica no permite la utilización de firmas digitales.

- No se puede garantizar integridad de los mensajes utilizando criptografía simétrica.

1.1.3.2. Criptografía asimétrica

A mediados de la década de los setenta, Whitfield Diffie y Martin Hellman, introdujeron los primeros conceptos de criptografía asimétrica, con el fin de encontrar una manera segura para el intercambio de claves simétricas.

La criptografía asimétrica se basa en algoritmos que manejan matemáticas más complejas que las utilizadas en algoritmos simétricos. Los algoritmos asimétricos demandan la generación de dos claves relacionadas matemáticamente, una clave es conocida como clave privada y la otra como clave pública.

El principio básico de la criptografía asimétrica es que sí se cifra un mensaje con una clave privada, éste solo puede descifrarse con su respectiva clave pública; y sí se cifra con una clave pública, solo se consigue descifrarlo con su clave privada como se muestra en la Figura I-II.

Es importante aclarar que una de las dos claves, no puede por sí sola cifrar y descifrar un mensaje; además, no se puede obtener una clave a partir de la otra. Esto permite que la clave pública pueda estar disponible para todos los usuarios.

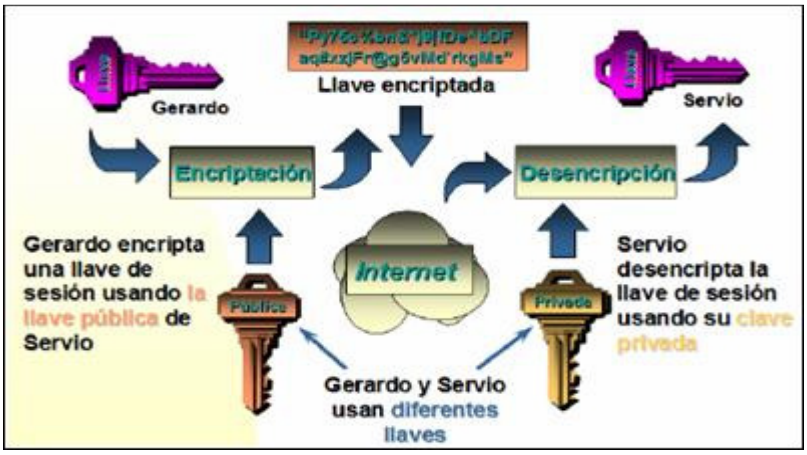


FIGURA I-II. Criptografía Asimétrica

En cambio, la clave privada debe estar disponible solo para el dueño de la pareja de claves. Si se cumple con esta condición, se puede intercambiar información entre usuarios sin la necesidad de establecer comunicaciones en las que se intercambie información con anterioridad; adicionalmente, se elimina el problema de la interceptación de claves.

1.1.3.2.1 Ventajas y Desventajas

a. Ventajas

Entre las principales ventajas de la criptografía asimétrica, con respecto a la criptografía simétrica se puede mencionar:

- La administración de claves asimétricas tiene menor complejidad.
- El número de claves involucradas en un sistema que utiliza criptografía asimétrica es el doble del número de participantes, cada participante posee una pareja de claves. Esto permite mejor escalabilidad.
- Debido a que la clave pública está disponible para todos los usuarios, la criptografía asimétrica no es susceptible a interceptación de claves.
- La criptografía asimétrica permite la utilización de firmas digitales.
- Con criptografía asimétrica se puede garantizar confidencialidad y autenticación.
- Utilizando criptografía asimétrica se puede garantizar la integridad de los mensajes.

b. Desventajas

Entre las principales desventajas de la criptografía asimétrica, con respecto a la criptografía simétrica se tiene:

- Es susceptible a ataques de suplantación; un atacante podría cambiar una clave pública y sustituir a un usuario legítimo.
- El tamaño del mensaje en texto cifrado es mayor al tamaño del mensaje en texto plano.
- La criptografía asimétrica consume mayores recursos.
- Requiere de claves de mayor tamaño para brindar el mismo nivel de seguridad.

1.1.3.2.2 Algoritmos Criptográficos Asimétricos

Entre los algoritmos asimétricos más difundidos se tiene a Diffie-Hellman, RSA, DSA.

a. Diffie-Hellman

Este algoritmo no se centra en el cifrado y descifrado de un mensaje; basa su operación en funciones matemáticas que utilizan ciertos parámetros para generar una clave secreta.

Este protocolo utiliza logaritmos discretos para mantener su seguridad. Se asume que es computacionalmente imposible calcular la clave secreta a partir de los valores públicos compartidos.

b. RSA (Rivest, Shamir, Adelman)

Este algoritmo garantiza los servicios de autenticación (firmas digitales) y confidencialidad (cifrado).

Se recomienda utilizar claves con una longitud de 1024 bits para datos importantes y de 2048 bits para datos críticos.

c. DSA (Digital Signature Algorithm)

Inicialmente DSA fue creado para manejar claves de 512 bits; posteriormente se estableció claves de hasta 1024 bits.

La generación de la firma digital es más rápido que en RSA; en cambio, la comprobación de la firma es más lento. Se considera que en la mayoría de casos, se realiza más de una comprobación de la firma digital de un mensaje, por lo que la comprobación debería ser más eficiente.

1.1.4. Funciones Hash

Una función hash es aquella que toma como entrada un mensaje y entrega como resultado un resumen conocido como valor hash; estas funciones tienen gran importancia en criptografía. Con el uso de funciones hash y criptografía asimétrica, se

puede garantizar el servicio de integridad de los datos, el establecimiento de firmas digitales.

1.1.4.1. Integridad de los Datos

Con el uso de funciones hash y criptografía asimétrica se puede garantizar el servicio de integridad. Dadas las características de una función hash, queda claro que si se aplica una función hash a un mensaje, el valor hash obtenido es como la huella digital del mensaje; si se altera tan solo un bit del mensaje original, el valor hash será diferente.

Se puede verificar la integridad de un mensaje enviando el mensaje y su valor hash al receptor; en el destino, el receptor puede aplicar la misma función hash al mensaje y luego comparar su resultado con el valor recibido. Para evitar que un atacante cambie el mensaje y el valor hash introduciendo valores falsos, el valor hash debe enviarse cifrado con la clave privada del emisor.

1.1.4.2. Principales Funciones Hash

Existen dos categorías de algoritmos hash altamente difundidos; en primer lugar los MD5 creados por RSA y en segundo lugar la serie SHA.

1.1.4.2.1 MD5 (Message Digest 5)

MD5 es la última versión de algoritmos hash de RSA, maneja optimización para procesadores de 32 bits; es uno de los algoritmos hash más difundidos, proporciona un buen nivel de seguridad y resulta más rápido que SHA.

1.1.4.2.2 SHA (Secure Hash Algorithm)

SHA es ligeramente más lento que MD5 y su diseño es similar al de MD4. Presenta mayor resistencia ante ataques.

1.1.5. Firma Digital

La firma digital es un código alfanumérico que se adjunta a un mensaje y que identifica a la persona o sistema que envío dicho mensaje.

Las firmas digitales son producto de la combinación de funciones hash y criptografía asimétrica. Los estándares que incluyen normas para el uso de firmas digitales son RSA Data Security y DSS.

Una firma digital es un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje. Ver Figura I.III.

Para firmar un documento digital, su autor utiliza su clave secreta, lo que impide que pueda después negar su autoría. La validez de dicha firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor.

En general, se dice que un usuario firma un mensaje de datos cuando lo cifra con su clave privada. Debido a que cifrar datos con criptografía asimétrica consume demasiados recursos, el concepto de firma digital se enfoca en cifrar el valor hash de un mensaje; de esta manera se garantiza autenticación e integridad.

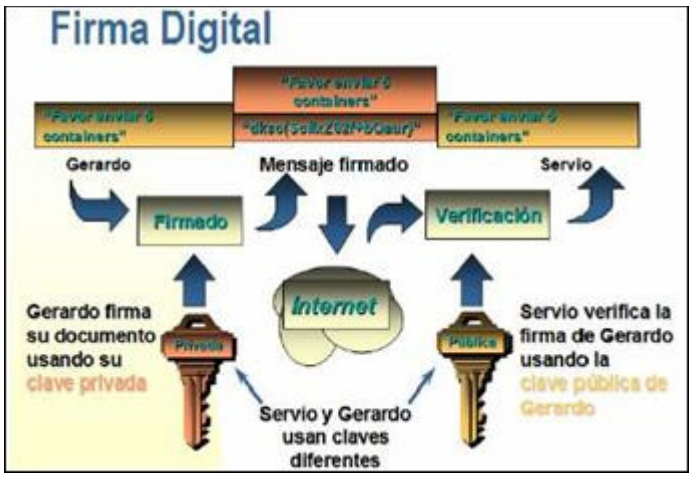


FIGURA I-III. Firma digital

La firma digital tiene una longitud de caracteres: mientras más larga dicha longitud, más dura e inviolable es la firma digital.

1.1.5.1. Proceso de Firma digital

Tal como se indica en el párrafo anterior. La firma digital es generada al momento de escribir un mensaje electrónico, pues depende del contenido del mismo y de la clave privada del usuario, típicamente almacenada en un token como se muestra en la Figura I-IV. Lo que se realiza es una operación matemática conocida como hash que se aplica sobre el mensaje electrónico para producir un resumen del mensaje (digest). El resultado es un extracto del mensaje de longitud fija que no puede ser convertida de vuelta al mensaje original (hash de una vía).

FIGURA I-IV. Token

El token es un dispositivo de almacenamiento de las claves pública y privada necesarias para generar la firma digital que se adjuntara a un documento.

Como se ha expresado esta operación convierte el mensaje electrónico de tamaño variable a un tamaño de longitud fija. Los algoritmos hash más utilizados para esta función son el MD5 ó SHA-1. La longitud del extracto que se consigue oscila entre 128 y 160 bits (según el algoritmo utilizado).

Este mensaje de tamaño constante es combinado con la clave privada del usuario mediante un algoritmo matemático. El algoritmo matemático más utilizado es RSA.

De esta forma se obtiene un extracto final cifrado con la clave privada del autor el cual se añadirá al final del texto original para que se pueda verificar la autoría e integridad del documento. Este extracto es conocido como firma digital. Si el texto original cambia el resultado del hash y algoritmo aplicado también deben cambiar. De no ocurrir esto, se

dice que el mensaje original ha sido adulterado. De esta manera se puede decir que la firma digital preserva la integridad del documento original.

Adicionalmente se puede decir que el mensaje no puede ser repudiado por su autor pues como se observó la firma digital usa la clave privada del autor que solamente es conocida por el mismo.

La ley de Comercio Electrónica ecuatoriana en su Art. 17 responsabiliza del uso o mal uso de la firma digital al propietario de la misma por lo que debe tenerse sumo cuidado de que caiga en manos extrañas.

El proceso que se sigue para firmar un documento digitalmente y recibirlo es el siguiente:

a. El usuario remitente prepara el mensaje a enviar.
b. El remitente, usando un software o hardware especializado, aplica un algoritmo hash sobre el texto a firmar
c. El remitente encripta el resultado del hash con su clave privada (extraída de un token) generando así la firma digital.
d. La firma digital se añade al final del texto original.
e. El remitente envía electrónicamente la firma digital y mensaje original al destinario.

   "El mensaje original puede estar encriptado o no. Esto no es un requisito para firmar un documento digitalmente"

f. El usuario de destinario recibe el documento firmado. Para constatar su origen usa la clave pública del remitente.

   De esta manera el destinatario sabe que el documento fue firmado por su remitente (y no hay forma de repudiarlo) y que no ha sufrido ninguna alteración en el camino (pues de otra manera su propia versión de hash no hubiese coincidido con la versión de hash del remitente).

1.1.5.2. Características de la Firma Digital

La firma digital tiene tres características importantes que son las siguientes:

- Es utilizada para garantizar que la persona o sistema que envío el mensaje es quien ha firmado digitalmente el documento y no puede repudiar el envío del mismo (No Repudio).
- El uso de la firma digital implica poder atribuir de forma indubitable el mensaje electrónico recibido a una determinada persona como autora del mensaje (Identidad).
- Consiste en asegurar que la información no ha sufrido cambios no autorizados, ya sea de manera accidental o intencional, una vez firmado. Es decir la firma digital, asegura que el mensaje recibido por el receptor es exactamente el mismo mensaje emitido por el emisor, sin que haya sufrido alteración alguna durante el proceso de transmisión del emisor al receptor (Integridad).

Además de estas tres características principales que cumple la firma digital, se habla de un cuarto elemento, que es la confidencialidad, que no es un requisito esencial de la firma digital si no accesorio de la misma. La confidencialidad se da cuando se encripta el mensaje original.

1.1.6. Certificados Digitales

Los certificados son credenciales digitales; en su forma más simple, un certificado contendrá una clave pública y el nombre de su propietario. De esta manera el nombre del usuario queda unido a su clave; así se genera confianza en la legitimidad de una clave pública.

Además es emitido por una empresa denominada "Autoridad de certificación" que garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.

Un certificado digital es un documento de acreditación que permite a las partes tener confianza en las transacciones en internet. Por tanto garantiza la identidad de su poseedor en internet mediante un sistema de claves administrado por una tercera parte de confianza.

Las recomendaciones para la generación de certificados digitales se encuentran registradas en la norma UIT-T X.509, esta norma contiene información sobre la sintaxis de los certificados digitales y nombres distinguidos.

En la actualidad se encuentra vigente la tercera versión (X.509v3), X.509v3 se enfocó en aumentar la seguridad y brindar mayor flexibilidad. En adelante, cuando se hable de certificados digitales, se hará referencia a la norma UIT-T X.509 en su tercera versión.

1.1.6.1. Formato de un Certificado Digital

Como se muestra en la Figura I-V, un certificado digital real almacena información adicional como fecha de expedición y expiración, nombre de la autoridad Certificadora que emitió el certificado y su firma, número de serie; en ocasiones, se encuentra información sobre los propósitos para los que fue creado.

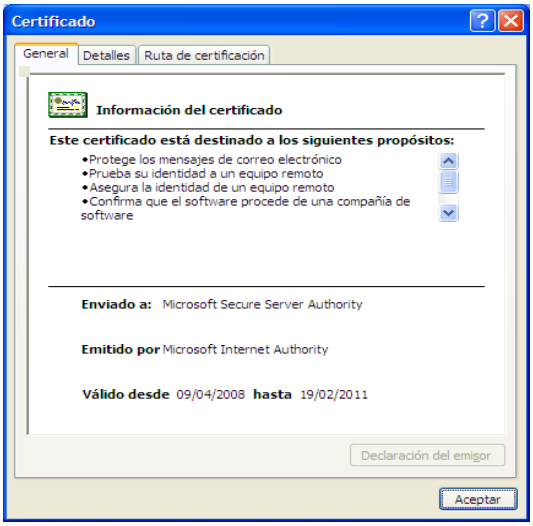


FIGURA I-V. Certificado Digital Real

El formato de un certificado digital está definido en la norma UIT-T X.509; si se cumple con el formato, un certificado puede leerse y escribirse por cualquier aplicación que obedece el estándar.

1.1.6.2. Campos Predeterminados

En la Figura I-VI se muestra la información que se encuentra registrada en un certificado que cumple con el estándar X.509. Dentro del formato se definen nueve campos; a continuación se presenta una descripción de cada campo.

- Versión: Indica la versión de la norma X.509 bajo la cual se creó el certificado; en este campo se puede tener registrada la primera, segunda o tercera versión del estándar.
- Número de Serie: Una autoridad certificadora AC marca un número en cada certificado que emite; este número es un identificador único que permite identificar al certificado de acuerdo a los registros de la autoridad certificadora AC.

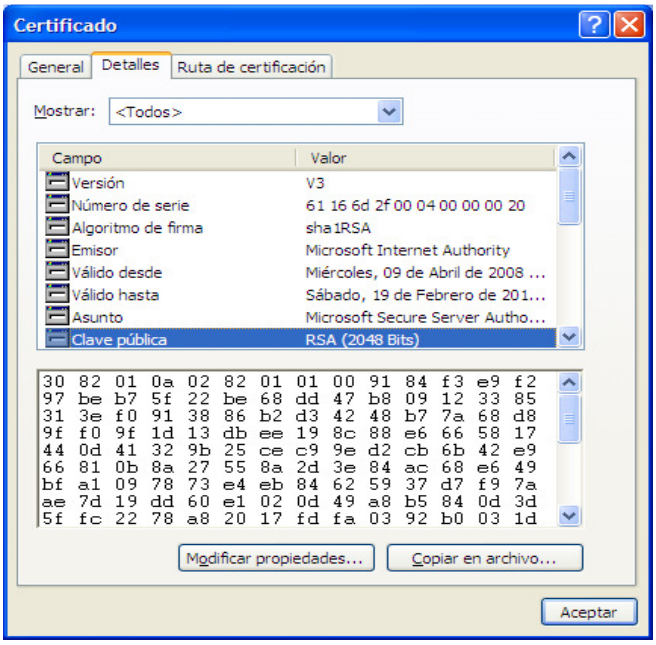


FIGURA I-VI. Información registrada en un Certificado Digital Real

- Firma: Indica el tipo de función *hash* y el algoritmo de encripción con que se firmó el certificado.
- Expedidor: Indica el nombre de la AC que expidió y firmó el certificado.

- Período de Validez: Define las fechas de expedición y expiración del certificado; la AC define el tiempo de duración del certificado de acuerdo a los propósitos para el que fue expedido.
- Propietario: Nombre del usuario o entidad propietaria de la clave pública que se adjunta al certificado.
- Información de la Clave Pública del Propietario: Contiene la clave pública del titular del certificado e información del algoritmo de encripción con que se puede utilizar dicha clave.
- Identificador del Expedidor: Este campo permite identificar a la autoridad certificadora de forma única.
- Extensiones: Este campo permite agregar información adicional manteniendo el formato del estándar.

CAPÍTULO II. INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

En este capítulo se muestra todos los aspectos relacionados a la infraestructura de clave pública, incluyendo los elementos de la Pki como son la autoridad de registro, directorios, entidad destino, entidad confiante, directivas, los tipos de arquitectura, servicios, ciclo de vida de claves, administración. Además se presenta la infraestructura de clave pública del Banco Central del Ecuador, elementos, autoridad de registro, autoridad certificadora, directorio, directivas, alcance y limitaciones, ventajas de la firma digital, aplicaciones.

2.1. Infraestructura de claves públicas

La criptografía asimétrica proporciona herramientas apropiadas para la implementación de servicios de seguridad, como es el caso de: autenticación, confidencialidad, integridad y aceptación.

Sin embargo, requiere de una infraestructura que brinde un sistema adecuado de administración de certificados digitales y parejas de claves: PKI.

PKI es una infraestructura compuesta por hardware, software, políticas, procedimientos, servicios, convenios y personas; estos elementos permiten gestionar la creación, distribución, administración, suspensión, reactivación y revocación de claves y certificados digitales. Con esto se logran niveles razonables de confianza a través de los servicios de autenticación, integridad, confidencialidad y aceptación.

2.1.1.1. Elementos de la Infraestructura de Clave Pública

Aunque la complejidad de una arquitectura PKI depende de los servicios a los que estará destinada, en general cuenta con elementos que le permiten mantener un nivel razonable de confianza.

2.1.1.1.1 Autoridad de registro

La Autoridad de Registro es la entidad encargada de garantizar el servicio de identificación dentro de la infraestructura de clave pública, siendo la responsable de la interacción entre los usuarios de certificados y la autoridad certificadora; acepta solicitudes de creación de certificados, valida los datos y finalmente envía la información necesaria a la autoridad certificadora. Cuando la autoridad certificadora emite un certificado se lo entrega a la Autoridad de Registro para que ésta lo entregue al usuario o lo deposite en un directorio.

Es tal vez el elemento más importante dentro de una infraestructura de clave pública, pues el nivel de confianza atribuido a ésta es proporcional a la cantidad y calidad de las pruebas solicitadas para establecer las identidades, y por supuesto la seguridad con que se custodia la información recolectada.

2.1.1.1.2 Autoridad certificadora y certificados digitales

La autoridad certificadora es el tercero de confianza que emite los certificados digitales de manera segura, para esto requiere de la implementación de un servidor de certificados; además, la autoridad certificadora tiene la obligación de administrar los certificados, lo que implica la expedición, suspensión, reactivación y revocación de éstos.

a. Emisión de certificados

Después de que la autoridad de registro ha realizado las verificaciones pertinentes, la autoridad certificadora se encarga de la emisión de certificados digitales; de acuerdo al propósito para el que fue diseñada la infraestructura de clave pública y el papel que efectúa la autoridad certificadora, ésta puede expedir diferentes tipos de certificados.

a.1. Tipos de certificados

Esta clasificación se basa en la clase de propietario de un certificado y las atribuciones que éste tiene con respecto a la emisión y uso de su certificado digital.

a.1.1. Certificados de entidad destino

Este tipo de certificado es expedido para un usuario final; éste usa su certificado como credencial para validar el vínculo entre su clave pública y su nombre de usuario o su nombre distinguido. Este tipo de certificado no permite que su propietario firme otros certificados digitales.

a.1.2. Certificados de autoridad certificadora

Un certificado de Autoridad Certificadora permite a su titular firmar certificados digitales de otros usuarios e incluso de otras autoridades certificadoras.

b. Suspensión, reactivación y revocación

Cuando una autoridad certificadora emite un certificado digital, adquiere la responsabilidad de suspender o revocar dicho certificado. La suspensión de un

certificado se presenta cuando el propietario del certificado notifica a la autoridad certificadora que no hará uso de éste durante un período, para evitar que durante su ausencia se haga uso del certificado la autoridad certificadora debe inhabilitarlo.

Cuando el usuario requiera hacer uso de su certificado nuevamente, la autoridad certificadora reactivará el certificado; sin embargo, es recomendable que en estos casos se emita un nuevo certificado para garantizar que todos los usuarios confíen en el certificado del usuario.

La revocación de un certificado es definitiva; es decir, cuando una autoridad certificadora revoca un certificado, éste queda inhabilitado hasta que se termine su período de validez. Una revocación se puede presentar por las siguientes razones:

- Compromiso de la Clave Privada relacionada con el propietario del certificado.
- Compromiso de la Clave Privada relacionada con el certificado de la autoridad certificadora que emitió el certificado.
- Se ha modificado el contenido del certificado.
- El certificado ha sido actualizado por otro.
- El usuario deja de pertenecer al sistema que requiere del uso de un certificado para la autenticación; esto se puede dar por cambio de funciones o desvinculación entre la empresa y el usuario.

Debido a que los certificados digitales son utilizados como credenciales para autenticar a su propietario ante un sistema u otros usuarios, la autoridad certificadora debe notificar a todas las entidades confiantes cuando un certificado es suspendido o revocado.

En general, la notificación de una revocación o suspensión se hace de manera indirecta, por medio de la publicación de listas de revocación de certificados o CRLs (Certificate Revocation List).

2.1.1.1.3 Directorios

Dentro de una PKI los directorios son la base para el sistema de distribución de certificados y listas de revocación. Dentro de algunas implementaciones los certificados

son distribuidos a los usuarios personalmente; en la mayor parte de casos, se los distribuye por medio de directorios.

Un directorio es una base de datos que permite encontrar información descriptiva basada en atributos; en general no soportan transacciones complejas. Las búsquedas de información soportan filtrado y sus actualizaciones son simples.

Un directorio tiene almacenada la información en una especie de árbol con varios niveles, éstos forman un esquema jerárquico en donde cada uno se representa por acrónimos; de esta manera una búsqueda se realiza de manera más eficiente.

La recomendación UIT-T X.509 especifica que para el uso de certificados digitales empleados para la autenticación, se debe manejar directorios que cumplan la norma UIT-T X.500 (Directory Access Protocolo-DAP), debido a que esta norma se adapta a la sintaxis de los certificados digitales.

Un directorio X.500 para certificados X.509 puede crearse sin usar técnicas de clave simétrica o de claves pública/privada; pero como X.509v3 se basa en certificados de clave pública, en general se manejan directorios para este tipo de certificados.

En la actualidad se ha difundido el uso de LDAP (Lightweight DAP). LDAP permite almacenar y recuperar certificados digitales, consumiendo menos recursos que X.500 y resulta menos complejo.

2.1.1.1.4 Entidad destino

La entidad destino está representada por el propietario del certificado, éste puede ser una persona, un equipo o cualquier entidad que requiera autenticarse ante un sistema o usuario utilizando certificados digitales. La entidad destino solicita su certificado a una autoridad de registro AR, cuando ésta ha identificado a la entidad, entrega la solicitud a la autoridad certificadora AC para que ésta cree el certificado digital.

El propietario del certificado es el responsable de proteger su clave privada. Para lograr que la implementación de infraestructura de clave pública PKI sea transparente para el

usuario, se puede recurrir al uso de tokens o tarjetas inteligentes para el almacenamiento de certificados y claves.

2.1.1.1.5 Entidad confiante

En general, es cualquier entidad que utiliza un certificado digital perteneciente a otra entidad; es decir, ésta valida un certificado para verificar una identidad. Cuando el certificado queda validado, la entidad confiante asume la autenticidad de la credencial electrónica.

La entidad confiante puede ser un cliente que realiza una compra a través de un servidor o el mismo servidor al validar las credenciales del cliente; también se pueden realizar validaciones entre clientes como en el caso de los correos electrónicos.

2.1.1.1.6 Directivas

Las directivas son las reglas que rigen una infraestructura de clave pública y deben estar disponibles para todos los usuarios de la infraestructura de clave pública y restringidas para todos los demás, pues contienen información del funcionamiento de la infraestructura de clave pública y esto puede revelar sus vulnerabilidades. Las directivas están compuestas por la política de certificación y una declaración de prácticas de certificación.

a. Política de certificación

Una política de certificación o CP (Certificate Policy) define reglas para el manejo de la información, procesos y principales usos de las herramientas de criptografía pública dentro de una organización. Por ejemplo, se define cómo se manejan las claves y certificados; además contiene información para el funcionamiento de la infraestructura de clave pública PKI.

El documento que contiene la política de certificación de una organización debe estar disponible para todos los usuarios del sistema, para que éstos tengan conocimiento de temas como:

Elementos y aplicabilidad de la infraestructura de clave pública.

- Obligaciones de cada elemento de la infraestructura de clave pública PKI y responsabilidades legales.
- Usos permitidos y prohibidos de los certificados.
- Entidades que pueden solicitar y validar un certificado digital.
- Tipos de certificado de acuerdo a los requisitos necesarios para la identificación del propietario.
- Relaciones de confianza con otras organizaciones.
- Legislación vigente.
- Directorios.
- Nivel de confidencialidad de los datos presentados por los usuarios al solicitar un certificado.
- Registro e identificación.
- Motivos para la revocación.
- Suspensión, reactivación y renovación de certificados.
- Y de ser necesario tarifas.

b. Declaración de prácticas de certificación

También conocida como CPS2, define cómo se va a implementar y dar soporte a las políticas de certificaciones. Contiene toda la información de los procedimientos necesarios para la expedición, suspensión, reactivación y revocación de certificados, así como también la forma en que se van a realizar los diferentes procesos dentro de la infraestructura de clave pública PKI.

Especifica en detalle los procedimientos para el registro de entidades destino; la forma en que se va a generar, almacenar y distribuir las parejas de claves y certificados. Dentro de las especificaciones se incluyen detalles específicos como:

La política de certificación con la que se asocia la declaración de prácticas de certificación .

- Información de todos los procesos por los que pueden pasar los certificados.

- Periodo de validez del certificado de la autoridad de certificación.
- Circunstancias bajo las cuales la autoridad certificadora puede revocar un certificado.
- Políticas de manejo de las listas de certificados revocados CRLs, intervalos de publicación y puntos de distribución.
- Algoritmos criptográficos utilizados por la autoridad certificadora.

2.1.2. Tipos de arquitectura

Las arquitecturas de infraestructura de clave pública pueden ser implementadas de diversas maneras, de acuerdo al número de autoridad certificadora y las relaciones existentes entre éstas. Entre los principales tipos de arquitectura se pueden mencionar a las arquitecturas planas, jerárquicas.

2.1.2.1. Arquitectura plana

Ésta es la forma más básica de arquitectura de infraestructura de clave pública, en esta arquitectura existe sólo una autoridad certificadora, la misma que está encargada de generar y distribuir los certificados y las listas de certificados revocados CRLs a las entidades destino. Este tipo de arquitectura no permite que otras autoridades certificadoras ingresen a la infraestructura de clave pública, por lo que la única autoridad certificadora existente no establece relaciones de confianza con otras autoridades certificadoras.

Todas las entidades confían en la autoridad certificadora y usan sólo los certificados expedidos por ésta, las entidades se comunican entre sí manteniendo como punto de confianza a la autoridad certificadora, como se muestra en la Figura II-I.

La arquitectura plana es la más fácil de implementar debido a que implica la creación y control de una autoridad certificadora; pero como consecuencia presenta un punto único de falla, si la clave privada de la autoridad certificadora se ve comprometida, todos los certificados emitidos deben ser revocados.

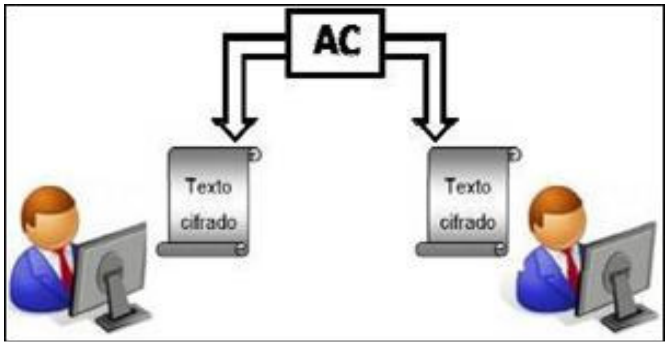


FIGURA II-I. Arquitectura Plana

Este tipo de arquitectura mantiene problemas de escalabilidad; sin embargo, es apropiada para pequeñas organizaciones con un número limitado de usuarios. A medida que el tamaño de la organización se incrementa, la arquitectura plana introduce problemas de funcionamiento para la infraestructura de clave pública.

2.1.2.2. Arquitectura jerárquica

La arquitectura jerárquica basa su funcionamiento en el establecimiento de entidades raíces y entidades subordinadas; sin embargo, cada autoridad certificadora dentro de la jerarquía debe cumplir funciones semejantes a las de una autoridad certificadora de arquitectura plana.

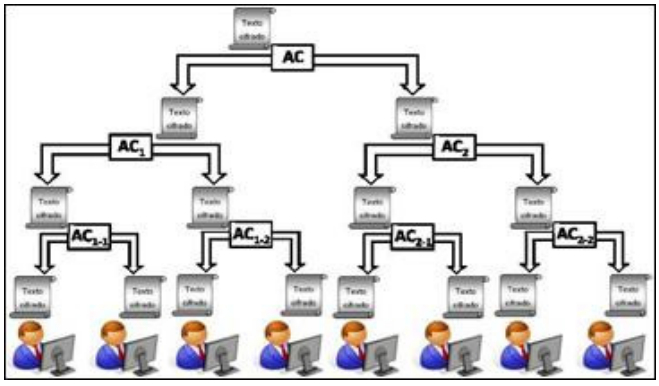


FIGURA II-II. Arquitectura Jerárquica

Dentro de este tipo de arquitectura, todas las autoridades certificadoras miembros de la infraestructura de clave pública mantienen relaciones de confianza conectadas por

enlaces superior subordinada, formando una estructura de árbol invertido como se muestra en la Figura II-II.

La estructura de árbol invertido mostrada en la Figura II-II indica que la autoridad certificadora raíz emitió los certificados del segundo nivel de autoridades certificadoras subordinadas, las misma que a su vez emitieron los certificados de un tercer nivel; las autoridades certificadoras del tercer nivel solo emiten certificados de entidad destino.

Las autoridades certificadoras subordinadas están supeditadas a las directivas impuestas por las autoridades certificadoras de jerarquía superior, esto facilita el manejo de directivas, debido a que cuando una autoridades, certificadoras de jerarquía superior emite un certificado para una subordinada, establece sus alcances y limitaciones de acuerdo a su política de certificación.

La autoridad certificadora raíz por lo general emite certificados para otras autoridades certificadoras y no para entidades destino; en cambio, las autoridades certificadoras subordinadas, pueden emitir certificados de otras autoridades certificadoras o de entidad destino de acuerdo a la estructura de la infraestructura de clave pública PKI.

Este tipo de arquitectura introduce mejores condiciones de escalabilidad, debido a que se puede asignar una autoridad certificadora subordinada por locación geográfica y a su vez ésta puede mantener autoridades certificadoras subordinadas.

2.1.3. Servicios de una Infraestructura de Claves Públicas

El objetivo de una infraestructura de clave pública es proveer confianza; para cumplir con este objetivo, la infraestructura de clave pública debe brindar múltiples servicios a sus usuarios, y siendo la criptografía de clave publica su pilar fundamental, los servicios básicos que brinda están relacionados con los siguientes puntos:

- Aplicación de firmas digitales para la identificación del emisor de mensajes o documentos electrónicos.
- Cifrado y descifrado de mensajes o documentos electrónicos.
- Trasmisión de claves simétricas para establecer comunicaciones seguras.
- Verificación de la integridad de mensajes o documentos electrónicos.

Para garantizar que todos los servicios tengan un nivel razonable de confianza, una Infraestructura se debe fundamentar en una generación de certificados digitales confiables.

2.1.3.1. Emisión de certificados confiables

Uno de los servicios que brinda la infraestructura de clave pública es obviamente la emisión de certificados digitales; generar un certificado seguro implica llevar a cabo las Siguientes etapas.

- Identificación del usuario que solicita el certificado: Es una de las responsabilidades de la autoridad de registro AR, contiene las siguientes etapas:
  - Recepción de solicitud: El usuario presenta una solicitud a la autoridad de registro, la cual debe estar acompañada por un formulario en donde se registran sus datos personales; de ser necesario el usuario debe presentar pruebas de los datos registrados en el formulario.
  - Verificación de datos: En está etapa se confirman los datos registrados en el Formulario presentado por el usuario
  - Evaluación: De acuerdo con los resultados obtenidos durante la verificación de los datos, se define la viabilidad de emitir o no el certificado.
- Verificación del contenido del certificado: De acuerdo al tipo de certificado y las funciones que éste va ha cumplir, la autoridad certificadora define qué tipo de información va ha contener y la estructura final del certificado; respetando el estándar establecido.
- Generación del certificado: Esta etapa contiene las siguientes sub etapas:
  - Generación de la pareja de claves publica/privada: Esta etapa puede ser ejecutada por el usuario o por la autoridad certificadora; sin embargo, es recomendable que el proceso de generación del certificado resulte transparente para el usuario. Por lo tanto, cuando se trate de usuarios ajenos al campo de la criptografía es conveniente que la autoridad certificadora se encargue de la generación de claves.

- Emisión del certificado y entrega a su propietario: La clave pública y el nombre del usuario son vinculados a un certificado digital; posteriormente, se publica en un directorio o se entrega personalmente a su propietario.

- Administrar certificados y claves: Esta etapa contiene todas las etapas concernientes al ciclo de vida de las claves y certificados.

Cada una de estas etapas debe cumplirse manteniendo de manera estricta la políticas de certificación y la declaración de políticas de certificación; además, se debe capacitar a los usuarios para que estén consientes del nivel de seguridad requerido en las etapas que requieran de su intervención.

2.1.3.2. Ciclos de vida de claves y certificados

El propósito de una infraestructura de claves públicas es el establecimiento de credenciales digitales confiables. Para lograr su propósito la infraestructura de clave pública asegura que la clave pública asociada con una clave privada pertenece al usuario registrado en un certificado; si la clave pública pertenece a otro usuario, no se cumple el propósito de infraestructura de clave pública. Por este motivo es fundamental establecer procedimientos adecuados para los procesos de administración de claves y certificados.

2.1.3.3. Administración de claves

La administración de claves contempla todos los aspectos relacionados con el ciclo de vida de las parejas de claves pública/privada dentro de infraestructura de clave pública; esto implica, las claves de las autoridades certificadoras y de todas las entidades destino

2.1.3.3.1 Selección del tipo clave

Para definir un tipo de clave se debe determinar primero la aplicación en la que ésta se va ha utilizar, de acuerdo a la aplicación seleccionada y el nivel de seguridad requerido por el sistema, se deben definir algoritmos, longitudes de claves y distribución, etc.

Se puede generar dos tipos de claves, las claves que están destinadas para cifrar y las claves que están para firmar digitalmente un mensaje o documento electrónico; por supuesto, existen claves que cumplirán los dos objetivos.

Las claves destinadas a cifrar son expedidas para brindar el servicio de encripción en dos tipos de ambientes: para el intercambio de claves y para cifrar documentos; en el primer caso las claves son utilizadas para el intercambio de claves simétricas con el fin de lograr comunicaciones seguras.

Cuando se utiliza las claves para cifrar mensajes o documentos, puede ser necesaria la implementación de un almacén de claves, esto permitirá que en caso de pérdida de la clave privada, la información pueda ser descifrada y recuperada.

Por otra parte, una clave expedida con el fin de firmar documentos digitales debe mantener la característica de singularidad, esta es la única forma en que se garantiza la autenticación y aceptación por medio de firmas digitales; por este motivo, una clave que se utiliza para firmar y cifrar mensajes no puede incluirse en un almacén de claves.

Las políticas relacionadas con los posibles usos de las claves deben contemplar todos los aspectos mencionados anteriormente; además, es primordial que los usuarios del sistema sean debidamente capacitados.

2.1.3.3.2 Generación y entrega de claves

Dentro de la generación de claves uno de los aspectos más importantes dentro de una infraestructura de clave pública es la definición del algoritmo que se va ha utilizar para cifrar y firmar mensajes digitalmente; este determinará las longitudes de claves posibles, nivel de confiablidad de las claves creadas, interoperabilidad, procesamiento requerido, etc.

Después de seleccionar el algoritmo, se debe establecer la longitud de las claves, ésta determina directamente el nivel de seguridad y por otra parte la cantidad de procesamiento que se va ha realizar para las validaciones de certificados y firmas digitales; es importante realizar una estimación adecuada, considerando el valor real de los datos que se piensa proteger y su tiempo de vida útil.

Después de la selección del algoritmo y la longitud de claves, la generación de claves se puede realizar de manera centralizada o distribuida. En un sistema centralizado, es la Autoridad certificadora la encargada de la generación de claves; esto resulta más amigable para el usuario y permite el almacenamiento de claves para cifrado.

Cuando se trata de sistemas que utilizan firmas digitales, es necesaria la implantación de un sistema distribuido en el que los usuarios generan sus propias claves sin la necesidad de intercambiarlas a través de una red, con el fin de crear las condiciones óptimas para garantizar los servicios de autenticación y aceptación.

2.1.3.3.3 Protección de claves

Las claves públicas deben estar disponibles para que todos los usuarios del sistema puedan validar las credenciales de otros usuarios cuando lo requieran, es recomendable que entidades ajenas al sistema no tengan acceso a éstas.

Por otra parte, el acceso a las claves privadas debe estar protegido por un sistema que establezca una auto-autenticación por parte del propietario de la clave; este sistema puede estar basado en contraseñas, biometría, tarjetas inteligentes o tokens, de acuerdo al nivel de seguridad requerido.

2.1.3.3.4 Almacenamiento de claves

El almacenamiento de las claves privadas va ha depender de la entidad propietaria de éstas; por ejemplo, las claves pertenecientes a autoridades certificadoras de la infraestructura de clave pública deberán guardarse en zonas de acceso restringido, las claves destinadas para firmas digitales deberán mantener la singularidad y las claves utilizadas para cifrar podrán copiarse con el fin de mantener un respaldo que permita la recuperación de datos.

Para mantener la singularidad de las claves utilizadas para firmas digitales, se puede utilizar dispositivos de almacenamiento como tarjetas inteligentes o tokens; estos dispositivos permiten generar y almacenar las claves privadas.

Cuando se requiera del establecimiento de almacenas de claves, éstos deben ubicarse en zonas restringidas y la información almacenada debe cifrarse.

2.1.3.3.5 Recuperación de claves

No todas las claves las claves son susceptibles de recuperación, como se ha dicho anteriormente. Cuando una clave privada se utiliza par firmas digitales, solo su propietario tiene acceso a éstas; por lo tanto si llega perderse, debe generarse una nueva pareja de claves.

En el caso de las claves de cifrado, se puede requerir la recuperación de la clave actual o de claves anteriores a ésta; las claves antiguas, sólo se puede utilizar para la verificación de firmas y para descifrar documentos, para esto se debe mantener un historial de las claves de cada usuario.

2.1.3.4. Administración de certificados

En el caso de la infraestructura de clave pública, la administración de certificados digitales es fundamental para establecer credibilidad, esto implica todos los procedimientos relacionados con el ciclo de vida de un certificado; por lo tanto, es necesario que todas la prácticas dentro de la infraestructura de clave publica sean consistentes para lograr que el registro, renovación y revocación de certificados mantengan razonables de confianza.

2.1.3.4.1 Registro de Certificados

Después que la Autoridad de Registro ha efectuado las verificaciones de identidad pertinentes y la Autoridad Certificadora ha sido notificada, los datos del usuario se registran en la infraestructura de clave pública, luego de lo cual el usuario podrá acceder a su certificado. Este certificado puede ser entregado al usuario personalmente o por medio de un directorio en el cual el usuario debe ingresar una contraseña o un secreto compartido entregado previamente por la Autoridad de Registro.

Para certificados que se van a utilizar para firmas digitales, los usuarios son los encargados de la generación de la pareja de claves; el usuario entrega su clave pública a

la Autoridad de Registro para que la Autoridad Certificadora la vincule al certificado. En estos casos, la descarga del certificado requiere que el usuario firme digitalmente la solicitud de registro como prueba de posesión de la clave privada, luego de los cual se permite descargar su certificado.

De acuerdo a la aplicación para la que estén destinados los certificados, al finalizar el proceso de registro, la Autoridad Certificadora ubica el nuevo certificado en un directorio público, par que los otros usuarios puedan acceder a este y validar diferentes transacciones.

2.1.3.4.2 Renovación de certificados

La renovación de un certificado digital conlleva un proceso de actualización de los datos del usuario, esto implica menor complejidad que el proceso de registro, debido a que la Autoridad de Registro y la Autoridad Certificadora ya tienen un registro del usuario, y por lo tanto la identidad ya ha sido verificada.

El proceso de renovación de certificados se realiza cuando las claves han expirado o cuando la clave privada se vio comprometida; también se pueden presentar en casos de cambios importantes de los datos del propietario del certificado.

2.1.3.4.3 Revocación de certificados

Debido a que los certificados digitales son utilizados como credenciales para autenticar a su propietario con un sistema u otros usuarios, es una tarea importante llevar un proceso de revocación y notificación de certificados comprometidos de manera eficiente.

La autoridad certificadora debe notificar a todas las entidades confiantes cuando un certificado es suspendido o revocado. En general esta notificación se hace de manera indirecta, por medio de la publicación de listas de revocación de certificados o CRLs(Certificate Revocation List).

a. Lista de revocación de certificados Crls

Una lista de revocación de certificados contiene información sobre certificados que han dejado de ser válidos, ya sea por suspensión o revocación; cuando un certificado es suspendido o revocado expira, se puede retirar de la lista.

2.1.4. Infraestructura de Clave Pública del Banco Central Del Ecuador

El objetivo de la Entidad de Certificación de Información, es establecer identidades digitales confiables entre sus participantes, es decir, el Banco Central del Ecuador actúa como el tercero confiable entre los usuarios en el proceso que usa para emitir la Firma Digital.

La principal función de la entidad de certificación es la emisión de certificados de Firma Digital para personas naturales, jurídicas o funcionarios públicos.

Mantiene una arquitectura plana; es decir, la autoridad certificadora de la infraestructura de clave pública del Banco Central del Ecuador solo puede emitir certificados de entidad destino.

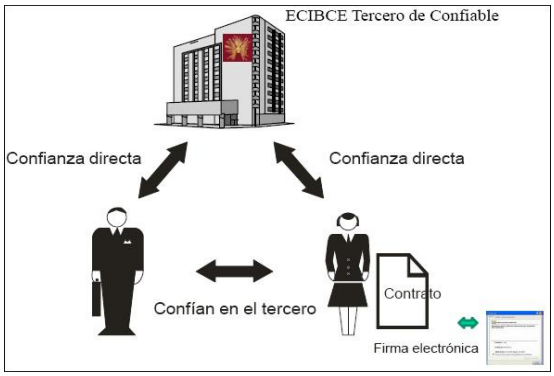


FIGURA II-III. Entidad Certificadora del B.C.E.

2.1.5. Usuario

Se entiende por usuario del certificado a la persona natural, jurídica, funcionario o servidor público que voluntariamente confía y hace uso de los Certificados de la ECIBCE.

2.1.6. Tipos de Certificados

2.1.6.1. Certificado de Firma digital de Persona Natural

Sirve para todo propósito, permite identificar a una persona natural, dentro del giro de sus negocios, y será responsable a título personal todo lo que firme, en forma electrónica, dentro del ámbito de su actividad y límites de su uso que correspondan.

2.1.6.2. Certificado de Firma digital de Persona Jurídica

Sirve para todo propósito, permite identificar a una persona jurídica de derecho privado, a través de su representante legal o de las personas que están perteneciendo a la empresa, quienes serán responsables en tal calidad de todo lo que firmen dentro del ámbito de su actividad y límites de uso que correspondan.

2.1.6.3. Certificado de Firma digital de Funcionario Público

Sirve para todo propósito, permite identificar a un funcionario o servidor público, quien será responsable a título de la institución pública que representa de todo lo que firme dentro del ámbito de su actividad y límites uso que correspondan.

2.1.7. Elementos de la PKI del Banco Central del Ecuador

Al igual que cualquier infraestructura de claves públicas, la infraestructura de clave pública del BCE está conformada por: autoridad certificadora, directorio, autoridad de registro, directivas.

2.1.7.1.1 Autoridad registro

La Autoridad de Registro está conformada por los Administradores de la Infraestructura de Clave Pública (cuatro administradores), los cuales tienen la obligación de realizar las comprobaciones necesarias para verificar si la información entregada por los usuarios es verdadera.

2.1.7.1.2 Autoridad certificadora

La autoridad certificadora de la infraestructura de clave pública del BCE es una Autoridad Certificadora raíz que puede expedir únicamente certificados de entidad destino.

2.1.7.1.3 Directorio

El directorio de la infraestructura de clave pública del BCE está conformado por un servidor Netware 5.1, el mismo que utiliza el protocolo LDAP para su funcionamiento. Netware es un sistema operativo diseñado por Novell, para brindar servicios de red, soportando características de seguridad para la autenticación y acceso a directorios LDAP.

Para el registro en el directorio, se ingresa cada identidad dentro de una jerarquía, con sus respectivos permisos. Para el manejo de los certificados digitales almacenado. Novell usa su NDS (Novell directory Services), el cual asocia a un certificado con su clave privada.

2.1.7.1.4 Directivas

La infraestructura de clave pública del BCE ha establecido políticas y procedimientos de seguridad que sirven de guía para que las entidades que interactúan con ésta mantengan un nivel adecuado de seguridad.

2.1.7.2. Alcance y Limitaciones de la Pki del BCE

- Infraestructura técnica. La infraestructura de clave pública del Banco Central del Ecuador cuenta con una infraestructura técnica que utiliza productos de seguridad Entrust.

  Los productos utilizados por la infraestructura de clave pública del Banco Central del Ecuador logran una autenticación segura.

  El servidor GetAccess proporciona control de acceso, mientras el servidor TruePass almacena datos de todos los accesos de los usuarios al sistema, registrando fecha, hora, nombre de usuario, dirección IP y verificación del certificado.

Para el acceso a los servidores, se cuenta con un sistema de autenticación híbrida que combina el uso de contraseñas con biometría; el acceso al centro de cómputo está permitido solo para el personal de seguridad informática del BCE. Además, los servidores se conectan a la red privada a través de un Firewall.

Como parte de la protección del sistema, se sacan copias incrementales de seguridad del estado de los servidores una vez al mes; una copia total es almacenada una vez al año, manteniendo cifrada la información almacenada.

- Arquitectura. La Pki del BCE mantiene una arquitectura plana; es decir, La autoridad certificadora raíz de la Pki del BCE, puede emitir certificados digitales destinados para usuarios finales.
- Plataforma. La Pki del BCE utiliza como plataforma el sistema operativo Solaris de Sun Microsystems, para los servidores TruePass, GetAccess, Self Administration y Roaming; Windows es utilizado para el servidor de certificados.
- Registro de usuarios. La autoridad de registro de la Pki del BCE se encuentra representada por los administradores de la Pki, el registro se lleva a cabo a partir de la solicitud de un usuario que ha llenado previamente el formulario DI-SI-0255, la información es validada por el administrador de la Pki.
- Nivel de confiabilidad. La Pki del BCE está destinada a brindar servicios de certificación a personas naturales, jurídicas y funcionarios públicos. La Pki del BCE goza de un nivel elevado de confiabilidad.

2.1.7.3. Gestión de las claves

2.1.7.3.1 Certificados de usuario final

En general, la ECIBCE seguirá una serie de estándares o normas a la hora de generar el par de claves, como prestador de servicios de certificación. Estas normas o estándares son los siguientes:

- El tamaño de las claves será como mínimo de 1024 bits.
- El algoritmo utilizado para la generación de las claves es el RSA.
- La generación de la función resumen (HASH) se realiza utilizando el algoritmo SHA1 de 160 bits.

- El período de validez de las claves va a ser, como máximo, de dos años desde que se emite o renueva el Certificado, o el máximo establecido por la legislación vigente.

2.1.7.3.2 Certificado raíz de la Autoridad Certificadora

Las claves de la AC se han mantenido depositadas custodiadas en un sistema seguro. El acceso a esas claves sólo se permite a personas debidamente autorizadas por la ECIBCE.

En su caso, si en algún momento se viera en la necesidad de la eliminación de las claves, el procedimiento que se seguirá será el de sobre escritura.

- El tamaño de las claves es de 2048 bits.
- El algoritmo utilizado para la generación de las claves es el RSA.
- La generación de la función resumen (HASH) se realiza utilizando el algoritmo SHA1 de 160 bits.
- El período de validez de las claves es como máximo, de veinte años

2.1.7.4. Ventajas de la firma digital

- Garantía de identidad del firmante y del documento firmado en la red,
- Validar la identidad del otro extremo de la comunicación
- Evita falsificaciones
- Brinda garantía de seguridad en el envió y acceso de datos de carácter confidencial
- Privacidad de información crítica
- Evita colas para tramites personales que requieren la presencia de un individuo, y desplazamiento
- Evita suplantación de identidad
- Transacciones seguras de forma remota
- Validez jurídica sin requerir la presencia física de los firmantes

2.1.7.5. Aplicaciones

Con la firma digital se pueden desarrollar proyectos como los siguientes:

- Trámites de gobierno (Gobierno Electrónico)
- Compras públicas
- Gestión Documental (Cero Papeles)
- Dinero Electrónico
- Balances Electrónicos
- Trámites judiciales y notariales
- Comercio Electrónico
- Facturación Electrónica
- Contratos Electrónicos
- Servicios Web

CAPÍTULO III. COMPARACIÓN DEL TOKEN PLATAFORMAS

En este capítulo se presenta la comparación, similitudes y diferencias que existen en las plataformas Windows XP y Linux Ubuntu 8.0.4 con respecto al funcionamiento del dispositivo Token para firma digital, el mismo que es proporcionado por la Entidad Raíz del Banco Central del Ecuador. Entre los parámetros a comparar se encuentra la portabilidad dentro de este están los navegares web, funciones criptográficas, Apis criptográficas, posteriormente se encuentra el parámetro de usabilidad dentro del cual esta los precios, desempeño criptográfico y finalmente el parámetro de Rendimiento dentro de este está la seguridad, flexibilidad para lo cual se realiza un análisis de cada una de sus características posteriormente se obtiene un resultado final.

3.1. Comparación de firmas digitales entre Windows y Linux

Se realizó la configuración para el funcionamiento del dispositivo Token para firma digital en las plataformas Windows XP y Ubuntu 8.0.4 que se encuentra en el Anexo A, los mismos que han permitido obtener las siguientes tablas con sus respectivos niveles de funcionalidad.

La técnica empleada para establecer el estudio comparativo entre las plataformas Windows y Linux con respecto al funcionamiento del dispositivo Token para firma digital es la denominada Técnica de Evaluación Heurística desarrollada por Jakob Nielsen.

Los parámetros que se considerado para este estudio comparativo son:

Portabilidad: Propiedad de un software para ser utilizadas en distintas computadoras.

- Navegadores Web
- Funciones Criptográficas
- APIs Criptográficos

Usabilidad: Medida en la que un producto se puede usar por determinados usuarios para conseguir unos objetivos específicos.

- Precios
- Desempeño Criptográfico

Rendimiento: Permite determinar resultados en tiempos de ejecución de un sistema.

- Seguridad
- Flexibilidad

La escala asignada para la evaluación esta referenciada bajo los distintos niveles que se muestran a continuación.

RANGO	PORCENTAJE	NIVEL
0 - 2	0% - 40%	Bajo
2.1 - 4	40.1% - 80%	Medio
4.1 - 5	80.1% - 100%	Alto

Tabla III-I. Niveles de evaluación

Fuente: Técnica de Evaluación Heurística

Los parámetros a evaluar están divididos de la siguiente manera: se ha considerado que la plataforma que cumpla con todas las variables o parámetros definidos anteriormente se les asignara los valores de 4.1-5 el cual indicará un nivel alto de funcionalidad, de igual forma un rango de 2.1-4 mostrará que la plataforma posee un nivel medio de funcionalidad y finalmente un rango de 0-2 evidenciará que la plataforma no cumple en su totalidad con los requerimientos básicos necesarios.

Los parámetros para definir la portabilidad de las plataformas son:

- **Navegadores Web**

  a. Internet Explorer
  b. FireFox
  c. Opera

Tecnologías	Parámetro Navegadores Web	Rango	Porcentaje
Windows	a,b	3,75	75%
Linux	b,c	3,75	75%

Tabla III-II. Parámetros navegador Web

- **Funciones Criptográficas**

  a. Generación de pares de llaves asimétrica (RSA)

b. Generación de llave simétrica (DES, 3DES, RC2)
c. Administración y almacenamiento de código interno
d. Firma digital interna

Tecnologías	Funciones Criptográficas	Rango	Porcentaje
Windows	a,b,c,d	5	100%
Linux	a,b,c,d	5	100%

Tabla III-III. Parámetros de Funciones Criptográficas

- **APIs Criptográficos:**

a. PKCS #11
b. Fips 140-1 Nivel 1 (certificado No. 161)

Tecnologías	APIs Criptográficos	Rango	Porcentaje
Windows	a,b	5	100%
Linux	a,b	5	100%

Tabla III-IV. Parámetros de APIs Criptográficas

Parámetros para definir la Usabilidad:

- **Precios:**

a. Alto
b. Medio
c. Bajo
d. Ninguno

Tecnologías	Precios	Rango	Porcentaje
Windows	Medio	2,5	50%
Linux	Medio	2,5	50%

Tabla III-V. Parámetros Precios

- **Desempeño Criptográfico**

a. 1021-bit y 2048-bit RSA
b. Generación de código en menos de 90 segundos
c. Firma digital en menos de un segundo

Tecnologías	Desempeño Criptográfico	Rango	Porcentaje
Windows	a,b,c	5	100%
Linux	a,b,c	5	100%

Tabla III-VI. Parámetros de Desempeño Criptográfico

Parámetros para definir el Rendimiento:

- **Seguridad**

a. Certificado Digital
b. Firma digital.

Tecnologías	Parámetro Seguridad	Rango	Porcentaje
Windows	a, b	5	100%
Linux	a, b	5	100%

Tabla III-VII. Parámetros Seguridad

- **Flexibilidad**

a. Alta

b. Media
c. Baja

Tecnologías	Parámetro Flexibilidad	Rango	Porcentaje
Windows	Alta	5	100%
Linux	Alta	5	100%

Tabla III-VIII. Parámetros flexibilidad

3.1.1. Similitudes y Diferencias

3.1.1.1. Precios

Tanto para la plataforma Windows, como para Linux el costo del dispositivo token usb de firma digital es el mismo, un costo de 79$. Adquiriendo el dispositivo de Firma digital se lo puede emplear en cualquiera de las dos plataformas. Esto implica que el costo del dispositivo se encuentra en un nivel medio, lo cual permite que cualquier usuario tenga la posibilidad de adquirir este dispositivo, por lo que su costo no es muy elevado.

3.1.1.2. Instalación

La instalación del dispositivo token usb de firma digital en la plataforma Windows XP posee un entorno gráfico, lo cual su interfaz resulta más amigable para el usuario y hace que sea más rápida su instalación, mientras que en la plataforma Linux Ubuntu 8.0.4 su entorno es a través de comandos por lo que su instalación es más lenta.

3.1.1.3. Seguridad

En lo que a seguridad se refiere, tanto en la plataforma Windows XP como en la plataforma Linux Ubuntu 8.0.4, el dispositivo token de firma digital si es seguro, por el certificado digital y firma digital que posee este dispositivo.

RESULTADOS DEL FUNCIONAMIENTO TOKEN

PORTABILIDAD				
Parámetros	**WINDOWS**		**LINUX**	
	Rango	**%**	**Rango**	**%**
Navegador Web	3,75	75%	3,75	75%
Funciones Criptográficas	5	100	5	100
APIs Criptográficos	5	100	4	80
Total	13,75	275	13,75	260
Promedio	**4,58**	**91,66**	**4,58**	**91,66**

Tabla III-IX. Resultados generales de portabilidad

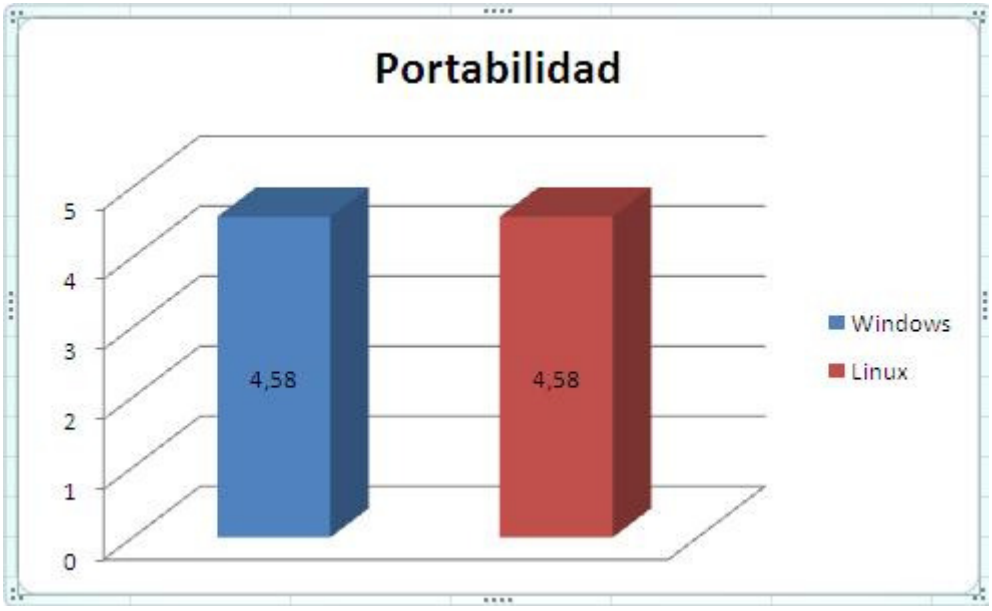


FIGURA III-I. Resultados portabilidad

Como resultado de la evaluación en portabilidad se puede apreciar en la Figura III-I, que la plataforma Windows XP con respecto al funcionamiento del dispositivo token de firma digital, su puntaje es de 4,58 que representa al 91,66%, dentro del rango de valores establecidos anteriormente, Mientras que en la plataforma Linux Ubuntu 8.0.4 se ha obtenido el mismo puntaje que la plataforma Windows XP, lo que significa que no existe diferencia alguna en portabilidad para el dispositivo token de firma digital.

USABILIDAD				
Parámetro	**WINDOWS**		**LINUX**	
	Rango	**%**	**Rango**	**%**
Precios	2,5	50	2,5	50
Desempeño Criptográfico	5	100	5	100
Total	7,5	150	7,5	150
Promedio	**3,75**	**75**	**3,75**	**75**

Tabla III-X. Resultados generales de usabilidad

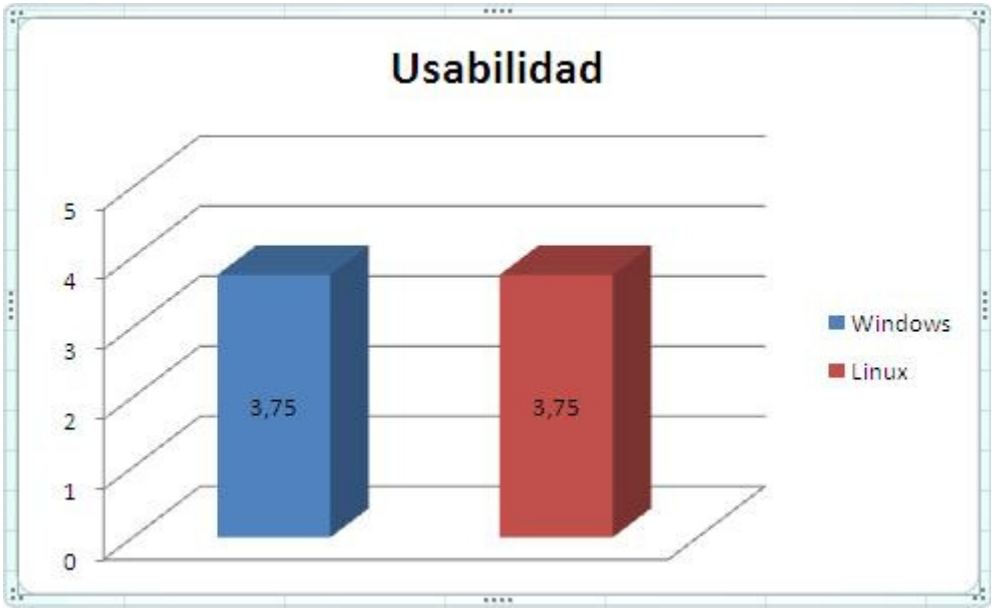


FIGURA III-II. Usabilidad

En la Figura III-II se muestra que el funcionamiento del dispositivo token de firma digital, tiene igual usabilidad con un valor de 3,75 correspondiente al 75% en las dos plataformas Windows XP y Linux Ubuntu 8.0.4, debido a que su desempeño de las características que brinda el dispositivo de firma digital es el mismo para ambas plataformas.

RENDIMIENTO				
Parámetros	**WINDOWS**		**LINUX**	
	Rango	**%**	**Rango**	**%**
Seguridad	5	100	5	100
Flexibilidad	5	100	5	100
Total	10	200	10	200
Parcial	**5**	**100,00**	**5**	**100,00**

Tabla III-XI. Resultados generales de rendimiento

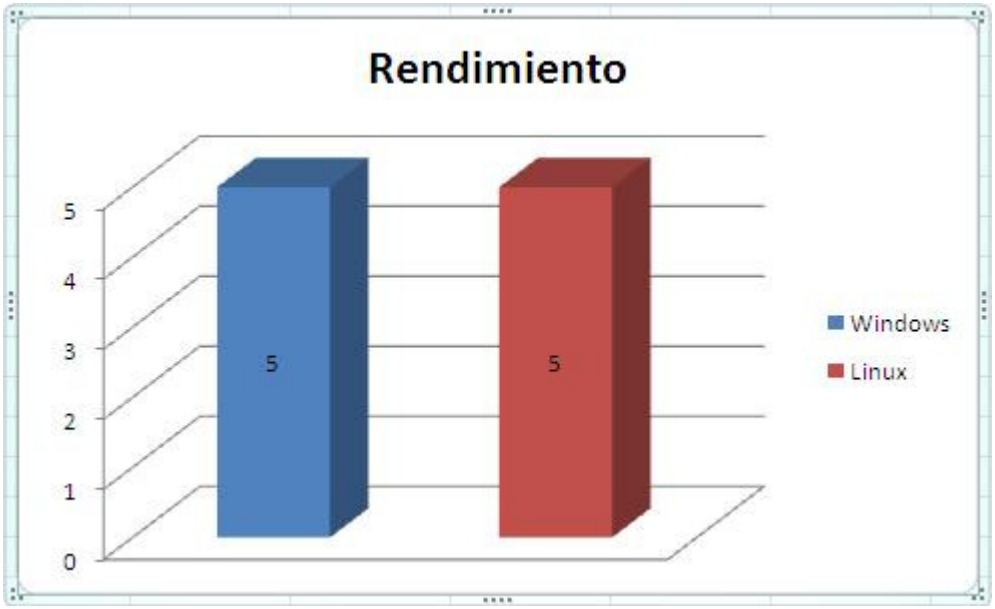


FIGURA III-III. Rendimiento

Como se puede observar en la Figura III-III, la plataforma Windows XP con respecto al funcionamiento del dispositivo token de firma digital, toma un valor de 5 que corresponde al 100%, mientras que la plataforma Linux Ubuntu 8.0.4 tiene el mismo puntaje, lo que significa que se encuentra en optimas condiciones este dispositivo.

RESULATADO GENERAL

Porcentaje General				
Parámetros	**WINDOWS**		**LINUX**	
	Rango	**%**	**Rango**	**%**
Portabilidad	4,58		4,58	
Usabilidad	3,75		3,75	
Rendimiento	5		5	
Total	13,33		13,33	
Parcial	**4,44**	**88,88**	**4,44**	**88,88**

Tabla III-XII. Resultados generales de las plataformas

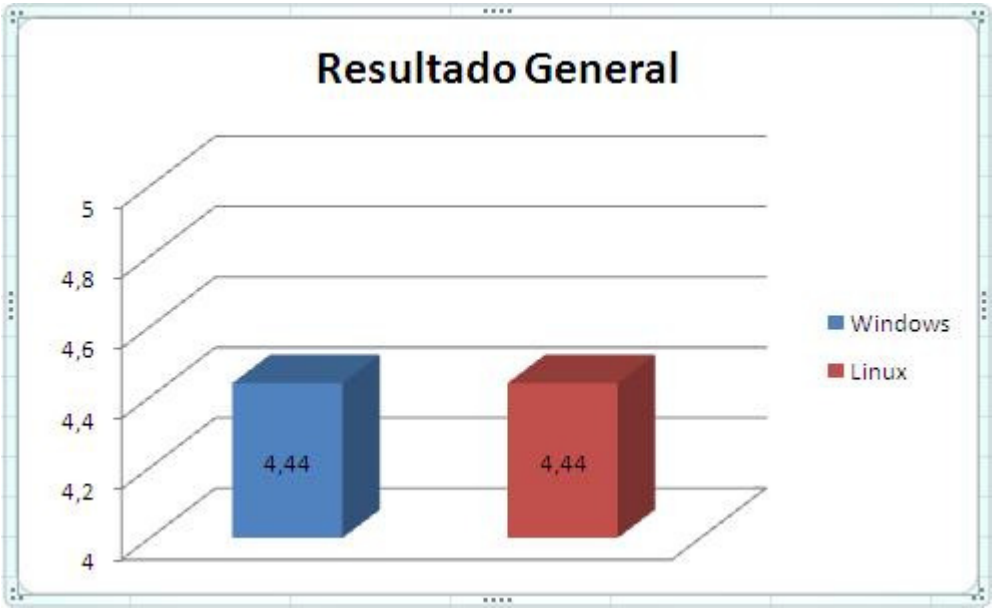


FIGURA III-IV. Resultado General

Tanto en la plataforma Windows XP como en Linux Ubuntu 8.0.4 se puede trabajar de igual forma sin ningún inconveniente con el dispositivo token usb de firma digital. Una de las ventajas de la plataforma Windows Xp es que su interfaz es grafica, la instalación del dispositivo token usb resulta más rápida, lo que permite que sea más manejable para los usuarios y optimizar el tiempo en esta plataforma, mientras que los usuarios que no se encuentran familiarizados con entornos de comandos es decir con la plataforma Linux se hará un poco difícil para los usuarios.

CAPÍTULO IV. DESARROLLO DEL PROTOTIPO

En este capítulo se presenta la historia, objetivos, misión, visión, organigrama del Hospital de Brigada N° 11 “Galápagos”, el análisis de la infraestructura de la situación actual de la institución, que incluye descripción, inventario hardware, inventario software, diagnostico de la red, además los requerimientos de la institución hardware y software, así como también el diseño en donde se presenta los pasos para obtener el dispositivo token para firma digital y finalmente la implementación del dispositivo token de la firma digital en la plataforma Windows XP para el Hospital de Brigada N° 11 “Galápagos”.

4.1. Ingeniería de la Información

4.1.1. Definición del ámbito

El Hospital de Brigada N° 11 "Galápagos" es una entidad de servicio público, sus documentos como oficios, memorándum, telegramas, son firmados de forma manual, por lo que deberían tener mayor seguridad para el envió de estos documentos ya que son confidenciales para la institución.

Todos estos elementos hacen que se requiera de herramientas tecnológicas que le permitan cumplir con sus objetivos. La iniciativa informática está encaminada a proveer de mejores sistemas de seguridad que permitan el envío de documentos confidenciales seguros.

Por lo que se ha visto la necesidad de realizar un prototipo de firmas digitales para el Hospital de Brigada N° 11 "Galápagos" y de esta manera poder enviar los documentos firmados digitalmente y pueda existir mayor seguridad en los datos.

4.1.2. Breve Historia

En 1966, cuando la Plaza de Riobamba militarmente constituía un centro de depósito de municiones se adecuó una instalación de sanidad, nivel Enfermería, en 1974, se produce una reorganización de las Unidades Militares de la Plaza de Riobamba y es así; que se crea las Unidades Militares ubicadas en el Campamento de la Hacienda de "San Nicolás" donde permanece hasta la actualidad; esta organización más compleja aumentó el número de personal y medios, obligando así mismo la ampliación de la unidad de sanidad militar, pasando de ser Enfermería a Policlínico, con consulta médica y odontológica.

En 1976, se asigna para el funcionamiento del policlínico la casona en la que hasta la actualidad permanece, viendo la necesidad de cubrir emergencias quirúrgicas, partos y otros procedimientos menores se aumenta los servicios técnicos creando un quirófano en la segunda planta a la derecha y se contrata los servicios de más personal civil paramédico.

En 1999 se inicia la construcción del nuevo hospital en el sector paralelo al coliseo de deportes que ha ido creciendo de a poco financiado con recursos internos de la Brigada. Actualmente se encuentra construido y en funcionamiento el nuevo hospital de Brigada N° 11 “Galápagos”.

4.1.3. Objetivos

- Modernizar la gestión Hospitalaria implantando una nueva estructura organizacional que privilegie el establecimiento y desarrollo de los procesos de calidad.

- Implementar sistema de Información e informática en redes como soporte a todos los procesos, con énfasis en los procesos médicos.

4.1.4. Misión y Visión

4.1.4.1. Misión

Ser un Hospital que brinde atención de salud reconocida por su calidad, con un talento humano dispuesto a una permanente superación, trabajando con infraestructura física y tecnológica renovadas, acorde a las necesidades y demandas de nuestros clientes dentro de un buen ambiente de trabajo.

4.1.4.2. Visión

Proporcionar servicios de sanidad en apoyo a las operaciones militares de la 11BCB Galápagos y brindar un servicio integral de salud, con calidad y calidez al personal militar, así como a las personas que lo requieran dentro de nuestra área de influencia.

Organigrama de Hospital de Brigada N° 11 “Galápagos”

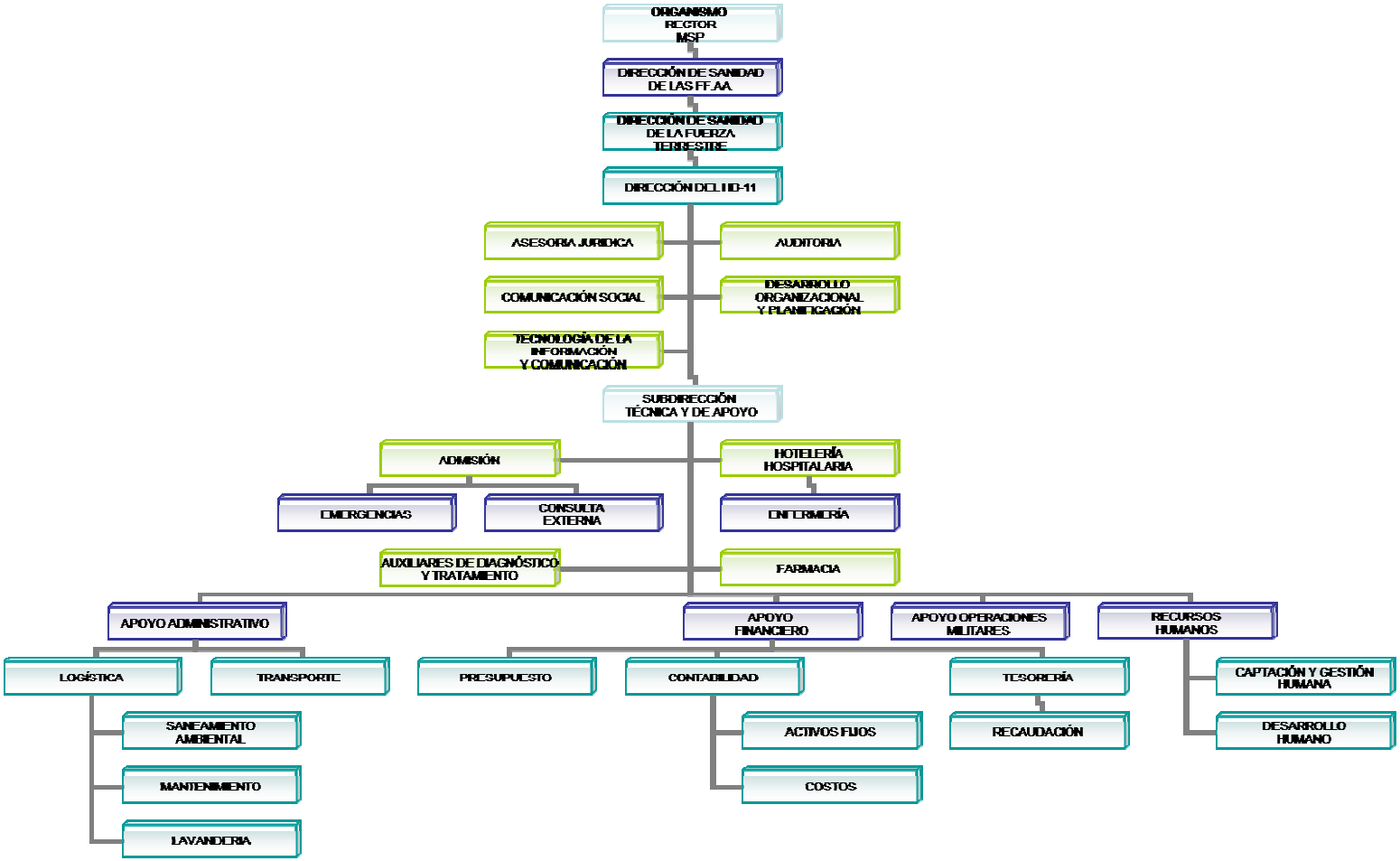


FIGURA IV-I. Organigrama Hospital de Brigada N° 11 “Galápagos”

4.2. Análisis

4.2.1. Funcionamiento de documentos

Actualmente en el Hospital de Brigada N° 11 "Galápagos", los documentos tales como memorándum, oficios, telegramas son firmados de forma manual, los mismos que son enviados a través de un mensajero de la institución, para que lleguen a sus diferentes destinos, como se muestra en la Figura IV-II.

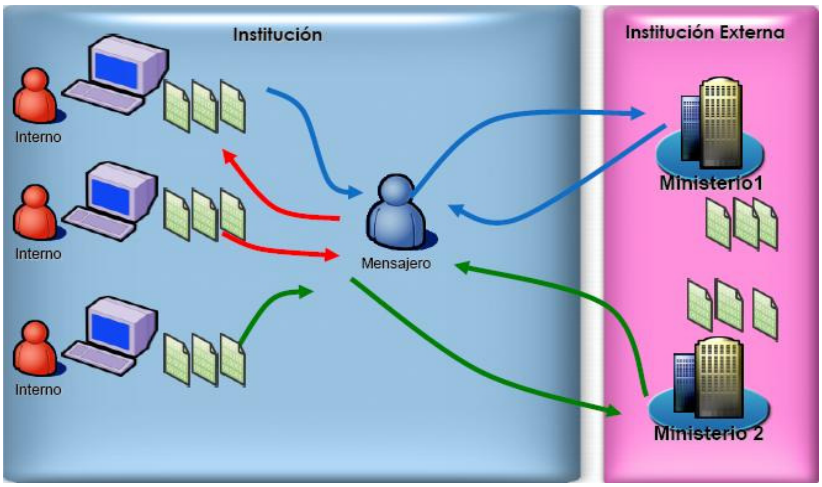


FIGURA IV-II. Situación Actual

4.2.1.1. Desventajas

- Perdida de documentación
- Tiempos de entrega altos
- Dependencia total del mensajero
- Mantener archivos físicos en cada área
- Utilización de papel

4.2.2. Análisis de Documentación

Los documentos que se deben enviar por correo electrónico son aquellos documentos que son confidenciales para la institución como lo son:

- Memorándum
- Oficios
- Telegramas

4.2.3. Usuarios

Los usuarios que deben utilizar el dispositivo token son aquellos que envían documentos confidenciales en el Hospital de Brigada N° 11 "Galápagos" los cuales son el Director, Sub Director, Financiero, Personal, Operaciones, Logística, ya que ellos envían información a las diferentes entidades como son al Ministerio de Defensa, Fuerza Área (comandancia, Brigadas, Hospitales), Ministerio de Finanzas, ISSFA.

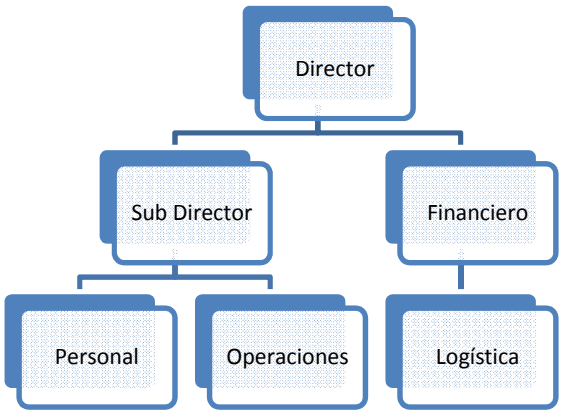


FIGURA IV-III. Usuarios que utilizan el token usb

4.2.4. Funcionamiento del Dispositivo Token

El usuario que va ha utilizar el dispositivo token de firma digital, debe primero instalar los drivers del dispositivo, posterior a ello debe conectar el token al puerto usb del computador, luego procederá ha firmar un documento digital.

Para firmar digitalmente no es necesario disponer de internet, mientras que para la verificación de la firma digital si se debe disponer de internet. Se deberá revisar los correos enviados diariamente.

El dispositivo token es personal, es decir cada persona debe poseer su token, el cual es responsable de todo el manejo que se le de a este dispositivo.

4.2.5. Flujo de Información

La manera como se enviara los documentos firmados digitalmente en el Hospital de Brigada N° 11 "Galápagos" es de la siguiente forma:

El personal de está institución, enviara sus documentos firmados digitalmente a través de correo electrónico a las diferentes instituciones ya se estos el Hospitales militares, comandancia, etc.

Posterior a ello, la institución que ha recibido el documento firmado, debe verificar a través de la página del Banco Central del Ecuador, en donde debe ingresar su nombre y correo electrónico de la persona que envió el correo electrónico.

Luego se visualiza los datos y el certificado digital con su clave pública, lo cual permite verificar si es la persona quien dice ser el que envió el documento como se muestra en la Figura IV-IV.

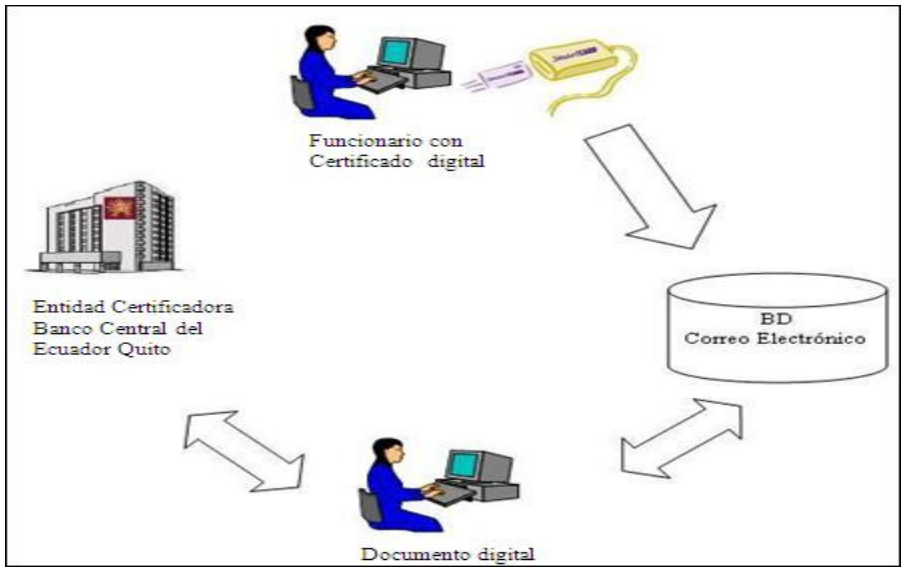


FIGURA IV-IV. Flujo de Información

4.2.5.1. Ventajas

- Acceso Web
- Interconectados con las entidades del estado
- Firma digital (inviolabilidad de la información)
- Tiempo de entrega y recepción inmediata
- Cero papeles
- Ahorro de espacio físico, costos operativos, costos de recursos
- Agilita la gestión de documentos en el sector público

4.2.6. Presupuesto

El costo del dispositivo token para firma digital es de $79, como en el Hospital de Brigada N° 11 "Galápagos", son seis las personas que van a utilizar este dispositivo, esto implica que la institución tiene que emplear un valor de $ 474.

4.2.7. Planificación Temporal

Se ha utilizado una herramienta de administración de proyectos flexible y eficaz, que permite controlar los proyectos, ayudando a mantener informados a quienes participan en ellos, permite controlar proyectos mediante la programación y el seguimiento de las actividades para supervisar su progreso. Este paquete es Microsoft Project.

(Ver Anexo B)

4.2.8. Propuesta

Según los resultados obtenidos anteriormente, la propuesta es realizar la implementación del prototipo de firmas digitales en la plataforma Windows XP, para el Hospital de Brigada N° 11 "Galápagos", debido a su fácil manejo y configuración del dispositivo en este Sistema Operativo.

4.2.9. Infraestructura Situación Actual

4.2.9.1. Descripción

- Actualmente la red tiene una topología en estrella.
- La dirección IP es clase A desde 10.1.1.1
- La red se encuentra estructurada con cable Par Trenzado UTP categoría 6
- Cuentan con Dos Servidores tipo BLADE marca HP con las siguientes características

    - Servidor de Base de Datos
    - Servidor de Aplicaciones

- Los servidores poseen el Sistema Operativo Linux Centos 5.4 de 32 bits
- El Protocolo que maneja es TCP/IP
- En cada uno de los segmentos tiene computadores de escritorio con Sistema Operativo Windows XP
- El Hospital de Brigada N° 11 "Galápagos" posee 45 computadoras de escritorio Tipo Clon, 6 computadoras portátiles de las cuales son 4 HP y 2 Toshiba. También cuentan con 16 impresoras matriciales Marca Epson, 8 impresoras Laser marca Samsung, 2 copiadoras/impresoras marca Xerox y Minolta.
- Para el acceso a Internet tiene contratado una cuenta corporativa banda ancha con la CNT de 1024 Kbps.

4.2.9.2. Inventario Hardware

En la tabla IV-I se muestra el inventario hardware con el que cuenta el Hospital de Brigada N° 11 "Galápagos".

Servidores	Marca	Ram	Disco Duro	Sistema Operativo	Funciones
Servidor 1	HP	512	120 GIGAS SCSI	CENTOS	Servidor de Base de Datos
Servidor 2	HP	512	120 GIGAS	CENTOS	Servidor de Aplicación
Áreas Administrativas /Medicas	CLON	256 Mb-4Gb	80Gb-320 Gb	Win XP-Win Vista	Administrativas / Medicas

Tabla IV-I. Inventario Hardware

4.2.9.3. Inventario Software

En la tabla IV .II se muestra el inventario software con el que cuenta la institución en sus diferentes departamentos.

Área de Farmacia	
Software	**Licencia**
SMARTSYS	Si
Área de Recaudación	
Software	**Licencia**
FACHOSMI	Si
ISSFA	Si
Área de Financiero	
Software	**Licencia**
SISCOP	Si
Área de Estadística	
Software	**Licencia**
HB11-CTT-SALUD	Si
Área de Emergencia	

Software	Licencia
HB11-CTT-SALUD	Si
Área de Personal	
Software	**Licencia**
HB11-CTT-SALUD	Si

Tabla IV-II. Inventario Software

4.2.9.4. Diagnostico de la Red

4.2.9.4.1 Usuarios de la red

Para una mejor atención y servicio a los usuarios del Hospital de Brigada N° 11 "Galápagos" la red se ha dividido en áreas de trabajo, esta distribución se detalla de la siguiente manera:

Consultorios de consulta externa, Consultorio de odontología, Banda Ergonométrica, Personal, Operaciones, Logística, Sistemas, Dirección, Subdirección Ayudantía, Financiero, Activos Fijos, Estadística, Información, Recaudación, Laboratorios, Rayos X, Emergencia, Hospitalización, Habitaciones de Hospitalización, Farmacia, Quirófanos, Bodegas, Rehabilitación, Jurídico.

4.2.9.4.2 Hardware de la red

Elementos Activos

En la Tabla IV-III se muestra el inventario hardware de la red con sus respectivos elementos activos.

EQUIPOS NETWORK			
Equipo	**N° de Equipos**	**Marca**	**Características**
Switch	1	3COM	48 Puertos 10/100/1000
Switch	2	CNET	48 Puertos 10/1001000
Modem	1	D-Link	4 Puertos

Tabla IV-III. Inventario Hardware de la red Elementos Activos

Elementos Pasivos

En la Tabla IV-IV se muestra el inventario hardware de la red con sus respectivos elementos pasivos.

EQUIPOS NETWORK			
Componentes	**N° de Componentes**	**Marca**	**Características**
Rack	1	Beacount	
Cable UTP Pachcord	110		Categoría 6

Tabla IV-IV. Inventario Hardware de la red Elementos Pasivos

Todas sus estaciones de trabajo utilizan sistema operativo de Microsoft Windows XP Y Windows vista, por lo que su personal está muy familiarizado con la forma en que trabajan estos sistemas.

Se presenta en el ANEXO C un diagrama de la red actual del Hospital de Brigada N° 11 "Galápagos".

4.2.10. Requerimientos

El Hospital de Brigada Nº 11 "Galápagos" ha considerado necesario firmar sus documentos digitalmente para que los mimos sean enviados de forma segura.

La institución se ha visto en la necesidad de adquirir dispositivos tokens para firmas digitales emitido por la entidad certificadora del Banco Central del Ecuador, y trabajar en la plataforma Windows XP, ya que todo su personal se encuentra familiarizado con la misma, debido a su entorno grafico lo que hace que sea fácil y amigable para los usuarios de está institución.

Las firmas digitales con la utilización del dispositivo token permite que se lo pueda utilizar para tramites externos, debido a que tiene validez legal, también se ha

considerado que para tramites internos, se crea la necesidad de tener una infraestructura de firmas digitales ver Anexo D.

4.2.11. Requerimientos Hardware en la plataforma Windows XP

En la tabla IV-V se muestra los requerimientos Hardware para el funcionamiento del dispositivo token.

Requerimientos Hardware	
Procesador	Core Duo
Memoria Ram	512 MB

Tabla IV-V. Requerimientos Hardware

4.2.12. Requerimiento Software en la plataforma Windows

En la tabla IV-VI se muestra los requerimientos software para el funcionamiento del dispositivo token para firma digital.

Requerimientos Software	
Sistema Operativo	Windows XP
Microsoft Office	Microsoft Word
Navegador	Internet Explorer 6 o superior

Tabla IV-VI. Requerimientos Software

4.3. Diseño

En la tabla IV-VII se muestra los pasos para obtener el token usb en la Entidad Certificadora que es el Banco Central del Ecuador.

Actor	Actividades
1. Solicitante	Obtiene el portal WEB de la Entidad de certificación de Información del Banco Central del Ecuador, el formulario de solicitud ECIBC-0267/0268/0269 y los requisitos para obtener el certificado digital de usuario final. Llena y entrega la solicitud adjuntando la documentación requerida a la Entidad de Certificación de Información del Banco Central del Ecuador.
2. Entidad de Certificación de Información	Verifica la información del solicitante, revisa la documentación requerida y se reserva el derecho de solicitar documentación adicional que certifique la identidad del solicitante La ECIBC acepta o niega la solicitud. En caso de negación presentará su resolución por escrito (correo electrónico de preferencia) al solicitante indicando las razones de su negación. Comunica al solicitante vía telefónica o correo electrónico la fecha y hora para la emisión del certificado digital, que será emitida en forma presencial.
3. Usuario	El solicita junto con el personal autorizado por la Entidad se Registro del Banco Central del Ecuador realiza la emisión del certificado digital en un dispositivo portable seguro token. Suscribe el contrato de prestación de Servicios respectivo.

Tabla IV-VII. Pasos para obtener el dispositivo Token de firma digital

4.3.1. Solicitud de los servicios de Certificación

4.3.1.1. Emisión de Certificados

Cuando una persona desea solicitar la emisión de un certificado de firma electrónica. El solicitante llena la solicitud correspondiente al tipo de certificado requerido, disponible en el portal Web de la ECIBCE y debe subir la documentación en formato electrónico de acuerdo al tipo de certificado.

La información suministrada se somete a un proceso minucioso de verificación para comprobar fehacientemente la identidad de la persona que está solicitando la emisión del certificado. La ECIBCE tiene la potestad de aprobar o no la emisión. Aprobada la emisión, el solicitante debe efectuar el pago de la tarifa respectiva.

Una vez realizado el pago, el solicitante será notificado para que acuda a la ECIBCE en fecha y hora para proceder a la identificación y emisión del certificado solicitado.

El solicitante/suscriptor debe presentarse ante la Autoridad de Registro de la ECIBCE con una cédula de ciudadanía válida y suficientemente clara y actualizada para permitir su inequívoca identificación y los originales del resto de la documentación solicitada; después debe suscribir el contrato de prestación de servicios y se le entrega el certificado emitido, para que proceda a ingresar su clave de seguridad.

Los certificados emitidos por la ECIBCE tienen un plazo de vigencia establecido en el propio certificado y siempre será acorde con la legislación vigente.

EMISIÓN DE CERTIFICADO DIGITAL
1. Creación del usuario para emitir el certificado ▪ Primer Nombre: Pilar ▪ Segundo Nombre: Gaibor ▪ Email:
2. Información del certificado

▪ Nombre: ▪ Apellido Paterno: ▪ Apellido Materno: ▪ Cedula de Identidad: ▪ Dirección: ▪ Teléfono: ▪ Ciudad ▪ Inicializar el dispositivo: ▪ Cambio de clave ▪ solicita la clave: Para proceder a firmar con el dispositivo. ▪ Realiza la prueba de Cifrado y firma

Tabla IV-VIII. Emisión de certificado digital

Posteriormente se obtiene personalmente el dispositivo token de firma digital en el Banco Central del Ecuador el cual permite firmar un documento digital.

4.3.2. Revocación y suspensión de Certificados

4.3.2.1. Revocación de certificado

Los Certificados son revocados cuando ocurre alguna de las circunstancias siguientes:

- Solicitud voluntaria del Suscriptor.
- Solicitud voluntaria del Solicitante.
- Pérdida o inutilización por daños del soporte del certificado.
- Fallecimiento del suscriptor, incapacidad sobrevenida, total o parcial, de cualquiera de ellos, terminación de la representación o extinción de la persona jurídica representada.
- Cese en su actividad del suscriptor.
- Cese en su actividad del prestador de servicios de certificación salvo que los certificados expedidos por aquel sean transferidos a otro prestador de servicios.
- Inexactitudes graves en los datos aportados por el suscriptor para la obtención del certificado, así como la concurrencia de circunstancias que provoquen que

dichos datos, originalmente incluidos en el certificado, no se adecuen a la realidad.

- Que se detecte que las claves privadas del suscriptor o de la autoridad certificadora han sido comprometidas, bien porque concurran las causas de pérdida, robo, hurto, modificación, divulgación o revelación de las claves privadas, bien por cualquier otra circunstancia, incluidas las fortuitas, que indiquen el uso de las claves privadas por persona distinta al titular.
- Por la resolución del contrato

4.3.2.1.1 Efectos de revocación

El efecto de la revocación del certificado es la pérdida de fiabilidad del mismo, originando el cese permanente de la operatividad del certificado conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación.

La revocación del certificado tendrá como consecuencia la notificación a terceros de que un certificado ha sido revocado, cuando se solicite la verificación del mismo.

4.3.2.2. Suspensión de certificados

El certificado es suspendido cuando existan indicios sobre la existencia de una causa de revocación. En la actualidad no se está proporcionando el servicio de suspensión debido a condicionantes técnicos.

4.3.2.2.1 Efectos y límites de la Suspensión

El efecto de la suspensión de los certificados es la pérdida de fiabilidad de los mismos, originando el cese temporal de la operatividad del certificado conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación. La suspensión de un certificado impide el uso legítimo del mismo por parte del suscriptor.

La suspensión del certificado terminará por cualquiera de las siguientes causas:

- Por decisión de la autoridad certificadora de revocar el certificado.

- Por decisión de la autoridad certificadora de levantar la suspensión del certificado, una vez considerada la improcedencia de la revocación.
- Por la finalización anticipada del procedimiento de revocación.

4.3.3. Procedimiento de suspensión y revocación

Se debe solicitar la suspensión/revocación en cuanto se tenga conocimiento de la concurrencia de alguna de las circunstancias contempladas en el apartado anterior:

- El suscriptor del certificado
- La autoridad de registro, respecto a aquellos certificados en cuya emisión hayan participado.
- La persona jurídica que conste en el certificado.

Asimismo, puede solicitar la suspensión/revocación cualquier tercero con un interés legítimo en caso de que tenga conocimiento de la existencia alguna de las siguientes causas:

- Pérdida del soporte del certificado.
- Fallecimiento del signatario.
- Incapacidad sobrevenida, total o parcial.
- Inexactitudes en el certificado.
- Compromiso de la fiabilidad del certificado.
- Compromiso de las claves.
- Cese del representante en el caso de los certificados con poderes.
- Extinción de la persona jurídica representada.

4.3.3.1. Recepción de solicitudes de suspensión y revocación

La solicitud de suspensión/revocación de certificados se puede dirigir a la autoridad certificadora en la forma de comunicación escrita o digital, o presentándose físicamente ante la ECIBCE aquel Solicitante/Suscriptor que solicite la suspensión/revocación

deberá solicitarla mediante el formulario respectivo de revocación disponible en la página del portal Web de la ECIBCE.

Cuando la persona que solicite la suspensión/revocación del certificado no sea el propio suscriptor, deberá ser solicitada por el Representante Legal, en caso de Persona Jurídica o Funcionario Público, y en caso de Persona Natural podrá gestionar de manera presencial una persona de confianza para validar el proceso.

4.3.3.2. Decisión de suspender y revocar

Una vez recibida y autenticada la solicitud de revocación, la ECIBCE procede a tramitar la suspensión/revocación efectiva del certificado. La decisión de suspender/revocar un certificado corresponde a la autoridad certificadora.

4.3.4. Caducidad de Certificados

Los Certificados caducarán por el transcurso del período operacional del mismo. La caducidad producirá automáticamente la invalidez del certificado, originando el cese permanente de su operatividad conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación.

La caducidad de un certificado impide el uso legítimo del mismo por parte del suscriptor.

4.3.5. Renovación de los servicios de Certificación.

4.3.5.1. Renovación de Certificados

Este procedimiento se establece para los casos en que el certificado vaya a caducar y el suscriptor simplemente desee utilizar un certificado con las mismas características que tenía el que venía utilizando válidamente hasta entonces.

En este caso, se le generarán nuevas claves; pero, únicamente se van a llevar a cabo unas medidas mínimas de comprobación, puesto que el antiguo certificado tiene plena vigencia y nada hace pensar, salvo que el suscriptor lo exprese, que alguno de sus datos ha cambiado o que ya no es posible confiar en el certificado.

4.3.6. Características de los Certificados y de la lista de Certificados

4.3.6.1. Características de los Certificados

- Los certificados emitidos por la ECIBE son almacenados en un dispositivo criptográfico (token), manteniendo niveles y estándares de seguridad. Los dispositivos son entregados de manera personal al suscriptor por parte de la autoridad certificadora o autoridad de registro de la ECIBCE.
- Los certificados de usuario final tiene una vigencia de 2 años, mientras que la vigencia del certificado raíz es de veinte años

4.3.6.2. Lista de Certificados

Los certificados una vez emitidos se publican en una base de datos o repositorio disponible públicamente. Esta operación es realizada por personal autorizado a partir de los archivos generados por la ECIBCE.

El Listado de Certificados esta a disposición de los usuarios en la página web de la ECIBCE. El Listado de Certificados suspendidos o revocados (CRL) esta a disposición de los usuarios en la página: http://www.eci.bce.ec/crl/eci_bce_ec_crlfile.crl

Los Certificados suspendidos y revocados aparecen como tales en la CRL durante un período mínimo de tres años, a partir del cual se eliminará los datos del Certificado definitivamente de la CRL y serán depositados en las oficinas de la AC durante un periodo de doce años.

4.3.6.3. Lista de Certificados Revocados (LCR)

El Banco Central del Ecuador, a través de la Entidad de Certificación de Información, es responsable de indicar en los certificados que emita, la dirección en Internet de su página en donde se localiza la Lista de Certificados Revocados y el Protocolo de Estatus de Certificados en Línea (OCSP), URL: http://ocsp.eci.bce.ec, para que de esta manera sea fácilmente accesible por los usuarios.

La ECIBCE mantiene publicada la Lista de Certificados Revocados con una periodicidad de cada 6 horas por 14 horas al día, es decir se hará pública la CRL 3 veces al día para que los usuarios puedan acceder a la verificación. Hay que recalcar que la

ECIBCE mantiene en línea la verificación del estado de un certificado mediante un repositorio LDAP, es decir, una vez revocado un certificado, inmediatamente al proceder a firmar un documento o mensaje de datos, le mostrará un mensaje indicando que el certificado se encuentra revocado.

Las CRL´s generadas por la ECIBCE tiene un tiempo de vigencia 24 horas, la ECIBCE actualiza y publica la CRL cada vez que un certificado es revocado o antes del vencimiento de la vigencia de la CRL si no se presentan solicitudes de revocación.

El Banco Central del Ecuador, a través de la Entidad de Certificación de Información, mantiene actualizada la LCR y la OCSP (en cuanto este servicio esté disponible), incluyendo todos los certificados revocados desde la última actualización.

A continuación se muestra los campos que contiene una Lista de Certificados Revocados (CRL):

Campo	Descripción
Versión	Versión de la lista
Emisor	Entidad de Certificación Emisora
Fecha efectiva	Fecha de publicación
Próxima actualización	Fecha de vencimiento
Algoritmo de firma	Algoritmo utilizado
Número CRL	Número de revocaciones
Identificador de clave de entidad emisora	Id de clave

Tabla IV-IX. Lista de Certificados Revocados (CRL)

4.4. Implementación

Se debe configurar el dispositivo token de firma digital en la plataforma Windows Xp, para su implementación del prototipo de firmas digitales. Ver Anexo E.

CONCLUSIONES

- El dispositivo token, emitido por la entidad certificadora, sirve para firmar digitalmente documentos confidenciales que se utilizan en el Hospital de Brigada N° 11 “Galápagos”, como oficios, memorándum, telegramas etc para enviar a las diferentes entidades.

- El uso de firmas digitales empleadas en los tramites que se realizan en el Hospital de Brigada N° 11 “Galápagos”, permite garantizar que la información enviada sea segura, es decir que no va ha existir falsificación de firma.

- Las firmas digitales, luego de haber firmado un documento, tiene validez legal a través del Consejo Nacional de Comunicaciones (CONATEL). Lo que significa que se puede utilizar para cualquier tipo de trámite.

- La configuración del dispositivo token es más rápida y sencilla en la plataforma Windows XP ya posee una interfaz grafica, mientras que en Linux Ubuntu. 8.0.4, la configuración es a través de comandos lo que implica que con lleve más tiempo.

RECOMENDACIONES

- En el Hospital de Brigada N° 11 “Galápagos”, las autoridades son cambiadas periódicamente, por lo que se deberá adquirir el dispositivo token cada determinado tiempo, lo que implica mayores gastos para la institución, lo cual no es conveniente adquirirlo.

- Si el intercambio de información es interno, es decir para utilizar todo el personal del Hospital de Brigada N° 11 “Galápagos”, lo conveniente será utilizar un servidor de correo interno.

- Debido a que la Escuela Superior Politécnica de Chimborazo, es una institución de prestigio, será conveniente crear una infraestructura de clave pública, ya que todas las personas confiarán en está institución para la emisión de certificados digitales.

- La infraestructura de clave publica del Banco Central del Ecuador tiene un tipo de arquitectura plana, es decir funciona para un grupo pequeño de personas, lo conveniente será desarrollar una infraestructura de clave pública con un tipo de arquitectura Jerárquica en donde va existir más de una autoridad certificadora además servirá para un grupo grande de personas.

Resumen

El objetivo de la investigación es implementar un prototipo de firmas digitales para el Hospital de Brigada N° 11 "Galápagos", a través de un dispositivo token usb de firma digital.

Para el desarrollo de es esta investigación, se adquirió un dispositivo token usb de firma digital de la entidad raíz del Banco central del Ecuador , el mismo que posee un certificado digital de un individuo, posteriormente se comprobó el funcionamiento del dispositivo token de firma digital en las dos plataformas Windows XP y Linux Ubuntu 8.0.4, luego de ello se procedió a realizar la comparación tomando parámetros con respecto a la firma digital, en donde se pudo comprobar que la plataforma Windows XP toma el valor de 4,44% que corresponde al 88,88% , mientras que la plataforma Linux Ubuntu 8.0.4 toma un valor de 4,44 % con un porcentaje del 88,88%, lo que se observa que no existe diferencia entre las dos plataformas, es decir que se puede firmas digitalmente un documento en cualquiera de las dos plataformas sin ninguna dificultad. En la plataforma Windows se tiene la ventaja de que su interfaz es grafica es decir amigable, para el usuario así como sus instalación es más rápida que en Linux. Por lo que se recomienda utilizar este tipo de tecnología, es decir el dispositivo de firmas digitales, en cualquiera de las dos plataformas.

Realizada la comparación de las plataformas entre Windows XP y Linux Ubuntu 8.0.4, se procedió a la implementación del prototipo de firmas digitales para el Hospital de Brigada N° 11 "Galápagos", a través de la utilización del dispositivo token usb de firma digital, el cual permite firmar digitalmente un documento digital.

Summary

The objective of the investigation is to implement a prototype of digital signatures for the Hospital of Brigade N° 11 " Tortoises ", through a device token usb of digital signature.

For the development of it is this investigation, a device token usb of digital signature of the entity root of the central Bank of the Ecuador, the same one was acquired that possesses a digital certificate of an individual, later on he/she was proven the operation of the device token of digital signature in the two platforms Windows XP and Linux Ubuntu 8.0.4, after it you proceeded to carry out the comparison taking parameters with regard to the digital signature where could be proven that the platform Windows XP takes the value of 4,44% that corresponds to 88,88%, while the platform Linux Ubuntu 8.0.4 taking a value of 4,44% with a percentage of 88,88%, what is observed that difference doesn't exist among the two platforms, that is to say that one can signatures digitally a document in anyone of the two platforms without any difficulty. In the platform Windows one has the advantage that their interfaz is graphic that is to say friendly, for the user as well as its installation is quicker than in Linux. For what is recommended to use this technology type, that is to say the device of digital signatures, in anyone of the two platforms.

Carried out the comparison of the platforms between Windows XP and Linux Ubuntu 8.0.4, you proceeded to the implementation of the prototype of digital signatures for the Hospital of Brigade N° 11 " Tortoises ", through the use of the device token usb of digital signature, which allows to sign a digital document digitally.

GLOSARIO

AR Dependencia del Banco Central encargada de la comprobación de identidades para la emisión de Certificados Digitales por parte de la ECIBCE

CA En criptografía una Autoridad de certificación (AC o CA por sus siglas en ingles Certification Authority) es una entidad de confianza, responsable de emitir y revocar los certificados digitales o certificados, utilizados en la firma digital, para lo cual se emplea el cifrado de clave publica.

Certificado Digital Es un documento digital mediante el cual un tercero confiable (CA) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave publica.

Clave privada Es la clave confidencial que mantiene en privado el usuario. Usada generalmente para descifrar los mensajes codificados y también para generar la firma digital.

Clave pública Es la clave del certificado digital que se utiliza para la verificación de la firma electrónica y el cifrado de datos.

Claves RSA Es el sistema criptográfico con clave pública RSA llamado así por sus creadores Ron Rivest, Adi Shamir y Len Adleman, es un algoritmo asimétrico que utiliza una clave pública, la cual se distribuye (en forma autenticada preferentemente),y otra privada, la cual es guardada en secreto por su propietario.

ECIBCE Es el Banco Central del Ecuador que emite certificados de firma electrónica y que puede prestar otros servicios relacionados con la firma digital, autorizada por el Consejo Nacional de Telecomunicaciones, según lo dispuesto en Ley de Comercio Electrónico, Firmas digitales y Mensajes de Datos y su Reglamento.

La ECIBCE será la encargada de la verificación de documentos e identificación de los solicitantes y suscriptores del certificado de firma electrónica y de completar el procedimiento definido para la emisión de certificados.

Firma digital Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos.

Ldap Es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP puede considerarse una base de datos (aunque su sistema de almacenamiento puede ser diferente) al que pueden realizarse consultas. Habitualmente, almacena la información de login (usuario y contraseña) y es utilizado para autenticarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados).

LCR Es una lista de certificados que han sido revocados, que no son válidos y en los que no debe confiar ningún usuario del sistema.

OCSP Online Certificate Status Protocol (OCSP) es un método para determinar el estado de revocación de un certificado digital X.509 en línea.

PKI En criptografía, una infraestructura de clave pública (o, en inglés, PKI, Public Key Infrastructure) es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

PC Contiene las reglas a las que se sujeta el uso de los certificados definidos en la política. Se describen los papeles, responsabilidades y relaciones entre el usuario final y la Autoridad de Certificación y las reglas de solicitud, adquisición gestión y uso de los certificados. Este documento matiza y complementa a la Declaración de Prácticas de Certificación (DPC) de la Autoridad de Certificación.

Solicitante La persona natural, jurídica, funcionario o servidor público que solicita la emisión de un Certificado por parte de la ECIBCE, sometiéndose al procedimiento de verificación de identidad y de creación del certificado de firma electrónica que la ECIBCE ha establecido para su emisión.

Suscriptor El suscriptor será la persona natural, jurídica o funcionario público a favor de la cual se ha emitido un certificado. Los suscriptores deberán ajustarse a lo señalado en la DPC, en la PC del certificado que han obtenido y, en su caso, en contrato de Prestación de Servicios suscrito con la ECIBCE los suscriptores deberán ajustarse a los procedimientos establecidos para la petición de cada tipo de certificado, y cumplir los requisitos que se establezcan en esta DPC.

Token Elemento físico donde se almacena en forma segura el certificado de firma digital que será emitido por la ECIBCE. Su uso es indispensable.

Usuario La persona natural, persona jurídica, funcionario público que confía en un Certificado emitido por la ECIBCE.

X.509 Eespecifica formatos estándar para certificados de claves públicas y un algoritmo de validación de la ruta de certificación.

ANEXOS

ANEXO A

Configuración del dispositivo Token para firma digital en Ubuntu 8.0.4

A continuación se presenta los pasos para el funcionamiento del dispositivo Token usb para firma digital en la plataforma Linux.

Requerimientos Hardware

Linux Ubuntu 8.0.4
1 Computador
1 dispositivo Token usb

Requerimientos Software

Linux Ubuntu 8.0.4
S.O. Ubuntu 8.4.0.
Libusb-dev_0.1.12-8_i386.deb
BsecPKlinux-2.0.0.0007.zip
libsfntpkcs11.so.2.0.0.7
Open Office 2.4 Versión 1.1
Internet Explorer 6 o superior

Instalación de drivers en el Sistema Operativo Ubuntu 8.0.4 para el funcionamiento del dispositivo Token para firma digital.

- Se debe ingresar a la página del Banco Central del Ecuador que se encuentra ubicado en la siguiente dirección http://www.bce.fin.ec/, luego dar click en la pestaña Entidad de Certificación, después se selecciona la opción 8 que dice Drivers del dispositivo portable seguro token y dar click en Linux para bajarse los drivers.

Luego de haber realizado lo anterior se procede con la instalación:

- Instalación de Certificados Raíz ECIBC.cer y ECIBCE.cer en Ubuntu versión 8.0.4
- Instalación de drivers en Ubuntu Token Ikey 2032
  - Instalar la librería libusb-dev
  - Bajarse la librería BsecPKlinux-2.0.0.0007.zip de la página del Banco Central del Ecuador, descomprimirla y copiar en la siguiente ubicación.

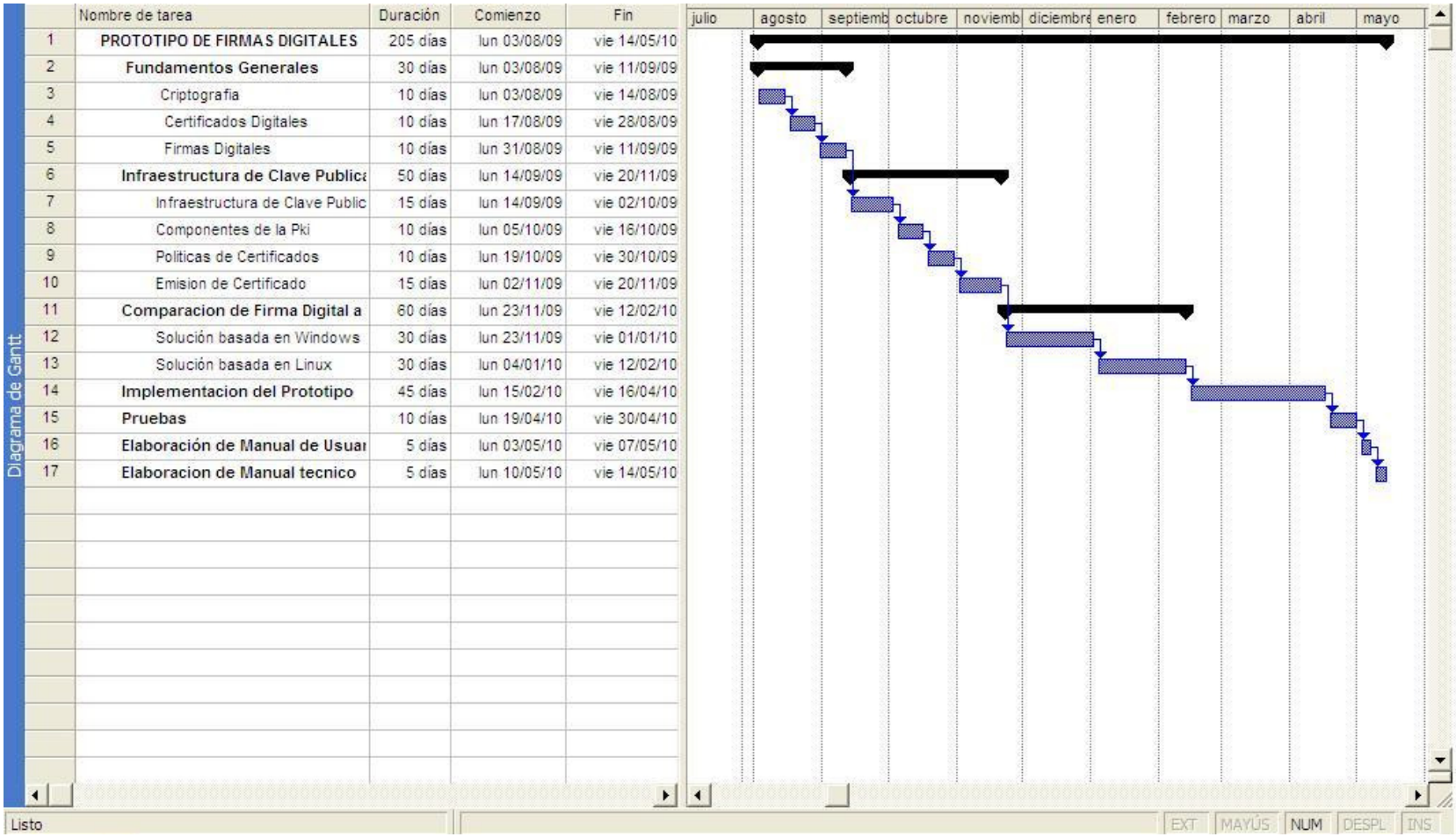
    cd/home/hb-11/Escritorio/BSecPKLinux-2.0.0.0007/

    chmod 755 install-BSecPK-v2.0.0.sh (cambio de permisos)

    ./install-BSecPK-v2.0.0.sh (ejecución de instalador)
  - Bajarse la siguiente librería libsfntpkcs11.so.2.0.0.7 del Banco central del Ecuador y copiar en el siguiente directorio /usr/local/SafeNet/lib
  - Luego Ejecutar ldconfig /usr/local/SafeNet/lib/ posterior a ello se debe reiniciar el computador
  - Para ver que el token funcione adecuadamente en un terminal se debe ejecutar lo siguiente, con el token conectado al computador TokenUtility
- Instalación de librería en Mozilla Firefox para poder firmar en Aplicaciones
  - Se debe abrir Mozilla Firefox, dentro del Menú Editar, Preferencias, Avanzadas, Cifrado, Dispositivos de Seguridad.
  - Luego cargar la librería libsfntpkc.so.2.0.0.7 de la siguiente ubicación /usr/local/SafeNet/lib/
  - Luego se debe abrir el Open Office, dentro del menú File, Firmas digitales.
  - Posteriormente se debe ingresar la contraseña o PIN
  - Luego se debe seleccionar el certificado con el que se va ha proceder a Firmar electrónicamente.

ANEXO B

Planificación Temporal



	Nombre de tarea	Duración	Comienzo	Fin
1	PROTOTIPO DE FIRMAS DIGITALES	205 días	lun 03/08/09	vie 14/05/10
2	Fundamentos Generales	30 días	lun 03/08/09	vie 11/09/09
3	Criptografia	10 días	lun 03/08/09	vie 14/08/09
4	Certificados Digitales	10 días	lun 17/08/09	vie 28/08/09
5	Firmas Digitales	10 días	lun 31/08/09	vie 11/09/09
6	Infraestructura de Clave Publica	50 días	lun 14/09/09	vie 20/11/09
7	Infraestructura de Clave Public	15 días	lun 14/09/09	vie 02/10/09
8	Componentes de la Pki	10 días	lun 05/10/09	vie 16/10/09
9	Politicas de Certificados	10 días	lun 19/10/09	vie 30/10/09
10	Emision de Certificado	15 días	lun 02/11/09	vie 20/11/09
11	Comparacion de Firma Digital a	60 días	lun 23/11/09	vie 12/02/10
12	Solución basada en Windows	30 días	lun 23/11/09	vie 01/01/10
13	Solución basada en Linux	30 días	lun 04/01/10	vie 12/02/10
14	Implementacion del Prototipo	45 días	lun 15/02/10	vie 16/04/10
15	Pruebas	10 días	lun 19/04/10	vie 30/04/10
16	Elaboración de Manual de Usuar	5 días	lun 03/05/10	vie 07/05/10
17	Elaboracion de Manual tecnico	5 días	lun 10/05/10	vie 14/05/10

ANEXO D

Configuración del Servidor de Correo Exchange Server

A continuación se presenta los pasos de configuración del Servidor de correo Exchange Server en la plataforma Windows.

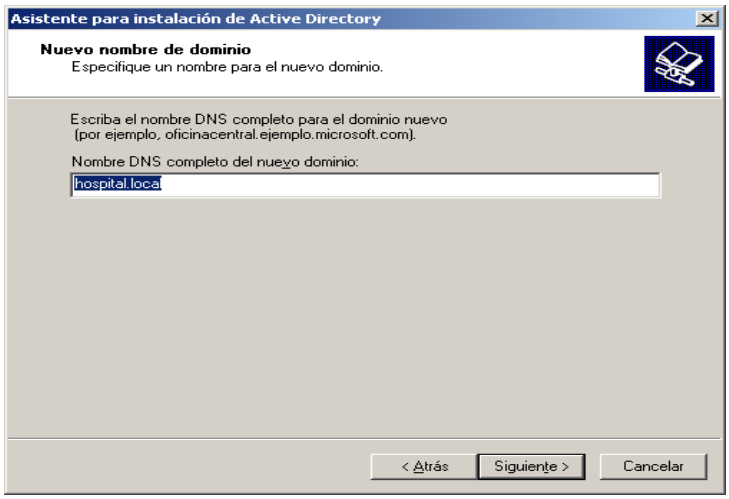
1. Instalación de Directorio Activo

Se debe ingresar por Inicio, Ejecutar, luego ingresar el comando Dcpromo.exe, y dar click en el botón Aceptar .

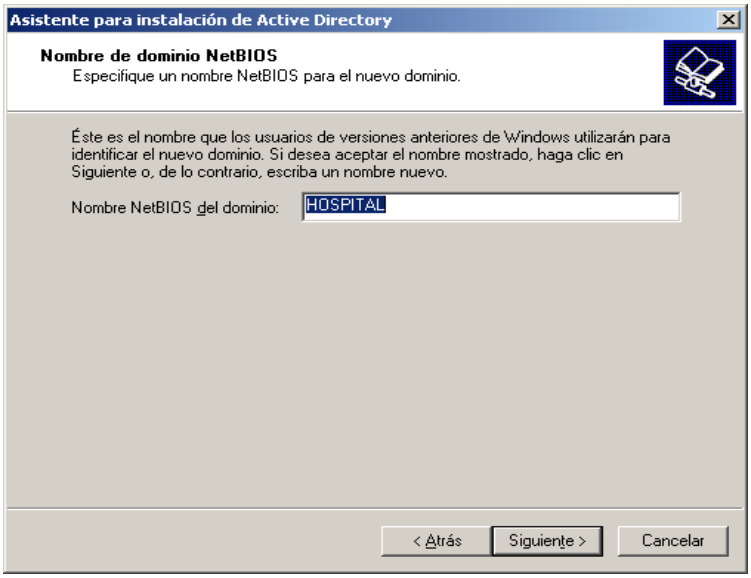
Luego se visualiza el tipo de controlador de dominio en el cual se debe escoger la opción de Controlador de dominio para un nuevo usuario y dar click en el botón Siguiente.

A continuación se escoge la opción de Dominio en un nuevo bosque, y dar click en el botón Siguiente.

Luego se debe ingresar el Nuevo nombre de dominio. En este caso hospital.local a continuación dar click en el botón Siguiente.



Después, se debe ingresar el nombre del domino NetBios en este caso se acepta el nombre mostrado que es HOSPITAL y dar click en el botón Siguiente.



Luego se muestra Carpetas de la base de datos y del registro, la cual se deja por defecto y dar click en el botón Aceptar.

Luego se debe escoger la opción Instalar y configurar este equipo de manera que utilice este servidor DNS como el preferido. Y después dar click en el botón Siguiente.

A continuación, se debe escoger la opción Permisos compatibles sólo con sistemas operativos de servidor Windows y pulsar el botón Siguiente.

En la siguiente figura, en el espacio DNS preferido se coloca la dirección IP que se esta utilizando y en el DNS alternativo se ubica la dirección del reenviador. Y dar click en botón Aceptar.

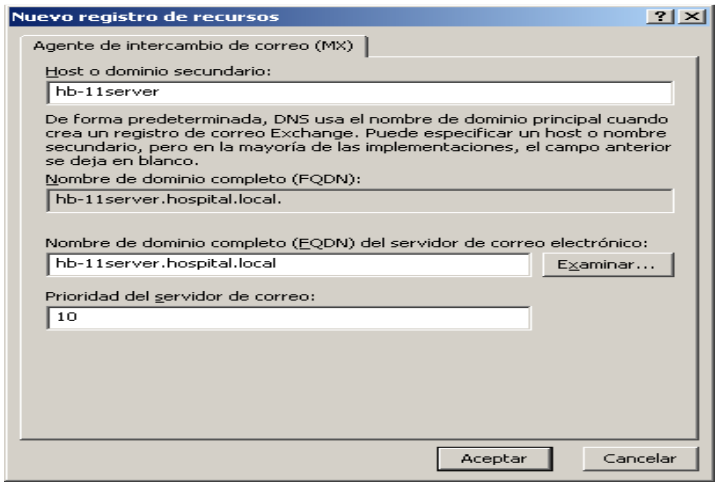
Luego muestra un aviso, que la instalación del directorio activo en la máquina termino satisfactoriamente.

2. Configuración del Servidor DNS

Se debe ingresar por Inicio, Administre su servidor, luego pulsar en Administrar este servidor DNS.

Luego en el equipo en el que se esta trabajando en este caso se llama hb-11server, el dominio es hospital.local y en la zona directa esta un registro (A) del equipo en el que se esta trabajando, seleccionar ese registro del servidor con el que se esta trabajando luego dar clic derecho en nuevo registro MX ese registro (A) ya existe.

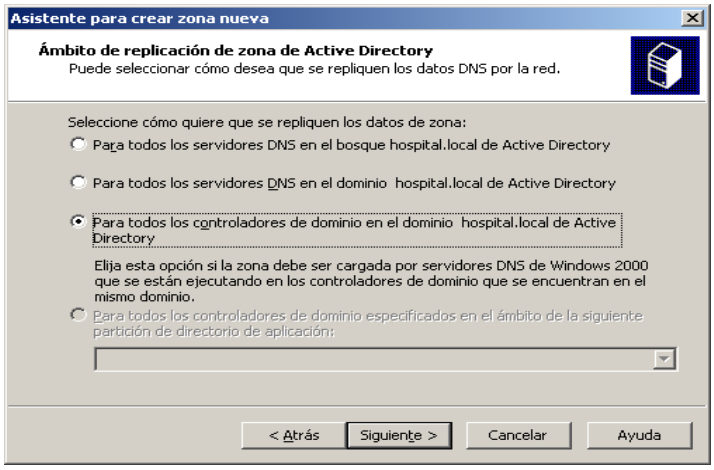
A continuación se debe ingresar hb-11server; y la prioridad del servidor de correo es 10 por defecto.



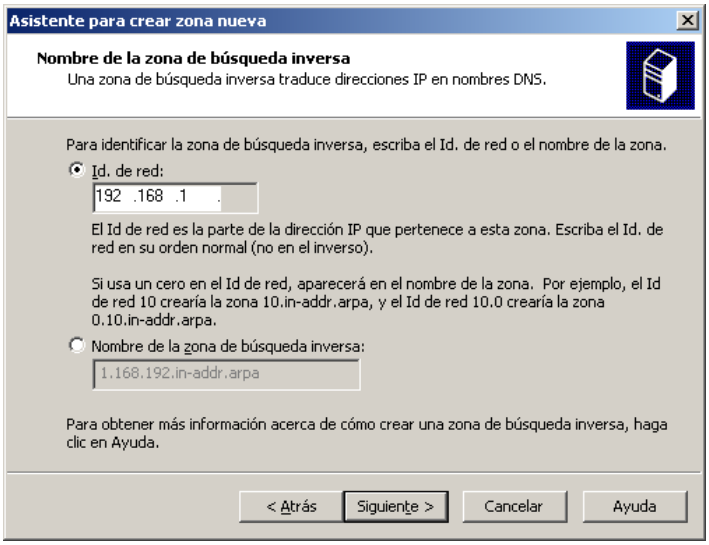
A continuación se debe dar click derecho en zona nueva.

Luego dar click en zona principal y pulsar el botón Siguiente

A continuación se presenta el Ámbito de replicación de zona de directorio activo, en donde se debe escoger la opción Para todos los controladores de dominio en el dominio hospital.local de Active Directory y posteriormente dar click en el botón Siguiente.



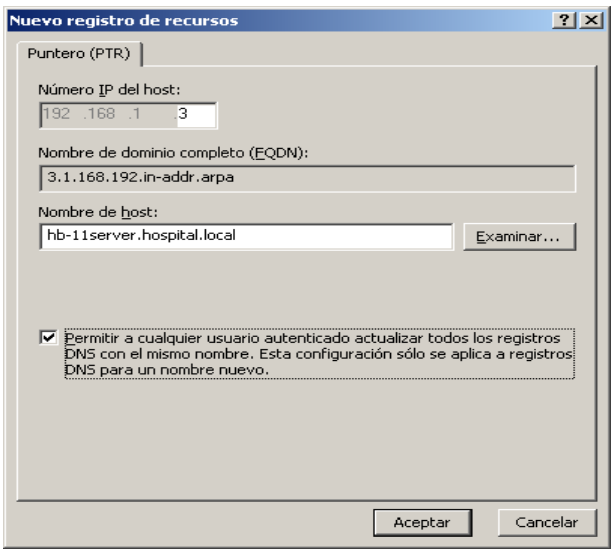
Luego se debe ingresar los tres primeros 8 bits de la dirección IP, en este caso "192.168.1.x". Luego dar click en el botón Siguiente.



A continuación se debe seleccionar la opción Permitir sólo actualizaciones dinámicas seguras y luego dar click en el botón Siguiente.

A continuación se debe dar click en la dirección inversa y en la parte derecha dar click derecho y seleccionar Nuevo puntero (PTR).

Luego muestra un Nuevo registro de recurso en el cual el Número IP de hosts se ingresa 3 en Nombre de host se ingresa hb-11server.hospital.local y por último activar la casilla y luego dar click en el botón Aceptar.



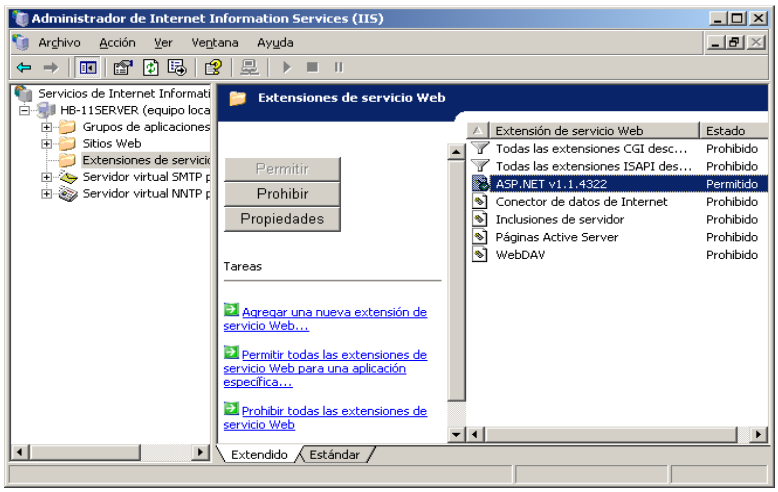
3. Instalación y habilitación de aplicaciones

Se debe Ingresar por Inicio, Panel de control, Agregar o quitar programas y Agregar o quitar componentes de Windows. A continuación se debe activar la casilla Servidor de aplicaciones luego dar click en el botón Detalles.

A continuación se debe activar las casillas ASP.NET, IIS luego dentro de esta se debe dar click en el botón Detalles.

Luego se debe activar las casillas de Servicio World Wide Web, NNTP Service y Servicio SMTP y luego dar click en el botón Aceptar.

Se debe ingresar por Inicio, Herramientas administrativas, Administrador de internet information service (IIS). Después ubicarse en HB-11SERVER, luego ubicarse en Extensiones de servicio Web y en ASP.net v1.1.4322 y dar click derecho sobre este y seleccionar Permitir.



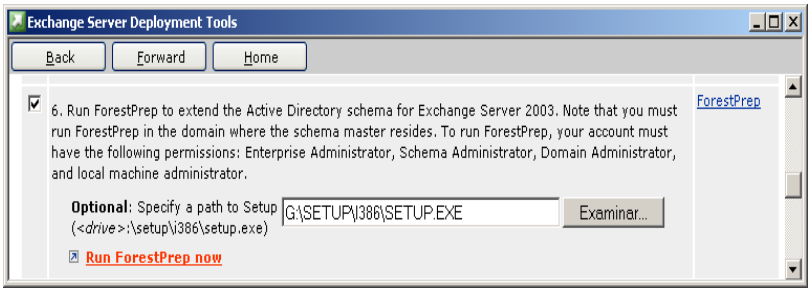
4. Instalación del servidor Exchange

Se debe ingresar el CD de Exchange, luego se debe dar click en herramientas de implementación de Exchange.

Luego se debe dar click en Implementar el primer servidor de Exchange 2003.

Posteriormente, se debe seleccionar Nueva instalación de exchage 2003, luego se debe activar las cinco primeras casillas para la instalación

A continuación buscar el foresprep, examinar (buscar la ruta) y luego dar click en ejecutar foresprep ahora.



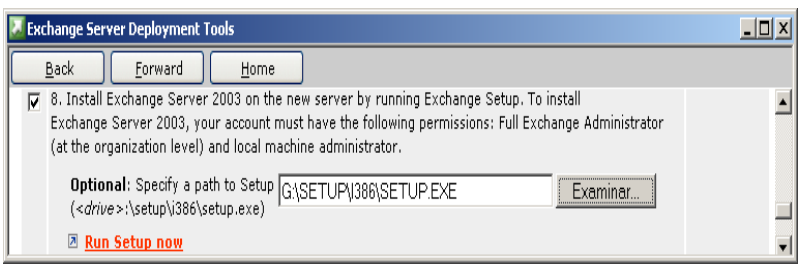
A continuación se debe seleccionar el componente que se va a instalar, en este caso forestprep, luego dar click en el botón Siguiente.

En este caso se va a escribir la cuenta de usuario que posee autoridad para instalar y administrar Exchange 2003 en todo él bosque; generalmente lo coloca por defecto, asumiendo que en el HOSPITAL, la cuenta para la administración total de Exchange es Administrador.

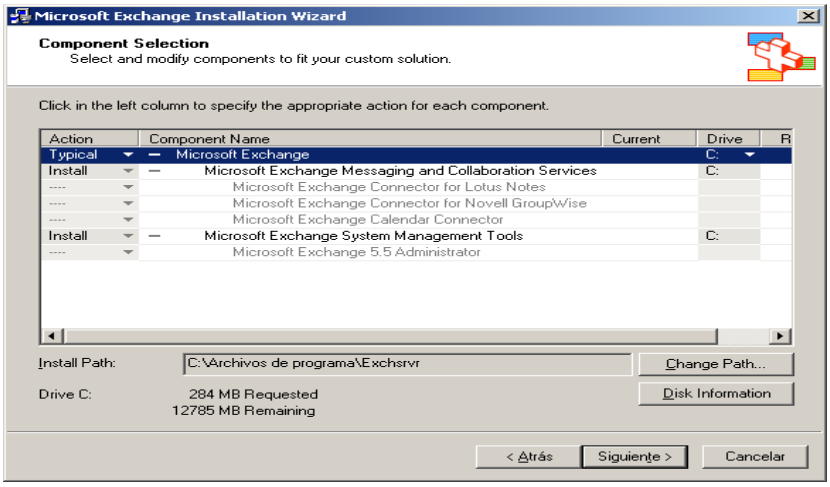
Posteriormente se debe Ejecutar domainprep, mediante el cuadro de herramientas buscar domainprep, examinar (buscar la ruta) y luego dar click en ejecutar domainprep ahora.

A continuación, se debe seleccionar el componente domainprep; luego dar click en el botón Siguiente.

Después se debe ejecutar el Exchange.



Luego se debe seleccionar una instalación típica, luego dar click en el botón Siguiente.



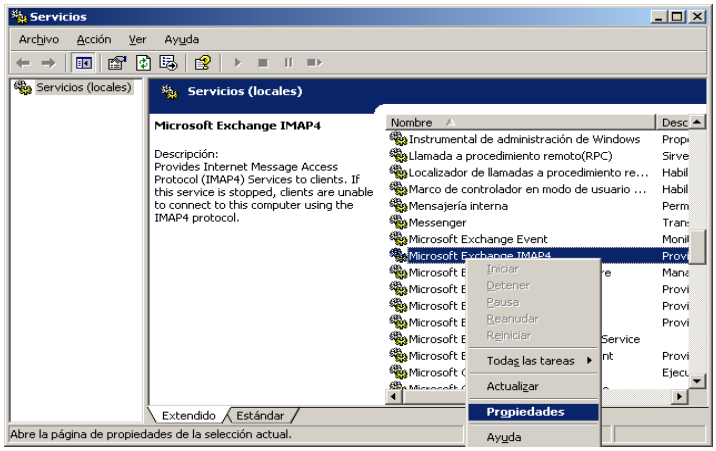
Luego se debe dar click en crear una nueva organización de Exchange.

A continuación, se debe dar un nombre a la organización, en este caso el nombre es HOSPI.

Posteriormente se debe instalar el Service Pack 2, donde se encuentra la actualización de Exchange para un mejor funcionamiento.

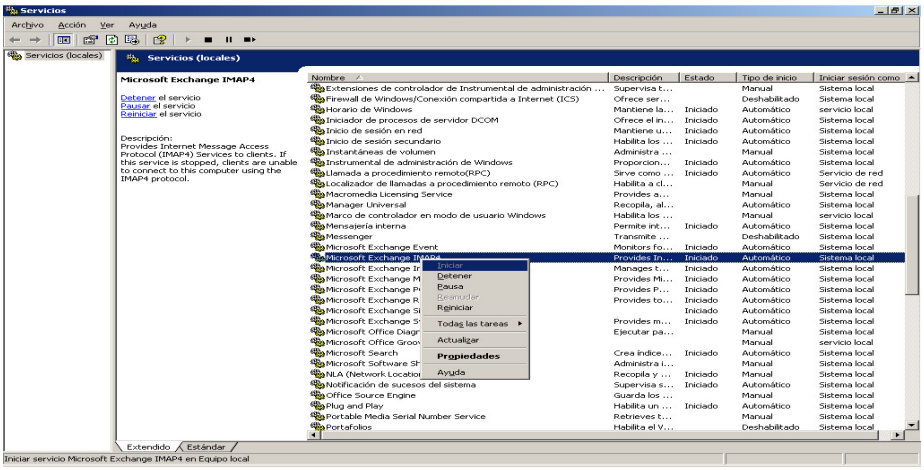
5. Inicio de servicios requeridos

Se debe ingresar por Inicio, Herramientas administrativas, Servicios. Luego se debe habilitar IMAP 4 (Protocolo de acceso a mensajes de Internet versión 4) a clientes, dar click derecho sobre el servicio IMAP 4 y en Propiedades.



Luego en Tipo de inicio se selecciona como Automático, después dar click en el botón Aceptar.

A continuación sobre el servicio IMAP dar click derecho y luego Iniciar.



El mismo procedimiento se realiza para los demás servicios como son POP3 (Protocolo de oficina se correo versión 3), Pila MTA, Operador del sistema motor de enrutamiento, servicio de eventos.

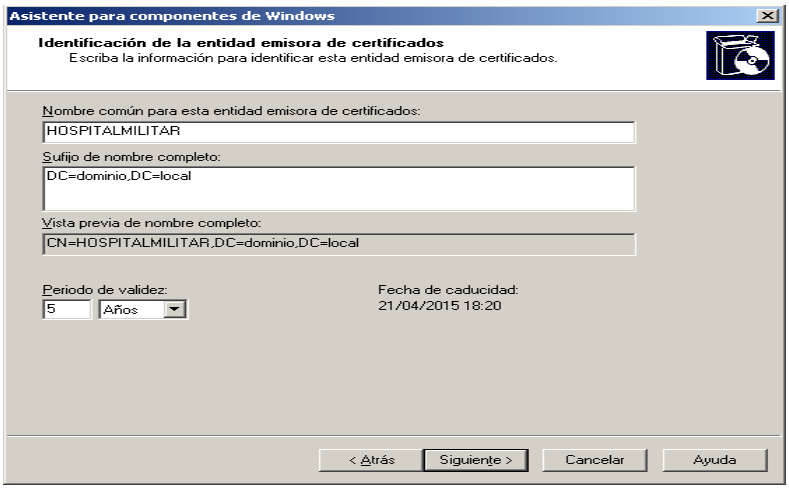
6. Instalación del certificado digital

6.1 Configurar el servicio de certificados

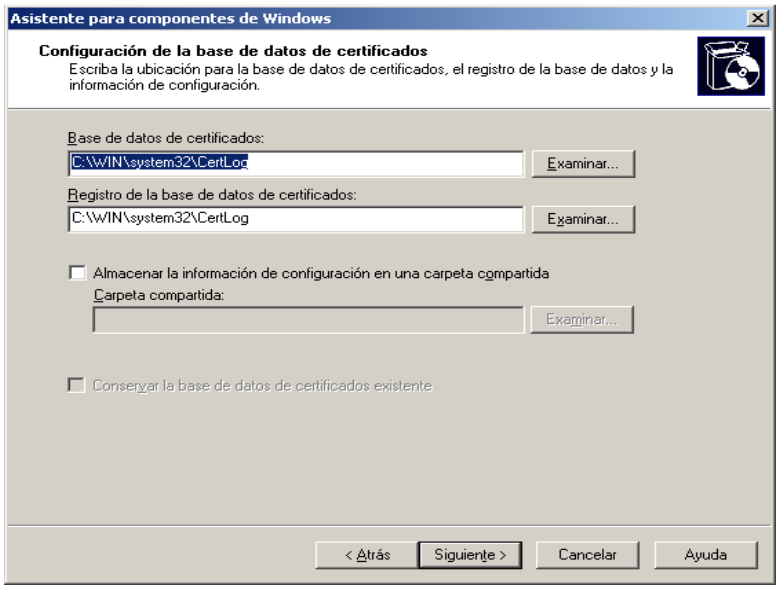
Se debe ingresar por Inicio, Panel de control, Agregar o quitar programas, Agregar o quitar componentes de Windows, luego se debe activar la casilla de Servicios de Certificate Server después dar click en el botón Detalles. A continuación se debe activar las dos casillas y dar click en el botón Aceptar.

Luego se debe escoger la opción de Entidad emisora raíz de la empresa y dar click en el botón Aceptar.

A continuación en la siguiente figura se ingresa el Nombre común para esta entidad emisora de certificados se debe ingresar en este caso HOSPITALMILITAR, luego pulsar el botón Siguiente.



Luego se muestra la configuración de la base de datos de certificados, luego pulsar el botón **Siguiente**.



6.2 Generar solicitud de certificado

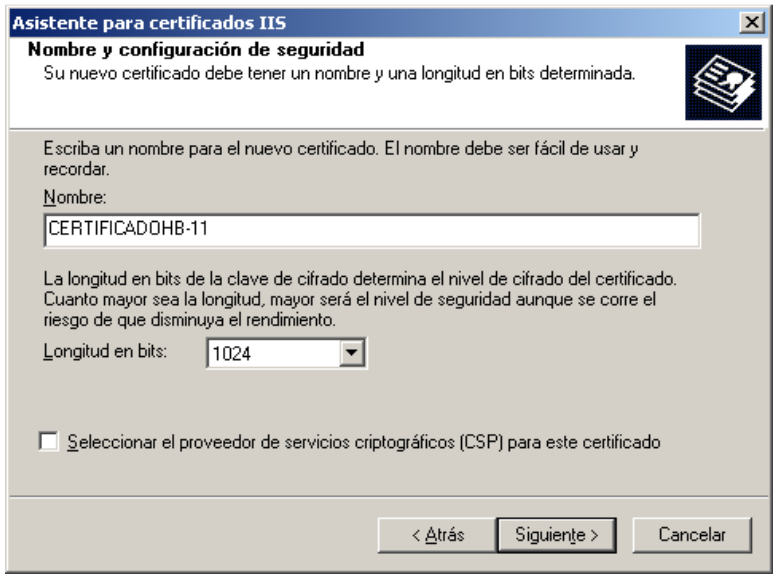
Se debe ingresar por Inicio, Todos los Programas, Herramientas Administrativas, Sitios Web, Sitio Web Predeterminado, click derecho Propiedades.

Luego ingresar a la pestaña de Seguridad de directorios, a continuación dar click en Comunicaciones Seguras, después dar click en el botòn Certificado de servidor.

A continuación se debe seleccionar Crear un certificado nuevo y luego dar click en el botón Aceptar.

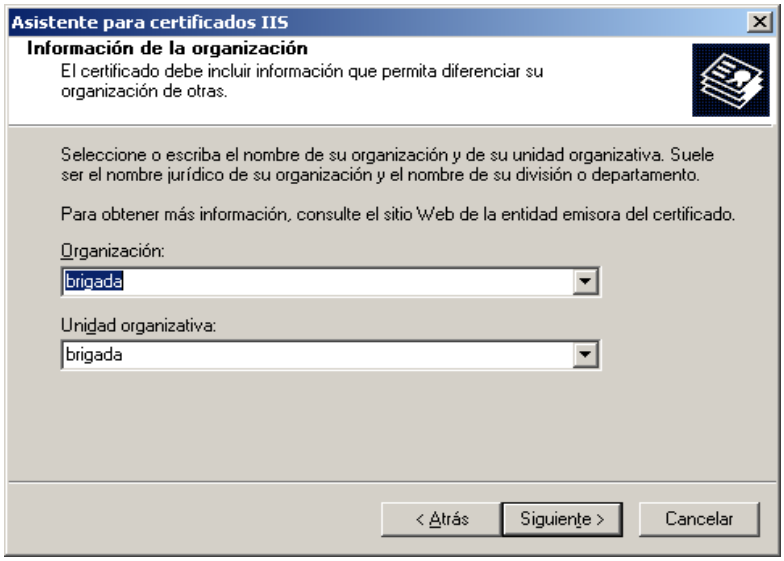
Luego se debe seleccionar la opción Preparar la petición ahora pero enviarla más tarde, y pulsar el botón Siguiente.

Después se debe ingresar el nombre del certificado, en este caso es CERTIFICADOH-B11. Después dar click en el botón Siguiente.



-

Luego se debe de ingresar la organización y la unidad organizativa en este caso se ingresra brigada y brigada respectivamente, luego dar click en el botón Siguiente.



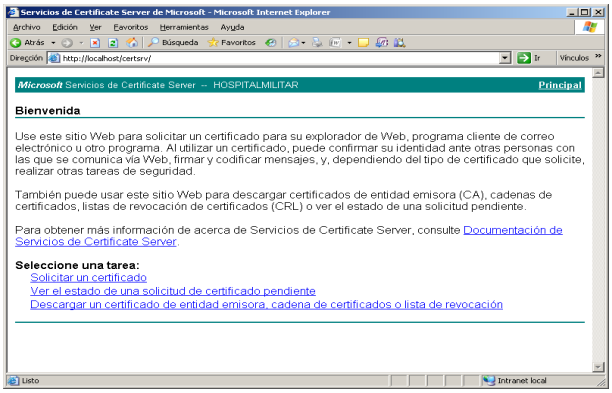
A continuación solicita el nombre del equipo, y luego dar click en el botón Siguiente.

Luego solicita la información geográfica, en este caso se introduce Ecuador, Chimborazo, Riobamba, luego dar click en el botón Siguiente.

A continuación se debe especificar el Nombre de archivo, dar click en el botón Siguiente.

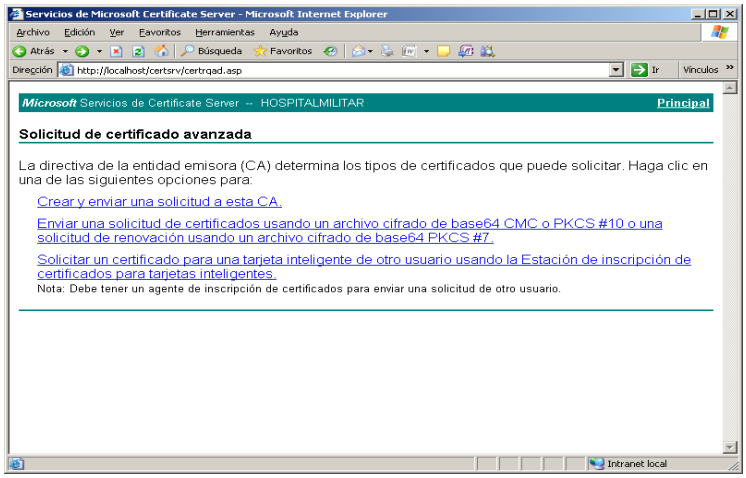
6.3 Enviar solicitud del certificado

Se debe ingresar la siguiente dirección http://localhost/certsrv/ en el navegador, luego se presenta una pantalla de Bienvenida, en donde se selecciona una tarea en este caso Solicitar un certificado.



A continuación se escoge el link de Solicitud avanzada de certificado.

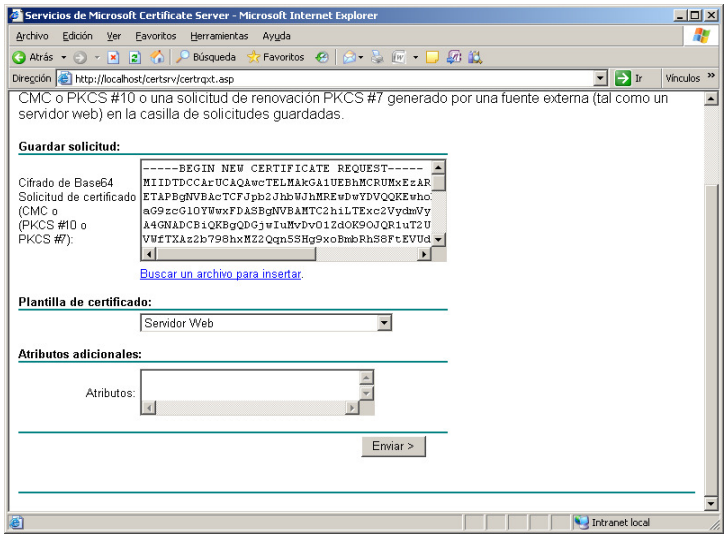
Posteriormente, se debe seleccionar Enviar una solicitud de certificados usando un archivo cifrado de base 64.



A continuación recordar que anteriormente cuando se estaba haciendo la petición del certificado el en ese momento genero un archivo. Pues lo que de debe hacer es ir a la ubicación que se le dio al archivo, abrirlo, seleccionar todo el texto que contiene y pegarlo en el área de guardar solicitud.

En la siguiente pantalla se muestra el archivo que es una representación codificada en Base 64 de la solicitud de certificado. La solicitud contiene la información especificada en asistente, así como la clave pública y la información firmada con la clave privada. Sobre el archivo se le da clip derecho y copiar.

Luego muestra la plantilla del certificado en donde se debe escoger la opción del Servidor Web, ya que este será utilizado en este medio y finalmente dar click en el botón enviar.



Luego se debe seleccionar Cifrado en Base 64 y luego Descargar certificado.

6.4 Instalar el certificado en el servidor Web

Ingresar por Inicio, Herramientas Administrativas, Sitios Web, Sitio Web Predeterminado, click derecho Propiedades.

Posteriormente se selecciona la pestaña Seguridad de directorios, Comunicaciones seguras, dentro de ella se pulsa Certificado de servidor.

Luego se escoge la opciòn Procesar la petición pendiente e instalar el certificado y dar click en el botón Siguiente.

En la siguiente pantalla que se muestra, se indica la ruta de acceso y nombre de archivo, luego dar click en el botón Siguiente.

A continuación en el Puerto SSL se debe habilitar el puerto 443 y pulsar el botón Siguiente.

7. Configurar los recursos para requerir el acceso mediante SSL.

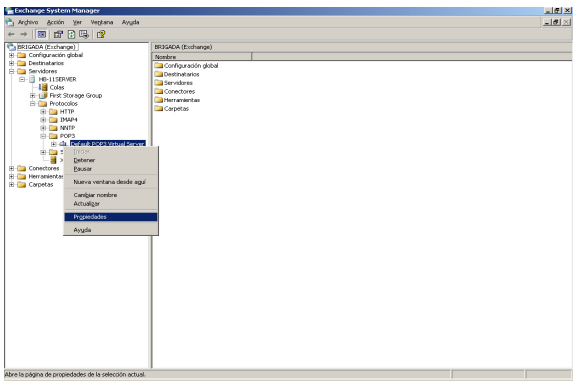
Se debe ingresar por Inicio, Herramientas administrativas, IIS, Sitios web, Sitio web predeterminado, click derecho Propiedades.

Luego se debe dar click en la pestaña Seguridad de directorios, en el área de Comunicaciones seguras dar clip en el botón Modificar.

Luego se presenta un asistente en el cual se debe habilitar Requerir canal seguro, Requerir cifrado de 128 bits, Omitir certificados de cliente, a continuación dar click en el botón Aceptar.

Posteriormente, solicita los nodos secundarios en donde se debe seleccionar Exchange. Luego dar click en el botón Aceptar.

A continuación se debe ingresar por Inicio, Todos los programas, Microsoft Exchange, Administrar el Sistema, Servidores, Protocolos, ubicarse en POP3 y desplegar luego dar clip derecho, Propiedades sobre Servidor virtual POP3.



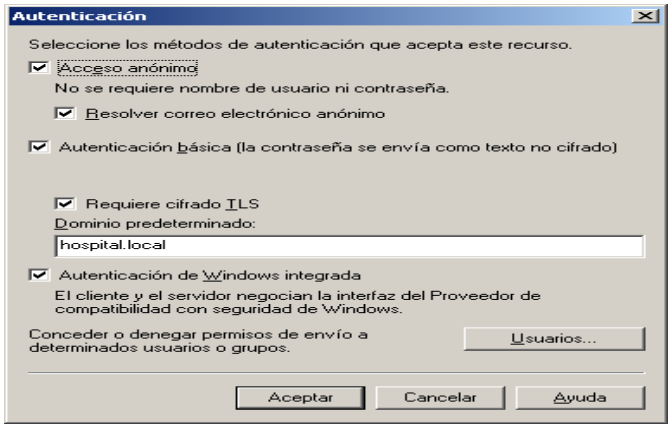
Luego dar click en la pestaña Acceso, en el área de Control de acceso y dar click en el botón Autenticación.

A continuación se debe activar las casillas de Autenticación básica, Requerir cifrado SSL/TLS. Luego dar click en el botón Aceptar.

Luego ubicarse en SMTP y desplegar el mismo, después dar click derecho, Propiedades sobre Servidor virtual SMTP.

A continuación se debe dar click en la pestaña Acceso, luego dar clip en el botón Autenticación.

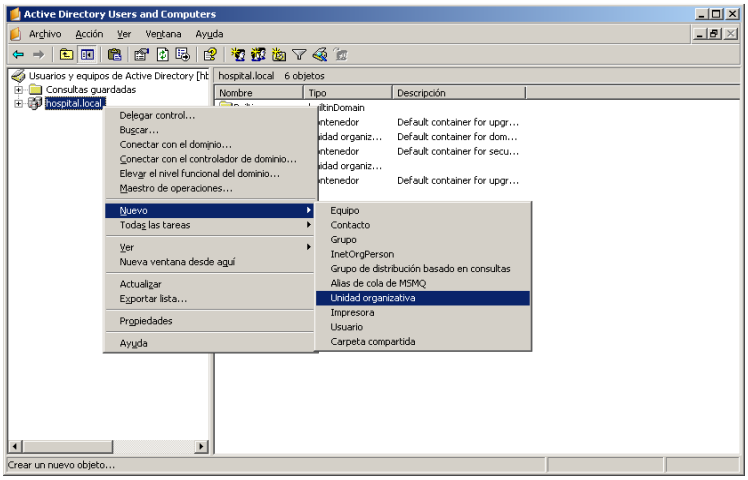
Se debe activar la casilla de Acceso Anónimo, Autenticación básica y Requiere cifrado TLS, especificar el dominio en este caso hospital.local, luego dar click en el botón Aceptar.



A continuación, dar click en la pestaña Seguridad saliente, activar la casilla Cifrado TLS, luego pulsar el botón Aceptar.

8. Creación de usuarios en el Servidor Exchange

Se debe ingresar por Inicio, Todos los programas, Microsoft Exchange, Active Directory, luego ubicarse sobre el dominio en este caso hospital.local, dar click derecho sobre este, Nuevo, Unidad Organizativa.



Se ingresa el nombre de la unidad organizativa en este caso se llama hospital HB-11, luego dar click en el botón Aceptar

Luego dentro de la unidad organizativa que se creo que fue hospital HB-11 se debe dar click derecho sobre este, Nuevo, Unidad organizativa.

Después se debe ingresar un nombre a la unidad organizativa, en este caso se llama usuarios, que es donde se va ha crear los usuarios que va a tener el servidor de correo Exchange.

Posterior a ello sobre la unidad organizativa usuarios, dar click derecho, Nuevo, Usuario.

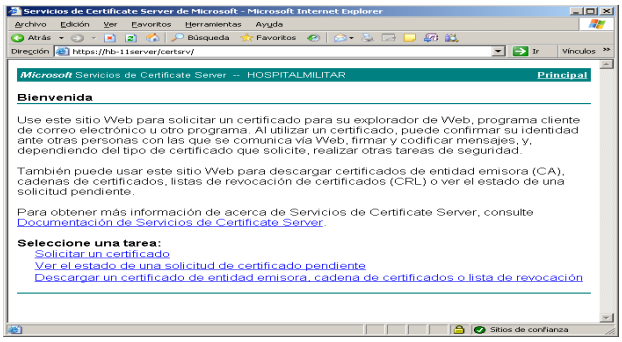
A continuación ingresa todos los campos solicitados, y dar click en el botón Aceptar.

Luego se debe ingresar una contraseña y después dar click en el botón Aceptar.

En un navegador se debe ingresar la siguiente dirección https://hb-11server/certsrv/

Luego se debe ingresar el nombre de usuario y contraseña.

En la siguiente figura muestra diferentes opciones, en donde se debe dar click en el link de Solicitar un certificado.



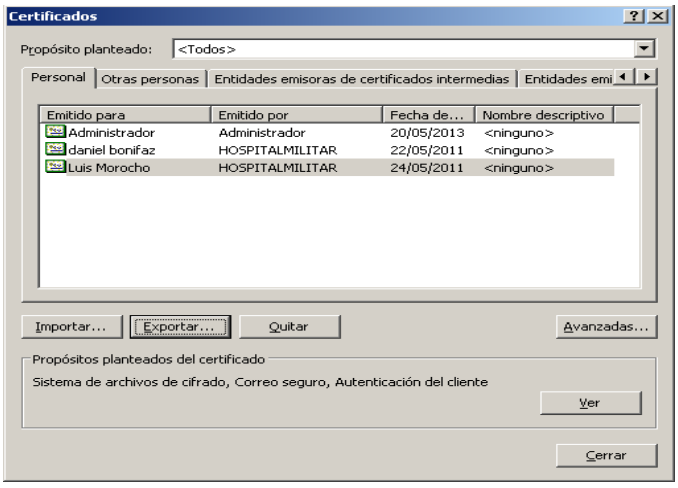
Luego se debe dar click en Certificado de usuario

A continuación se debe dar click en el botón Enviar.

Después se debe dar click en Instalar este certificado.

Para verificar que el certificado se ha instalado se debe ir a Panel de control y abrir Opciones de internet, en la pestaña de Contenido dar click sobre el botón de Certificados

Luego en la siguiente figura, se visualiza el certificado instalado y es de Luis Morocho y dar click en el botón Exportar



Posterior a ello se debe seleccionar la opción Exportar la clave privada, y luego dar click en el botón Siguiente.

A continuación se debe seleccionar la opción de Intercambio de información personal PKCS # 12 y activar la casilla de Permitir protección segura luego dar click en el botón Siguiente.

Luego se debe ingresar una contraseña.

Después se debe indicar la ruta donde se desea guardar el certificado.

A continuación se procede a firmar digitalmente un documento, para lo se crea un documento en Word.

Para realizar la firma digital en un documento se debe ingresar por Inicio, Preparar, Agregar una firma digital. Posteriormente se debe seleccionar el certificado con el cual se desea firmar el memorándum en este caso se ha seleccionado el certificado con el nombre de Luis Morocho.

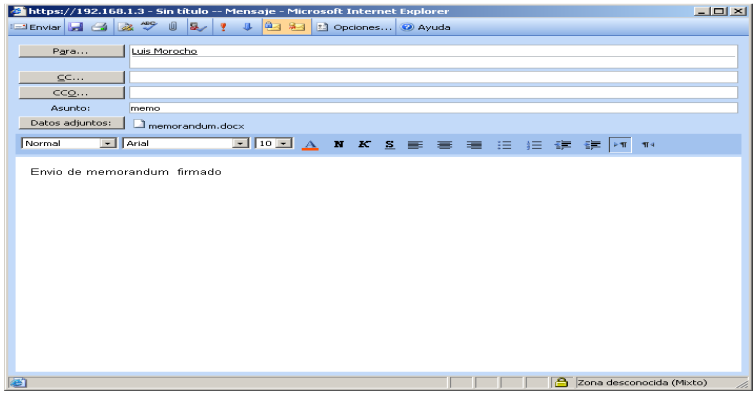
Luego se debe ingresar la razón para firmar el documento en este caso la razón es MEMORANDUM.

Posteriormente en la siguiente figura se muestra el documento firmado.

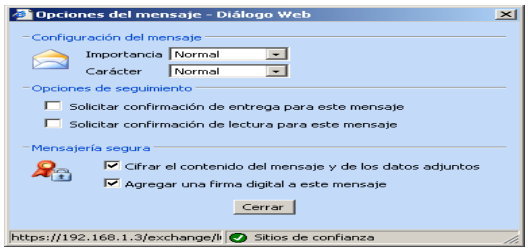
Luego de haber firmado el documento se puede enviar por correo firmado y cifrado desde el servidor a la máquina cliente, para ello se debe ingresar la siguiente dirección en el internet Explorer https://hb-11server/exchange/

Luego se debe ingresar el usuario y contraseña, para lo cual se debe logearse como el usuario del certificado.

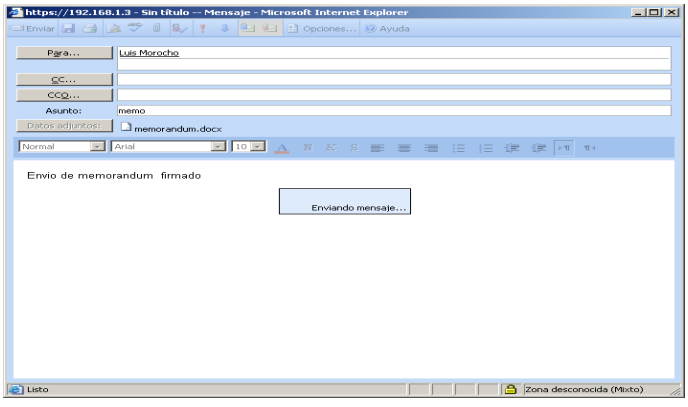
Luego en la figura que se muestra, se envía el correo para Luis Morocho, el Asunto como memo, y el documento en este caso el memorándum Firmado, luego se firma y se cifra el correo y se envía.



En la siguiente figura que se muestra se cifra y se agrega una firma al mensaje posteriormente se envía el correo.



A continuación en la siguiente figura, se visualiza el proceso de envió de correo a Luis Morocho.



9. Importación del certificado en la máquina cliente

Para poder visualizar el mensaje enviado de Luis Morocho desde el servidor a Luis Morocho a la maquina cliente, se debe realizar la importación del certificado en la máquina cliente en este caso el certificado de Luis Morocho.

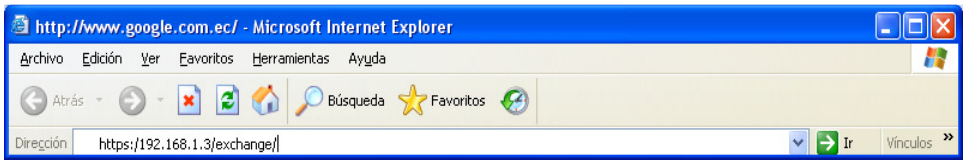
Se debe dar click en el certificado de Luis Morocho, que es el asistente de importación del certificado, luego dar click en el botón Siguiente.

Se especifica el nombre de archivo que se desea importar, en este caso certi_morocho.pfx

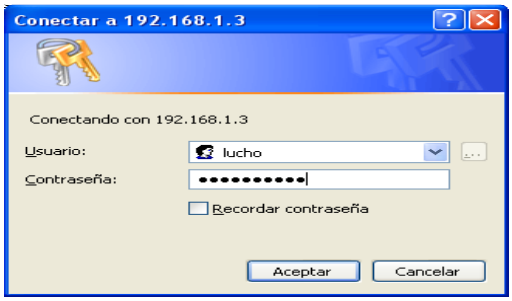
Se debe ingresar la misma contraseña con la que se exporto el certificado.

Se muestra el Almacén de Certificados y se debe dar click en el botón Aceptar

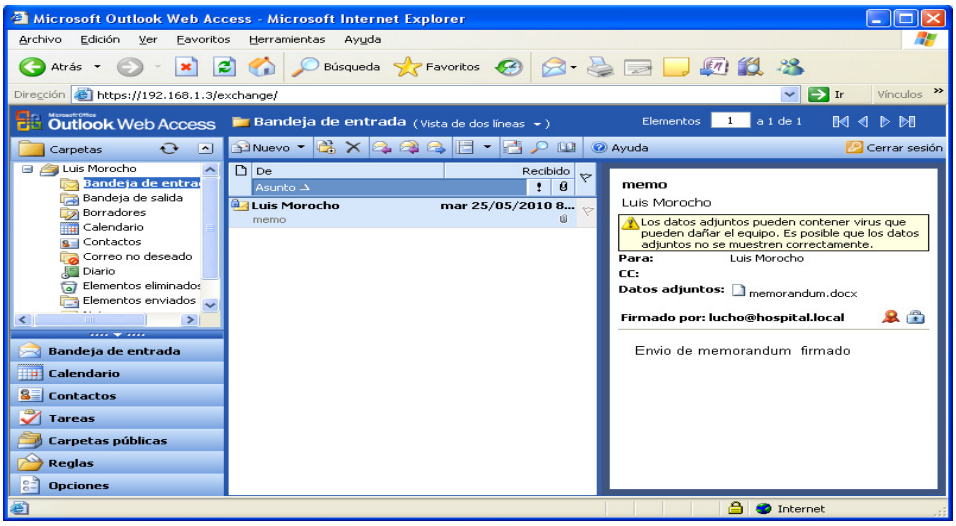
Luego se ingresa la siguiente dirección https://192.168.1.3/exchange/



Luego en la siguiente figura, se debe ingresar el nombre del usuario y la contraseña.



Y finalmente en la siguiente figura, se visualiza el mensaje enviado firmado y cifrado para Luis Morocho.


Microsoft Outlook Web Access - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos
Dirección https://192.168.1.3/exchange/
Ir Vínculos
Outlook Web Access
Bandeja de entrada (Vista de dos líneas)
Elementos 1 a 1 de 1
Carpetas
Luis Morocho
Bandeja de entra
Bandeja de salida
Borradores
Calendario
Contactos
Correo no deseado
Diario
Elementos eliminados
Elementos enviados
Nuevo
Ayuda
Cerrar sesión
De
Recibido
Asunto
Luis Morocho
mar 25/05/2010 8...
memo
memo
Luis Morocho
Los datos adjuntos pueden contener virus que pueden dañar el equipo. Es posible que los datos adjuntos no se muestren correctamente.
Para: Luis Morocho
CC:
Datos adjuntos: memorandum.docx
Firmado por: lucho@hospital.local
Envio de memorandum firmado
Bandeja de entrada
Calendario
Contactos
Tareas
Carpetas públicas
Reglas
Opciones
Internet

ANEXO E

Configuración y funcionamiento del dispositivo Token para firma digital en la plataforma Windows XP.

Se debe ingresar a la página web www.bce.fin.ec sección Entidad de Certificación, luego dar click en Entidad de Certificación Raíz del Banco Central del Ecuador, y a continuación dar clip derecho en descargar y guardar el certificado raíz ECIBC.cer en el disco duro del computador.

Luego de guardar el certificado ECIBC.cer en el computador , dar doble click en el mismo para instalar.

Después se procede a instalar el certificado ECIBC.cer

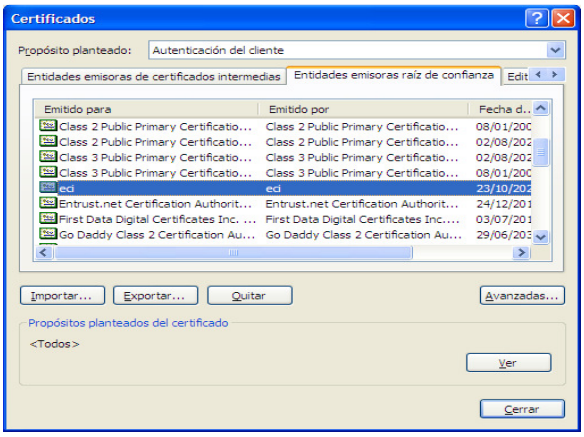
A continuación se debe dar click en el botón Abrir.

Luego se muestra el certificado, al cual se debe dar click en el botón Instalar el certificado.

A continuación se presenta el asistente de finalización de instalación del certificado raíz, luego dar click en el botón Finalizar.

Luego se debe verificar si realmente se ha instalado el certificado, para ello se debe ingresar por Internet Explorer, Herramientas, Opciones de internet, Contenido, Certificados.

Luego, se debe verificar si el certificado raíz se ha instalado para ello se debe dar click en la pestaña Entidades emisoras raíz de confianza como se puede observar si se encuentra instalado el certificado raíz del Banco Central del Ecuador eci.



Después nuevamente se debe ingresar a la página web del Banco Central de Ecuador, con la siguiente dirección www.bce.fin.ec y luego dar clip en la pestaña Entidad de Certificación, después seleccionar Certificado Raíz de la Entidad de Certificación Raíz de Información, y a continuación clip derecho en el certificado a ser descargado en este caso ECIBCE.cer y guardar el certificado raíz en el disco duro del computador.

Posterior a ello se debe dar doble click sobre el certificado ECIBCE.cer.

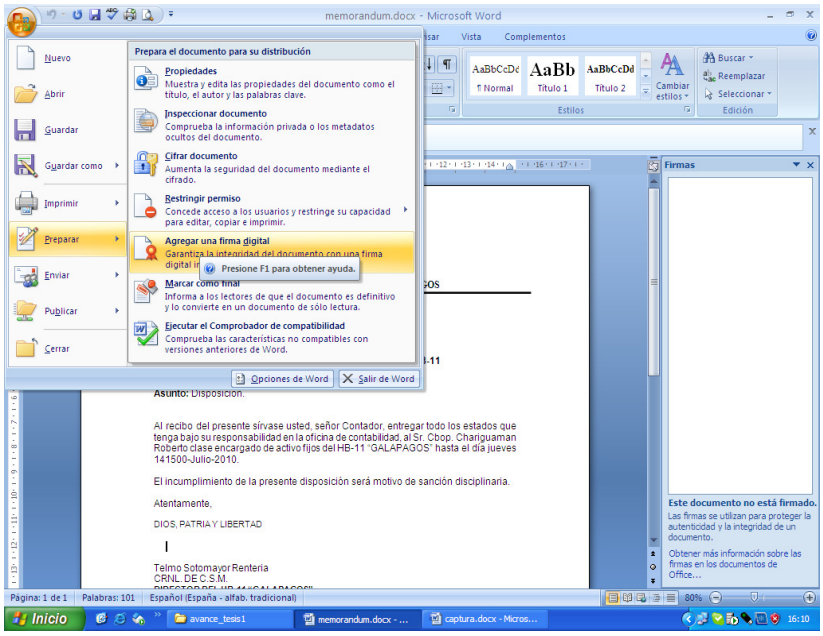
Luego se debe dar click en el botón Abrir

A continuación, se debe dar click en la pestaña General y dar clip en el botón Instalar el certificado luego da click en el botón Aceptar.

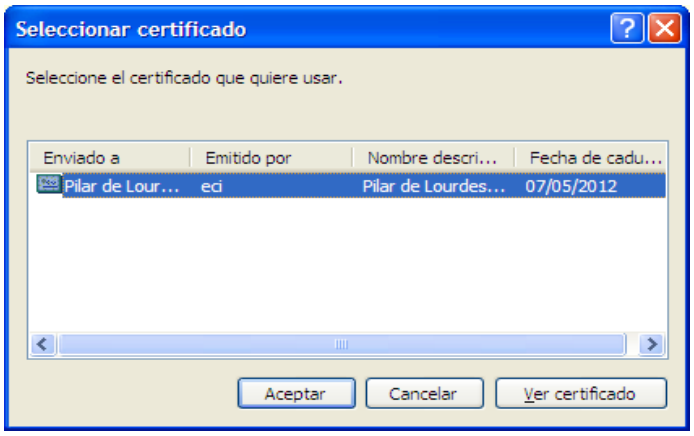
Después se debe dar click en el botón Aceptar.

Ahora con los drivers instalados del dispositivo Token. Se procede ha firmar un documento. Para ello se debe crear un documento y guardarlo.

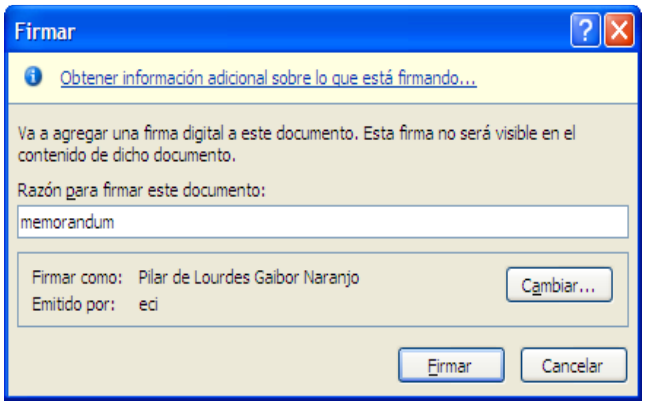
Posteriormente se debe conectar el Token usb a la máquina, luego ingresar por Inicio, Preparar, Agregar una firma digital. .



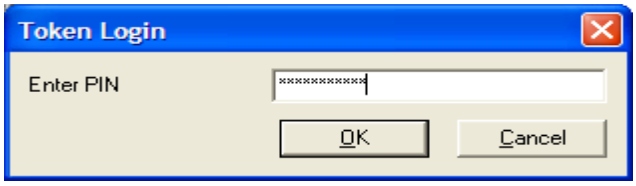
Luego aparece una ventana a la cual se debe dar click en el botòn Cambiar y después se debe seleccionar el certificado con el cual se va ha realizar la firma del documento, en este caso como solo existe este certificado se va ha firmar con el certificado de Pilar de Lourdes Gaibor Naranjo y dar click en el botòn Aceptar.



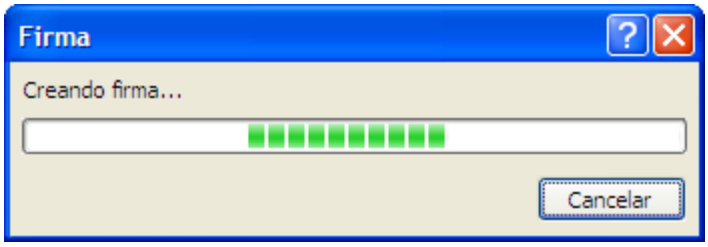
A continuaciòn se debe ingresar la razon a firmar este documento en este caso se llama memorandum y luego dar click en el botòn Firmar.



Posteriormente, se debe ingresar la clave o PIN del Token usb generada en la Entidad Raíz del Banco Central del Ecuador.



A continuación en la siguiente figura se visualiza el proceso de creación de la firma digital.



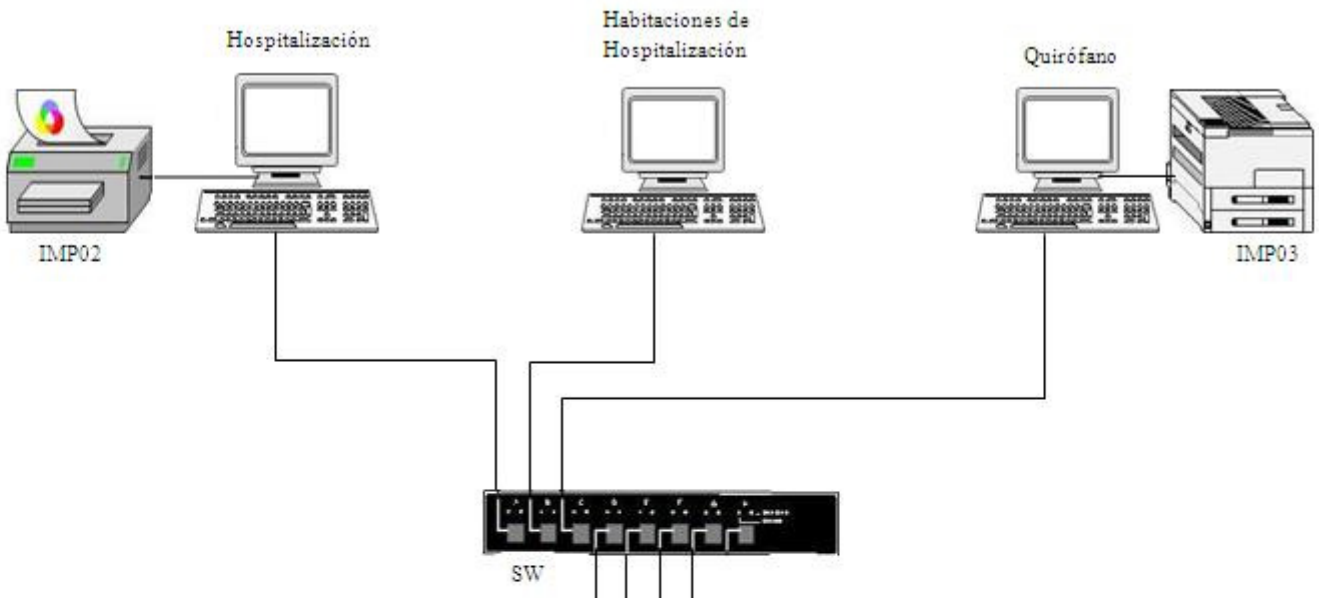
Posteriormente se visualiza el documento firmado por Pilar de Lourdes Gaibor Naranjo

Posteriormente para verificar que el documento enviado ha sido firmado por pilar gaibor se debe consultar el certificado, para ver si se encuentra clave pública.

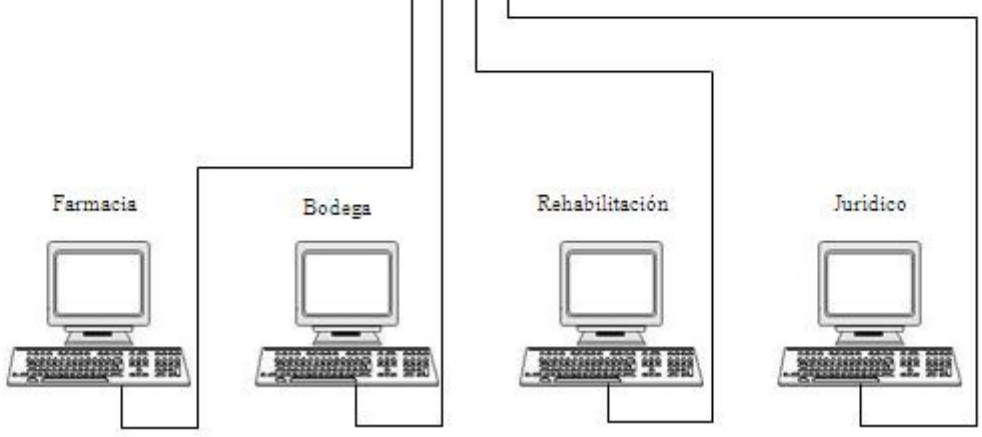
Luego de haber ingresado los datos de pilar gaibor se visualiza los datos que contiene el certificado en la siguiente pantalla.

Nombre	Apellidos	Nombre Distintivo (DN)	Numero de Serie	Correo Electronico	Fecha de Emision	Fecha Vencimiento	Estado	Tipo	Descarga (identificador digital cer)
Pilar de Lourdes	Gaibor Naranjo	cn=Pilar de Lourdes Gaibor Naranjo,ou=eci,o=bce,c=ec	4900f99f	pili_gaibor@yahoo.es	Fri May 07 09:25:51 ECT 2010	Mon May 07 09:55:51 ECT 2012	Valido	Firma Digital	
Pilar de Lourdes	Gaibor Naranjo	cn=Pilar de Lourdes Gaibor Naranjo,ou=eci,o=bce,c=ec	4900f99e	pili_gaibor@yahoo.es	Fri May 07 09:25:51 ECT 2010	Mon May 07 09:55:51 ECT 2012	Valido	Encripción	

BLOQUE B

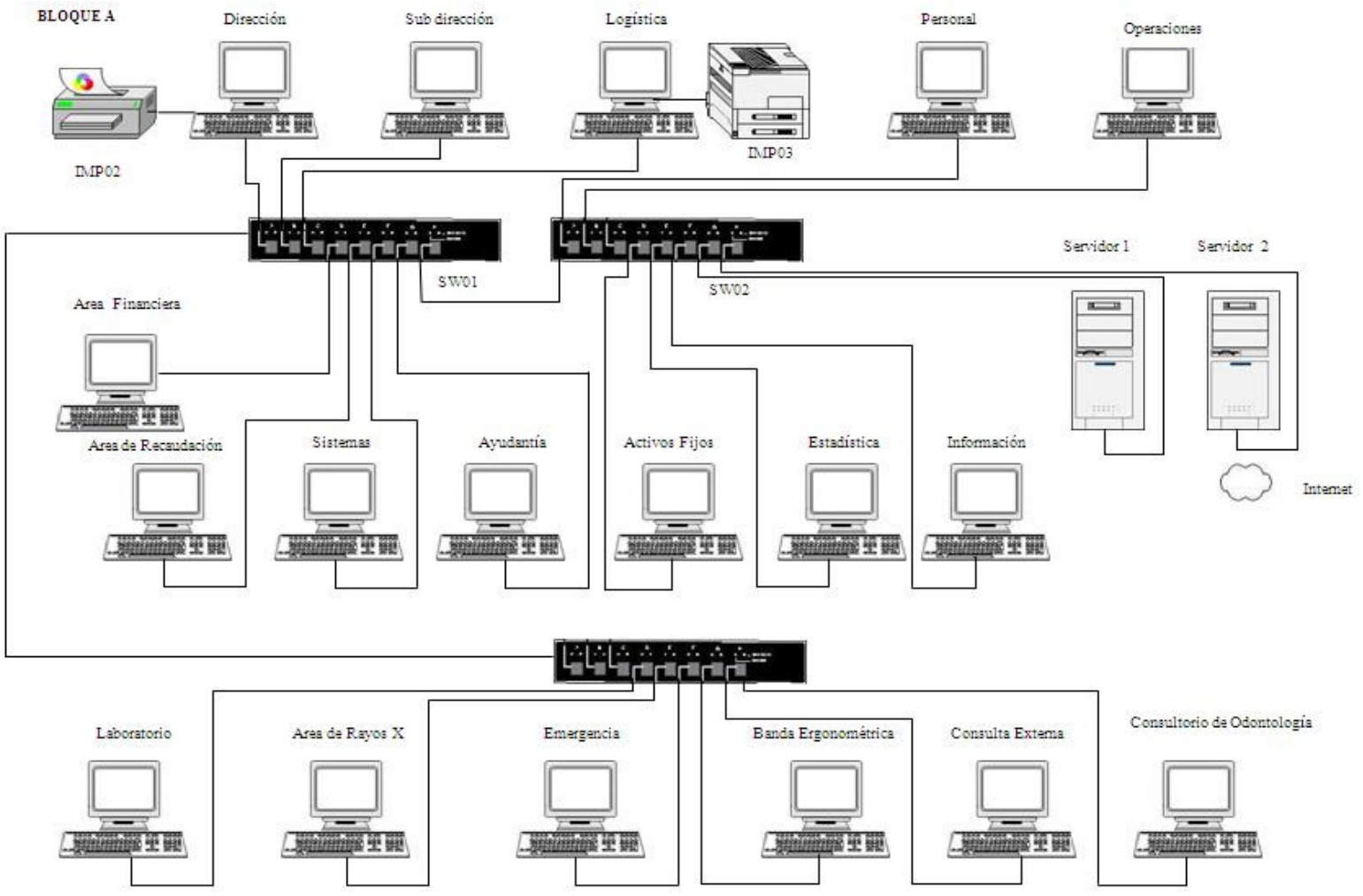


BLOQUE C



Anexo C

Diagrama de la Red del Hospital de Brigada N° 11 “Galápagos”



BIBLIOGRAFÍA

BIBLIOGRAFIA GENERAL

- **ALVAREZ, B.R**. Avances en criptología y seguridad de la información. España. Díaz de Santos. Madrid. 2009. 697p.
- **AGUILERA, P.** Seguridad Informática. 2da.ed. España. Editex. Madrid. 2008. 240p
- **AGUIRRE, J.** Seguridad Informática y Criptografía, 6ta.ed. España. Universidad Politécnica de Madrid. Madrid. 2008. 576p.
- **BORJA LAZARO, R.** Certificación de la firma digital. España. FOREM. Madrid. 2008. 500p.
- **NASH, A. DUANE, W. JOSEPH, C.** Infraestructura de clave pública. Colombia. Eder Mauricio Hernández. Bogotá. 2008. 500p.
- **SERRAT, M.** Ubuntu Linux. España. RA-MA. Madrid. 2009. 468p.
- **STALLINGS, W.** Fundamentos de seguridad en redes. 2da.ed. España. Pearson Educación. Madrid. 2008. 432p
- **LANLARD, B.** Exchange server 2008. España. ENI. Barcelona. 2008.456p

REFERENCIAS WEB

- **Cifrado**
  http://www.kriptopolis.org/cifrado-gmail-reloaded
  (2010/04/07)
- **Creación de Firmas Digitales**
  http://al93.wordpress.com/2008/04/13/crear-firmas-digitales/
  (2010/08/01)
- **Criptografía**
  http://www.scribd.com/doc/11972496/criptografia
  (2010/07/10)

- **Esquemas de autenticación de mensajes utilizando algoritmos hash**
  http://www.cujae.edu.cu/Eventos/CITTEL/Memorias/CITEL2004/Trabajos/CIT060.pdf
  (2010/08/11)
- **Fundamentos Generales de Firma Digital**
  http://en.wikipedia.org/wiki/Firma_Digital
  (2010/08/20)
- **Firma digital**
  http://dspace.ups.edu.ec/bitstream/123456789/199/4/Capitulo%203.pdf
  (2010/08/15)
- **Firma manuscrita, Firma digital**
  http://www.almendron.com/politica/pdf/2003/spain/spain_0392.pdf
  (2010/07/06)
- **Integridad y confidencialidad de la información**
  http://www.cypsela.es/especiales/pdf206/confidencialidad.pdf
  (2010/06/06)
- **Manual PKI**
  http://www.bce.fin.ec/files.php?file=./documentos/ElBancoCentral/EntidadCert/indice.htm
  (2010/07/23)
- **Protocolos de correo infraestructura de clave publica**
  http://leibniz.iimas.unam.mx/~yann/Crypto/Clase09.pdf
  (2010/05/13)