ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERÍA

DISEÑO E IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA DE CLAVES PÚBLICAS JERÁRQUICA CON CERTIFICADOS DIGITALES X.509 Y SU APLICACIÓN EN REDES 802.11 CON EL ESTÁNDAR 802.1X

TOMO I

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

SHIRMA DAYUMA ORTIZ BOADA

DIRECTOR: ING. PABLO HIDALGO

Quito, Octubre de 2006

DECLARACIÓN

Yo Shirma Dayuma Ortiz Boada, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Shirma Dayuma Ortiz Boada

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Shirma Dayuma Ortiz Boada, bajo mi supervisión.

_____

Ing. Pablo Hidalgo

DIRECTOR DE PROYECTO

AGRADECIMIENTO

A mi pequeñita (mi madre) por todo el apoyo y cariño entregado durante esta época de aprendizaje y crecimiento. A mi hermana Carola por su amistad y compañía. A mi padre y hermano, por su apoyo incondicional.

A Jorge, por estar siempre ahí, por esperar, por comprender; porque en estos cinco años has sido: mi amor, mi mejor amigo y compañero.

Al Ing. Pablo Hidalgo, por ser siempre un Maestro dentro de clases y proceder como un Padre fuera de ellas, por decir “podemos”, por haber guiado mis pasos y los de mis amigos durante nuestro paso por la Carrera de Ingeniería en Electrónica y Redes de Información.

A mis amig@s: Alexander, Álvaro, Andrés, Angie, Carlos, Criss, David (☺), Diego, Edú, Gabriel, Jady, Lore, LuchitoGG y Pablito, por su compañía y ayuda en los momentos difíciles, por saber esperar y comprender, escuchar y aconsejar y en algunos momentos incluso callar (y en otros hablar de más!).

Al Ing. Marcelo Balarezo, por su ayuda desinteresada.

Finalmente, al Ph. D. Iván Bernal y al Ing. Néstor Salazar, porque me enseñaron algo difícil de aprender en un aula, disciplina.

Gracias

DEDICATORIA

A mi Dr. Navarrete.

PRESENTACIÓN

Las redes corporativas han incrementado el uso de la tecnología inalámbrica debido a características como movilidad, traslado y rápida instalación, principalmente a nivel ejecutivo-administrativo y técnico; en cualquier caso, la información manejada por cada uno de estos grupos es importante e inclusive vital para una empresa.

Para redes corporativas, en donde se intercambia entre usuarios información estratégica crítica como: información de propiedad intelectual, estrategias de negocios, investigaciones sobre nuevos productos, información de clientes, etc., la seguridad es un asunto que debe analizarse cuidadosamente.

La comodidad ofrecida por las redes inalámbricas trae consigo un riesgo mayor al que se ven expuestas las redes cableadas, debido a que las señales de datos se trasladan por aire, lo que permite que éstas sean interceptadas fácilmente; esto se ha convertido en un gran problema de seguridad.

Por esto la implementación de una WLAN[1] (*Wireless Local Area Network*) corporativa debe contemplar estrategias que brinden un nivel razonable de seguridad, debido a que el costo que puede causar la pérdida de información crítica es elevado.

Otra tendencia que se está marcando, es la implantación de las herramientas “cero papeles”, debido a que los documentos electrónicos facilitan la búsqueda, distribución y almacenamiento de información; además, la legislación existente en el país reconoce su valor jurídico.

Con la utilización de certificados digitales se puede obtener comodidad y seguridad dentro de la red inalámbrica, mediante la utilización del estándar 802.1x; entonces, se logra procesos más ágiles al utilizar herramientas como “cero papeles”, manteniendo un nivel elevado de seguridad.

---

[1] Según la firma de investigación *Gartner Inc*. en el año 2010, el 80% de los procesos empresariales clave involucrarán el intercambio de información en tiempo real relacionada con los trabajadores móviles.

La solución propuesta provee un nivel de seguridad elevado, debido a que se realiza autenticación con certificados digitales, éstos permiten el intercambio de claves simétricas que cambian dinámicamente para cifrar cada conexión establecida. El intercambio de claves simétricas se realiza con encripción asimétrica, lo que garantiza que sólo los involucrados tendrán acceso a éstas.

La instalación de una PKI empresarial proporciona flexibilidad para la expedición de certificados digitales para miembros de la organización, clientes, socios y equipos; además, permite definir directivas propias y establecer jerarquías que admiten autoridades certificadoras por departamento, manteniendo la seguridad de la autoridad certificadora central.

Se escoge como plataforma para la implementación de la PKI el sistema operativo *Windows*, debido a que éste soporta todas las herramientas necesarias para la implementación de una PKI, presentando ventajas al disponer de documentación en varios idiomas, soporte para actualizaciones y mantenimiento, etc.; esto ha logrado que *Windows* conserve el 80 % del mercado mundial.

Otro factor para la elección de *Windows 2003 Server* como plataforma de la PKI, es que ha sido valorado internacionalmente; la *Federal Bridge Certification Authority* ha aprobado la PKI de *Microsoft* como una plataforma confiable para todas las Agencias Federales de los Estados Unidos después de rigurosas pruebas de seguridad, compatibilidad e interoperabilidad.

La opción planteada merece una inversión que se justifica para empresas en donde los usuarios que manejan terminales móviles operan datos corporativos críticos. El nivel de seguridad proporcionado es alto y además tiene un respaldo jurídico.

RESUMEN

El Capítulo inicial contiene una descripción de las principales herramientas de seguridad en redes, como: encripción, funciones *hash*, firmas y certificados digitales. Con estos conceptos se profundizará después en el estudio de PKI, tratando temas que incluyen: arquitectura, servicios prestados, modelos de confianza, aplicaciones y administración.

En el proyecto se explicará los principales conceptos concernientes a WLANs, poniendo énfasis en el estándar IEEE 802.11 por ser el predominante en el mercado. Luego, se analizarán los principales mecanismos de seguridad disponibles para WLANs, presentando una comparación basada en sus características y nivel de seguridad. El estudio se enfoca finalmente en la utilización de una PKI Jerárquica con el estándar 802.1x.

Se presenta un enfoque de la situación del país con respecto a PKI, analizando el avance en la legislación con leyes como: Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos e implicaciones en el Código Penal; la Ley y su reglamento se incluyen en el Anexo 1. Lo concerniente a la legislación vigente en el país se tratará dentro de cada sección del trabajo cuando sea conveniente.

También se estudiarán las perspectivas de PKI en el Ecuador, enfocándose en la PKI del BCE[1], su funcionamiento, los servicios que brinda, su inserción en el mercado, etc. Para la evaluación se realizó un estudio de mercado dirigido a: Administradores de la PKI, Responsables y Usuarios de certificados; los resultados obtenidos a través del estudio de mercado se encuentran registrados en los Anexos: 2, 3 y 4, respectivamente.

La implementación consta de dos partes; la primera es la configuración de la PKI Jerárquica; la segunda parte constituye la implementación de una solución de seguridad para WLANs, utilizando la PKI para la autenticación EAP-TLS[2].

---

[1] Banco Central del Ecuador.

[2] *Extensible Authentication Protocol-Transport Layer Security*.

Para la implementación de la PKI Jerárquica se utiliza como plataforma el sistema operativo *Windows 2003 Server Enterprise*; dentro de la sección concerniente a la implementación de la PKI, se detallarán sus ventajas y desventajas.

La implementación se inicia con la planeación de la PKI Jerarquía teniendo en cuenta: directrices de una empresa, arquitectura, impacto en los usuarios, administración, contenido de los certificados, modelos de confianza, operación, aspectos jurídicos, políticas y procedimientos de manejo de certificados y control de operación de las Autoridades Certificadoras.

La Autoridad Certificadora Subordinada de la infraestructura PKI solo podrá expedir certificados de entidad destino[1]; en cambio, la Autoridad Certificadora Raíz podrá expedir certificados auto-firmados y para otras Autoridades Certificadoras. La Autoridad Certificadora Raíz se mantendrá sin conexión y aislada por motivos de seguridad. La PKI diseñada cuenta con una CP[2] y una CPS[3], éstas se encuentran registradas en los Anexos 5 y 6, respectivamente.

La segunda parte de la implementación presenta una solución para seguridad en WLANs utilizando la PKI para la autenticación EAP-TLS. Se implementa un servidor RADIUS para el acceso a la red y se utilizará la PKI para la expedición de certificados.

La solución establecida está destinada a dar seguridad al segmento de red inalámbrica dentro de la red LAN por ser éste el más vulnerable, no se estudian ni se implementan mecanismos de seguridad de interconectividad de redes extremo a extremo. La solución no está destinada a una aplicación específica, si no más bien para la conectividad de la red LAN inalámbrica.

Las pruebas correspondientes a la implementación se realizarán a nivel de laboratorio. Estas pruebas se efectuarán de acuerdo a las políticas y procedimientos diseñados.

---

[1] Usuarios finales.

[2] *Certificate Policy* o Política de Certificación.

[3] *Certification Practice Statement* o Declaración de Prácticas de Certificación.

ÍNDICE DE CONTENIDO

TOMO I

CAPÍTULO 1

CAPÍTULO 3

CAPÍTULO 6

ANEXOS

GLOSARIO DE ACRÓNIMOS

Capítulo 1

SEGURIDAD EN REDES UTILIZANDO CRIPTOGRAFÍA

1. SEGURIDAD EN REDES UTILIZANDO CRIPTOGRAFÍA

1.1. INTRODUCCIÓN

En la actualidad, el uso de documentos electrónicos como una herramienta para mejorar la eficiencia en las operaciones de una empresa, se ha difundido enormemente, debido a ventajas como: rapidez en las transacciones, reducción de costos, fácil distribución y almacenamiento, etc.

Un factor que ha permitido este avance tecnológico es el Internet, el cual consigue que redes corporativas compartan información sin importar su ubicación geográfica; además, facilita la interacción con clientes y socios mediante información intercambiada electrónicamente.

Dentro de redes corporativas en todo el mundo, la información es creada, distribuida y almacenada en formato electrónico. Información estratégica como la de propiedad intelectual, patentes, estrategias de negocios, nuevos productos, clientes, etc., se intercambia con gran agilidad mediante el uso de correo electrónico u otra herramienta.

Sin embargo, para que las ventajas de los documentos electrónicos entreguen resultados favorables, se debe distinguir claramente quién puede acceder y a qué información; por ejemplo, a qué información puede acceder un cliente, qué se puede compartir entre socios, y principalmente qué información pertenece solamente a la empresa.

Y por supuesto, dentro de una red corporativa, en el sitio en el que se manejan documentos electrónicos, se debe tener un mecanismo que permita garantizar que el usuario que accede a cierta información, es quien dice ser.

1.1.1. RÉGIMEN LEGAL: MENSAJES DE DATOS

Los beneficios que brindan los documentos electrónicos no serían de tanta utilidad si no hubiera una legislación que respalde su uso. La Ley 67[1], brinda un marco jurídico en el que se establece que los documentos electrónicos tienen igual valor que los documentos escritos.

Además, la Ley determina que: “Los mensajes de datos estarán sometidos a las leyes, reglamentos y acuerdos internacionales relativos a la propiedad intelectual”, esto es importante en la medida en que se establece quien es el dueño de la información generada electrónicamente; y por lo tanto, quien tiene derecho a hacer uso de ésta.

En el Ecuador la Ley 83[2], instaura garantías sobre la propiedad Industrial[3], y estipula que salvo pacto en contrario o disposición especial, la titularidad de las obras creadas bajo relación de dependencia laboral corresponde al empleador; es decir, se reconoce como “autor” de la información generada dentro de una empresa a la persona jurídica que representa a dicha empresa.

Por lo anterior, los documentos electrónicos pueden ser utilizados en el Ecuador dentro de redes corporativas como documentos legales; reconociéndose como titular de la información almacenada en estos documentos al empleador.

Las transacciones producidas mediante el uso de documentos electrónicos tienen un carácter legal, siempre y cuando se cumpla con la legislación existente.

---

[1] Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos – Anexo 1.

[2] Ley de Propiedad Intelectual.

[3] Incluye entre otros: invenciones, información no divulgada y los secretos comerciales e industriales.

1.1.2. SEGURIDAD EN REDES

Si la información de una empresa viaja libremente por la red (*intranet*, *extranet* o Internet), ésta se encuentra desprotegida; personas internas o externas a la empresa, podrían tener acceso la información o a los recursos y hacer uso indebido de éstos, provocando perjuicios.

Para proteger la información y los recursos, se podría pensar en restringir el acceso a éstos (esconderlos). Sin embargo, el avance tecnológico alcanzado y la creciente tendencia al comercio electrónico, han logrado que las empresas estén obligadas a compartir información a través de sus redes corporativas y de Internet.

Siendo así, se debe encontrar estrategias que permitan un acceso máximo para todo aquel que tenga derecho a hacer uso de la información y de los recursos de manera lícita; por otra parte, las estrategias encontradas deben evitar estrictamente el acceso para todos los demás.

Para crear estas estrategias, la seguridad en redes provee mecanismos que garantizan que la información y los recursos se encuentren disponibles para los usuarios autorizados, guardando un nivel aceptable de protección contra intrusos o accesos ilícitos.

Para poner en práctica una política de seguridad en redes corporativas, se requiere realizar una inversión; pero por supuesto, vale la pena ya que se está protegiendo segmentos estratégicos como: la información y los recursos, y más aún, la operación de la empresa.

1.1.2.1. Definiciones

En el ámbito de la seguridad en redes se utiliza con frecuencia los siguientes términos:

a. Vulnerabilidad

Una vulnerabilidad es una debilidad (interna) de un sistema; se produce por fallas en su diseño, implementación o administración, haciendo que éste sea frágil y se vea expuesto ante amenazas.

b. Amenaza

Una amenaza es cualquier acción o evento que pueda poner en riesgo el funcionamiento de un sistema.

c. Defensa

La defensa contempla estrategias creadas para proteger un sistema o sus partes, puede implicar medidas para eliminar o reforzar vulnerabilidades.

d. Ataque

Un ataque es cualquier técnica o acción utilizada para aprovechar una vulnerabilidad; puede realizarse con la intención de encontrar vulnerabilidades y aprender de ellas. En el peor de los casos, puede tener como objetivo el robo, modificación o eliminación de información estratégica, e incluso un sabotaje a la operación de una empresa.

d.1. Tipos de Ataques

Existe dos tipos de ataques: los ataques pasivos y los ataques activos. Esta clasificación se basa en los objetivos y efectos que puede tener un ataque.

d.1.1. Ataques Pasivos

Un ataque pasivo, es aquel que no causa daños o cambios dentro de un sistema, su función en muchos casos es el aprendizaje de la estructura de una red; este tipo de ataque, se utiliza para determinar zonas críticas o vulnerabilidades del sistema.

d.1.2. Ataques Activos

Un ataque activo se realiza con la intención de producir daños en un sistema o con el fin de extraer información confidencial de una empresa. Generalmente, los ataques activos son más fáciles de detectar debido a que se registra fallas en el funcionamiento del sistema atacado.

e. Política de Seguridad

Una política de seguridad determina las reglas generales bajo las cuales debe funcionar un sistema. El detalle de cómo se pondrán en ejecución estas reglas se establece en una declaración de prácticas; ésta contiene los procedimientos relacionados con cada aspecto contemplado dentro de la política de seguridad.

La política de seguridad y la declaración de prácticas deben expresarse de manera formal en un documento. Una política de seguridad puede ser de tipo permisivo o prohibitivo. Una política de seguridad permisiva, establece que todo lo que no está expresamente prohibido, está permitido; por otro lado, una política de seguridad prohibitiva determina que todo lo que no está expresamente permitido, está prohibido.

Los componentes de una política de seguridad van a variar de acuerdo a las particularidades del sistema que se pretende proteger; por lo general una política de seguridad incluirá las siguientes secciones:

- **Presentación**.- Esta sección contiene información general de la política de seguridad.

- **Publicación**.- En esta sección se incluye información relacionada con los puntos de distribución del documento que contiene la política de seguridad.

- **Controles de Seguridad Física**.- La seguridad física está relacionada con la protección del cuarto de equipos o de los establecimientos destinados para la instalación del sistema.

- **Controles de Seguridad del Personal**.- Esta sección contiene los roles o papeles que se pueden asignar al personal para mantener la operación del sistema.

- **Recuperación en Caso de Desastre**.- Esta sección considera los posibles eventos que pueden alterar del funcionamiento del sistema, y las medidas que deben tomarse en caso de presentarse alguno.

- **Controles de Seguridad Técnica**.- Esta sección está relacionada con los elementos tecnológicos que se utilizan dentro del sistema, puede hacer referencia a módulos de *software* o *hardware*.

  Requisitos Comerciales y Legales.- De ser necesario, esta sección contiene las tarifas vigentes para la comercialización de servicios o bienes producidos a través del sistema. Además, contiene la política de confidencialidad, los derechos de propiedad intelectual, así como también las obligaciones y responsabilidad de cada elemento del sistema.

  Para finalizar, se incluye una sección en la que se hace referencia a la legislación aplicable de acuerdo al país en que se ejecute la política.

Para la creación de una política de seguridad, se debe identificar y clasificar todos los activos pertenecientes al sistema, esto permitirá realizar un análisis de riesgos para priorizar la asignación de recursos de acuerdo a la criticidad y valor de cada activo o grupo de activos.

1.1.2.2. Estrategias

Se debe considerar que por definición ningún sistema es seguro, cada sistema tiene vulnerabilidades descubiertas y ocultas; adicionalmente, existen individuos que día a

día intentan explotar dichas vulnerabilidades. Ante esta situación, cada empresa debe asumir estrategias que le permitan proteger su información, recursos y funcionamiento.

Para lograrlo se puede asumir ciertas estrategias. A continuación se da una visión de las diferentes estrategias, cada una puede ser utilizada de forma individual o en conjunto.

a. Prevención

Contempla la preparación anticipada ante actos ilícitos que puedan poner en riesgo el funcionamiento de un sistema; implica la aplicación de medidas que aseguren los recursos, éstas se deben modificar continuamente de acuerdo a las circunstancias y vulnerabilidades encontradas. Esta estrategia es la más recomendable, debido a que resulta más eficiente y efectiva.

b. Detección

Involucra un monitoreo constante, para encontrar conductas extrañas o propias de un ataque; si se detecta anomalías, se protege el sector que está siendo atacado. Es una estrategia que implica un nivel de riesgo, ya que si un ataque no es detectado a tiempo, puede causar grandes pérdidas.

c. Respuesta

Esta estrategia se relaciona con acciones y procedimientos que se deben efectuar en caso de que un sector del sistema o todo el sistema sea atacado; implica la implementación de una política de seguridad, en donde se determinen claramente los responsables de la ejecución de políticas y procedimientos. El cumplimiento estricto de la política es esencial.

Esta estrategia arriesga la operación de la empresa, pues un ataque puede haber causado pérdidas considerables antes de que se aplique el procedimiento planeado;

además, puede tratarse de un ataque nuevo, y por lo tanto, no se tendrá un plan apropiado para su contención.

1.1.2.3. Modelos

Los modelos de seguridad en redes permiten definir la forma en la que se van a proteger los recursos y la información dentro de una red. Ningún modelo garantiza la seguridad total de un sistema, los modelos pueden fallar.

a. Seguridad en la Oscuridad

Este modelo consiste en la utilización de elementos propietarios no difundidos; permite la protección del sistema debido a que los posibles atacantes no conocen el funcionamiento de dichos elementos, y por lo tanto, no conocen sus vulnerabilidades.

No es recomendable, pues una revisión abierta de cualquier sistema permite encontrar sus vulnerabilidades y por supuesto eliminarlas o reforzarlas; además, se puede descubrir el funcionamiento del sistema oculto con lo que se pierde la protección que brinda el “secreto”.

b. Perímetro de Defensa

Este modelo implica la determinación de zonas críticas. De acuerdo al nivel de criticidad de cada zona, se incluye a ésta dentro de perímetros de seguridad; en cada perímetro se implementan niveles de protección acordes con sus requerimientos.

Este modelo es vulnerable a ataques internos, debido a que los usuarios internos conocen de la existencia de zonas críticas y pueden tener acceso a éstas.

c. Defensa en Profundidad

Este modelo intenta lograr que cada parte del sistema tenga su propia frontera de seguridad; su administración resulta compleja y costosa, pues se debe establecer la mejor forma para asegurar un elemento a partir de sus particularidades.

1.1.3. SERVICIOS QUE BRINDA LA SEGURIDAD EN REDES

La seguridad en redes se encarga de brindar servicios que permiten que la información y los recursos estén disponibles para todos los usuarios lícitos y protegidos contra accesos indebidos. En esta sección se detallan los principales servicios y sus funciones.

1.1.3.1. Confidencialidad

Este servicio permite mantener la privacidad de la información; es decir, solo los usuarios que posean una autorización legítima pueden acceder y entender cierta información. Para conseguir esto, la información que se desea proteger es cifrada; de esta manera, incluso si un intruso tiene acceso a la información no podrá entender su contenido.

La Ley 67 introduce reformas al Código Penal que incluyen sanciones con prisión de seis meses a un año y una multa de quinientos a mil dólares, para los empleados que utilizando medios electrónicos violen la privacidad de la información; no se establece sanciones para atacantes externos.

Existen penas mayores para quienes obtengan información relacionada con la seguridad nacional o secretos comerciales e industriales. Si la información es divulgada las sanciones alcanzan penas de hasta seis años de prisión, con una multa de hasta diez mil dólares.

La Ley no contempla medios que garanticen el reconocimiento económico en caso de que los daños causados por la violación de la confidencialidad de los datos causen perjuicios irreparables y pérdidas económicas o de credibilidad.

1.1.3.2. Integridad

Este servicio se encarga de garantizar que la información llegue a su destino durante el tiempo que es útil y sin ningún tipo de alteración. Para lograr esto, el emisor saca un resumen de la información enviada y adjunta este resumen a la información.

En el destino el receptor separa la información del resumen y vuelve a realizar el mismo procedimiento para obtener su propio resumen; luego, compara los dos resúmenes, si coinciden, el mensaje no ha sido alterado y se puede confiar en su contenido.

Según la Ley un mensaje permanece íntegro mientras su contenido se mantenga completo e inalterado, excepto por algún cambio de formato producido durante el proceso de comunicación, almacenamiento o presentación.

En el Reglamento se limita las condiciones establecidas en la Ley, reconociendo la integridad de un mensaje de datos siempre y cuando el mensaje esté firmado electrónicamente. Esto garantiza de manera estricta el servicio de integridad, proporcionando adicionalmente autenticación del emisor.

1.1.3.3. Disponibilidad

Este servicio se relaciona con políticas de prevención contra la interrupción de la operación de un sistema. Sí las condiciones lo ameritan y se cuenta con los recursos económicos necesarios, se debe proporcionar redundancia en los sectores críticos, con el fin de corregir fallas en éstos de manera inmediata.

La disponibilidad se mide por el porcentaje de tiempo que un sistema permanece operativo con respecto al tiempo que queda deshabilitado por fallas. En caso de

interrupción se mide por el tiempo que tarda el sistema en volver a su funcionamiento normal.

La disponibilidad de un sistema puede depender del funcionamiento de una infraestructura física o del acceso a la información. Dentro de las reformas al código penal incluidas en la Ley 67, se establece penas con prisión de hasta cinco años a quien cause daños a la información almacenada electrónicamente.

Para quien cause daños a infraestructuras o instalaciones físicas, causando problemas para la transmisión o recepción de los datos, se establece penas con prisión de hasta cuatro años. De manera similar al caso de confiabilidad, la Ley no establece reposición económica en caso de pérdidas.

1.1.3.4. Identificación

Es el proceso mediante el cual se establece la identidad de un individuo en particular. Se puede identificar a personas o entidades, para esto se llevan a cabo procedimientos que garanticen que la identidad presentada corresponde a la entidad. Por ejemplo, se puede requerir la presentación de una cédula de identidad personal, pasaporte, fotografías, dirección, teléfono e incluso referencias personales.

Este servicio requiere la verificación de los datos presentados por la persona o entidad a identificar, la comprobación de dichos datos se puede realizar contactando a otras instituciones que confirmen que los datos o documentos presentados son fiables.

Al finalizar la identificación de una entidad en particular, la autoridad que ha verificado los datos, puede entregar credenciales que certifiquen que ha realizado la identificación de dicha entidad.

La autoridad que presta este servicio, debe garantizar que los datos proporcionados por una entidad serán utilizados solo dentro del proceso que permita su identificación; además, se debe garantizar que la información entregada no será divulgada.

La Ley determina que el titular de los datos puede autorizar (o no) el uso de éstos para determinados fines, garantizando de esta manera los derechos de privacidad, intimidad y confidencialidad consignados en la Constitución.

1.1.3.5. Autenticación

Es un proceso en el cual una autoridad apoyándose en credenciales o información presentadas por una entidad verifica su identidad; requiere que otra autoridad haya expedido previamente las credenciales presentadas o que la información relacionada con la entidad se encuentre registrada y sea factible su verificación.

Por ejemplo, para identificar a una persona utilizando una cédula de identidad, se requiere que previamente una autoridad A[1] haya emitido dicha cédula; para la autenticación se revisa que la fotografía y la firma de la persona concuerden las registradas en la cédula.

La Ley 67, en su artículo 10 establece que: “Salvo prueba en contrario se entenderá que un mensaje de datos proviene de quien lo envía”, esto se reconoce siempre y cuando la verificación entre el emisor y su firma electrónica resulte exitosa.

El requerir de una firma electrónica para realizar la autenticación del emisor de un mensaje implica la implementación de una infraestructura; esta infraestructura requiere una inversión y no todas las empresas están interesadas o poseen los recursos necesarios.

---

[1] La autoridad A se encargó previamente de la identificación de la persona.

En el caso de personas naturales, resulta más complicado, debido a que en el país al momento no existe una infraestructura reconocida legalmente que posibilite el manejo de firmas electrónicas.

a. Técnicas de Autenticación

Se tiene varias técnicas de autenticación, cada una brinda determinado nivel de seguridad e implica una inversión. La seguridad encontrada no se mide por la cantidad de recursos invertidos en cada técnica, sino por la forma en que se aplica y protege.

a.1. Secretos Compartidos

Se utiliza en sistemas que no requieren mayor seguridad, al aplicar esta técnica el sistema realiza una o varias preguntas y si el usuario conoce las respuestas queda autenticado.

Debido a que más de un usuario puede conocer una respuesta en particular, para asegurar que los usuarios que ingresan al sistema sean legítimos, se puede requerir una verificación con más de una pregunta.

a.2. Contraseñas

Es la técnica de autenticación más difundida, se trata de relacionar a un nombre o identificador de usuario con una contraseña. Para ingresar a un sistema el usuario ingresa su identificador y su contraseña, si existe correspondencia el usuario queda autenticado.

La contraseña no debería viajar por la red en texto plano[1], y por supuesto, el usuario no debería revelar[2] su contraseña a otros usuarios o almacenarla en un lugar visible o accesible para intrusos, esto implica capacitación.

---

[1] Información que no ha pasado por ningún proceso de encripción.

[2] "Un *password* debe ser como un cepillo de dientes. Úsalo cada día; cámbialo regularmente; y NO lo compartas con tus amigos." Cristian F. *Borghello*.

Hay que considerar que las contraseñas definidas por los usuarios generalmente no tienen suficiente aleatoriedad; por otro lado, si se imponen reglas como longitud o inclusión de caracteres, las contraseñas resultan difíciles de memorizar, por lo cual los usuarios tienden a escribirlas en lugares que resultan fáciles de detectar para los intrusos.

Otro problema se presenta debido a que los usuarios utilizan la misma contraseña en diferentes sistemas; y claro está, no todos los sistemas tienen el mismo nivel de criticidad.

a.3. *Tokens*

Esta técnica utiliza pequeños dispositivos llamados *tokens* para la autenticación. En la figura 1.1, se muestra un *token* tipo llavero, existen también modelos que se asemejan a tarjetas inteligentes.

Figura 1.1 Token

Un *token* tiene almacenada una semilla única, ésta permite que cada dispositivo genere un conjunto único de números seudo-aleatorios; entonces se identifica a un usuario por el conjunto de números que puede generar su *token*. Cada número se genera una sola vez de acuerdo a las condiciones del momento.

Cada *token* se relaciona con un PIN (*Personal Identification Number*), éste cumple una función similar a la de las contraseñas; para la autenticación un servidor verifica que el nombre de usuario, el PIN y el número generado pertenezcan al mismo usuario, en caso de éxito, se completa el proceso de autenticación.

a.4. Tarjetas inteligentes

Las tarjetas inteligentes son dispositivos compuestos por un microprocesador, memorias (RAM, ROM y EEPROM[1]), un armazón y opcionalmente un acelerador criptográfico; cuentan con un sistema operativo, el mismo que es almacenado en la memoria ROM.

La memoria RAM es utilizada para realizar cálculos, la memoria EEPROM es utilizada para almacenar nombres de usuarios, contraseñas y en general datos que permitan obtener información del usuario portador de la tarjeta. Al igual que los *tokens*, requieren de una contraseña o PIN para la autenticación.

a.5. Biometría

Esta técnica consiste en medir ciertos rasgos físicos de un usuario; por ejemplo, huellas dactilares, rostro, voz, el iris del ojo, etc. Su consistencia radica en que los datos biométricos son únicos para cada usuario.

De acuerdo al rasgo seleccionado se crea una plantilla, ésta contiene las principales características que se van a tomar en cuenta para el registro de los datos; es decir, no se registra todo el patrón biométrico. Registrar solo ciertas características permite mantener datos compactos.

Una característica de la biometría es que "es una credencial irrevocable[2]", esto quiere decir que aunque un usuario deje de pertenecer a un sistema, el siempre tendrá sus rasgos biométricos.

Aun más, el usuario puede autenticarse en diferentes sistemas con el mismo rasgo (¡misma contraseña en sistemas con diferente nivel de seguridad!); por esto y por su

---

[1] *Electrically Erasable Programmable Read-Only Memory*, esta memoria permite borrar e ingresar datos, no requiere de energía para conservar los datos almacenados.

[2] NASH, Andrew. PKI-Infraestructura de Claves Públicas. Capítulo 9, página 374.

característica de irrevocables, los registros biométricos deben estar cifrados y protegidos contra intrusos.

La estructura de un sistema biométrico es compleja; sin embargo, para los usuarios presenta gran facilidad de uso, debido a que no requiere que éstos tengan un nivel de conocimientos o que memoricen claves complicadas.

b. Factores de Autenticación

Para la verificación de una identidad se debe tener un procedimiento acorde con el nivel de seguridad requerido. Los esquemas de seguridad contemplan la combinación de diferentes técnicas de autenticación (algo que se conoce, algo que se tiene y algo que se es) para alcanzar un nivel aceptable de seguridad.

- **Factor-1**.- Este factor de seguridad contempla la utilización de una sola técnica de autenticación; por ejemplo, contraseñas, biometría o secretos compartidos. Es el esquema de autenticación más difundido debido a que requiere menos recursos.

- **Factor-2**.- El factor-2 utiliza una combinación de dos técnicas basadas en “algo que se conoce”, “algo que se tiene” o “algo que se es”; esta combinación garantiza un mayor nivel de seguridad.

- **Factor-3**.- Este nivel de autenticación implica la combinación de tres técnicas: “algo que se conoce”, “algo que se tiene” o “algo que se es”; su implementación requiere de una mayor inversión.

1.1.3.6. Control de Acceso

Este servicio consiste en autorizar a usuarios lícitos el acceso a recursos e información de acuerdo a su perfil. Adicionalmente, determina lo que está permitido

dentro de un sistema; existen usuarios que tienen privilegios y otros que tienen restricciones.

1.1.3.7. Aceptación

Este servicio permite garantizar que un usuario no pueda negar que realizó determinada acción. Para garantizar este servicio, se necesita que los mensajes contengan un registro del tiempo en que fueron enviados y recibidos; además deben estar firmados digitalmente.

La Ley reconoce el Sellado de tiempo (registro de tiempo), siempre y cuando los mensajes sean enviados a través de una entidad acreditada por el CONATEL. Al realizar el sellado de tiempo, se debe anexar al mensaje la hora y fecha exacta en que el mensaje de datos fue recibido por la entidad acreditada; y la fecha y hora exacta en la que el mensaje fue entregado al destinatario.

El reconocimiento del sellado de tiempo permite proteger sistemas en los que se realizan transacciones críticas. La inversión requerida para acceder a este tipo de tecnología será necesaria dentro de empresas que manejen patentes o información de propiedad intelectual; también cuando se realicen transacciones que involucren grandes sumas de dinero.

1.2. CRIPTOGRAFÍA

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.

La criptografía se divide en dos ramas, la criptología y el criptoanálisis. La criptología se encarga del desarrollo de nuevos y mejores algoritmos que permitan realizar una encripción más robusta.

El criptoanálisis en cambio, se encarga de desarrollar y utilizar herramientas que prueben los algoritmos desarrollados por los criptólogos. Su objetivo es encontrar vulnerabilidades en los algoritmos con el fin de “romper” los textos cifrados con éstos.

Éste es un proceso cíclico, cuando los criptoanalistas encuentran debilidades en el diseño de cierto algoritmo, se informa a los criptólogos; éstos trabajan con la información encontrada para eliminar o reforzar las vulnerabilidades de sus algoritmos, luego de lo cual los entregan para un nuevo análisis.

Los desarrolladores de algoritmos no pueden tener en cuenta todos los escenarios o ataques; con el trabajo en conjunto se verifica el nivel de seguridad proporcionado por cada algoritmo y al encontrar sus debilidades se los puede modificar. Este proceso ha logrado que los algoritmos que prevalecen se fortalezcan.

1.2.1. ENCRIPCIÓN

La encripción es la técnica que permite cifrar un mensaje de datos mediante el uso de algoritmos criptográficos. Al cifrar un mensaje, se obtiene confidencialidad de la información; además, con el uso de la encripción, se puede lograr integridad, autenticación y aceptación.

1.2.1.1. Criptosistema

Un criptosistema es un sistema de encripción que está formado por los elementos que forman parte del proceso y permite cifrar y descifrar mensajes; los algoritmos

utilizados dentro de un criptosistema deben garantizar que el proceso de encripción sea eficiente y seguro.

Los algoritmos son públicos, la seguridad del sistema reside en el secreto de la clave con la que se realiza el cifrado; dicho de otra manera, la fortaleza de un sistema criptográfico radica en la imposibilidad computacional de encontrar la clave que se utiliza para cifrar.

Un criptosistema está formado por los siguientes elementos:

- **Espacio de Mensajes.-** Está compuesto por los elementos y reglas que permiten crear un mensaje legible (en texto plano).

- **Espacio de Textos Cifrados.-** Está formado por todos los elementos y reglas que permiten crear un mensaje cifrado.

- **Espacio de Claves.-** Está compuesto por todas las claves que se pueden utilizar para cifrar o descifrar un mensaje con un algoritmo específico.

- **Transformaciones de Cifrado y Descifrado.-** La transformación de cifrado es la aplicación de una clave sobre un mensaje en texto plano, con el fin de convertirlo en un texto cifrado. La transformación de descifrado es el proceso inverso.

De acuerdo a la forma en la que se realiza la encripción de los datos, se puede tener criptosistemas basados en bloque y basados en flujo. Los criptosistemas basados en bloque trabajan con unidades de datos de longitud fija; por su parte los criptosistemas basados en flujo trabajan cifrando símbolo a símbolo, letra a letra ó palabra a palabra.

1.2.1.2. Elementos a Considerar para las Técnicas de Encripción

Existen dos técnicas de encripción, la encripción simétrica y la asimétrica. Cada técnica utiliza claves y algoritmos para el proceso de encripción. En esta sección se da una visión sobre los elementos que se deben considerar en el momento de seleccionar un algoritmo y la longitud de una clave.

a. Algoritmos

Un algoritmo de encripción determina cómo se modifican los datos para transformar un texto plano en un texto cifrado. El emisor (quien cifra) y el receptor (quien descifra), tienen que utilizar el mismo algoritmo; además, el emisor debe poseer la clave que le permita cifrar el mensaje y el receptor debe poseer una clave adecuada para descifrarlo.

Un algoritmo determina además el tamaño de la clave que se puede utilizar en el proceso de encripción; el o los tamaños soportados determinan cuan seguro es el algoritmo. Se puede considerar a un algoritmo como “seguro” cuando ha soportado criptoanálisis exhaustivo, y se ha comprobado que resulta imposible descifrar un texto sin la posesión de la clave con la que fue cifrado.

b. Claves

Una clave es como una llave, si se cifra con ésta (se cierra) un texto plano; el texto cifrado, solo puede ser descifrado (abierto) utilizando la misma clave o una clave que guarde cierta relación matemática con la clave que participó en el proceso de encripción.

La longitud de la clave es muy importante, si una clave tiene una longitud de 64 *bits*, se tienen teóricamente 2^{64} (18446744073709551616) posibles combinaciones; en cambio, una clave con una longitud de 1024 *bits*, llega a tener hasta 2^{1024} combinaciones ($1{,}79*10^{308}$ posibles claves).

Un atacante que pretenda encontrar una clave, necesita grandes cantidades de recursos para lograr su objetivo; estadísticamente debe probar por lo menos el cincuenta por ciento de todo el espacio de claves antes de encontrar la clave adecuada y lograr descifrar un mensaje.

Asimismo, el tamaño de una clave determina el nivel de procesamiento que debe realizar un equipo para cifrar y descifrar. Por supuesto, el procesamiento utilizado para cifrar y descifrar un mensaje conociendo la clave, es insignificante comparado con el procesamiento requerido para encontrar una clave que permita descifrar un mensaje.

c. Generadores de Números Aleatorios

La generación de números aleatorios es usada durante la creación de claves. Los generadores de números aleatorios cumplen con la función de entregar secuencias de unos (1) y ceros (0); con una característica, en cada punto, el siguiente *bit* no puede ser descubierto basándose en el *bit* anterior.

Un generador de números aleatorios con un mal diseño, puede excluir ciertas combinaciones y generar otras con más frecuencia; entonces, se reduce el espacio de claves. Es por esto que el número de claves que se puede generar de acuerdo a una longitud determinada es teórico.

Si se utiliza un generador de números aleatorios deficientemente, éste no cubre todo el espacio de claves, causando dos problemas. En primer lugar, resulta menos complicado encontrar una clave; en segundo lugar, muestra un nivel de seguridad irreal.

d. Administración de Claves

Los métodos de administración de claves son muy importantes y tienen que ver con la generación segura de éstas, su distribución y almacenamiento. Una vez que se

genera una clave aleatoria, ésta debe mantenerse en secreto. Es necesario crear políticas en donde se detalle claramente el procedimiento a seguir durante la vida útil de las claves, para que los usuarios no introduzcan vulnerabilidades relacionadas con prácticas inadecuadas.

1.2.2. ENCRIPCIÓN SIMÉTRICA

La encripción 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 1.2 muestra el proceso de encripción 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.

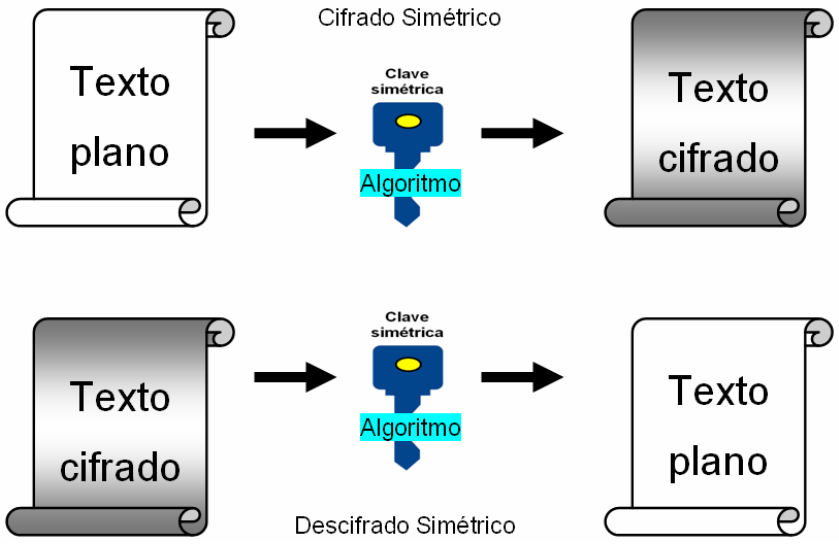

Figura 1.2 Encripción Simétrica

La encripción 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.

1.2.2.1. Administración de claves Simétricas

La generación de una clave para cada comunicación que se inicie con cada receptor introduce un problema de administración de claves. Se debería garantizar que la clave con la que se cifró una sesión sea almacenada de forma segura, para que se pueda identificar con facilidad la clave que se utilizó para cifrar una comunicación en particular.

Si se asume que no se requiere un nivel de seguridad excesivo y que por lo tanto solo se tendrá una clave por cada receptor, se debe tener un mecanismo que garantice que las claves están protegidas y que solo los involucrados en una comunicación podrán descifrar un mensaje en particular.

Pero incluso, en un sistema en el que se genera una clave por cada pareja (emisor-receptor), se tiene una gran cantidad de claves. Por ejemplo, dentro de un sistema en donde se cuente con 4 participantes, se debe generar una clave para cada pareja; esto implica doce claves.

En un sistema que utilice encripción simétrica, el número de claves que se genera es igual al número de participantes (N) multiplicado por el número de participantes menos uno (N -1); casi el cuadrado del número de participantes.

Otro aspecto importante a considerar es el intercambio de las claves simétricas. Cuando se inicia una comunicación, alguien debe generar la clave y entregársela al otro participante; después de lo cual los datos enviados serán cifrados con la clave generada, conviene conseguir una vía segura para el intercambio de claves.

¿Pero, cómo transferir la clave con seguridad? En realidad, al utilizar sólo encripción simétrica, la única forma de transferir la clave es en texto plano; por lo cual, si ésta es enviada por una red, puede ser interceptada por un atacante.

También podría transferirse mediante dispositivos de almacenamiento; el inconveniente aquí es que para garantizar que solo el emisor y el receptor tienen acceso a la clave, éstos deberían reunirse para intercambiarla.

Si se trata de una comunicación que se realizará por una sola ocasión, sería mejor que se entregue el mensaje directamente. Sin embargo, si se va a realizar más de una comunicación y se puede realizar el encuentro, ésta sería la mejor forma de garantizar el acceso exclusivo a la clave; en muchos casos, dicho encuentro será complicado.

A pesar de mostrar una complicada administración de claves, la encripción simétrica brinda un excelente nivel de seguridad siempre y cuando se mantenga el secreto de la clave; consume menores recursos en comparación con la encripción asimétrica, ofreciendo un nivel de seguridad similar, con claves de menor tamaño.

1.2.2.2. Ventajas y Desventajas

a. Ventajas

Entre las principales ventajas de la encripción simétrica, con respecto a la encripción 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 de fuerza bruta que una clave asimétrica de mayor tamaño.
- La encripción simétrica consume menores recursos. La encripción simétrica es 100 veces más rápida si se realiza en sistemas basados en *software* y hasta 10000 veces más rápida en sistemas basados en *hardware*[1].
- La encripción simétrica garantiza la confidencialidad de la información.

b. Desventajas

Entre las principales desventajas de la encripción simétrica, con respecto a la encripción 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 encripción simétrica es aproximadamente el cuadrado del número de participantes.
- Debido a que se utiliza la misma clave para cifrar y descifrar, la encripción simétrica no permite la utilización de firmas digitales.
- No se puede garantizar integridad de los mensajes utilizando encripción simétrica.

1.2.2.3. Algoritmos Criptográficos Simétricos

Entre los algoritmos simétricos más difundidos se tiene a DES, 3-DES, IDEA, CAST, RC4 y AES.

---

[1] KOMAR, Brian. *Windows Server 2003 PKI Certificate Security*. *Microsoft Press*. Estados Unidos. 2004.

a. DES (Data Encryption Standard)

Es uno de los mejores algoritmos simétricos y ha sido ampliamente utilizado. Fue creado por IBM[1] a finales de los 70; su implementación original se diseñó para realizar los procesos de encripción sobre *hardware*.

Fue declarado como estándar X9.52 por la ANSI[2] y reconocido por el NIST[3] en 1977[4]. Ratificado como estándar oficial por las agencias federales de Estados Unidos en 1983, 1988, 1993 y 1999, luego de lo cual se asumió una transición en la que se utilizó 3-DES; finalmente, fue reemplazado por AES.

Este algoritmo utiliza encripción en bloque, cada bloque tiene una longitud de 64 *bits*, con claves de 64 *bits* para la encripción. Cada clave cuenta con un *bit* de paridad por cada *byte*, por lo que la longitud real de la clave es de 56 *bits*.

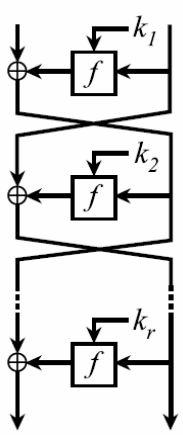

Figura 1.3 Ciclos Feistel[5]

Durante la encripción genera 16 ciclos, en cada ciclo se cifra un bloque con una subclave obtenida de la clave simétrica. Su característica principal es que para

---

[1] *International Business Machines*.

[2] *American National Standards Institute.*

[3] *National Institute of Standards and Technology.*

[4] FIPS PUB 46-3: *Data Encryption Standard* (DES).

[5] RSA *Laboratories*. *RSA Laboratories' Frequently Asked Questions About Today's Cryptography, v4.0*. 1998.

descifrar un mensaje, se utiliza el mismo procedimiento y las mismas subclaves; esto se conoce como encripción *Feistel*. En la figura 1.3 se ilustra el proceso.

La clave simétrica DES, puede ser utilizada dentro de un proceso de comunicación para cifrar y descifrar un mensaje o para generar y verificar un código de autenticación de mensaje[1]. DES puede ser utilizado también por un solo usuario, para cifrar datos almacenados en un disco duro al que tengan acceso múltiples usuarios.

Debido al tamaño limitado de su clave, DES ha sido roto. Se ha demostrado que con una inversión de un millón de dólares en equipo sofisticado, se puede encontrar la clave simétrica en aproximadamente tres horas y media.

b. 3-DES (triple DES)

3-DES proporciona mayores niveles de seguridad que DES. Se ejecuta el proceso de encripción sobre un texto plano utilizando DES, la diferencia es que el proceso se efectúa tres veces sobre el mismo mensaje.

Existen tres métodos para implementar 3-DES:

- Tres cifrados DES utilizando tres claves diferentes.
- Tres operaciones DES manteniendo la secuencia cifrado-descifrado-cifrado con tres claves diferentes.
- Se mantiene el método anterior, con una diferencia, se utiliza la misma clave al cifrar.

El utilizar distintas claves durante el proceso de cifrado-descifrado-cifrado proporciona mayor nivel de seguridad.

---

[1] MAC (*Message Authentication Code*).

c. IDEA (Internacional Data Encryption Algorithm)

IDEA forma parte de los algoritmos simétricos que utilizan encripción en bloque; cada bloque tiene una longitud de 64 *bits* con claves de 128 *bits* para la encripción. Fue creado por *Swiss Federal Institute* a inicios de los noventa y desde su desarrollo teórico ha sido analizado y discutido ampliamente.

El proceso de encripción contempla ocho ciclos complejos en donde se utiliza subclaves; las subclaves empleadas para el proceso de descifrado son generadas a partir de las subclaves de cifrado. La seguridad de IDEA se basa en el uso de tres tipos de operaciones aritméticas en las que se maneja palabras de 16 *bits*.

Su estructura de encripción fue diseñada para ser fácil de implementar sobre *software* o *hardware*. Sin embargo, algunas de las operaciones aritméticas consumen demasiados recursos cuando se genera la encripción sobre *software*; como resultado, la velocidad de IDEA al implementarse sobre *software* es similar a la de DES.

IDEA ha pasado exitosamente el criptoanálisis y se lo considera un algoritmo seguro; además, no tiene prohibiciones de exportación debido a que fue desarrollado fuera de los Estados Unidos.

d. CAST (Carlisle Adams, Strafford Travares)

Este algoritmo fue creado por *Carlisle Adams* y *Strafford Travares*. Se basa en encripción en bloque, establece bloques de 64 *bits*. Las claves pueden tener una longitud variable entre 40 *bits* y 256 *bits*.

Fue patentado por *Entrust Technologies* y se mantuvo entre los 15 algoritmos candidatos para reemplazar a DES como estándar oficial para la encripción en los Estados Unidos.

e. RC4 (Rivest Cipher # 4)

RC4 es un algoritmo basado en encripción continua, fue diseñado por *Ron Rivest* de RSA[1] *Data Security*. Soporta claves de longitud variable con operaciones orientadas a *byte*. El algoritmo se basa en permutaciones[2] randómicas; por cada *byte* cifrado se requiere de ocho a dieciséis operaciones de máquina, por lo que su implementación sobre *software* se considera adecuada.

Criptoanalistas independientes a RSA *Laboratories*[3] han analizado el algoritmo y es considerado seguro, existe una condición especial para la exportación fuera de Estados Unidos, por lo que puede ser utilizado con facilidad.

f. AES (Advanced Encryption Standard)

En enero de 1997[4], el NIST anunció la decisión de encontrar un estándar sucesor para DES; en septiembre del mismo año, se convocó a un concurso en donde el estándar ganador sería nombrado AES y registrado como norma federal FIPS[5] 197 de los Estados Unidos.

El proceso de selección finalizó en el 2000. *Rijndael* fue el ganador del concurso y ahora es conocido como AES, este estándar reemplazó a DES como norma dentro de los Estados Unidos. Maneja encripción en bloque, con bloques de 128 *bits*, usando claves de 128 (AES-128), 192 (AES-192) y 256 (AES-256) *bits*.

Rijndael fue diseñado para manejar tamaños de bloque adicionales, sin embargo éstos no se adoptaron como parte de la norma.

---

[1] RSA-*Rivest, Shamir* y *Adelman*.

[2] Alterar el orden de los símbolos siguiendo cierta regla.

[3] Sector de RSA dedicado al criptoanálisis.

[4] RSA *Laboratories*. *RSA Laboratories' Frequently Asked Questions About Today's Cryptography, v4.0*. 1998.

[5] *Federal Information Processing Standards.*

La norma incluye las siguientes secciones:

- Definiciones, acrónimos, parámetros del algoritmo, símbolos y funciones.
- Notación y convenciones utilizadas para la descripción del algoritmo, incluyendo el orden y la numeración de *bits*, *bytes* y palabras.
- Propiedades matemáticas útiles para el entendimiento del algoritmo.
- Descripción del algoritmo, en donde se exponen temas como cifrado y rutinas de descifrado.
- Implementación, en donde se especifica la longitud de la clave y restricciones; también se establecen longitudes de bloque y claves adicionales.

La norma finaliza con varios apéndices que incluyen ejemplos para la implementación del algoritmo. El NIST espera mantener este algoritmo como norma oficial durante los próximos veinte o treinta años.

g. NMC Stream

NMC *Stream* fue creado por el ecuatoriano Néstor Marroquín Carrera; este algoritmo simétrico opera bajo la modalidad de los criptosistemas basados en flujo. Para su funcionamiento utiliza un generador de números seudo-aleatorios que recibe como semilla una clave simétrica de longitud *n*, ésta tiene por defecto una longitud de 240 *bits* y puede incrementarse en múltiplos de 30 *bytes*.

El algoritmo está basado en las definiciones hechas en 1917 por *Mauborgne* y *Vernam*. Durante el proceso de encripción el generador de números aleatorios crea cadenas arbitrarias de longitud *n*/3, estas cadenas son combinadas con el mensaje original aplicando una función XOR (OR exclusivo).

Hasta el momento, el único ataque que se considera posible es el de fuerza bruta; de otra manera, resulta computacionalmente inviable[1] descifrar un texto cifrado sin la posesión de la clave simétrica.

[1] NMC Research. Algoritmo NMC Stream, Descripción y Formalización. Febrero 2004.

1.2.3. ENCRIPCIÓN ASIMÉTRICA

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

La encripción 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 encripción 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. En las figuras 1.4 y 1.5 se muestran las posibles secuencias para cifrar y descifrar un texto plano utilizando encripción asimétrica.

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.

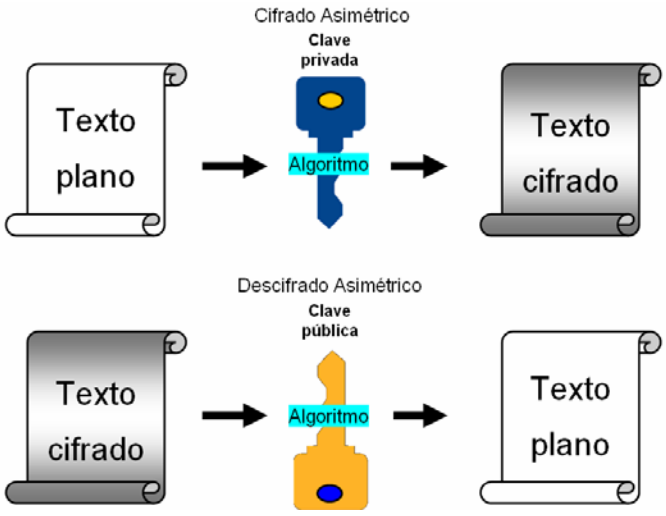

Figura 1.4 Encripción Asimétrica: cifrado con clave privada, descifrado con clave pública

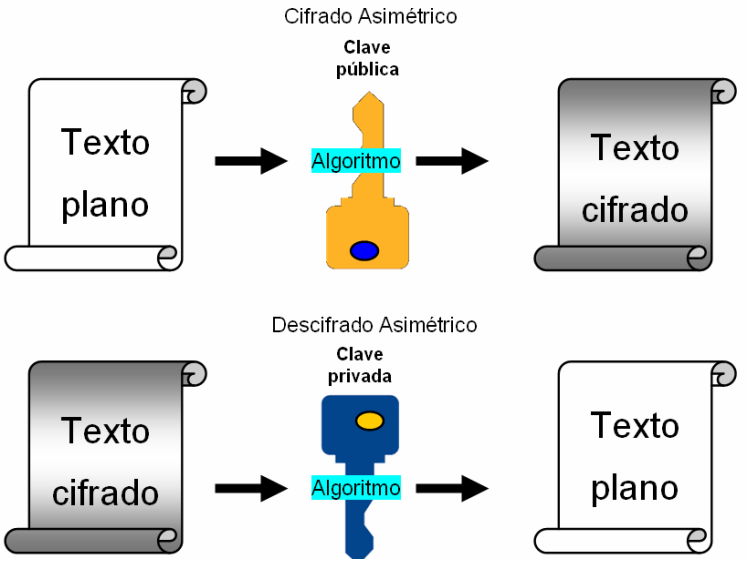

Figura 1.5 Encripción Asimétrica: cifrado con clave pública, descifrado con clave privada

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.

Para garantizar confidencialidad en una comunicación entre un emisor y un receptor se seguirá la siguiente secuencia:

1. El emisor consigue la clave pública del receptor.
2. El emisor cifra el mensaje utilizando la clave pública del receptor.
3. Se envía el mensaje cifrado, éste solo puede descifrarse con la clave privada del receptor; por lo tanto, solo el receptor tendrá acceso al mensaje en texto plano.
4. El receptor descifra el mensaje utilizando su clave privada.

Si se desea garantizar la autenticación en una comunicación entre un emisor y un receptor se seguirá la siguiente secuencia:

1. El emisor cifra el mensaje con su clave privada.
2. Se envía el mensaje cifrado[1].
3. El receptor consigue la clave pública del emisor.
4. El receptor descifra el mensaje utilizando la clave pública del emisor. Al descifrar el mensaje con la clave pública del emisor, se determina que fue cifrado con su clave privada. Se garantiza que el emisor envió el mensaje[2].

Para garantizar confidencialidad y autenticación en una comunicación entre un emisor y un receptor se seguirá la siguiente secuencia:

1. El emisor consigue la clave pública del receptor.
2. El emisor cifra el mensaje M1 con su clave privada, genera el mensaje M2.
3. El emisor cifra el mensaje M2 utilizando la clave pública del receptor, genera el mensaje M3.
4. Se envía el mensaje M3.
5. El receptor consigue la clave pública del emisor.
6. El receptor descifra el mensaje M3 utilizando su clave privada (confidencialidad), obtiene el mensaje M2.
7. El receptor descifra el mensaje M2 utilizando la clave pública del emisor (autenticación), obtiene el mensaje M1.

El emisor podría invertir el orden de cifrado; primero cifrar el mensaje utilizando la clave pública del receptor, luego cifrar con su clave privada; pero, ¿para qué darle información de quien envió el mensaje a un posible atacante? Un sistema se mantendrá más seguro mientras menos información se revele de su funcionamiento.

---

[1] El mensaje podrá descifrarse solo con la clave pública del emisor. Debido a que la clave pública está disponible para todos los usuarios, todos podrán descifrar el mensaje y establecer quien lo envió.

[2] Solo el emisor tiene acceso a la clave privada; por lo tanto, se realiza la autenticación.

1.2.3.1. Administración de Claves Públicas y Claves Privadas

La administración de claves es un tema trascendental. Cuando se maneja encripción asimétrica, se genera una pareja de claves por cada usuario; todos los participantes intercambian su clave pública, este número de claves, permite una administración menos compleja. Ahora, cada usuario debe almacenar un número de claves públicas igual al número de participantes y proteger su clave privada.

Las claves públicas pueden estar disponibles teóricamente para todos los usuarios; sin embargo, es una práctica recomendable restringir el acceso, de modo que solo los interesados accedan a las claves.

Debe existir una zona en la que los usuarios puedan obtener las claves públicas de los otros usuarios y publicar su propia clave pública, al estilo de un directorio telefónico, para que los usuarios legítimos sean capaces de obtener de manera inequívoca las claves públicas de otros usuarios.

Por otra parte, se debe evitar que un intruso cambie las claves públicas almacenadas en un directorio o que suplante a un usuario legítimo intercambiando la clave pública del usuario por su clave pública.

La administración de las claves privadas es más crítica, de acuerdo al propósito para el que se generaron las claves. Sí una clave privada fue generada con el propósito de cifrar datos y realizar firmas digitales, se requiere que estrictamente esté solo al alcance de quien generó la clave.

Por otra parte, si las claves se generan con el único propósito de cifrar la información, puede ser necesario crear una copia de la clave privada y almacenarla en una base de datos de claves; de esta manera si la clave se pierde, se puede acceder a la copia y recuperar la información cifrada.

La base de datos de claves debe estar cifrada; para acceder a ésta, es recomendable establecer condiciones en las que dos o más administradores ingresen su contraseña.

1.2.3.2. Ventajas y Desventajas

a. Ventajas

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

- La administración de claves asimétricas tiene menor complejidad.
- El número de claves involucradas en un sistema que utiliza encripción 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 encripción asimétrica no es susceptible a interceptación de claves.
- La encripción asimétrica permite la utilización de firmas digitales.
- La encripción asimétrica es la base del comercio electrónico.
- La encripción asimétrica sirve como herramienta para lograr el servicio de aceptación.
- Con encripción asimétrica se puede garantizar confidencialidad y autenticación.
- Utilizando encripción asimétrica se puede garantizar la integridad de los mensajes.

b. Desventajas

Entre las principales desventajas de la encripción asimétrica, con respecto a la encripción 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 encripción asimétrica consume mayores recursos.
- Requiere de claves de mayor tamaño para brindar el mismo nivel de seguridad.

En la tabla 1.1 se muestra información sobre el tiempo requerido para encontrar una clave de encripción simétrica, encripción de curva elíptica y de encripción RSA[1]. Para este experimento se considera que se cuenta con un presupuesto de 10 millones de dólares y que cada *Mbyte* de memoria cuesta 50 centavos de dólar.

Clave simétrica	Clave EC	Clave RSA	Tiempo para encontrar la clave	Número de máquinas	Memoria requerida
56	112	430	Menos de 5 min.	10^5	Cualquiera
80	160	760	600 meses	4300	4 GB
96	192	1020	3 millones de años	114	170 GB
128	256	1620	10^{16} años	.16	120 TB

Tabla 1.1 Comparación de la Fortaleza de claves simétricas, EC y RSA[2]

1.2.3.3. Algoritmos Criptográficos Asimétricos

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

a. Diffie-Hellman

Whitfield Diffie y *Martin Hellman* realizaron la primera publicación acerca del algoritmo en el año 1976[3], la publicación llevaba el nombre "*New Directions in Cryptography*".

---

[1] Estas técnicas de encripción se estudiarán en la siguiente sección.

[2] RSA *Laboratories. A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths.* Robert D. Silverman. Abril 2000.

[3] IEEE *Information Theory Society Newsletter*. Marzo 2004.

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.

Para que dos usuarios puedan generar una clave, en primer lugar, el emisor y el receptor acuerdan dos parámetros públicos *p* y *g*. El parámetro *p* es un número primo elevado y el parámetro *g* (llamado generador) es un entero menor que *p*.

Cada usuario genera su propio número aleatorio; a partir de los dos valores públicos y el número aleatorio de cada uno, se calcula un valor público que se puede compartir. Ambos participantes intercambian el valor generado y a partir de los dos resultados, cada individuo calcula por su cuenta la clave con la que se cifrará la sesión.

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 cuando el número primo *p* es suficientemente grande.

b. RSA (Rivest, Shamir, Adelman)

RSA *Data Security* fue creado por *Ron Rivest*, *Adi Shamir*, y *Leonard Adleman* de RSA *Security* en 1977[1]; este algoritmo garantiza los servicios de autenticación (firmas digitales) y confidencialidad (cifrado). El proyecto RSA *data security* fue financiado parcialmente con fondos del gobierno de Estados Unidos, su patente se declaró el 29 de septiembre de 1983 y expiró el 29 de septiembre del 2000.

El algoritmo se basa en que resulta fácil multiplicar dos números primos muy elevados, pero la operación inversa resulta complicada. Así, el algoritmo toma dos números primos elevados *p* y *q*, luego calcula su producto *n=p*q*; *n* toma el nombre de módulo.

---

[1] *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.* RSA-1997.

Entonces, se escoge un número *e*, menor que *n* y que se acerque al producto (*p*-1)(*q*-1), de tal manera que *e* y (*p*-1)(*q*-1) no tengan un factor común excepto 1. Luego, se encuentra otro número *d* tal que (d - 1) es divisible para (*p*-1)(*q*-1). El valor *e* es conocido como exponente público y al valor *d* como exponente privado.

Para la generación de la clave pública se utiliza la pareja (*n*, *e*), y para la clave privada (*n*, *d*). Los factores *p* y *q* deben ser guardados con la clave privada o destruidos. Este proceso garantiza un gran nivel de dificultad para encontrar la clave privada a partir de la clave pública.

Un atacante puede descifrar un texto cifrado solo si logra encontrar los números *p* y *q* o la clave privada. Sí la clave es protegida adecuadamente, la única forma sería entonces encontrar los números *p* y *q*, por esto se recomienda utilizar claves con una longitud de 1024 *bits* para datos importantes y de 2048 *bits* para datos críticos.

Otro método para romper RSA es utilizar técnicas avanzadas basadas en la matemática del algoritmo; para este ataque se requieren mayores recursos y se logra descifrar un mensaje sin necesidad de la clave privada. Este proceso se realiza para descifrar un mensaje en particular.

En la práctica, la mayor parte de los ataques tiene éxito, no por las debilidades del algoritmo, sino más bien, por una debilidad en una aplicación insegura o un mal manejo de la clave privada.

c. DSA (Digital Signature Algorithm)

Fue publicado dentro del estándar DSS (*Digital Signature Standard*) como parte del proyecto *Capstone*[1] en 1994. DSS fue seleccionado por el NIST en cooperación con

[1] *Capstone* es un proyecto del gobierno de Estados Unidos, en el que se desarrollan normas para la criptografía a largo plazo, las agencias responsables del proyecto son el NIST y el NSA.

la NSA[1], para ser el estándar de autenticación (firmas digitales) del gobierno de Estados Unidos. Inicialmente DSA fue creado para manejar claves de 512 *bits*; luego el NIST reviso el estándar y 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.

DSA se basa en cálculos de algoritmos discretos, centrándose en ciertos subgrupos. Este método no ha recibido hasta ahora ataques importantes. Los ataques exitosos se presentan cuando se usa generadores aleatorios con diseños deficientes.

d. ECC (Elliptic Curve Cryptography)

La encripción de curva elíptica fue propuesta inicialmente por *Victor Miller* y *Neal Koblitz* a mediados de 1980[2]. El estándar plantea que los algoritmos asimétricos pueden generarse reemplazando la aritmética modular por funciones definidas en curvas elípticas.

Estos algoritmos se pueden basar en productos de números primos o en algoritmos discretos. Los sistemas basados en productos consumen cantidades semejantes de recursos que los sistemas RSA, brindando una seguridad equivalente. Los sistemas basados en algoritmos discretos consumen menores recursos y logran niveles similares de seguridad.

Para la encripción, se selecciona dos puntos *G* y *H* en una curva elíptica tal que *H = kG*; luego se calcula el entero *k*. Este método es mucho más eficiente que otros métodos; como resultado, claves de menor tamaño brindan el mismo nivel de

[1] *National Security Agency.*

[2] *Elliptic Curve Cryptosystems*. Mugino Saeki.

seguridad consumiendo menores recursos. Los sistemas basados en encripción de curva elíptica por el momento, sólo son vulnerables a ataques de fuerza bruta.

1.2.4. COMBINACIÓN ENTRE ENCRIPCIÓN SIMÉTRICA Y ENCRIPCIÓN ASIMÉTRICA

La encripción simétrica garantiza el servicio de confidencialidad. En cambio, la encripción asimétrica garantiza los servicios de autenticación, confidencialidad e integridad; adicionalmente permite el uso de firmas digitales y bajo ciertas condiciones puede cumplir incluso con el servicio de aceptación.

Por otra parte, la encripción asimétrica es de 100 a 10000 veces más lenta que la encripción simétrica, aumenta el tamaño de los mensajes y requiere de claves de mayor tamaño para garantizar la misma resistencia.

Se obtiene mejores resultados al combinar la encripción simétrica y la encripción asimétrica. Si se desea garantizar la autenticación y confidencialidad en una comunicación, consumiendo menores recursos y aprovechando las ventajas de cada técnica, se seguirá la siguiente secuencia:

1. El emisor genera una clave simétrica aleatoria *s*.
2. El emisor consigue la clave pública del receptor.
3. El emisor cifra la clave simétrica *s* con su clave privada, genera el mensaje *S*.
4. El emisor cifra el mensaje *S* utilizando la clave pública del receptor, genera el mensaje *S1*.
5. Se envía el mensaje *S1*.
6. El receptor consigue la clave pública del emisor.
7. El receptor descifra el mensaje *S1* utilizando su clave privada (confidencialidad de la clave simétrica), obtiene el mensaje *S*.

8. El receptor descifra el mensaje *S* utilizando la clave pública del emisor (autenticación), obtiene la clave simétrica *s*.
9. Cuando el emisor y el receptor tienen la clave simétrica, los dos pueden empezar una comunicación cifrada con encripción simétrica (confidencialidad de los datos).

Como la clave simétrica tiene un tamaño reducido (128 *bits*), utilizar encripción asimétrica no afecta de gran manera el consumo de recursos, manteniendo la confidencialidad de la clave simétrica y logrando autenticación. Además, se elimina el problema de interceptación de las claves simétricas.

La clave simétrica generada se utiliza solo para esta comunicación; luego se descarta por lo que se elimina también el problema de administración de claves simétricas.

1.3. 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 encripción asimétrica, se puede garantizar el servicio de integridad de los datos, el establecimiento de firmas digitales y el sellado de tiempo.

1.3.1. PROPIEDADES

Una función *hash* debe cumplir con las siguientes propiedades: facilidad de cálculo, unidireccionalidad, compresión, difusión, reserva y resistencia a colisión.

- **Facilidad de Cálculo**.- Una función *hash*, debe ejecutar operaciones que generen un resultado de manera rápida y sin consumir demasiados recursos para cualquier entrada (mensaje).

- **Unidireccionalidad**.- La unidireccionalidad es la propiedad que garantiza que una función *hash* se puede realizar solamente en una vía; es decir, si se aplica una función *hash* a un mensaje en particular y se obtiene un valor *hash a*, debe resultar computacionalmente imposible encontrar el mensaje a partir del valor *a*.

- **Compresión**.- La compresión garantiza que no importa el tamaño del documento[1] al que se aplique la función *hash*, el resultado tendrá una longitud fija y menor al tamaño del documento. De esta manera no se revela el tamaño real del documento y el valor *hash* ocupa recursos limitados al ser enviado por la red.

  Esta propiedad se logra dividiendo al documento en bloques de longitud fija; si es necesario, se agrega *bits* en el último bloque. Luego se aplica la función a cada bloque obteniendo un resumen de cada uno. Se unen los resúmenes y se vuelve a realizar el mismo proceso; al final se obtiene un resumen con una longitud determinada.

- **Difusión**.- El valor *hash* debe ser el resultado de cálculos aplicados a todo el documento o mensaje original.

- **Reserva**.- Esta propiedad garantiza que al aplicar una función *hash* a un mensaje determinado, el valor *hash* obtenido, no revelará nada del mensaje original; por lo tanto, no se puede encontrar el mensaje a partir del valor *hash*.

---

[1] El documento puede tener cualquier tamaño.

- **Resistencia a Colisión**.- Se tienen dos tipos de resistencias a la colisión: el primero se conoce como resistencia a colisión simple y el segundo como resistencia a colisión fuerte.

  La resistencia a colisión simple, garantiza que si se conoce un mensaje *X* y se aplica una función *hash* al mensaje, es computacionalmente imposible encontrar un mensaje *Y* (diferente de *X*) que produzca el mismo valor *hash*.

  La resistencia a colisión fuerte, garantiza que es computacionalmente difícil, encontrar dos mensajes que al ser transformados por la misma función *hash* den como resultado el mismo valor *hash*.

1.3.2. INTEGRIDAD DE LOS DATOS

Con el uso de funciones *hash* y encripción 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.

Si se desea enviar un mensaje *m* y garantizar el servicio de integridad, se seguirá la siguiente secuencia:

1. El emisor obtiene el valor *hash h* del mensaje *m*.

2. El emisor cifra el valor *hash h* con su clave privada, genera el mensaje *H*[1].
3. El mensaje *H* y el mensaje *m* son agrupados y forman el mensaje M.
4. Se envía el mensaje M.
5. El receptor consigue la clave pública del emisor.
6. El receptor recibe el mensaje M y lo separa obteniendo el mensaje *H* y el mensaje *m*.
7. El receptor descifra el mensaje *H* utilizando la clave pública del emisor (autenticación), obtiene *h*.
8. El emisor aplica la función *hash* al mensaje *m* y obtiene su valor *hash h'*.
9. El emisor compara *h* con *h'*, si son iguales[2], comprueba la integridad del mensaje *m*.
10. Si descubre que el mensaje fue cambiado, puede pedir una retransmisión.

Si se desea enviar un mensaje *m* y garantizar los servicios de autenticación, confidencialidad e integridad, se seguirá la siguiente secuencia:

1. El emisor genera una clave simétrica aleatoria.
2. El emisor obtiene el valor *hash h* del mensaje *m*.
3. El emisor cifra el mensaje *m* con la clave simétrica y genera el mensaje M.
4. El emisor consigue la clave pública del receptor.
5. La clave simétrica y el valor *hash h* son agrupados, forman el mensaje M1.
6. El emisor cifra el mensaje M1 con su clave privada, genera el mensaje M2.
7. El emisor cifra el mensaje M2 utilizando la clave pública del receptor, genera el mensaje M3.
8. Los mensajes M y M3 son agrupados, forman el mensaje M4.
9. Se envía el mensaje M4.

---

[1] También se incluye información del algoritmo *hash* que se usó para obtener el valor *hash*, de esta manera el receptor sabrá qué algoritmo usar para verificar la integridad de los datos.

[2] Puesto que *h* fue cifrado con la clave privada del emisor y nadie más tiene acceso a ésta, si los valores *h* y *h'* son iguales, significa que el mensaje recibido fue el enviado.

10. El receptor consigue la clave pública del emisor.
11. El receptor recibe el mensaje M4 y lo separa obteniendo los mensajes M y M3.
12. El receptor descifra el mensaje M3 utilizando su clave privada (confidencialidad de clave simétrica y valor *hash h*), obtiene el mensaje M2.
13. El receptor descifra el mensaje M2 utilizando la clave pública del emisor (autenticación), obtiene el mensaje M1 (la clave simétrica y el valor *hash h*).
14. El receptor separa el mensaje M1, obtiene la clave simétrica y el valor *hash h*.
15. El receptor descifra el mensaje M con la clave simétrica (confidencialidad de los datos) y obtiene el mensaje *m*.
16. El receptor aplica la función *hash* al mensaje *m* y obtiene su valor *hash h'*.
17. El receptor compara *h* con *h'*, si son iguales, comprueba la integridad del mensaje *m*.
18. Si descubre que el mensaje fue cambiado en el camino, puede pedir una retransmisión.

Este proceso se puede realizar para un mensaje o para varios mensajes. Si se van a intercambiar varios mensajes el procedimiento es similar, la diferencia radica en que la clave simétrica sólo se envía con el primer mensaje; luego, se cifra toda la comunicación con la clave simétrica, enviando con cada mensaje su valor *hash*.

Siguiendo este procedimiento se garantiza los servicios de confidencialidad, integridad y autenticación de manera eficiente; el uso de encripción asimétrica no consume demasiados recursos debido a que las longitudes de la clave simétrica y el valor *hash* se encuentran alrededor de 128 *bits* cada una.

1.3.3. PRINCIPALES FUNCIONES *HASH*

Existen dos categorías de algoritmos *hash* altamente difundidos; en primer lugar los MD# creados por RSA y en segundo lugar la serie SHA incorporada en el proyecto *Capstone*.

1.3.3.1. MD# (*Message Digest* #)

Los algoritmos *hash* MD2, MD4, y MD5 fueron creados por *Ron Rivest* de RSA *Security* en 1989, 1990 y 1992, respectivamente. 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.

Esta familia de algoritmos puede recibir como entrada mensajes de cualquier longitud entregando valores *hash* de 128 *bits*. La descripción de los tres algoritmos se encuentra documentada en los RFCs (*Request for Comment*) 1319, 1320 y 1321.

MD2 confirma que la longitud del mensaje en *bits* sea divisible para 16[1], si es necesario aumenta *bits* en el final del mensaje. A continuación, agrega al final del mensaje un bloque de 16 *bits* de *checksum* (verificación). MD2 ha mostrado debilidades de colisión cuando no agrega el valor *checksum*.

MD4 verifica la longitud del mensaje en *bits* sea divisible para 512. Luego se agrega 64 *bits* en donde se representa la longitud original del mensaje. El mensaje se procesa en bloques de 512 *bits*, sometiendo cada bloque a tres ciclos de cálculos. MD4 presenta también vulnerabilidad de colisión.

MD5 es una versión mejorada de MD4, es ligeramente más lento pero en compensación es más seguro. El algoritmo maneja bloques de 512 *bits*, cada bloque es sometido a cuatro ciclos de cálculos. Se han encontrado vulnerabilidades de colisión en MD5.

---

[1] Trabaja con bloques de 16 *bits*.

1.3.3.2. SHA (*Secure Hash Algorithm*)

SHA es el algoritmo reconocido como estándar *hash* seguro por el NIST (FIPS 180); este estándar forma parte del proyecto *Capstone* y fue publicado en 1994. Es ligeramente más lento que MD5 y su diseño es similar al de MD4. Presenta mayor resistencia ante ataques de fuerza bruta.

SHA-1 (FIPS 180-1) es la revisión de SHA, se encuentra registrado como norma ANSI X9.30. El algoritmo trabaja sobre mensajes de menos de 2^{64} *bits* entregando valores *hash* con una longitud de 160 *bits*; tiene mayor resistencia a colisión.

El estándar actual (FIPS 180-2) especifica cuatro variaciones para la representación de los datos, SHA-1, SHA-256, SHA-384 y SHA-512; cuando un mensaje tiene una longitud menor que 2^{64} se ocupa SHA-1 y SHA-256, en cambio si el tamaño del mensaje es menor a 2^{128} se ocupa SHA-384 y SHA-512.

En la tabla 1.2 se muestran los valores característicos de cada variación del algoritmo SHA.

Algoritmo	Longitud del Mensaje	Tamaño del Bloque	Optimización para procesadores	Longitud del valor *hash*
SHA-1	$<2^{64}$	512 *bits*	32 *bits*	160 *bits*
SHA-256	$<2^{64}$	512 *bits*	32 *bits*	256 *bits*
SHA-384	$<2^{128}$	1024 *bits*	64 *bits*	384 *bits*
SHA-512	$<2^{128}$	1024 *bits*	64 *bits*	512 *bits*

Tabla 1.2 Valores característicos de las variaciones de SHA

El estándar actual fue publicado en agosto de 2002; se encuentra vigente como norma desde febrero de 2003 y está limitado a las restricciones de exportación establecidas por las agencias federales de los Estados Unidos para datos técnicos y dispositivos de encripción.

1.4. FIRMAS DIGITALES

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

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 encripción 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.

El uso de firmas digitales es de suma importancia para el desarrollo del comercio electrónico, pues permite que un usuario asuma la titularidad de cierta transacción. Si un emisor desea firmar digitalmente (autenticación) un mensaje *m* y enviar el mensaje a un receptor, debe seguir los siguientes pasos:

1. El emisor obtiene el valor *hash h* del mensaje *m*.
2. El emisor cifra el valor *hash h* con su clave privada, genera el mensaje *H*.
3. Los mensajes *m* y *H* son agrupados, forman el mensaje M (el mensaje ha sido firmado digitalmente).
4. Se envía el mensaje M.
5. El receptor consigue la clave pública del emisor.
6. El receptor recibe el mensaje M, lo separa y obtiene los mensajes *m* y *H*.
7. El receptor descifra el mensaje *H* utilizando la clave pública del emisor (autenticación-verifica la firma digital), obtiene el valor *hash h*.
8. El receptor aplica la función *hash* al mensaje *m*, obtiene su valor *hash h'*.
9. El receptor compara *h* con *h'*, si son iguales, comprueba la integridad del mensaje *m* y la firma digital del emisor.

Para garantizar la confidencialidad de los datos, se debe cifrar el mensaje con la clave pública del receptor.

1.4.1. SERVICIO DE ACEPTACIÓN

Las firmas digitales garantizan de manera limitada el servicio de aceptación, debido a que un usuario puede realizar cierta transacción, firmar digitalmente el mensaje producto de la transacción y posteriormente negarlo argumentando que su clave privada se vio comprometida o fue falsificada.

Para garantizar de mejor manera el servicio de aceptación, se creó el concepto de sellado de tiempo. Para esto, un tercer usuario recibe el mensaje producto de la transacción y verifica la firma digital; si la firma corresponde al emisor, adjunta al mensaje la fecha y hora exacta en la que recibió el mensaje.

La hora anexada al mensaje debe ser firmada digitalmente por el tercero; esto garantiza que la hora no será adulterada. De esta manera, se tiene el respaldo de la firma digital del emisor con la fecha y hora en que se emitió la transacción.

1.4.2. RÉGIMEN LEGAL: FIRMAS DIGITALES

Según la Ley un mensaje se considera firmado electrónicamente, siempre y cuando la clave privada haya estado bajo el manejo exclusivo de su titular y la firma electrónica sea enviada simultáneamente con el mensaje; indica además que si un usuario firma electrónicamente un mensaje, éste aprueba el contenido de éste.

La firma digital está limitada al modelo de encripción asimétrica; mientras que la firma electrónica abarca un concepto más amplio en el que se puede incluir otro tipo de técnicas como por ejemplo la biometría. El establecer el concepto de firma electrónica en lugar de firma digital mantiene la neutralidad tecnológica.

En Ecuador, una firma electrónica tiene los mismos efectos que una firma manuscrita; por lo tanto, su titular tiene las mismas obligaciones que establece la ley para el empleo de la firma manuscrita; con esto los documentos electrónicos tienen un valor legal igual al de su contraparte en papel.

La duración de una firma electrónica es indefinida, pero ésta puede ser revocada, anulada o suspendida; sin embargo, la extinción de una firma “no exime a su titular de las obligaciones previamente contraídas derivadas de su uso”. Además, una firma electrónica puede ser extinguida por voluntad, fallecimiento o incapacidad de su titular, disolución o liquidación de la persona jurídica propietaria de la firma y por causa judicialmente declarada.

El usuario titular de una firma electrónica tiene obligaciones, éstas se determinan en el artículo 17 de la Ley; entre otras se indican las siguientes:

- El titular es responsable de establecer medidas de seguridad que eviten el uso indebido de su firma electrónica.
- Debe notificar a terceros en caso de que su firma electrónica se vea comprometida.
- Debe responder por el uso indebido de su firma electrónica; excepto si su firma fue comprometida, incluso si el titular “no hubiere actuado con la debida diligencia”.

Al establecer políticas de seguridad dentro de una empresa se debe introducir a la par capacitación para los usuarios; si las políticas involucran firmas digitales, la capacitación debe incluir información sobre el régimen legal vigente.

1.5. CERTIFICADOS DIGITALES

Hasta el momento, no se ha resuelto el problema de la suplantación de usuarios o de sus claves públicas. Un certificado digital [1], provee un mecanismo que permite obtener un mejor nivel de resistencia a la suplantación.

[1] Es una técnica de autenticación.

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, protegiéndola de suplantación o alteración.

Por otra parte, se brinda un ambiente más amigable para los usuarios; debido a que ya no se tiene que buscar en un directorio la clave pública de un usuario en particular, ahora se podrá descargar su certificado digital.

Las recomendaciones para la generación de certificados digitales se encuentran registradas en la norma UIT-T[1] X.509, esta norma contiene información sobre la sintaxis de los certificados digitales y nombres distinguidos[2].

En la actualidad se encuentra vigente la tercera versión (X.509v3), ésta se aprobó en 1996. 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[3] versión.

1.5.1. FORMATO DEL CERTIFICADO

Como se ve en la figura 1.6, un certificado digital real almacena información adicional como fecha de expedición y expiración, nombre de la AC (Autoridad Certificadora[4])

---

[1] Unión Internacional de Telecomunicaciones: Sector de Normalización de las Telecomunicaciones.

[2] Es el nombre que se registra en el certificado para identificar a un usuario de forma única. Un nombre distinguido contiene información del nombre de su propietario. También puede contener atributos que identifiquen funciones del usuario de acuerdo a su perfil; además, puede indicar un nivel dentro de una jerarquía.

[3] La norma X.509v3 no establece un algoritmo criptográfico en particular; sin embargo, un anexo informativo describe el algoritmo de RSA.

[4] Entidad que emite el certificado digital.

que emitió el certificado y su firma, número de serie; en ocasiones, se encuentra información sobre los propósitos para los que fue creado.

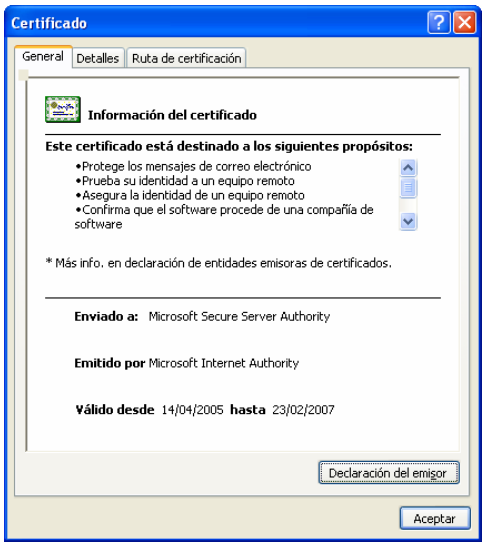

Figura 1.6 Certificado Digital Real

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.

1.5.1.1. Campos Predeterminados

En la figura 1.7 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 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 AC.

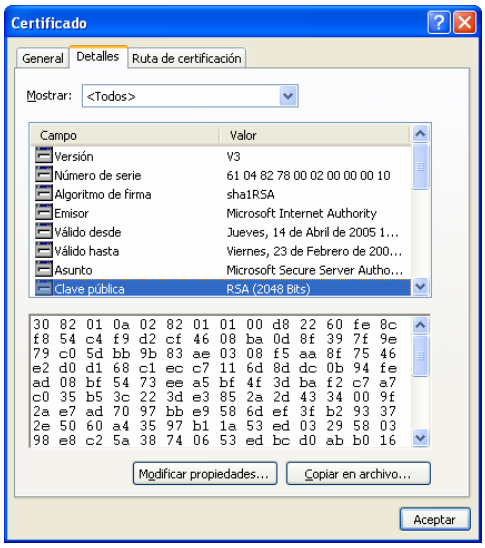

Figura 1.7 Información registrada en un Certificado Digital Real

- **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 AC de forma única, se puede habilitar opcionalmente para las versiones 2 y 3 del estándar.

- **Extensiones**.- Este campo permite agregar información adicional manteniendo el formato del estándar.

a. Extensiones de Certificado

El uso de extensiones en un certificado permite agregar información específica acerca del propósito del certificado, se tienen diferentes grupos de extensiones.

a.1. Indicadores de Carácter Crítico

Este indicador especifica si el campo de extensiones debe considerarse crítico o no; en caso de que se haya marcado como crítico, es necesario realizar las verificaciones que permitan asegurar la validación del certificado.

a.2. Extensiones de Claves

Este grupo de extensiones proporciona información sobre las claves usadas por la AC y por el propietario del certificado; adicionalmente incluye restricciones sobre el manejo de las claves.

a.3. Extensiones de Directiva

Este grupo permite establecer directivas que indican la forma en que se debe manejar el certificado. Puede incluir detalles sobre circunstancias en las que un certificado puede usarse de cierta manera; también incluye restricciones de uso.

a.4. Extensiones de Información del Propietario y Expedidor del Certificado

Este grupo contiene extensiones que proporcionan información sobre alias o diferentes esquemas de nombres que pueden ser utilizados por la AC o por el titular del certificado.

a.5. Extensiones de Restricción de Ruta del Certificado

Este grupo de extensiones presenta información sobre la potestad de una AC de expedir certificados digitales para otras ACs; si estas extensiones se encuentran

marcadas en un certificado, restringen a la AC a expedir certificados con una longitud de ruta menor a la suya.

Dentro de este grupo de extensiones se encuentra la extensión *BasicConstraints*; esta extensión determina la longitud de ruta. La longitud de ruta fija el número de niveles de ACs subordinadas. Si el campo está marcado como crítico y la longitud de ruta es igual a cero, la AC solo puede generar certificados para usuarios finales.

Si la ruta es diferente de cero, el número registrado indica el máximo número de niveles de ACs subordinadas, antes de que en un nivel una AC subordinada llegue a tener una longitud de ruta igual a cero y por lo tanto solo pueda expedir certificados para usuarios finales. Este campo se marca como crítico, de no ser así, se considera que el certificado pertenece a un usuario final.

Figura 1.8 Ruta de un Certificado

La extensión *PolyConstraints* establece restricciones para que certificados emitidos por ACs subordinadas cumplan con directivas aceptables. La norma recomienda marcar este campo como crítico, pero no es un requisito.

1.5.2. RÉGIMEN LEGAL: CERTIFICADOS DIGITALES

La Ley 67 define a un certificado de firma electrónica como un: “mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada”. Según la Ley, un certificado digital tiene como fin legitimar la identidad de su titular; sin embargo, no limita su uso exclusivamente para la autenticación.

El formato establecido contempla todos los campos incluidos en el estándar X.509; adicionalmente, se exige información sobre la ubicación domiciliaria de la AC y del titular del certificado, así como de manera obligatoria se debe incluir en un certificado su propósito o restricciones de uso.

La duración de un certificado digital se puede establecer libremente entre la AC y su titular, por defecto se establece una vida útil de dos años. Un certificado puede ser extinguido por solicitud de su titular, extinción de la firma electrónica o expiración.

Si el titular de un certificado digital solicita su extinción, ésta es reconocida desde el momento en que se comunica a la AC que expidió el certificado. Se contempla también casos especiales; por ejemplo, en caso de muerte o secuestro del titular, la extinción o suspensión del certificado se darán inmediatamente.

Dentro del Capítulo concerniente a Certificados Digitales, la ley establece libertad para que los usuarios acuerden entre sí el uso de determinados tipos de firmas electrónicas y certificados; con esto, si dos instituciones concuerdan en el uso de determinada tecnología, ésta será reconocida.

Capítulo 2

SEGURIDAD EN REDES LAN INALÁMBRICAS

2. SEGURIDAD EN REDES LAN INALÁMBRICAS

2.1. ASPECTOS GENERALES DE LAS REDES INALÁMBRICAS

El incremento de dispositivos portátiles e inalámbricos es más común día a día, debido a sus ventajas; los usuarios encuentran en este tipo de tecnologías la posibilidad de desplazarse sin permanecer ligados a un sistema cableado.

Los fabricantes por su lado crean nuevos productos, esforzándose por encontrar diseños que permitan mayor movilidad con un mínimo consumo de batería. Una muestra de esto es el Safari Tecnológico[1] de la revista *PCWorld*, en el que se incluyen varios productos portátiles e inalámbricos, éstos se muestran en la figura 2.1.

Figura 2.1 Dispositivos inalámbricos y herramientas[2]

[1] PCWorld. Safari tecnológico-guía de compras. Diciembre 2004.

[2] De 23 productos "sobresalientes" para el año 2005, la revista *PCWorld* incluye 16 dispositivos portátiles de los cuales 8 pueden interactuar con redes inalámbricas.

El desarrollo alcanzado se ve reflejado también en el incremento en el uso de redes inalámbricas, debido a que éstas proporcionan a los usuarios la capacidad de mantener una comunicación durante periodos considerables de tiempo[1] y desde su ubicación geográfica.

2.1.1. CARACTERÍSTICAS Y DESAFÍOS

Desde su creación las redes inalámbricas han logrado avances significativos, las velocidades de transmisión y la duración de las baterías se han incrementado, por lo que se encuentran difundidas en el mundo entero.

Las redes inalámbricas usan como medio de transmisión el aire, esto permite que un usuario transmita y reciba datos mientras se desplaza, facilitando conexiones en sitios donde no existe cableado.

Presentan gran flexibilidad cuando se requieren infraestructuras temporales o en lugares donde resulta complicada la instalación del cableado. La adición de nuevos usuarios no demanda modificación de la red existente por lo que resulta sencilla.

Por el momento, el uso de redes inalámbricas no ha superado al de las redes cableadas, esto se debe a que las redes cableadas ofrecen mayores velocidades de transmisión, proporcionan mejores niveles de seguridad y son menos costosas. A pesar de sus limitaciones, las redes inalámbricas han logrado posesionarse como un complemento de las redes cableadas y en algunos casos como una alternativa.

Al instalar una red inalámbrica es importante brindar los mismos servicios encontrados dentro de una red cableada y con un desempeño equivalente, para esto se debe tener en cuenta los siguientes aspectos:

---

[1] El tiempo de la comunicación se encuentra limitado por la duración de las baterías.

- La distancia que se puede cubrir con una potencia aceptable de señal no mantiene un radio constante, debido a interferencias originadas por otras ondas o por la presencia de obstáculos.
- La duración de las baterías de los dispositivos móviles debe cubrir las necesidades de los usuarios; la capacidad de desplazamiento se ve ligada a la duración de las baterías.
- En las redes inalámbricas las señales viajan por el aire y pueden ser interceptadas fácilmente, por lo que se requiere implementar mecanismos que brinden niveles aceptables de seguridad.
- La velocidad de transmisión es menor que la encontrada en redes cableadas tradicionales y tiende a disminuir a medida que un usuario se aleja de la estación base.
- Se requiere equipos diseñados bajo estándares con el fin de lograr compatibilidad entre equipos de diferentes fabricantes.
- La cobertura proporcionada por una red inalámbrica sólo se puede determinar al realizar pruebas.
- Aunque no se ha comprobado, se piensa que las señales emitidas dentro de una red inalámbrica pueden causar daños a la salud; la FCC[1], recomienda cumplir con límites de exposición, manteniendo una distancia mínima de 20 cm. entre las antenas y el cuerpo de una persona.

2.1.2. TIPOS DE REDES INALÁMBRICAS

Esta clasificación se la hace tomando como referencia el área de cobertura proporcionada por cada tipo de red.

[1] *Federal Communications Commission.*

2.1.2.1. WWAN (*Wireless Wide Area Networks*)

Las redes inalámbricas de área extendida son aquellas que operan en un área de cobertura que abarca grandes regiones, estas regiones llegan a cubrir países o partes de continentes. Las WWAN proporcionan velocidades de transmisión bajas, que oscilan entre 10 y 300 Kbps.

Entre las WWAN más difundidas se encuentran las redes de telefonía celular, siendo las más populares, las que utilizan como plataforma la tecnología GSM (*Global System for Mobile Communications*).

2.1.2.2. WMAN (*Wireless Metropolitan Area Networks*)

Son aquellas que proporcionan cobertura en áreas que abarcan ciudades o *campus*; generalmente se utilizan para brindar servicios de última milla.

El IEEE [1] aprobó en abril del 2002 el estándar 802.16 [2]; el estándar admite comunicaciones *fullduplex* cubriendo varios kilómetros con velocidades de transmisión de 50, 100 y hasta 150 Mbps, de acuerdo al tipo de modulación empleada y a la distancia desde la antena transmisora.

2.1.2.3. WLAN (*Wireless Local Area Networks*)

Las redes inalámbricas de área local cubren áreas pequeñas como oficinas, edificios, *campus*, etc.; su cobertura está limitada a segmentos locales. Dispositivos como PCs de escritorio, *laptops*, impresoras, PDAs (*Personal Digital Assistant*), etc., acceden a estas redes mediante una tarjeta de red inalámbrica.

---

[1] *Institute of Electrical and Electronic Engineers*.

[2] *Air Interface for Fixed Broadband Wireless Access Systems.*

El IEEE creó el estándar 802.11 para la implementación de este tipo de redes, éste es uno de los estándares más difundidos en el mundo y define velocidades de transmisión de hasta 54 Mbps.

2.1.2.4. WPAN (*Wireless Personal Area Networks*)

Este tipo de redes cubren segmentos de corto alcance dentro del área de una PC. En general, se utilizan para conectar accesorios o dispositivos periféricos; por ejemplo, teclados, *mouses*, impresoras, celulares, etc. Las WPANs tienen velocidades de transmisión limitadas, actualmente llegan a velocidades de hasta 1 Mbps.

Uno de los estándares más difundidos es *Bluetooth*, creado por las empresas *Ericsson*, IBM, *Intel*, *Nokia* y *Toshiba*. Estas empresas emitieron la primera versión del estándar en julio de 1999; luego, el IEEE aprobó en el año 2002 el estándar 802.15, el cual contempla las especificaciones para el diseño de redes de área personal y se basó en el estándar *Bluetooth*.

2.1.3. VENTAJAS Y DESVENTAJAS

En el momento de seleccionar un tipo de tecnología es necesario establecer los beneficios que ésta brinda y sus posibles falencias; de acuerdo a esto se pueden tomar decisiones considerando los requerimientos de los usuarios.

2.1.3.1. Ventajas

Entre las principales ventajas de las redes inalámbricas, con respecto a las redes cableadas, se pueden mencionar:

- La movilidad, ya que un usuario puede mantener una comunicación mientras se desplaza.

- No se requiere que los usuarios permanezcan conectados a un sistema cableado (depende de la duración de las baterías).
- Permiten fácil escalabilidad, un usuario puede ingresar a la red sin necesidad de montar nueva infraestructura (cableado).
- Su implementación es sencilla.
- Presentan gran flexibilidad para la instalación de redes temporales.
- Los estándares existentes se encuentran muy difundidos.

2.1.3.2. Desventajas

Entre las principales desventajas de las redes inalámbricas, con respecto a las redes cableadas, se pueden mencionar:

- Las velocidades de transmisión alcanzadas son menores que las que se logra en redes cableadas.
- Los costos de los equipos son mayores en comparación con los dispositivos necesarios para redes cableadas.
- Al utilizar el aire como medio de transmisión, las señales son interceptadas fácilmente, esto introduce problemas de seguridad.
- Por el momento no existe una compatibilidad total entre productos de diferentes fabricantes.
- La duración de las baterías es limitada.
- Para realizar transmisiones utilizando ciertos rangos de frecuencias, se requiere de licencias otorgadas por el gobierno. El rango de frecuencias libre de licencias se ha ocupado por diferentes tecnologías, por lo que en ciertos lugares se encuentra saturado.

A pesar de sus limitaciones, la gran flexibilidad, movilidad y escalabilidad proporcionadas por las redes inalámbricas, han logrado que su uso se incremente y

que se siga mejorando los estándares existentes, mientras se diseñan nuevos equipos en base a dichos estándares.

2.2. EL ESTÁNDAR IEEE 802.11

Las redes corporativas han incrementado el uso de tecnología inalámbrica debido a características como movilidad, traslado y rápida instalación. Usuarios que desempeñan sus funciones a nivel ejecutivo-administrativo utilizan este tipo de tecnología por la comodidad que brinda; en cambio usuarios que ejecutan funciones a nivel técnico las utilizan por la necesidad de traslado.

El IEEE 802.11 es el estándar para WLANs más difundido a nivel mundial; fue publicado en junio de 1997. Sus especificaciones abarcan la capa física y parte de la capa de enlace del modelo OSI (*Open System Interconnection*).

2.2.1. ARQUITECTURA DEL ESTÁNDAR IEEE 802.11

El estándar 802.11 define normas que indican la forma en que se debe realizar el intercambio de información entre dispositivos dentro de redes WLAN, estableciendo bandas de frecuencias, velocidades de transmisión y tipos de modulación.

2.2.1.1. Bandas ISM (Industrial, Científica y Médica)

La FCC ha creado normas para limitar los rangos de frecuencias que se pueden utilizar dentro de una WLAN (802.11). Dentro de estas normas se determina el uso de las bandas asignadas para ISM, estas bandas se encuentran localizadas en 900 MHz, 2.4 GHz y 5 GHz.

Para el uso de estas bandas no se requiere de la adquisición de licencias, esto ha permitido que las WLANs se desarrollen. Debido a que no se requiere realizar una inversión para transmitir en estas bandas, otros sistemas las utilizan (no solo WLANs), por lo que en ciertos lugares estas frecuencias se encuentran saturadas.

2.2.1.2. Variaciones del Estándar

El IEEE ha realizado varias publicaciones del estándar 802.11, cada publicación determina diferentes bandas de frecuencias, velocidades de transmisión y tipo de modulación, manteniendo el mismo control de acceso al medio.

a. 802.11

Fue el primer estándar para WLANs, 802.11 describe el funcionamiento de dispositivos inalámbricos, estableciendo velocidades de transmisión de 1 y 2 Mbps, trabaja en las bandas ISM y toma como frecuencia de operación 2.4 GHz; fija canales para la transmisión con un ancho de banda de 20 MHz, manteniendo una separación entre canal de 30 MHz.

El estándar contempla tres tipos de modulación: DSSS (*Direct Sequence Spread Spectrum*), FHSS (*Frequency Hopping Spread Spectrum*) y DFIR (*Diffuse Infrared*).

a.1. DSSS

Las señales ocupan un ancho de banda determinado de acuerdo a su naturaleza; *Direct Sequence* utiliza matemáticas avanzadas para distribuir una señal en un ancho de banda mayor mientras se disminuye la potencia con que se transmite la señal. El receptor realiza la operación inversa obteniendo la señal con su ancho de banda original.

Debido a que cada rango de frecuencias puede ser afectado por la presencia de ruidos específicos, es posible detectarlos y eliminarlos; además si se encuentra

interferencia en un segmento determinado del rango total de frecuencias, la información distribuida en el resto del rango permite recuperar la señal.

Al transmitir las señales en rangos de frecuencia extensos y con una potencia baja, las señales son percibidas como ruido. Esto incrementa de cierta manera la seguridad porque se necesita un receptor especializado para poder diferenciar la señal del ruido real; sin embargo, un atacante puede conseguir un receptor apropiado, por lo que se requiere mecanismos de seguridad adicionales.

a.2. FHSS

Frequency Hopping logra velocidades de transmisión equivalentes a *Direct Sequence* con un menor consumo de potencia. Esta tecnología depende de cambios rápidos en la frecuencia que se utiliza para realizar una transmisión; es decir, la señal se transmite en un determinado rango de frecuencias y luego en otro.

El salto entre rangos de frecuencia se produce de manera seudo-aleatoria; tanto el transmisor como el receptor tienen almacenada una semilla que les permite determinar en qué rango se transmite una señal en un determinado momento.

a.3. DFIR

DFIR requiere el establecimiento de una línea de vista para realizar una transmisión. Esto limita la movilidad dentro de una red; por este motivo, este tipo de tecnología no se ha difundido dentro de las redes WLAN.

b. 802.11a

Las especificaciones 802.11a y 802.11b se publicaron en 1999[1] como un anexo al estándar 802.11. El estándar 802.11a describe la operación de dispositivos inalámbricos que operan en la banda de 5 GHz, esto hace que los dispositivos

[1] *Official IEEE 802.11 Working Group Project Timelines* - 09/01/06. Todas las alusiones a fechas de aprobación o publicación de estándares o *drafts* IEEE, hacen referencia a esta fuente.

diseñados bajo el estándar 802.11a sean incompatibles con dispositivos que trabajan en otras bandas de frecuencias.

El estándar establece velocidades de transmisión de 6, 9, 12, 18, 24, 36, 48 y 54 Mbps. Para transmitir los datos se utiliza OFDM (*Orthogonal Frequency Division Multiplexing*); esta técnica divide el ancho de banda total de un canal en 64 rangos de frecuencias, 48 son utilizados para la transmisión de datos, 4 para sincronización y los 12 rangos restantes son utilizados como portadoras nulas.

802.11a no ha logrado popularizarse en el mercado, debido a que las tarjetas inalámbricas 802.11a consumen mayor potencia; además, al operar en la banda de 5 GHz el área de cobertura disminuye.

c. 802.11b

802. 11b mantiene un método similar de modulación que 802.11, con una diferencia, puede operar con velocidades de transmisión de 5.5 y 11 Mbps. Este aumento en la velocidad se produce debido a que utiliza un tipo mejorado de modulación, HR/DSSS (*High-Rate*/DSSS).

El estándar soporta compatibilidad con 802.11 (DSSS) y velocidades de 1 y 2 Mbps; trabaja en la banda de 2.4 GHz, conservando el mismo esquema para el establecimiento de canales.

d. 802.11g

Esta serie fue aprobada en junio del 2003, provee velocidades de transmisión similares a 802.11a, pero trabaja en la banda de 2.4 GHz por lo que mantiene una compatibilidad con 802.11b. Utiliza como técnica de modulación OFDM.

e. Comparación

En la tabla 2.1 se incluye información de las diferentes series del estándar 802.11, en base a esta información se puede decidir qué tipo de tecnología adoptar dentro de una WLAN.

Característica	802.11	801.11a	802.11b	802.11g
Banda de Frecuencia	2.4 GHz	5 GHz	2.4 GHz	2.4 GHz
Máxima Velocidad de Transmisión	2 Mbps	54 Mbps	11 Mbps	54 Mbps
Técnica *Spread Spectrum*	DSSS y FHSS	OFDM	HR/DSSS	OFDM
Compatibilidad entre series 802.11	802.11	802.11a	802.11 y 802.11b	802.11, 802.11b y 802.11g
Ancho de Banda[1]	83.5 MHz	300 MHz	83.5 MHz	83.5 MHz
Número de Canales sin solapamiento[1]	3	4	3	3
Potencia máxima de AP	100 mW	100 mW (FCC) 40 mW (ETS[2])	100 mW	100 mW
Equipos que causan interferencia	Teléfonos inalámbricos a 2.4 GHz, hornos microondas, video inalámbrico, dispositivos *Bluetooth*.	Teléfonos inalámbricos a 5 GHz, dispositivos *HiperLAN*[3].	Teléfonos inalámbricos a 2.4 GHz, hornos microondas, video inalámbrico, dispositivos *Bluetooth*.	Teléfonos inalámbricos a 2.4 GHz, hornos microondas, video inalámbrico, dispositivos *Bluetooth*.

Tabla 2.1 Comparación entre las diferentes series del estándar 802.11

El comité IEEE 802.11 y la alianza Wi-Fi [4] se ocupan actualmente de la estandarización e interoperatividad de dispositivos inalámbricos; el comité 802.11 se encarga del diseño de especificaciones, seguridad, interoperatividad y calidad de servicio.

---

[1] *Network Logistics Company*. *Wireless LAN Security & Manageability*. 2005.

[2] *European Telecommunication Standard*.

[3] HiperLAN (*HIgh PErformance Radio* LAN), estándar Europeo para redes inalámbricas.

[4] Por la necesidad de encontrar interoperabilidad entre dispositivos inalámbricos, los fabricantes se unieron en 1991 para formar la WECA (*Wireless Ethernet Compatibility Alliance*); la WECA tenía como propósito desarrollar estándares. La WECA luego cambió su nombre a Wi-Fi (*Wireless Fidelity*).

Wi-Fi por su parte se encarga de comprobar la interoperatividad entre equipos 802.11 producidos por diferentes fabricantes; realiza pruebas y expide certificados para los productos que las aprueben.

f. Otras series 802.11

La IEEE ha desarrollado otras extensiones del estándar 802.11, a continuación se presenta un resumen de las más importantes:

- **802.11d**.- Este estándar fue aprobado en el año 2001; contiene recomendaciones complementarias para el desarrollo de dispositivos basados en el estándar 802.11 publicado en el año 1999.

- **802.11e**.- Esta serie fue desarrollada con el objetivo de garantizar la calidad de servicio (QoS[1]) para datos que requieren ser transmitidos en tiempo real dentro de redes WLAN 802.11; su contenido fue aprobado en el año 2005.

  Para garantizar la QoS, 802.11e utiliza para el control de acceso HCF[2] con dos métodos: EDCA[3] y HCCA[4]; éstos definen clases de tráfico, lo cual les permite asignar prioridades altas para tráfico sensible a retardos como: voz y video.

- **802.11f**.- Fue aprobado en el año 2006, este estándar contiene recomendaciones que permiten lograr interoperabilidad en sistemas que utilizan APs de distintos fabricantes.

---

[1] *Quality of Service*.

[2] *Hybrid Coordination Function*.

[3] *Enhanced Distributed Channel Access*.

[4] *HCF Controlled Channel Access*.

- **802.11h**.- Este estándar fue aprobado en el año 2003. Se desarrolló con el objetivo de regular el uso de la banda de 5 GHz de acuerdo a especificaciones definidas por la UIT[1] para países Europeos, debido a que éstos utilizan esta banda para: transmisiones satelitales, sistemas militares de radar, etc.

  El estándar define dos mecanismos: DFS[2] y TPC[3], éstos deben ser implantados en dispositivos WLAN 802.11a. DFS permite que un AP detecte interferencia en un canal y seleccione automáticamente un canal libre. Por otra parte, TPC garantiza que la potencia de la señal no interfiera con las transmisiones de otros dispositivos.

- **802.11n**.- Esta variación del estándar cuenta actualmente con su primer *draft*, el mismo que fue aprobado en el año 2006. En el *draft* se define 2 canales de 20 o 40 MHz para la transmisión; éstos pueden utilizar las bandas 2.4 GHz y 5 GHz. 802.11n está diseñado para mantener compatibilidad con las series 802.11b y 802.11g[4].

  802.11n utiliza la tecnología MIMO[5] desarrollada por *Airgo*[6], ésta permite alcanzar velocidades de hasta 600 Mbps, debido a que se pueden utilizar dos o más antenas para transmitir. En la práctica los dispositivos desarrollados bajo este pre-estándar alcanzan un *throughput*[7] de hasta 95 Mbps con una distancia máxima de 18,29 metros[8].

---

[1] *Unión Internacional de Telecomunicaciones*.

[2] *Dynamic Frequency Selection*.

[3] *Transmit Power Control*.

[4] http://www.netgear.es/noticias/press.php?id=64.

[5] *Multiple-Input/Multiple-Output*.

[6] http://www.wi-fiplanet.com/news/article.php/3578886.

[7] Velocidad de transmisión efectiva.

[8] http://www.pcmag.com/article2/0,1895,1977784,00.asp.

Tecnologías propietarias denominadas *rate doubling* alcanzan (teóricamente) hasta 108 Mbps.

2.2.1.3. Pila de Protocolos

El estándar 802.11 define especificaciones para la capa física y la sub-capa MAC (*Media Access Control*) del modelo OSI. Las series 802.11a, 802.11b y 802.11g, determinan variaciones en la capa física, manteniendo el mecanismo de acceso al medio; en la figura 2.2 se muestra la pila de protocolos establecidos en el estándar 802.11 y sus diferentes capas física.

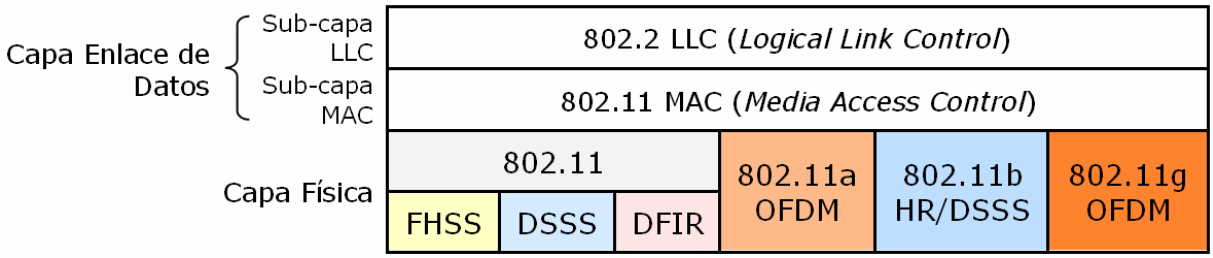

Figura 2.2 Variaciones de la Pila de Protocolos 802.11

La capa física está formada por dos sub-capas; PLCP (*Physical Layer Convergence Procedure*) y PMD (*Physical Medium Dependent*). PLCP es la encargada de acoplar la trama de acuerdo al medio físico y PMD se encarga del método de transmisión.

La sub-capa MAC 802.11 establece mecanismos que permiten a una estación acceder al medio para transmitir y recibir datos. Es diferente a las sub-capas MAC de sistemas cableados porque se debe controlar el acceso en un entorno diferente.

Dentro de las especificaciones de la sub-capa MAC 802.11 se contempla problemas como estaciones ocultas y estaciones expuestas. En la figura 2.3 se muestra una estación oculta, la estación A no conoce de la comunicación entre C y B, por lo tanto, determina que el medio está libre y transmite datos a B.

En la figura 2.4 se muestra una estación expuesta, la estación A está transmitiendo, B desea comunicarse con C pero escucha la transmisión de A y piensa que el medio está ocupado.

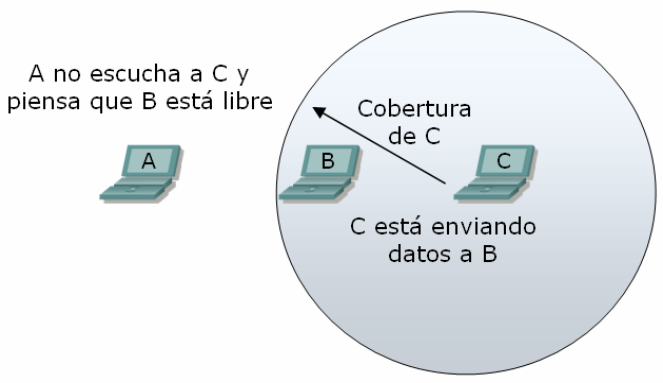

Figura 2.3 Estación oculta

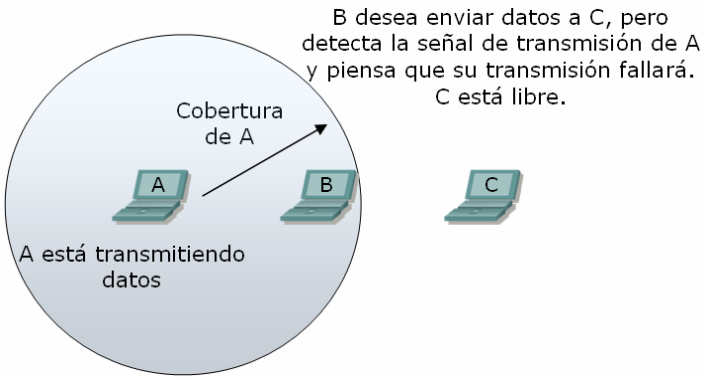

Figura 2.4 Estación expuesta

Para solucionar estos problemas, se utiliza dos tipos de acceso al medio, FCD[1] y FCP[2], FCD se encuentra activado por defecto y utiliza la técnica CSMA/CA[3] para acceder al medio; FCP se activa opcionalmente, esta técnica posee una estación de control central que otorga permisos a las otras estaciones para transmitir, por lo tanto no existen colisiones.

---

[1] Función de Coordinación Distribuida.

[2] Función de Coordinación Puntual.

[3] *Carrier Sense Multiple Access/Collision Avoidance.*

Para controlar los problemas de ruido e interferencia, 802.11 permite fragmentar las tramas, cada fragmento se envía numerado y posee su propio *checksum*. Además, se utilizan acuses de recibo con la técnica de parada y espera.

2.2.2. OPERACIÓN DE UNA RED 802.11

Para que una red 802.11 entre en operación, conviene definir primero diferentes parámetros; a continuación se presentan conceptos necesarios para implementar este tipo de redes.

2.2.2.1. Elementos

Dentro de una red 802.11 se pueden tener los siguientes elementos:

- **Estación**.- Cualquier dispositivo que contiene una tarjeta de red inalámbrica que soporte el estándar IEEE 802.11.

- **AP *(Access Point)***.- Un AP es una entidad que proporciona a las estaciones acceso a un sistema de distribución. Un AP además, convierte tramas de un formato inalámbrico al formato utilizado dentro de las redes cableadas.

- **BSS (*Basic Service Set*)**.- Un BSS está formado por un conjunto de estaciones controladas por una sola función de coordinación.

- **DS (*Distribution System*)**.- Cuando varios APs se encuentran dentro de un área, éstos deben comunicarse entre sí para determinar los movimientos de las estaciones. Un DS es un componente lógico que interconecta a los APs para formar una WLAN, permitiendo enviar tramas entre estaciones.

- **ESS (*Extended Service Set*)**.- Un ESS está formado por un conjunto de BSSs interconectados e integrados a una LAN cableada; para una estación esto es transparente y se ve como un solo BSS.

- **SSID (*Service Set Identifier*)**.- El SSID es el identificador único de una WLAN, puede contener de 2 a 32 caracteres alfanuméricos y debe configurarse en todos los clientes y APs de la WLAN. El SSID es utilizado para diferenciar una WLAN de otra y se utiliza como un mecanismo básico de seguridad.

- ***Beacons***.- Son tramas pequeñas que se envían desde los APs hacia las estaciones (o entre estaciones), con el fin de sincronizar las transmisiones dentro de una WLAN. Las *beacons* se usan también para negociar parámetros de modulación, entrega del SSID [1] de la red, velocidades soportadas e información que les indica a las estaciones si pueden transmitir información en ese momento.

- **Portal**.- Es el punto de conexión entre una WLAN y una red exterior a ésta.

2.2.2.2. Acceso a una Red WLAN

Cuando un cliente enciende su tarjeta inalámbrica, ésta empieza a “escuchar” el medio para determinar si se encuentra dentro del área de cobertura de una WLAN; sí se encuentra una red disponible, detecta las tramas *beacon*, las examina y obtiene el SSID que le permitirá ingresar a la red. El proceso de escucha toma el nombre de escaneo; se tiene dos tipos de escaneo: activo y pasivo.

a. Escaneo Activo

En este tipo de escaneo, una estación envía tramas hacia otras estaciones o hacia el AP, cada trama contiene el SSID de la red a la que la estación desea asociarse; de esta manera, solo las entidades que se identifican con dicho SSID responden a las demandas de la estación.

---

[1] Por defecto, el SSID se envía en las tramas *beacon* en texto plano.

Si existen varios APs o estaciones con el mismo SSID, la estación inicia una comunicación con el dispositivo que ofrece mejores condiciones para la transmisión.

b. Escaneo Pasivo

En el escaneo pasivo, las estaciones escuchan cada canal por un período determinado; al recibir tramas *beacon*, la estación verifica las características de la red y espera hasta recibir un SSID; cuando identifica su SSID se comunica con la entidad que envío la trama *beacon*.

Si la estación no tiene configurado un SSID y recibe tramas desde diferentes redes, ésta intenta adherirse a la red que entrega mejores niveles en la potencia de señal y el menor BER (*Bit Error Rate*).

2.2.2.3. Topologías

Una red 802.11 puede tener dos tipos de topología, la topología de red independiente o *ad hoc* y la topología de red de infraestructura.

a. Redes Ad Hoc

Estas redes están formadas por un grupo de estaciones que se comunican entre sí sin la intervención de un AP, por este motivo se las conoce también como BSS independiente; por lo general, se utilizan para formar redes temporales.

Una red de este tipo puede formarse por 2 o más estaciones. Los clientes se comunican entre sí mediante conexiones *peer to peer* y asignan a uno de los miembros de la red para enviar las tramas *beacon*.

b. Redes de Infraestructura

Este tipo de red usa un AP como punto central de control dentro de un BSS, el AP controla las comunicaciones entre los diferentes dispositivos inalámbricos dentro del área de cobertura.

Una red de infraestructura puede estar compuesta por uno o varios BSSs interconectados entre sí; adicionalmente, posee por lo menos un portal que le permite comunicarse con redes exteriores.

2.2.2.4. Servicios

El estándar 802.11 establece 9 servicios, éstos pueden ser proporcionados por el DS o por las estaciones. Los cinco servicios proporcionados por el DS hacen referencia a la comunicación entre estaciones dentro y fuera de un BSS:

- **Asociación**.- Este servicio se utiliza para que una estación se conecte con un BSS, la asociación puede realizarse entre estaciones o entre una estación y un AP. El proceso de asociación dentro de una WLAN es equivalente a conectar un dispositivo a un puerto dentro de una LAN cableada.

  Cuando una estación se asocia a un BSS, ésta comunica las características que soporta (velocidad de transmisión, modulación, etc.) y de acuerdo a estas características se realizan las siguientes comunicaciones.

- **Disociación**.- Se usa este servicio para terminar una conexión dentro de un BSS; este servicio puede ser utilizado por una estación o por un AP.

- **Reasociación**.- Si una estación se encuentra en movimiento, puede encontrar un AP que brinde mejores condiciones de transmisión; en este caso, la estación debe asociarse con el nuevo AP, esta asociación no requiere volver a comunicar las características soportadas por la estación.

- **Distribución**.- Este servicio proporciona la capacidad de entregar las tramas enviadas a una estación dentro o fuera de un BSS.

- **Integración**.- Las tramas soportadas dentro de una WLAN no son iguales a las establecidas para redes exteriores. El servicio de integración es el encargado de modificar el formato de la trama 802.11 y adaptarlo a un formato soportado por una red que maneje un estándar diferente.

Los cuatro servicios proporcionados por las estaciones en cambio se relacionan con la comunicación entre estaciones dentro de un BSS:

- **Autenticación**.- Después de realizar una asociación exitosa, una estación debe mostrar su identidad; si a partir de su identidad se comprueba que la estación forma parte de una red, ésta queda autenticada y puede empezar la comunicación con otras estaciones de la red.

- **Desautenticación**.- Este servicio se da cuando una estación autenticada desea abandonar la red.

- **Privacidad**.- Este servicio es el encargado de mantener la confidencialidad de la información intercambiada entre las estaciones que forman parte de una WLAN.

- **Entrega de Datos**.- Este servicio establece procedimientos para transmitir y recibir datos desde y hacia las estaciones. Es un servicio no confiable.

2.2.2.5. Soporte de Movilidad

El soporte de movilidad dentro de una red 802.11 debe permitir que una estación miembro de un ESS se traslade dentro de éste de un BSS a otro sin perder conectividad. El estándar no contempla la posibilidad de mantener la comunicación al trasladarse de un ESS a otro ESS.

2.3. ASPECTOS PRINCIPALES DE SEGURIDAD

Cuando las WLAN fueron introducidas al mercado, se pensó que se difundirían rápidamente; sin embargo, sus limitaciones contuvieron a su éxito. Una de las principales causas por la que administradores y usuarios prefieren aún las redes cableadas a las WLANs es la inseguridad inherente a su medio de transmisión.

2.3.1. CONSIDERACIONES BÁSICAS

Al utilizar como medio de transmisión el aire, las redes inalámbricas son más susceptibles a vulnerabilidades relacionadas con la integridad y la confidencialidad de los mensajes en comparación con las redes cableadas.

La integridad de los mensajes se ve afectada por diferentes factores, las WLANs se ven expuestas a un medio ruidoso y con interferencias; las señales transmitidas son afectadas por los obstáculos (*multipath*[1]). Adicionalmente, de acuerdo a la posición de un usuario, los datos se transmiten con diferentes velocidades lo que causa problemas de sincronización.

En el caso de confidencialidad, si un atacante desea interceptar los datos que viajan por una red, requiere un acceso físico al medio de transmisión. En el caso de las LANs tradicionales, debe acceder al cableado, lo que brinda un nivel básico de confidencialidad.

En cambio, los límites de una WLAN no están definidos por locales o edificios, las señales transmitidas por el aire traspasan paredes y pueden llegar a lugares donde

[1] Desvanecimiento por múltiple trayectoria.- Al encontrar un obstáculo, la señal se refleja y llega a su destino por diferentes trayectorias.

un atacante esté esperando una oportunidad; incluso dentro del área de cobertura esperada, un usuario lícito puede acceder a información no autorizada.

Por otra parte, los usuarios tampoco tienen definida un zona específica en donde sus transmisiones resultan seguras, si se excede la distancia desde un AP legítimo, se puede ingresar a redes peligrosas en donde el intercambio de información resulte perjudicial.

Es importante tener en cuenta que una WLAN está expuesta a todos los ataques aplicables a una LAN cableada, con una diferencia, en este tipo de redes su medio de transmisión está expuesto. Los ataques de suplantación, interceptación de los mensajes y negación del servicio pueden realizarse sin mucho esfuerzo ubicando un AP ilícito cerca del área de cobertura de la red.

Incluso en redes en las que la información transmitida se considere trivial, se debe tener en cuenta un nivel básico de seguridad para la configuración de los equipos. En estos casos, no se considera como parte fundamental la protección de la información sino más bien el funcionamiento de la red.

Si un administrador no toma las medidas pertinentes, un ataque puede dejar fuera de servicio a la red. Pero se debe considerar algo peor, un ataque podría dejar fuera de funcionamiento redes externas y eso perjudica la imagen de una empresa e incluso puede cuasar perjuicios económicos y legales.

Por lo mencionado anteriormente, se vuelve indispensable la introducción de políticas de seguridad elementales, esto incrementa la complejidad en los procesos de administración de una red; sin embargo, garantiza niveles aceptables de operación y en algunos casos incrementa la eficiencia en los procesos.

Una WLAN casi siempre está ligada a una LAN cableada, si no se toma medidas adecuadas, la red inalámbrica introduce vulnerabilidades a la red cableada. Por este

motivo, para establecer políticas de seguridad, no solo se debe considerar los requerimientos de la WLAN, también se debe analizar las condiciones de la red LAN y sus puntos críticos.

2.3.2. ADMINISTRACIÓN DE UN AP

La administración de un AP es importante ya que permite brindar seguridad al sistema, logrando un mejor funcionamiento. A continuación se presenta una lista de prácticas recomendadas para obtener niveles de seguridad.

- Para adquirir un AP, primero se debe realizar un análisis del nivel de seguridad requerido dentro de la red y de acuerdo a esto, determinar sus capacidades y nivel de Interoperabilidad.
- Cambiar los parámetros que vienen configurados por defecto es esencial; por ejemplo: nombre, SSID, parámetros de direccionamiento IP, comunidad SNMP[1], DNS[2], NTP[3], HTTP[4], *Telnet*, usuarios y contraseñas, etc.
- Realizar un análisis de los servicios que debe brindar el AP; los servicios que no sean necesarios deben desactivarse; por ejemplo, DHCP[5], CDP[6], etc.
- Si no se va a monitorear el AP, mantener SNMP habilitado puede resultar peligroso; las versiones 1 y 2 de SNMP, envían mensajes en texto plano, éstos contienen información del funcionamiento y topología de la red. Un atacante puede usar esa información para encontrar puntos vulnerables del sistema y causar daños.

---

[1] *Simple Network Management Protocol.*

[2] *Domain Name Service.*

[3] *Network Time Protocol.*

[4] *Hypertext Transfer Protocol.*

[5] *Dynamic Host Configuration Protocol*.

[6] *Cisco Discovery Protocol*.

- Se recomienda mantener habilitado SNMP si se cuenta con un monitoreo que permita envío de mensajes SNMP versión 3, esta versión soporta autenticación y encripción con lo que se logra cierto nivel de seguridad.
- En caso de manejar sistemas de administración con versiones anteriores a la versión 3 de SNMP, se debe crear listas de acceso que limiten el envío de información SNMP; es recomendable establecer permisos de solo lectura dentro de estas listas de acceso.
- En el caso de *Telnet*, es recomendable deshabilitar esta funcionalidad y habilitarla sólo cuando se requiera hacer mantenimiento de la configuración.
- Parámetros como el identificador de la comunidad SNMP y el SSID no deben proporcionar información sobre la red o el nombre de la empresa.
- Se debe deshabilitar el *broadcast* de SSID dentro de las tramas *beacon*.
- El *firmware*[1] de los APs y de las tarjetas inalámbricas debe estar siempre actualizado, con esto se refuerzan o eliminan las vulnerabilidades (conocidas) introducidas por la operación de *software* o *hardware*.
- Para la configuración de los APs, se debe crear usuarios con perfiles de lectura-escritura, y para el monitoreo con perfiles de solo lectura.
- Realizar un análisis de los tipos de filtrado que se deben aplicar dentro de la red; se tienen varios tipos de filtrado: SSID, MAC, IP y de protocolos.
- En el caso de tener usuarios en la red con perfiles que involucren diferentes privilegios, se deben implementar VLANs (*Virtual* LAN) y asignar a cada una su propio SSID.
- Definir una técnica de autenticación, determinando si se autenticará solo la red o es necesaria una autenticación mutua (cliente/servidor).
- Los usuarios de la red deben ser capacitados para que no introduzcan malas prácticas.
- Si la información transmitida por la red es crítica, ésta debe estar cifrada.

[1] Microcódigo que contiene instrucciones que permiten manejar el *hardware* de dispositivos electrónicos.

En el caso de redes corporativas, los requerimientos de seguridad son mayores, por lo que se debe manejar un sistema de administración y autenticación centralizado.

2.3.2.1. Control de Acceso Físico al AP

Para evitar que un atacante tenga acceso a información de configuración o que realice re-configuraciones, se debe prevenir accesos de usuarios no autorizados a los APs. Normalmente, los administradores deben ser los únicos autorizados para realizar configuraciones de equipos, y por lo tanto el acceso de usuarios debe ser restringido.

2.3.3. TIPOS DE AUTENTICACIÓN EN WLANs

Los tipos de autenticación están atados al SSID que se configure en el AP. Si se requiere que usuarios con diferentes perfiles o actividades reciban los servicios del mismo AP, se pueden configurar múltiples SSIDs.

Cuando un cliente ingresa en el área de cobertura de una red, primero debe autenticarse con el AP. Un AP soporta tres mecanismos o tipos de autenticación y puede usar más de uno a la vez, los tipos de autenticación son:

- **Autenticación WEP**[1].- Este tipo de autenticación se puede aplicar de tres formas: *none*, *shared-key* y *open*, cada una se explicará en la siguiente sección.

- **Autenticación EAP**.- Este tipo de autenticación provee altos niveles de seguridad dentro de una red inalámbrica, maneja autenticación mutua por

[1] *Wired Equivalent Privacy.*

medio de un servidor RADIUS[1]. Utiliza una clave dinámica para cifrar cada sesión establecida lo que garantiza un nivel de seguridad similar al de un segmento cableado.

Utilizar diferentes tipos de autenticación con un solo SSID introduce vulnerabilidades para los usuarios con perfiles más críticos; si se va a implementar diferentes técnicas es recomendable establecer diferentes niveles de seguridad con el uso de múltiples SSIDs, cada uno asignado a una VLAN diferente.

2.3.4. WEP

Fue publicado dentro de las especificaciones del estándar 802.11, con el fin de proveer confidencialidad, autenticación e integridad a una WLAN, para que ésta tenga niveles de seguridad similares a los encontrados en una red cableada.

Por sus características, WEP es una solución para WLANs pequeñas en las que no se requiere niveles elevados de seguridad. Su implementación resulta fácil y no requiere de inversiones adicionales; por ser parte de 802.11 soporta interoperabilidad con clientes basados en distintas plataformas.

2.3.4.1. Confidencialidad

Para garantizar la confidencialidad de los datos WEP trabaja con RC4; para el proceso de encripción se generan 4 claves a partir de una clave estática, cada clave puede tener una longitud de 40[2] *bits*. A continuación se agrega un VI[3] de 24 *bits* con

---

[1] *Remote Authentication Dial In User Service*.

[2] Algunos fabricantes soportan claves con una longitud de 104 *bits*.

[3] Vector de Inicialización.

lo que se obtiene claves de 64 *bits*; se selecciona una de las 4 claves para cifrar todas las sesiones.

El VI se incluye también en cada trama y se envía por la red en texto plano, cuando se han ocupado todos los posibles valores del VI, se reinicia la secuencia. Este proceso introduce vulnerabilidades, debido a que la reutilización del VI le permite a un atacante capturar paquetes válidos y reenviarlos cuando detecte reutilización del VI; adicionalmente, su uso reduce el tamaño real de la clave WEP.

2.3.4.2. Autenticación WEP

Para garantizar la autenticación, la clave estática debe ser conocida solo por los usuarios lícitos de la red; WEP especifica tres tipos de autenticación:

- ***None***.- En este tipo no se requiere que los usuarios conozcan la clave estática, si un usuario conoce el SSID de la red, puede ingresar a ésta.

- ***Shared Key Authentication***.- Dentro de este tipo de autenticación, el cliente envía una petición hacia el AP, luego, el AP envía un desafío (en texto plano) al cliente, el cliente cifra el desafío con la clave WEP y lo devuelve. El AP comprueba que el desafío se haya cifrado con la clave apropiada; de ser así, envía una respuesta al cliente indicándole que ha sido autenticado.

- ***Open System Authentication***.- En este tipo de autenticación se permite que cualquier dispositivo inalámbrico se asocie a la red; pero, para que un dispositivo asociado consiga el permiso de trasmitir, éste debe conocer la clave WEP de la red.

El nivel de seguridad proporcionado por WEP es limitado, si la clave se ve comprometida, las comunicaciones de todos los usuarios pueden ser descifradas. Por otra parte, no provee mecanismos que protejan a la red de ataques internos.

2.3.4.3. Integridad

WEP garantiza la integridad de los mensajes calculando el valor *hash* del *payload* de una trama mediante CRC-32 [1] . Este mecanismo introduce vulnerabilidades relacionadas con las características de linealidad de CRC-32; además, el valor *hash* obtenido es independiente de la clave WEP o del VI, esto permite que un atacante introduzca paquetes ilícitos dentro de la red.

2.3.5. WPA (Wi-Fi *Protected Access*)

Debido a las vulnerabilidades encontradas en WEP, la Wi-Fi *Alliance* basándose en especificaciones establecidas por el grupo de trabajo 802.11i[2] introduce WPA en el año 2002.

WPA tiene como objetivo mejorar los niveles de seguridad en redes basadas en el estándar 802.11. Para esto, incorpora mecanismos de seguridad como TKIP (*Temporal Key Integrity Protocol*), MIC *(Message Integrity Check*), mejoras en la generación de VI, KMF (*Key Mixing Function*), *Re-Keying* y soporte del estándar 802.1x.

- **TKIP**.-Como su nombre lo indica, TKIP utiliza claves dinámicas para el cifrado de los mensajes, la clave puede cambiarse para cada usuario, para cada sesión (teniendo una duración limitada) y por cada paquete enviado; adicionalmente, incrementa la longitud de la clave de 40 a 104 *bits*.

- **MIC**.- Esta herramienta se utiliza para garantizar la integridad de los mensajes; para esto, se agrega al mensaje un MAC (*Message Authentication Codes*). Un

[1] Código de redundancia cíclica que obtiene un valor *hash* de 32 *bits*.

[2] Estándar diseñado para proveer de un mecanismo de seguridad para redes 802.11.

MAC tiene una longitud de 32 *bits* y se genera a partir de los datos y las direcciones MAC origen y destino.

- **Mejoras en la Generación de VI**.- MIC no detecta cuando un paquete válido es retransmitido, WPA soluciona este problema asociando el MIC (cifrado) con el número de secuencia del paquete.

- **KMF**.- La función de combinación de claves genera claves que se utilizan durante un período determinado. Se combina la dirección MAC[1] de origen y la clave WEP para crear una clave maestra; utilizando el algoritmo *Feistel* se cifra la clave maestra combinada con el número de secuencia del paquete, se obtiene un bloque de 128 *bits*, este bloque se utiliza para cifrar el paquete.

- ***Re-Keying***.- Su función es generar dos claves temporales a partir de una clave maestra y de claves de encripción. Una de las claves temporales tiene una longitud de 128 *bits* y se usa para la encripción, la otra clave tiene una longitud de 64 *bits* y es utilizada para garantizar integridad de los datos.

2.4. ESTÁNDAR 802.1X

El estándar 802.1x fue aprobado en junio del año 2001 por el IEEE[2], su nombre original es "*Port-Based Network Access Control*"; este estándar contiene normas para el control de acceso y la autenticación dentro de redes LAN y MAN.

802.1X utiliza las características de acceso físico de los estándares IEEE 802, para proporcionar un mecanismo que permita autenticar y autorizar a dispositivos

[1] La dirección MAC de un dispositivo es un identificador único, al combinarla con la clave WEP se obtiene una clave propia del dispositivo.

[2] En el mismo año se reconoce como estándar por la ANSI (*American National Standard*).

relacionados con un puerto, con características de conexión punto a punto; en caso de que los procesos de autenticación y autorización fallen, se aplican mecanismos que evitan el ingreso a la red.

Dentro del estándar un puerto es un punto que liga a un dispositivo a la infraestructura LAN; se puede utilizar para la autenticación puertos de puentes MAC, servidores, *routers* y las asociaciones entre estaciones y APs en WLANs 802.11.

2.4.1. DEFINICIONES

Para el entendimiento de 802.1x es necesario conocer las siguientes definiciones:

- **EAP**.- El protocolo EAP fue desarrollado por el IETF [1] y se encuentra registrado en el RFC 3748. EAP define una técnica de encapsulación con un formato de trama que permite el intercambio de credenciales.

  Soporta diferentes protocolos de capa enlace, por este motivo se seleccionó para trabajar conjuntamente con 802.1x para realizar la autenticación en diferentes ambientes (LAN, MAN y WAN; cableados o inalámbricos).

- **Autenticador**.- Es la entidad ubicada en un segmento LAN que facilita la autenticación de otra entidad en un enlace punto a punto. Solo sirve como un punto intermedio a través del cual el servidor de autenticación y el suplicante intercambian credenciales.

- **Servidor de Autenticación**.- Es una entidad que provee el servicio de autenticación a un autenticador. Este servicio determina si las credenciales presentadas por un suplicante son válidas para completar el proceso de

[1] *Internet Engineering Task Force*.

autenticación. El servidor de autenticación presta los servicios de AAA[1] dentro de redes WLANs, el más utilizado es el servidor RADIUS.

- **Puerto de acceso a la Red**.- Es el punto de conexión entre un sistema y una LAN. Puede ser un puerto físico; por ejemplo, un puerto MAC conectado físicamente a un segmento. También puede ser lógico; por ejemplo, una asociación entre una estación y un AP.

- **PAE (*Port Access Entity*)**.- Es la entidad de protocolo asociada con el puerto, ésta soporta funcionalidades del protocolo asociadas con el autenticador, el suplicante o los dos.

- **Suplicante**.- Es la entidad ubicada en un segmento LAN que solicita una autenticación a un autenticador en un enlace punto a punto.

- **Sistema**.- Dispositivo que se conecta a una LAN por uno o más puertos; por ejemplo, estaciones, servidores, puentes, *routers*, etc.

- **EAPOL (EAP *over* LANs)**.- Protocolo que define la técnica de encapsulación para intercambio de paquetes EAP entre PAEs suplicantes y PAEs autenticadoras dentro de ambientes LAN.

2.4.2. FUNCIONAMIENTO DE 802.1X

El estándar 802.1x define mecanismos que permiten realizar el intercambio de credenciales y la validación o negación de acceso entre el cliente y el servidor de autenticación. En la figura 2.5 se muestra un esquema con los elementos necesarios para la operación del estándar 802.1x.

---

[1] *Authentication, Authorization and Accounting*.

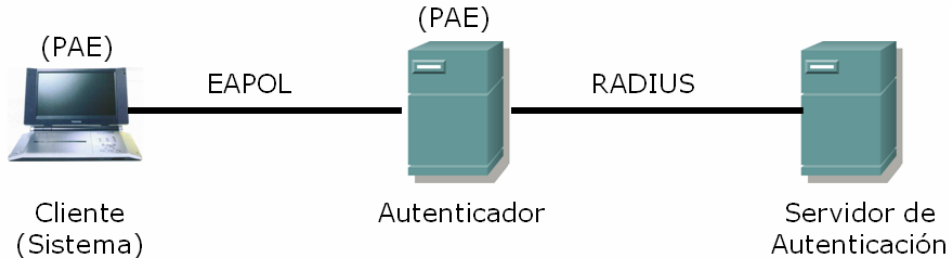

Figura 2.5 Esquema 802.1x

El autenticador sirve como un puente entre el cliente y el servidor de autenticación durante del proceso de autenticación. El protocolo EAPOL[1] es utilizado para el intercambio de paquetes entre el autenticador y el cliente mediante un puerto no controlado. Para la comunicación entre el autenticador y el servidor se utiliza el protocolo RADIUS.

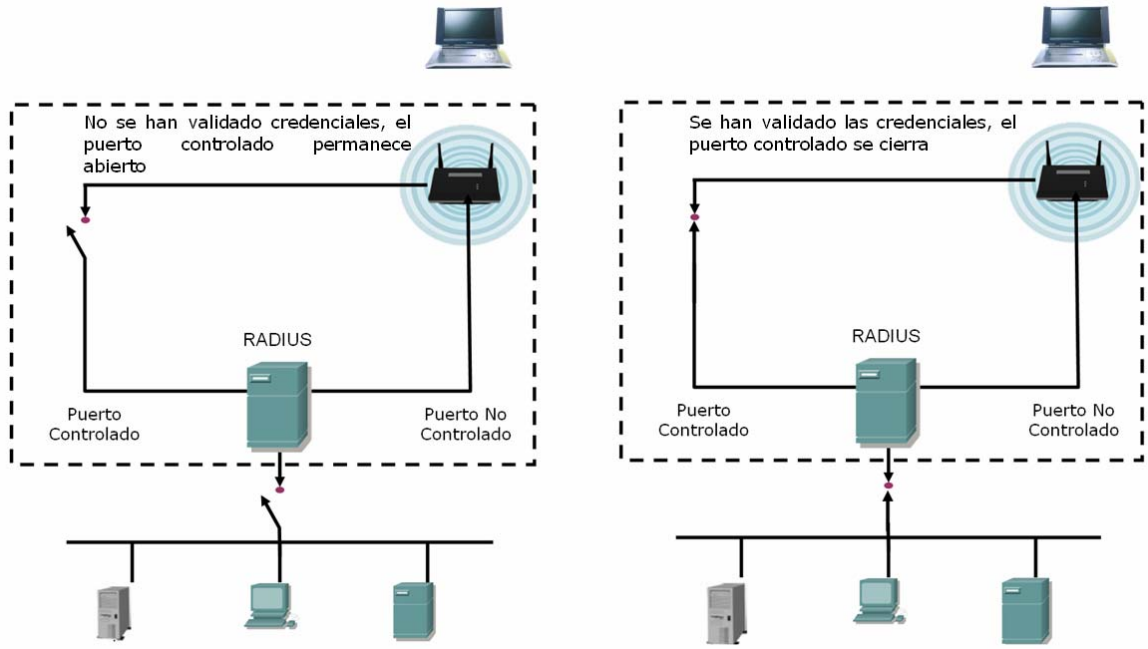

Figura 2.6 Puertos en 802.1x

Como se muestra en la figura 2.6, cuando el proceso de validación de credenciales ha sido exitoso, el servidor activa un puerto controlado a través del cual el cliente tiene acceso a la red.

[1] Cuando se utiliza 802.1x dentro de WLANs, se conoce a EAPOL como EAPW (EAP *over* WLAN).

El proceso de autenticación es definido enteramente en el servidor; por este motivo, si se llega a cambiar la técnica de autenticación, las modificaciones en los clientes son mínimas.

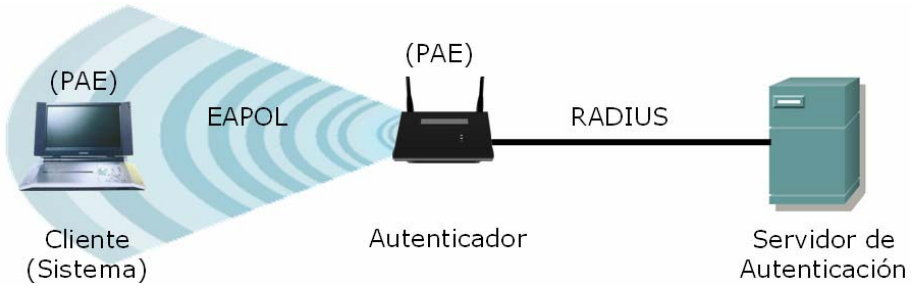

Figura 2.7 Esquema de funcionamiento de 802.1x para WLANs

En ambientes inalámbricos, el AP cumple la función de autenticador y se utiliza un servidor RADIUS para autenticar las credenciales del cliente como se muestra en la figura 2.7. La conexión entre el cliente y el autenticador se realiza también a través de un puerto lógico no controlado; a través de este canal se intercambian credenciales y respuestas de acceso.

Durante el intercambio de credenciales, el cliente recibe una clave que le permite cifrar sus mensajes durante una sesión, el AP identifica al cliente al reconocer su clave. Si el cliente no posee una clave válida, el AP descarta sus paquetes. Cuando la validación se ha completado, el cliente tiene acceso a la red a través del puerto lógico controlado.

2.4.3. RADIUS

El estándar RADIUS define un esquema de cliente/servidor que brinda los servicios AAA. Las especificaciones de autenticación y autorización se encuentran registradas en el RFC 2865; las especificaciones que se refieren a *Accounting* están registradas en el RFC 2866.

Un servidor RADIUS tiene características que lo hacen compatible con varias plataformas de *software* y *hardware*; su administración es centralizada, soporta varias técnicas de autenticación y permite realizar consultas para la autenticación en una base de datos local o realizar una solicitud para que otro servidor realice la validación.

Varias empresas de *software* han lanzado al mercado sus versiones comerciales de servidores RADIUS; por ejemplo, ACS[1] de Cisco, *Odyssey Server* de *Funk Software*, IAS[2] *Server* de *Microsoft*, etc.; además, existen versiones de *software* libre como *FreeRadius* que presenta versiones disponibles para *Windows* y *Linux*.

Al seleccionar un servidor RADIUS, se debe verificar compatibilidad con *software*, *hardware* y bases de datos; además, se debe comprobar que soporte varios tipos de autenticación.

2.4.3.1. Características de Funcionamiento de un servidor RADIUS

Un servidor RADIUS es normalmente un sistema multiusuario. Los clientes RADIUS envían peticiones de autenticación al servidor RADIUS central, el servidor tiene registros de todos los usuarios e información de los servicios a los que éstos pueden acceder dentro de la red.

Cuando un usuario intenta autenticarse, por defecto, los puertos de acceso a los servicios de una red se encuentran bloqueados, el tráfico permitido se limita a los procesos necesarios para la autenticación; cuando el servidor ha validado las credenciales del usuario, se le permite acceder a la red e intercambiar información.

---

[1] *Access Control Server.*

[2] *Internet Authentication Service.*

Los paquetes que se intercambian durante el proceso de autenticación manejan un formato propio del protocolo RADIUS; esta encapsulación se conoce como *EAP over RADIUS.* Dentro de la trama RADIUS se tiene un campo “código”, éste determina el tipo de paquete, en la tabla 2.2 se muestran los tipos de paquete soportados.

Valor	Nombre del Campo	Descripción
1	*Access-Request*	Cliente: Petición de acceso
2	*Access-Accept*	Servidor: Petición aceptada
3	*Access-Reject*	Servidor: Petición rechazada
4	*Accounting-Request*	Cliente: Petición de Registro
5	*Accounting-Response*	Servidor: Respuesta de Registro
11	*Access-Challenge*	Servidor: Desafío para autenticación
12	*Status-Server*	Reservado (experimental)
13	*Status-Client*	Reservado (experimental)
255	*Reserved*	Reservado

Tabla 2.2 Valores del campo Código de la trama RADIUS

Para identificar una sesión con un usuario determinado, la trama incluye el campo identificador, de esta manera el servidor asocia una respuesta a las solicitudes de un cliente RADIUS.

Si una validación fue exitosa, el servidor genera una clave WEP de manera aleatoria y la entrega al AP, para que éste a su vez la envíe al usuario; la clave se utilizará para cifrar la sesión actual del usuario.

2.4.3.2. Operación RADIUS

Cuando una estación ingresa al área de cobertura de una WLAN que realiza autenticación mediante 802.1x y un servidor RADIUS, se establece el siguiente procedimiento:

- El AP envía un desafío a la estación.

- La estación recibe el desafío y responde con su identidad.
- El AP reenvía la identidad de la estación al servidor.
- El servidor verifica la identidad del cliente y solicita un tipo de credencial de acuerdo al perfil de la estación.
- La estación envía su credencial al servidor.
- El servidor valida la credencial de la estación, si ésta es legítima transmite una clave WEP de sesión al AP.
- El AP envía al cliente la clave.
- Cuando el servidor autentica al cliente, el proceso se repite en reversa y el cliente autentica al servidor.

Si se desea aumentar el nivel de seguridad, se puede realizar el proceso de autenticación periódicamente.

a. Configuración del servidor RADIUS en un AP

La comunicación con un servidor RADIUS y los servicios AAA por defecto se encuentran deshabilitados en un AP; para evitar problemas de seguridad, sólo se deben configurar estos servicios si son necesarios para la autenticación en la red.

Para configurar autenticación en una WLAN utilizando un servidor RADIUS, se debe configurar en el AP la dirección IP[1] del servidor y definir una lista de métodos para la autenticación, y opcionalmente para el *accounting*.

La lista de métodos define procedimientos y secuencias necesarias para el proceso de autenticación y autorización, o para el registro de *accounting*. Se puede utilizar listas de métodos para designar uno o más protocolos de seguridad, de este modo se tienen alternativas en caso de que el método inicial falle.

[1] *Internet Protocol.*

El *software* del AP selecciona por defecto el primer método que se encuentra en la lista, si este método no responde, selecciona el siguiente. Este proceso continúa hasta que la comunicación sea exitosa; de no ser así se prohíbe el acceso a la red.

2.5. EAP-TLS

EAP es un protocolo diseñado para optimizar los procesos de autenticación mediante la transmisión de credenciales; no es un método de autenticación en sí, sino más bien un mecanismo que soporta la transmisión de distintos tipos de credenciales de acuerdo a la técnica que se utilice para la autenticación. Sus especificaciones se encuentran registradas en el RFC 3748.

802.1X utiliza EAP para la negociación de la técnica de autenticación y sus parámetros entre el cliente y el autenticador, se requiere que un servidor valide las credenciales.

2.5.1. INFRAESTRUCTURA EAP

Para mantener el control en el proceso de comunicación entre el cliente y el autenticador, la trama EAP incluye los campos identificador y código; el campo identificador relaciona a una petición con una respuesta, este campo se marca con el mismo valor para una pareja petición/respuesta.

El campo código permite determinar si se trata de una petición (1) o de una respuesta (2), también puede indicar si se ha tenido éxito (3) o fracaso (4) durante el proceso de entrega de las credenciales.

Existen distintos esquemas de autenticación EAP, el protocolo EAP está formado por un conjunto de módulos que proporcionan compatibilidad de arquitectura con

cualquiera de sus distintos esquemas. Para que el proceso de autenticación pueda realizarse, el cliente y el autenticador deben tener instalado el mismo módulo de autenticación EAP.

2.5.1.1. Módulos EAP

Existen diferentes módulos de autenticación EAP, cada módulo permite transmitir credenciales específicas. La trama EAP incluye el campo tipo, éste permite identificar el tipo de módulo que se utiliza en el proceso de autenticación.

Los valores del campo tipo incluidos en la tabla 2.3 contemplan todos aquellos que se han implementado, con excepción de OTP y GTC que se incluyen por ser parte del estándar. Dentro de redes WLAN se encuentra difundido el uso de los siguientes tipos de EAP: Desafío MD5, TTLS, PEAP, FAST, LEAP y EAP-TLS.

- **Desafío MD5**.- MD5 utiliza para la autenticación un desafío que se envía al cliente, el cliente debe cifrar el desafío con una clave compartida y enviar el resultado al autenticador; el autenticador compara el valor recibido con su propio resultado, si el valor coincide, el cliente queda autenticado.

- **EAP-TTLS**.- Fue creado *Funk Software* y *Certicom*, su estado de I-D[1] se encuentra caducado, provee autenticación segura mediante el establecimiento de un túnel con el protocolo TLS; las claves necesarias para cifrar los datos se generan por cada sesión.

  Después de establecer el túnel TLS, se produce la autenticación del servidor mediante certificados digitales, los clientes se autentican utilizando

[1] *Internet Draft*.

contraseñas. Las contraseñas son validadas en el servidor utilizando CHAP[1], PAP[2], MSCHAP y MSCHAPv2[3].

Valor	Nombre del Campo	Implementados	Norma
1	Identidad	Si	RFC 2284
2	Notificación	Si	RFC 2284
3	NAK	Si	RFC 2284
4	Desafío MD5	Si	RFC 2284
5	OTP[4]	No	RFC 2284
6	GTC[5]	No	RFC 2284
10	*DSS Unilateral*	Si	De facto
11	KEA	Si	De facto
12	KEA-*Validate*	Si	De facto
13	EAP – TLS	Si	RFC 2716
14	*Defender Token*	Si	De facto
17	LEAP[6]	Si	De facto
19	SRP-SHA1 *Part* 1	Si	De facto
21	EAP - TTLS[7]	Si	De facto
24	EAP-3Com *Wireless*	Si	De facto
25	PEAP[8]	Si	De facto
26	MS-EAP-*Authentication*	Si	De facto
28	*CRYPTOCard*	Si	De facto
254	Tipos expandidos	-----	-----
255	Uso experimental	-----	-----
-----	EAP-FAST[9]	Si	De facto
-----	EAP-SIM[10]	Si	De facto

Tabla 2.3 Valores del campo tipo de la trama EAP

[1] *Challenge Authentication Protocol*.

[2] *Password Authentication Protocol*.

[3] Versión 2 de CHAP de *Microsoft*.

[4] *One Time Password*.

[5] *Generic Token Card*.

[6] *Lightweight* EAP. Cisco.

[7] *Tunneled* TLS. *Funk Software*.

[8] *Protected* EAP. *Microsoft.*

[9] *EAP-Flexible Authentication via Secure Tunneling*. *Cisco*.

[10] *Subscriber Identity Module*. *Cisco.*

- **PEAP**.- Es un protocolo propietario de *Microsoft*, provee niveles similares de seguridad que EAP-TTLS, este tipo de autenticación permite transmitir otros tipos de EAP sin necesidad de establecer un túnel TLS.

  El usuario debe enviar su contraseña hacia el servidor RADIUS, la identidad del usuario es protegida mediante el uso de MSCHAPv2. El servidor RADIUS se autentica utilizando un certificado digital.

- **EAP-FAST**.- Éste es un protocolo propietario de *Cisco*. Para la autenticación se utiliza PAC (*Protected Access Credential*) en lugar de usar un certificado digital. La PAC puede manejarse dinámicamente por el servidor de autenticación y ser distribuida a los clientes a través de un dispositivo de almacenamiento o mediante sesiones seguras.

- **LEAP**.- Este método también es propietario de *Cisco*, permite conexiones seguras dentro de una WLAN entre clientes y APs *Cisco Aironet Series*. La técnica que se usa para la autenticación está basada en contraseñas y nombres de usuarios almacenados en la base de datos de un servidor RADIUS.

  Las contraseñas no se envían por la red directamente, para el proceso de autenticación, el cliente envía al servidor su nombre de usuario junto con un desafío generado a partir de su contraseña; utilizando el desafío del cliente, el servidor genera su propio desafío y se lo envía al cliente, cuando se ha realizado la validación correspondiente el cliente queda autenticado.

Los módulos EAP que utilizan contraseñas para la autenticación de usuarios y no implementan un túnel seguro para transmitirlas son vulnerables a ataques de diccionario.

2.5.1.2. Autenticación con EAP-TLS

Este protocolo fue creado por *Microsoft* y se encuentra registrado en el RFC 2716, provee autenticación mutua con un alto nivel de seguridad; durante el proceso de autenticación, tanto el cliente como el servidor requieren certificados digitales.

EAP-TLS necesita de una infraestructura que permita mantener una administración adecuada de los certificados. Su implementación demanda de una inversión superior a la requerida por otros módulos EAP; por esto es recomendable para redes corporativas con un gran número de usuarios o en redes donde se requiera un alto nivel de seguridad.

a. Características

Trabaja sobre PPP (*Point to Point Protocol*) en enlaces punto a punto. Soporta el uso de tarjetas inteligentes, proporcionando un método de generación de claves dinámicas y autenticación más eficaz.

EAP-TLS sólo se admite en servidores RADIUS que sean miembros de un dominio. Los servidores de acceso remoto que se ejecutan como servidores independientes o miembros de un grupo de trabajo no admiten EAP-TLS.

b. Establecimiento de una Conexión con EAP-TLS

Cuando un cliente ingresa en el área de cobertura de un AP (autenticador), éste envía al AP una trama EAPOL *start*, para indicarle que desea establecer una conexión.

A continuación el AP solicita la identidad del cliente mediante una trama EAP de tipo EAP-Request/Identity, la identidad del cliente se envía en texto plano en una trama EAP-Response/Identity; luego, el AP encapsula la trama y se la envía al servidor en una trama RADIUS *Access Request*, que contiene el identificador del cliente.

El cliente y el servidor poseen una clave maestra, con esta clave establecen un túnel, si el servidor comprueba que el cliente posee la clave maestra envía un mensaje RADIUS *Access Success* hacia el AP, este mensaje contiene una clave de sesión que es enviada luego desde el AP hacia el cliente dentro de un mensaje EAP *Success*; entonces, el cliente obtiene su clave de sesión.

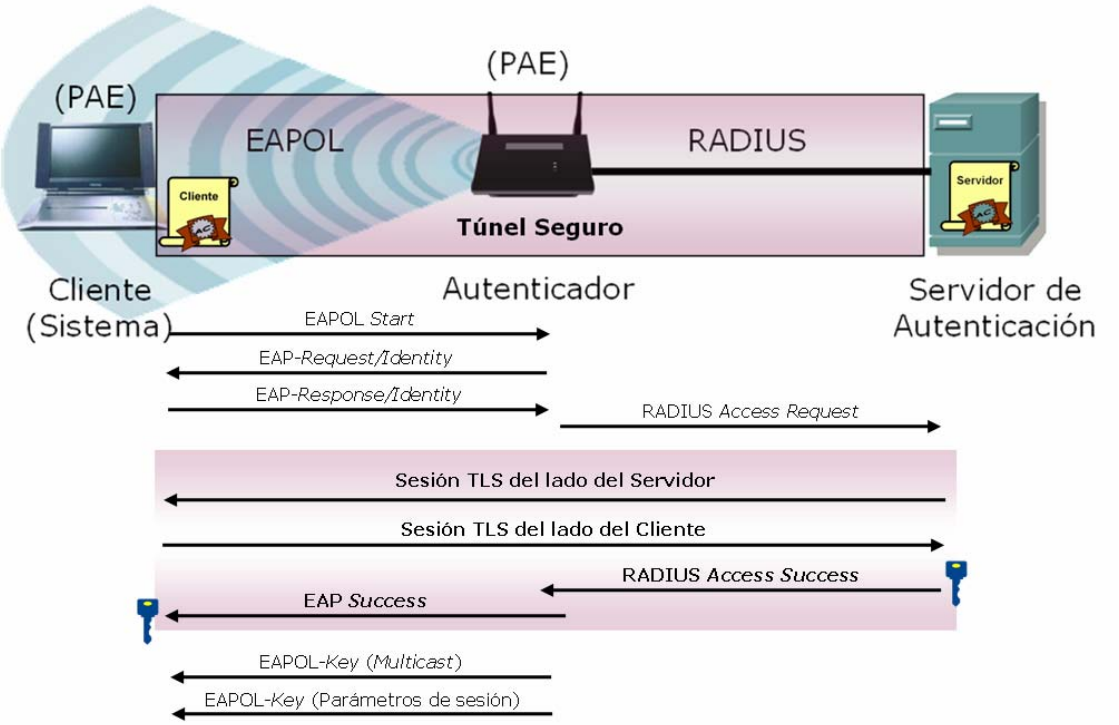

Figura 2.8 Inicio de una sesión EAP-TLS

El AP envía además dos tramas EAPOL-*Key* cifradas con la clave de sesión; la primera trama contiene una clave para mensajes *Multicast*, la segunda trama contiene los parámetros que se utilizarán durante la sesión. Este proceso se encuentra graficado en la figura 2.8.

Con la clave de sesión se inicia una comunicación cifrada entre el cliente y el servidor; ésta se inicia con un paquete EAP-TLS/*Start* enviado por el servidor, este paquete indica que el tipo de autenticación será EAP-TLS (EAP-*Type*=EAP-TLS), la trama tiene marcado el *bit* de inicio y no incluye datos.

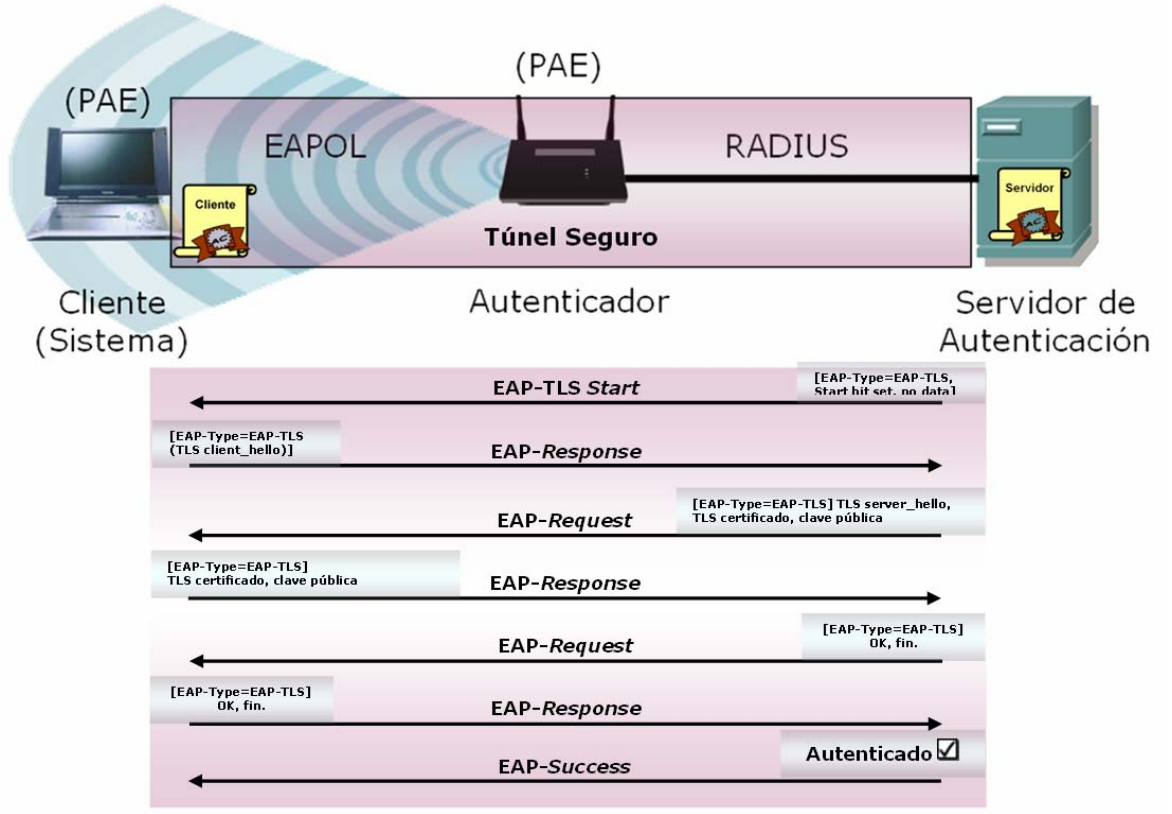

Figura 2.9 Establecimiento de una sesión EAP-TLS

Como respuesta el cliente envía una trama EAP-*Response*, esta trama contiene información TLS *client_hello* con los parámetros TLS soportados por el cliente; por ejemplo: versión TLS, identificador de sesión, un número generado aleatoriamente y características de encripción.

El servidor responde con una trama EAP-*Request* marcada con EAP-*Type*=EAP-TLS. El campo de datos de este paquete encapsula información TLS *server_hello* con los parámetros soportados por el servidor, este paquete incluye además el certificado digital del servidor y su clave pública.

Entonces el cliente envía una trama EAP-*Response* marcada con EAP-*Type*=EAP-TLS que contiene información sobre los parámetros seleccionados después de la negociación; incluye también su certificado digital y su clave pública, indica que la negociación ha terminado.

El servidor acepta los parámetros enviados por el cliente con una trama EAP-*Request* marcada con EAP-*Type*=EAP-TLS; en esta trama indica también que la negociación ha terminado.

El cliente contesta con una trama EAP-*Response* informando que recibió la trama; finalmente, el servidor envía una trama EAP-*Success* indicando que la autenticación fue exitosa. Este proceso se encuentra graficado en la figura 2.9.

c. Comparación entre los Diferentes Módulos EAP

El incremento en el nivel de seguridad dentro de una red siempre involucra inversión y un aumento en los procesos de administración. Cuando una red es más segura, los procesos se vuelven más complejos y por lo tanto se elevan los costos; además, se requieren equipos con mayores capacidades y sistemas operativos que manejen mayores funcionalidades.

Existen técnicas que logran que una WLAN sea extremadamente segura, esto es muy deseable; pero, debido a que involucran una inversión, siempre es necesario realizar un análisis previo que permita descubrir cuál es el nivel de seguridad que una red necesita, incluso si se cuenta con recursos ilimitados.

Para este análisis, se debe tener en cuenta que soluciones como WEP y WPA, ofrecen niveles básicos de seguridad, teniendo como ventaja sus bajos costos, otra ventaja es que no requieren de *software* especializado en el cliente. Estas soluciones son ideales para hogares y pequeñas empresas en donde no se maneje información que involucre propiedad intelectual.

Por otra parte, las soluciones 802.1x/EAP requieren de la implementación de un servidor RADIUS, lo que implica costos, requerimientos de administración y de ser posible una política de seguridad; sin embargo, si se demanda limitar la inversión,

soluciones como Desafío MD5, LEAP y FAST brindan un nivel aceptable de seguridad.

Las soluciones Desafío MD5, LEAP y FAST son recomendables para redes de medianas empresas en donde la información tiene importancia, pero no es la base fundamental para la operación de la empresa. También hay que considerar que soluciones como LEAP y FAST son propietarias y por lo tanto requieren equipos *Cisco* para ser implementadas.

Cuando se requiere compatibilidad e interoperabilidad, lo mejor que se puede escoger son las soluciones basadas en estándares, desafío MD5 y EAP-TLS[1], ya que son ideales. EAP-FAST y EAP-TTLS se encuentran definidos como I-Ds, aunque el *draft* de EAP-TTLS se encuentra caducado.

Para empresas con redes corporativas o para empresas en donde la información es crítica, lo más recomendable es la implementación con soluciones que involucren certificados digitales como EAP- TLS, PEAP y EAP – TTLS, pues brindan mayores niveles de seguridad.

Para PEAP y EAP-TTLS se requiere la creación de una autoridad certificadora, pues solo se necesita expedir certificados para los servidores y por lo tanto, no se requiere de una infraestructura que consuma mayores recursos.

En cambio, EAP-TLS requiere de la implementación de una PKI[2], lo que implica una inversión de tiempo y dinero e incremento en los procesos de administración; en este caso es obligatoria una política de seguridad. Esta solución garantiza un alto nivel de

---

[1] A pesar de que EAP-TLS fue creada por *Microsoft*, después de que se publicó su RFC varias empresas implementaron esta solución por lo que se la puede ejecutar en todo tipo de ambientes.

[2] *Public Key Infrastructure*.

seguridad debido a que establece un túnel seguro y la autenticación mutua se lleva a cabo con el uso de certificados digitales.

Característica	WEP/WPA	MD5	TTLS	PEAP	FAST	LEAP	TLS
Estándar	802.11	RFC 3748	I-D	---	I-D	---	RFC 2716
Certificado en el Cliente	No	No	No	No	No	No	Si
Certificado en el servidor	No	No	Si	Si	No	No	Si
Intercambio de claves WEP dinámicas	Si	No	Si	Si	Si	Si	Si
Suplantación de AP	No	No	No	No	Si	Si	No
Creador	IEEE	WS[1]	*Funk*	WS	*Cisco*	*Cisco*	WS
Atributos de autenticación	Mutua	Una Vía	Mutua	Mutua	Mutua	Mutua	Mutua
Servidor RADIUS	N/A	Si	Si	Si	Si	Si	Si
Protección de la identidad del cliente	No	No	Si	No	No	No	No
Plataformas de Cliente soportadas	*Linux*, *Windows* y *Mac*	*Linux*, *Windows* y *Mac*	*Linux*, *Windows* y *Mac*	*Windows*	*Linux*, *Windows* y *Mac*	*Linux*, *Windows* y *Mac*	*Linux, Windows*[2] y *Mac*
Ambientes recomendados para la solución	Hogar y pequeñas empresas	Empresas: pequeñas medianas	Mediana Corporativa	Mediana Corporativa	Mediana Corporativa	Mediana Corporativa	Mediana Corporativa
Requerimientos administración	Bajo	Bajo	Medio-Alto	Medio-Alto	Medio	Medio	Alto
Costo	Bajo	Medio	Medio-Alto	Medio-Alto	Medio	Medio	Alto
Dificultad de la Implementación	Fácil	Moderada	Moderada	Moderada	Moderada	Moderada	Compleja
Seguridad Inalámbrica	Pobre	Pobre	Alta	Alta	Alta	Alta[3]	Muy Alta

Tabla 2.4 Comparación entre las diferentes soluciones de seguridad para WLANs

[1] *Microsoft*.

[2] Solo plataformas que soporten ambientes ubicados dentro de dominios.

[3] Si se refuerza los generadores aleatorios para la generación de contraseñas.

Por otra parte, debido a que EAP-TLS involucra expedición de certificados para los clientes de una WLAN, también provee herramientas para asegurar el servicio de aceptación, por lo que es ideal para empresas en donde se realiza transacciones entre los usuarios.

La implementación de EAP-TLS en muchos casos puede aumentar la complejidad de la administración de una red; pero, en redes con usuarios distribuidos en distintas zonas geográficas facilita los procesos de administración que tienen que ver con el control de usuarios, pues se puede establecer una AC subordinada por cada zona mediante una jerarquía. Así se establece la identidad de un usuario y se lo ubica en una zona determinada y de ser necesario en un departamento de la empresa.

En la tabla 2.4 se muestra un cuadro con las diferentes características de cada solución.

d. Ventajas y Desventajas de EAP-TLS

Es importante establecer los beneficios que brinda EAP-TLS y sus posibles falencias y de acuerdo a esto seleccionar el tipo de redes a las que se adapta con mayor facilidad para evitar sub-utilización de los recursos.

d.1. Ventajas de EAP - TLS

Entre las principales ventajas de EAP-TLS, con respecto otras técnicas utilizadas para brindar seguridad dentro de redes WLAN se pueden mencionar:

- Utiliza certificados digitales como credenciales de clientes y servidores.
    - Establece una autenticación con un alto nivel de seguridad.
    - Facilita el establecimiento del servicio de aceptación.
    - Permite un mayor control de los usuarios.
    - Establece facilidades para la administración de acuerdo a la ubicación geográfica de un usuario e incluso al área en que se desempeña.

- Brinda confidencialidad de la información al establecer un túnel seguro.
- Es la solución que brinda el mayor nivel de seguridad para WLANs.
- Es un estándar lo que garantiza compatibilidad e interoperabilidad con varias plataformas.

d.2. Desventajas de EAP – TLS

Entre las principales desventajas de EAP-TLS, con respecto otras técnicas utilizadas para brindar seguridad dentro de redes WLAN se pueden mencionar:

- Requiere de la implementación de una PKI, en redes pequeñas esto incrementa innecesariamente los costos y los procesos de administración.
- El establecimiento de un túnel seguro requiere que los equipos tengan mayores capacidades, para que esto resulte transparente para los usuarios.
- Se encuentra poco difundida debido a que requiere de una infraestructura compleja.

2.5.1.3. IEEE 802.11i

El IEEE aprobó el estándar IEEE 802.11i en el año 2004, incluye WEP, TKIP y MIC; soporta AES-CCMP[1] con claves de 128 *bits* para la encripción de datos, las claves son generadas por PRF[2]. Establece cuatro tipos de claves, una clave maestra PMK[3] y tres claves que se obtienen a partir de ésta, KCK[4], KEK[5] y TK[6]; adicionalmente, define autenticación mediante 802.1x.

---

[1] *AES in **C**ounter Mode with **CBC-MAC** **P**rotocol.*

[2] *Pseudo-Random Function*.

[3] *Pairwise Master Key*, se utiliza como *token* para autorizar una sesión.

[4] *Key Confirmation Key*, se utiliza como clave de autenticación de sesión.

[5] *Key Encryption Key*, es utilizada para cifrar las claves.

[6] *Temporal Key*, se utiliza para cifrar una sesión.

802.11i define una arquitectura flexible que le permite adaptarse a diferentes ambientes como empresas grandes, medianas y pequeñas, usuarios finales, aplicaciones de hogar, etc.; proporcionando un *roaming* eficiente entre APs. Este estándar está enfocado en brindar los servios de autenticación, autorización, confidencialidad e integridad de los datos en redes 802.11.

Capítulo 3

INFRAESTRUCTURA DE CLAVES PÚBLICAS (PKI)

3. INFRAESTRUCTURA DE CLAVES PÚBLICAS (PKI)

La encripción 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. En este capítulo se estudiarán todos los aspectos relacionados con PKI, incluyendo: elementos, tipos de arquitectura, servicios prestados, ciclo de vida de claves y certificados, modelos de confianza, aplicaciones, y administración.

También se estudiarán las perspectivas de PKI en el Ecuador, enfocándose en el funcionamiento del PKI de la Banco Central, los servicios que brinda, su inserción en el mercado y una evaluación del progreso alcanzado mediante un estudio de mercado. Finalmente, se expondrán algunos de los estándares desarrollados por el Grupo de Trabajo PKIX[1] de la IETF.

3.1. AUTORIDAD CERTIFICADORA

Como se vio en el capítulo uno, un certificado digital es una credencial electrónica que permite vincular la identidad de un usuario con su pareja de claves pública/privada; por sus características, esta técnica de autenticación funciona como la principal herramienta para realizar transacciones seguras a través de una red.

Una de sus principales ventajas es que al utilizar certificados digitales, no se requiere que las partes que intervienen en una transacción intercambien información

[1] PKI X509.

previamente o se conozcan de antemano (teóricamente); ya que si un usuario posee la clave privada relacionada con la clave pública almacenada en un certificado, se comprueba que es el dueño del certificado digital y queda autenticado.

3.1.1. NECESIDAD DE CREAR CONFIANZA

Si cada usuario emite su propio certificado digital, un atacante puede suplantar un certificado real y sustituirlo por su propio certificado, de esta manera cuando un usuario lícito descargue su certificado e intente comprobar la identidad registrada en éste, el atacante demostrará que posee la clave privada y podrá suplantar al dueño legítimo de la identidad.

Esto implica la necesidad de un sistema de confianza vinculado a la autenticación basada en certificados digitales; este sistema se basa en la existencia de un tercero de confianza o TTP (*Trusted Third Party*).

En general, se conoce al tercero de confianza como AC (Autoridad Certificadora), debido a que se encarga de verificar la identidad de cada usuario y la autenticidad de sus claves pública/privada, luego de lo cual vincula el nombre del usuario y su clave pública a un certificado digital.

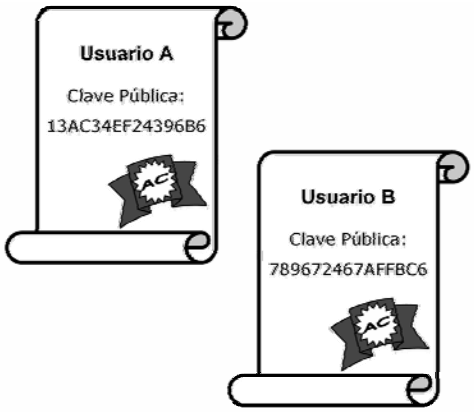

Figura 3.1 Certificados Digitales firmados por Autoridad Certificadora

Para evitar que los certificados generados por una determinada AC sean alterados posteriormente, ésta firma digitalmente cada certificado como se muestra en la figura 3.1, de esta manera los certificados se vuelven una estructura auto-protegida.

Para que el usuario A pueda confiar en la identidad registrada en el certificado del usuario B, y a su vez, el usuario B en la identidad registrada en el certificado del usuario A sin la necesidad de conocerse previamente, pueden acudir a una AC que goce de la confianza de los dos, y que certifique la legitimidad de sus identidades y la correspondencia entre las parejas de claves por medio de la expedición de un certificado digital.

El usuario A y el usuario B, deben tener registrada la clave pública de la AC para comprobar que la firma consignada al certificado es auténtica; en el mejor de los casos, tendrán su certificado digital o podrán descargarlo de un directorio.

Entonces, cada usuario puede obtener el certificado digital del otro y verificar la firma digital de la AC; con esto, se garantiza que el certificado no ha sido alterado y que la clave pública pertenece al usuario registrado en el certificado. Cuando un certificado se ha validado (correspondencia entre clave pública y privada), el propietario del certificado queda autenticado.

3.2. APLICACIONES QUE UTILIZAN CERTIFICADOS DIGITALES

Existen varias aplicaciones basadas en protocolos que manejan certificados digitales durante los procesos de autenticación y/o encripción; entre las principales aplicaciones se pueden mencionar:

- Establecimiento de sitios *Web* seguros.
- Creación de correos electrónicos seguros.
- Autenticación dentro de WLANs.

- Y en general la implantación de VPNs (*Virtual Private Network*).

3.2.1. SITIOS WEB SEGUROS

Las aplicaciones que utilizan certificados digitales para la autenticación de sitios *Web* son tal vez las más difundidas actualmente, estas aplicaciones permiten realizar transacciones seguras a través de un portal sin la necesidad de conocer al propietario del sitio o a sus auspiciantes.

Este tipo de aplicaciones utilizan protocolos que permiten una autenticación del lado del servidor [1]; es decir, el servidor posee un certificado digital que le permite autenticarse y establecer sesiones seguras a través de una red. Entre los protocolos más utilizados para crear sitios *Web* seguros se tiene a SSL (*Secure Sockets Layer*) y TLS (*Transport Layer Security*).

3.2.1.1. SSL

SSL es el protocolo más utilizado para la autenticación de sitios *Web*, fue publicado por *Netscape*, con el propósito de proveer privacidad e integridad entre dos aplicaciones que se comunican entres sí; actualmente su estado es I-D y se encuentra vigente la versión 3 publicada en 1996.

El protocolo está formado por dos capas, la capa inferior conocida como SSL *Record Protocol* puede funcionar sobre un protocolo de capa transporte confiable y es la encargada de la encapsulación de varios protocolos de capas superiores.

---

[1] También soportan autenticación del lado del cliente, pero esto no se utiliza frecuentemente a través de Internet.

La capa superior de SSL utiliza SSL *Handshake Protocol*; este protocolo permite al servidor y al cliente autenticarse entre sí, negociando el algoritmo y las claves de encripción antes de que el protocolo de aplicación transmita o reciba los primeros *bytes* de datos.

Las conexiones generadas al utilizar SSL proveen privacidad de los datos utilizando encripción simétrica, las claves simétricas son definidas inicialmente durante el proceso de *handshake*, siendo compatible con DES, RC4, etc.

SSL logra la autenticación del servidor utilizando encripción asimétrica con certificados digitales (RSA, DSS, etc.), la autenticación puede realizarse del lado del servidor o mutuamente entre cliente y servidor.

Para proporcionar integridad, SSL utiliza MACs (*Messages Authentication Codes*); los códigos MACs pueden utilizar los protocolos SHA o MD5 para el cálculo de los valores *hash* de los mensajes transmitidos.

Una ventaja de SSL es que el protocolo es independiente de la aplicación; es decir, un protocolo de capa superior puede funcionar conjuntamente con SSL de manera transparente.

3.2.1.2. TLS

El diseño de TLS se basó en SSL, la versión 1 de este estándar se encuentra registrada en el RFC 2246, publicado en Enero de 1999; además, se cuenta con la versión 1,1 en estado I-D, publicada en el 2005. El propósito de TLS fue proveer privacidad e integridad de los datos dentro de una comunicación entre aplicaciones.

Al igual que su predecesor, es independiente de la aplicación y se compone de las capas *Record Protocol* y *Handshake Protocol*, éstas cumplen con las mismas funciones.

Para lograr privacidad TLS utiliza encripción simétrica, las claves utilizadas durante la comunicación se generan por cada sesión establecida garantizando la reserva de la información. Para lograr una autenticación segura, TLS utiliza certificados digitales, siendo compatible con RSA y DSS.

La principal diferencia entre SSL y TLS es que TLS utiliza HMAC (*Hash* MAC) para comprobar la integridad de los paquetes, HMAC puede funcionar con una gran variedad de funciones *hash*, siendo compatible con MD5 y SHA-1(se pueden definir otros algoritmos); el algoritmo *hash* que va a ser utilizado dentro de una comunicación se define dentro del proceso de *handshake*.

3.2.2. CORREO ELECTRÓNICO SEGURO

Una de las aplicaciones más utilizadas en Internet es el correo electrónico o *e-mail*. Actualmente, se envían mensajes dentro de organizaciones o fuera de ellas; estos mensajes viajan por las redes en texto plano y de manera insegura, siendo susceptibles a modificaciones y suplantaciones durante el trayecto.

Considerando el amplio uso de los *e-mails* dentro de todo tipo de empresa u organización, es necesario utilizar aplicaciones que utilicen protocolos que incluyan servicios de autenticación y encripción de los mensajes. Entre los protocolos más utilizados para lograr aplicaciones de correo electrónico seguro se tiene a S/MIME (*Secure/ Multipurpose Internet Mail Extensions*) y PGP (*Pretty Good Privacy*).

3.2.2.1. S-MIME

MIME es un protocolo diseñado para proporcionar mecanismos que permiten enviar diferentes tipos de archivos a través de Internet y de forma transparente para el usuario; sus especificaciones se encuentran registradas en los RFCs 2045, 2046,

2047, 2049 y 4289[1]. Este estándar define formatos, cabeceras y cuerpos, tipos de medio, procedimientos de registro, estructura del mensaje, etc.

El estándar MIME especifica todos los valores y campos que proveen la estructura esencial para la transmisión de mensajes, pero no especifica ningún tipo de seguridad para proteger la información enviada a través de una red.

Debido a la falta de sistemas de seguridad dentro del estándar MIME, empresas como *Qualcomm*, *Microsoft*, *Lotus*, *VeriSign*, *Netscape* y *Novell* (entre otras) crearon S-MIME. El estándar general se encuentra registrado en los RFC 3850 y 3851; en diciembre de 2005 se expidió el RFC 4262 con información específica para el manejo de certificados X.509.

S-MIME define servicios que permiten utilizar la sintaxis PKCS#7[2] para el manejo de de firmas digitales y encripción de archivos que se transmiten utilizando MIME. No se limita solo a correos electrónicos, puede utilizarse con todos los tipos de mensajes soportados por MIME.

Dentro de sus especificaciones se permite cifrar una parte de un mensaje[3] o todo el mensaje y firmarlo digitalmente; también se puede firmar el mensaje y cifrarlo después, para lo cual se utiliza CMS (*Cryptographic Message Syntax*). S/MIME utiliza por defecto SHA-1 para asegurar integridad y DSA para firmas digitales y autenticación.

---

[1] La serie 2045-2049 fue publicada en Noviembre de 1996 y el RFC 4289 se publicó en Diciembre de 2005.

[2] Estándar diseñado por RSA *Laboratories*, define la sintaxis general para mensajes que incluyen elementos criptográficos como firmas digitales y encripción.

[3] O partes.

3.2.2.2. PGP

PGP maneja criptosistemas de clave pública, para proveer a aplicaciones de correo electrónico [1] los servicios de autenticación y confidencialidad; generalmente, es utilizado para correos enviados a través de Internet. Fue desarrollado en 1991 por *Phil R. Zimmerman*; ha ganado gran popularidad y es utilizado por millones de personas dentro de la *World Wide Web*.

Entre las características que han logrado que PGP llegue a ser tan popular como herramienta de seguridad se puede mencionar a su gran flexibilidad para funcionar sobre un gran número de plataformas; además, la encripción de los mensajes es segura y rápida.

La IETF publicó en 1996 el RFC 1991 con especificaciones que definen el funcionamiento de PGP; además, para lograr la interoperatividad con sistemas S/MIME, publicó en 1997 y 1998 los RFCs 2440 y 3156, respectivamente. También se cuenta con versiones comerciales de PGP, su última versión comercial es la 9[2].

PGP brinda los servicios de integridad (SHA-1 con clave de 160 *bits*), autenticación con firmas digitales, compresión, intercambio de claves simétricas (RSA o *Diffie−Hellman*), encripción[3], conversión a base 64[4] y segmentación de los mensajes transmitidos.

Para lograr una autenticación segura PGP utiliza certificados digitales, éstos se almacenan en un servidor de certificados; soporta dos formatos de certificados: X.509 y certificados con formato PGP.

---

[1] Se puede utilizar también para cifrar archivos en disco.

[2] El código fuente de la versión 8 está liberado y se lo puede descargar de la página oficial de PGP: http://www.pgpi.org/.

[3] IDEA, 3−DES o CAST−128, la clave simétrica generada se utiliza únicamente durante una sesión.

[4] Para lograr compatibilidad con diferentes formatos.

Además, utiliza dos tipos de claves conocidas como *PGP Keys* y *Key Ring*; las claves PGP son la pareja de claves pública/privada de cada usuario. Las claves conocidas como *Rings*, pueden ser públicas o privadas, las *Rings* públicas contienen una colección de las claves públicas de todos los usuarios PGP del sistema.

Cada usuario del sistema maneja una o varias parejas de claves pública/privada, las claves *Rings* privadas contienen estas parejas de claves; para proveer de confidencialidad e integridad a las parejas de claves, todas las parejas utilizadas por un usuario se empaquetan y se cifran con una clave simétrica obtenida a partir de una contraseña proporcionada por el usuario.

3.2.3. AUTENTICACIÓN DENTRO DE WLANS

Como se vio en el Capítulo 2, existen varios esquemas que utilizan certificados digitales para la autenticación dentro de redes WLAN; estos esquemas se basan en el estándar 802.1X que utiliza las características de acceso físico de los estándares IEEE 802, para proporcionar los servicios de autenticación y control de acceso.

3.2.3.1. PEAP

Es un protocolo propietario de *Microsoft*, para la autenticación el usuario debe enviar su contraseña hacia el servidor, la identidad del usuario es protegida mediante el uso de MSCHAPv2, cuando la clave es validada el usuario queda autenticado. El servidor se autentica ante el usuario utilizando un certificado digital.

3.2.3.2. EAP-TTLS

Fue creado por *Funk Software* y *Certicom*, provee una autenticación segura mediante el establecimiento de un túnel con el protocolo TLS. Después de establecer

el túnel TLS, se produce la autenticación del servidor mediante certificados digitales; los clientes se autentican utilizando contraseñas. Las contraseñas son validadas en el servidor utilizando CHAP, PAP, MS-CHAP y MS-CHAPv2.

3.2.4. VPNs

Una VPN forma un túnel virtual, éste permite a un usuario lograr una comunicación segura a través de una conexión entre su estación de trabajo y un servidor corporativo. Este tipo de tecnología se utiliza en redes públicas para el establecimiento de conexiones seguras, obteniendo privacidad sin la necesidad de la contratación de líneas dedicadas.

En general, las VPNs se utilizan para facilitar conexiones en tres tipos de situaciones: clientes remotos, conexión con múltiples oficinas y accesos *extranet*. Actualmente, se encuentra muy difundido el uso del protocolo IPSec (*Internet Protocol Security*) para el establecimiento de VPNs.

3.2.4.1. IPSec

Fue desarrollado por el IETF para proveer soluciones de seguridad compatibles con el protocolo IP[1] y se encuentra registrado en el RFC 2401; puede funcionar en ambientes UDP[2] o TCP[3] siendo compatible con el protocolo ICMP[4].

IPSec utiliza certificados digitales para establecer niveles de confianza adecuados antes de formar la VPN. Su diseño le permite brindar los servicios de autenticación

---

[1] No es compatible con IPX.

[2] *User Datagram Protocol*.

[3] *Transmission Control Protocol*.

[4] *Internet Control Message Protocol*.

(certificados digitales), integridad y confidencialidad; cuenta adicionalmente con un sistema de administración de claves y protección contra ataques tipo *replay*[1].

Para conseguir seguridad en las comunicaciones, IPsec emplea los protocolos AH (*Authentication Header*) y ESP (*Encapsulating Security Payload*), con el fin de proteger la privacidad de los paquetes; cuando se inicia una sesión IPSec, se negocian todos los parámetros que se van a utilizar entre el cliente y el servidor, no se requiere utilizar AH y/o ESP obligatoriamente.

El protocolo IPSec soporta dos modos de trabajo, modo túnel y modo transporte; el modo túnel permite proteger el paquete IP completo, mientras que el modo transporte cifra sólo los datos de capas superiores.

Para proteger la integridad de los paquetes, IPsec emplea HMAC conjuntamente con una clave secreta a la que se aplica una función *hash* (MD5 o SHA), el HMAC resultante es incluido en la cabecera del protocolo IPsec; el receptor puede verificar la integridad del paquete basándose en la clave secreta de sesión.

La confidencialidad se logra utilizando encripción simétrica de los paquetes, las especificaciones IPsec exigen la implementación de NULL y DES; también soporta 3DES, AES y otros.

3.3. ARQUITECTURA PKI

El concepto de AC introduce un conflicto, el hecho de que una AC emita certificados digitales, no implica que otros usuarios confíen en éstos; entonces, ¿cómo encontrar una entidad a la que todos los usuarios le tengan confianza?, y si se encuentra una

[1] Este tipo de ataque se encuentra bajo la categoría de negación de servicio, su objetivo es saturar a un servidor reenviando mensajes lícitos.

AC que goce de la confianza de todos los usuarios; ¿cómo solucionar los problemas de escalabilidad, administración o compromiso de su clave[1]?

Se puede considerar que ciertas entidades pueden ser confiables para un grupo de usuarios, para determinadas transacciones y bajo ciertas circunstancias, de esta manera no es necesario que una única AC emita todos los certificados.

Sin embargo, esta solución no funciona a gran escala, debido a que no permite que usuarios que pertenecen a distintos sectores realicen transacciones entre sí, al menos no sin conseguir primero los certificados de las ACs que emitieron los certificados de los involucrados en la transacción, lo que introduce nuevamente el peligro de la suplantación de certificados.

Debido a la falta de escalabilidad, complicada administración y falta de credibilidad de una sola AC (no todos los usuarios confían en ésta), se creó el concepto de PKI (*Public Key Infrastructure*).

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.

Existen varias recomendaciones y estándares que establecen normas para el funcionamiento de PKI, a continuación se presenta una lista con las principales recomendaciones existentes.

---

[1] Si la clave privada de la AC se ve comprometida, todos los certificados digitales emitidos a partir de la fecha de compromiso de la clave deben ser revocados y la AC pierde credibilidad.

- **Q.817**: Certificados digitales de la infraestructura de claves públicas de la red de gestión de las telecomunicaciones y perfiles de listas de revocación de certificados. UIT-T[1].

- **X.509**: *Information technology – Open systems interconnection – The directory: public-key and attribute certificate frameworks*. UIT-T.

- **RFC 3280**: *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. IETF.

- **RFC 3647**: *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*. IETF.

- **PKCS [2]** : Estándares desarrollados por RSA *laboratories* para lograr interoperabilidad entre aplicaciones que utilizan encripción asimétrica para la autenticación.

- **TS 101 456 v1.2.1**: *Policy requirements for certification authorities issuing qualified certificates*. ETSI[3].

- **TS 102 042 v1.1.1**: *Policy requirements for certification authorities issuing public key certificates*. ETSI.

3.3.1. ELEMENTOS PKI

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.

---

[1] Unión Internacional De Telecomunicaciones: Sector de Normalización de las Telecomunicaciones.

[2] *Public Key Cryptography Standards*.

[3] *European Telecommunications Standards Institute*.

3.3.1.1. AR (Autoridad de Registro)

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

Es tal vez el elemento más importante dentro de una PKI, 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.

Por ejemplo, se puede expedir un certificado tan sólo con la presentación de un correo electrónico vía *Web*[1]; por otro lado, para lograr un mayor nivel de confianza se puede solicitar la presencia del individuo con un formulario respaldado con documentación como una cédula de identidad personal, pasaporte, fotografías, dirección, teléfono e incluso referencias personales.

Después de comprobar la identificación de una entidad en particular, la AR que ha verificado los datos, certifica que una identidad es auténtica y que los datos proporcionados son confiables y reales. Esta certificación de confianza hace referencia únicamente a la identidad y no al comportamiento de la entidad propietaria de la identidad.

La AR también está encargada de proporcionar a los usuarios información relacionada con las directivas de la PKI y el ciclo de vida de certificados y claves, lo que implica notificar a los usuarios en caso de compromiso de claves o revocación de certificados.

---

[1] Este procedimiento no arrojará mucha confianza.

Una AR puede estar conformada por personal de una empresa, por un servidor o por una combinación de ambos; el establecer ARs formadas por personal de una organización garantiza niveles elevados de seguridad debido a que las verificaciones se realizan personalmente.

En general, una infraestructura PKI cuenta con una AR cuando necesita niveles adecuados de escalabilidad y seguridad o cuando se maneja sucursales distribuidas en diferentes zonas geográficas. Cuando la infraestructura es limitada, las funciones de la AR son transferidas a la AC.

a. Régimen Legal: AR

El Reglamento de la Ley 67 (Ley de Comercio Electrónico) establece como responsabilidad de la AR la verificación de todos los datos que se van a incluir en un certificado digital. Los documentos utilizados durante el proceso de verificación podrán ser solicitados por el CONATEL para comprobar su autenticidad y exactitud.

La autoridad que presta este servicio, debe garantizar que los datos proporcionados por un usuario serán utilizados únicamente dentro del proceso que permita su identificación y que la información suministrada no será divulgada y permanecerá bajo custodia.

El CONATEL expidió adicionalmente la Resolución 584 el 23 de octubre de 2003, ésta incluye el “Reglamento para Acreditación de Servicios de Comercio Electrónico”; con el fin de regularizar todos los aspectos relacionados con PKI.

La resolución 584 indica que una entidad de registro debe certificarse con el CONATEL, para lo cual debe estar relacionada con una AC acreditada o con una AC extranjera registrada y autorizada por el CONATEL.

3.3.1.2. AC y Certificados Digitales

La AC 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 AC 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 AR ha realizado las verificaciones pertinentes, la AC se encarga de la emisión de certificados digitales; de acuerdo al propósito para el que fue diseñada la PKI y el papel que efectúa la AC, 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 ACs. En el caso de certificados emitidos para otras ACs, se tiene la siguiente sub-clasificación:

- **Certificados Auto-Expedidos**.- Este tipo de certificados tiene como característica que el nombre de propietario coincide con el nombre de la AC que firma el certificado.

A pesar de pertenecer al mismo dueño, la clave pública registrada en el certificado no corresponde a la clave privada del que lo firma. Este procedimiento se lleva a cabo cuando una pareja de claves ha caducado; entonces, se firma con la clave privada antigua para validar la clave pública nueva.

- **Certificados Auto-Firmados**.- Éste es un caso particular del anterior, se presenta cuando la clave pública validada y la clave privada con que se firma son pareja, en la figura 3.2 se muestra un certificado auto-firmado.

Figura 3.2 Certificado Digital Auto-firmado

- **Certificados Cruzados**.- Son certificados expedidos para una AC y firmados por una segunda AC; a su vez la primera AC puede firmar el certificado de la segunda. En la figura 3.3 se tiene el certificado digital de la Autoridad Certificadora 2, éste está firmado por la Autoridad Certificadora AC.

Figura 3.3 Certificado Digital Cruzado

b. Suspensión, Reactivación y Revocación

Cuando una AC 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 AC que no hará uso de éste durante un período, para evitar que durante su ausencia se haga uso del certificado la AC debe inhabilitarlo.

Cuando el usuario requiera hacer uso de su certificado nuevamente, la AC 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 AC 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 AC 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 AC 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*).

b.1. Régimen Legal: Suspensión, Reactivación, Revocación y CRLs

La eliminación de los derechos del uso de un certificado conlleva tanta responsabilidad como su expedición. La Ley 67 indica que un usuario se someterá a la suspensión de su certificado si se comprueba irregularidades en la información que presentó para acceder al certificado o si incumple las directivas de la AC.

La AC tiene la obligación de notificar al titular del certificado de la suspensión y sus causas; cuando se hayan eliminado las causas de la suspensión la AC debe reactivar el certificado.

Según la Ley 67, es el CONATEL y no la AC el ente encargado de las revocaciones. El CONATEL podrá revocar un certificado cuando la AC cese en sus actividades y los certificados vigentes no sean asumidos por otra o cuando se produzca la quiebra técnica de la AC; el CONATEL está obligado a notificar al titular de la revocación y sus causas. Como se puede observar los motivos de revocación difieren del estándar.

Tanto la suspensión como la revocatoria tienen efecto desde el momento en que se notifica al titular; cuando se trate de terceros afectados, la revocación y suspensión tendrán efecto desde el momento en que se publique la CRL correspondiente.

La AC es responsable de la publicación de CRLs y la respectiva notificación a todas las entidades pertinentes, si la notificación o publicación no se realizan a tiempo, se la considera responsable de los perjuicios.

c. Régimen Legal: AC

La Ley 67 establece que una AC puede estar conformada por empresas unipersonales o personas jurídicas, que gocen de la autorización del CONATEL. Dentro de la Resolución 584, el CONATEL obliga a las ACs a obtener un título habilitante para su acreditación.

Para obtener una acreditación, una AC debe demostrar solvencia técnica, logística y financiera para prestar servicios a sus usuarios; debe garantizar asistencia permanente, inmediata, confidencial, oportuna y segura del servicio de certificación. Además, está obligada a mantener sistemas de respaldo de toda la información relacionada con los certificados que ha expedido.

Las revocaciones y suspensiones deben ser ordenadas por el Superintendente de Telecomunicaciones. Para asegurar a los usuarios en los casos en que las revocaciones o notificaciones no se den de forma oportuna, la AC debe entregar una garantía, si ésta no es suficiente, la AC debe responder con su patrimonio.

Cuando una AC sea responsable de daños y perjuicios a cualquier entidad[1], ésta se atendrá a las sanciones previstas en la Ley Orgánica de Defensa del Consumidor. Para que una AC descargue responsabilidades sobre los usuarios que realizaron actos indebidos, ésta debe incluir en los contratos una cláusula de responsabilidad en la que se contemplen garantías.

Finalmente, se delega al COMEXI[2] para la promoción y difusión del uso de tecnologías que involucren el uso de firmas electrónicas y comercio electrónico; el CONATEL queda delegado como organismo de regulación, autorización y registro de las ACs acreditadas y la Superintendencia de Telecomunicaciones queda encargada del control de las entidades acreditadas.

3.3.1.3. 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

---

[1] Persona natural o jurídica.

[2] Consejo de Comercio Exterior e Inversiones.

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.

Existen diferentes maneras de proporcionar un servicio de directorio. Algunos servicios de directorio son locales, por lo que proporcionan un servicio restringido; otros servicios son globales, generalmente distribuidos.

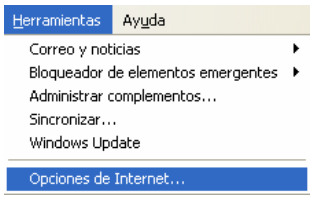

Figura 3.4 Menú del IE

Un usuario puede encontrar certificados almacenados en el navegador de su PC; en la figura 3.4 se muestra el menú de Herramientas del IE[1]. Al seleccionar Opciones de Internet se despliega la ventana mostrada en la figura 3.5; la pestaña de contenido permite seleccionar el botón Certificados. Como se ve en la figura 3.6 éste despliega información de los certificados almacenados en el IE.

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

[1] *Internet Explorer*.

UIT-T X.500 (*Directory Access Protocol*-DAP), debido a que esta norma se adapta a la sintaxis de los certificados digitales.

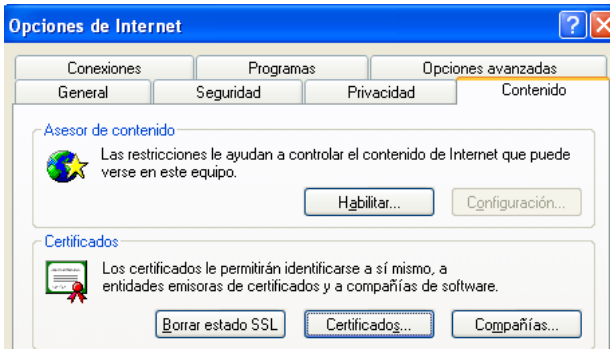

Figura 3.5 Opciones de Internet de IE

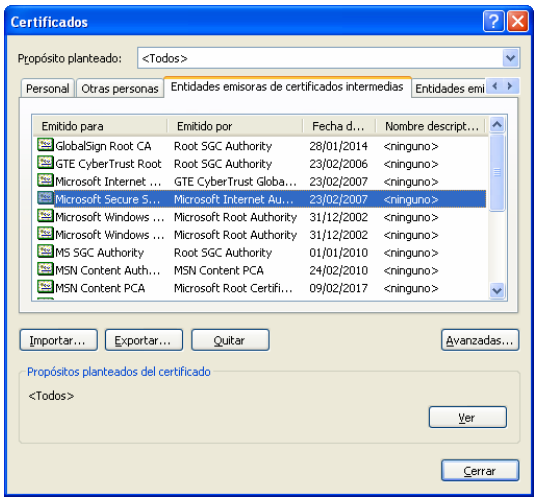

Figura 3.6 Certificados almacenados en el directorio de IE

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), la versión tres de esta recomendación se encuentra registrada en el RFC 2251 y fue publicada por la IETF en 1997, ésta se halla basada en la norma X.500.

LDAP permite almacenar y recuperar certificados digitales, consumiendo menos recursos que X.500[1] y resulta menos complejo; funciona sobre TCP/IP, por lo que permite gran interoperatividad.

Adicionalmente, la IETF ha definido el RFC 2585[2] con especificaciones para el uso de directorios FTP[3] y HTTP[4] para la descarga de certificados y CRLs.

3.3.1.4. 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 AR, cuando ésta ha identificado a la entidad, entrega la solicitud a la 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 PKI sea transparente para el usuario, se puede recurrir al uso de *tokens* o tarjetas inteligentes para el almacenamiento de certificados y claves.

3.3.1.5. 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.

---

[1] La norma X.500 cubre todas las capas del modelo OSI.

[2] *Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP*.

[3] *File Transfer Protocol*.

[4] *Hypertext Transfer Protocol*.

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.

3.3.1.6. Directivas

Las directivas son las reglas que rigen una PKI y deben estar disponibles para todos los usuarios de la PKI y restringidas para todos los demás, pues contienen información del funcionamiento de la PKI 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 PKI.

El documento que contiene la CP 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 PKI.
- Obligaciones de cada elemento de la 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.

Una CP debe funcionar en forma paralela a la política de seguridad de la empresa; pero cuando se trata de entablar relaciones de confianza con otras organizaciones, las CPs se toman como referencia. Si al comparar las CPs involucradas, éstas manejan niveles de seguridad equivalentes, las organizaciones pueden crear una relación de confianza entre sí.

Las políticas de certificación se identifican por OIDs (*Object Identifiers*, basados en ASN.1[1]), estos identificadores forman entre sí una estructura de árbol constituida por una secuencia de enteros que permite la localización de una CP.

b. Declaración de Prácticas de Certificación

También conocida como CPS[2], define cómo se va a implementar y dar soporte a las CPs. 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 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:

---

[1] *Abstract Syntax Notation One*. Es una notación única que permite codificar un mensaje de manera independiente del lenguaje y la plataforma. UIT-T *Study Group* 17.

[2] *Certification Practice Statement*.

- La CP con la que se asocia la CPS.
- Información de todos los procesos por los que pueden pasar los certificados.
- Periodo de validez del certificado de la AC.
- Circunstancias bajo las cuales la AC puede revocar un certificado.
- Políticas de manejo de las CRLs, intervalos de publicación y puntos de distribución.
- Algoritmos criptográficos utilizados por la AC.

3.3.2. TIPOS DE ARQUITECTURA

Las arquitecturas PKI pueden ser implementadas de diversas maneras, de acuerdo al número de ACs y las relaciones existentes entre éstas. Entre los principales tipos de arquitectura se pueden mencionar a las arquitecturas planas, jerárquicas y tipo malla.

3.3.2.1. Arquitectura Plana

Ésta es la forma más básica de arquitectura PKI, en esta arquitectura existe sólo una AC, la misma que está encargada de generar y distribuir los certificados y las CRLs a las entidades destino. Este tipo de arquitectura no permite que otras ACs ingresen a la PKI, por lo que la única AC existente no establece relaciones de confianza con otras ACs.

Todas las entidades confían en la AC y usan sólo los certificados expedidos por ésta, las entidades se comunican entre sí manteniendo como punto de confianza a la AC, como se muestra en la figura 3.7.

La arquitectura plana es la más fácil de implementar debido a que implica la creación y control de una AC; pero como consecuencia presenta un punto único de falla, si la

clave privada de la AC se ve comprometida, todos los certificados emitidos deben ser revocados, lo que implica un desplome completo de la PKI.

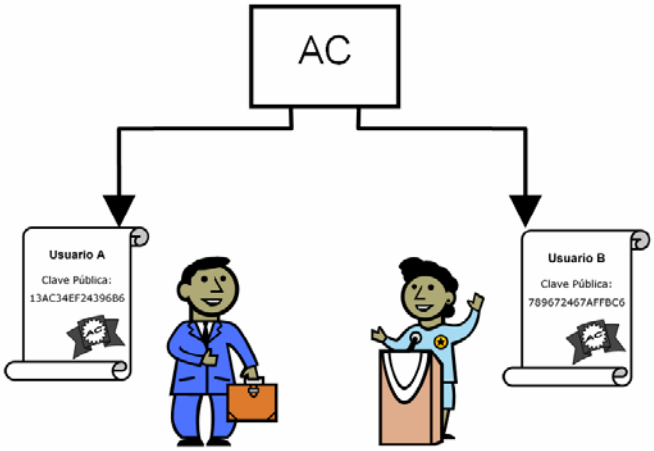

Figura 3.7 Arquitectura Plana

En caso de compromiso de la clave privada de la AC, todas las entidades que dependen de sus servicios de certificación deben ser informadas inmediatamente, luego de lo cual la AC debe ser remplazada por una nueva. El compromiso de la clave privada implica también la pérdida de confianza en la PKI; por esto, su clave privada debe guardarse conservando un alto nivel de seguridad.

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 PKI.

Actualmente se cuenta con varios sistemas de PKI basados en una arquitectura plana, como las ACs no establecen relaciones de confianza entre ellas, son los usuarios los encargados de mantener listas de ACs de su confianza y verificar las CRLs emitidas por cada una; por el momento, esto permite la autenticación de servidores *Web* sin la necesidad de una estructura PKI mundial.

Esto funciona siempre y cuando los usuarios estén capacitados para distinguir entre una AC confiable y otra que no lo es, en la mayoría de los casos los usuarios no cuentan con el conocimiento necesario y aceptan confiar en certificados que no han sido expedidos bajo un sistema adecuado.

3.3.2.2. Arquitectura Jerárquica

Si bien es cierto que una arquitectura plana funciona de manera adecuada cuando se trata de organizaciones pequeñas, ésta deja de ser funcional cuando las organizaciones incrementan su tamaño. A medida que las organizaciones van creciendo, la delegación de la administración y distribución de claves y certificados se convierte en un factor primordial para lograr eficiencia en los procesos PKI.

Para distribuir las funciones de una única AC entre múltiples ACs se requiere de otro tipo de estructura. Para esto, la arquitectura jerárquica basa su funcionamiento en el establecimiento de entidades raíces y entidades subordinadas; sin embargo, cada AC dentro de la jerarquía debe cumplir funciones semejantes a las de una AC de arquitectura plana.

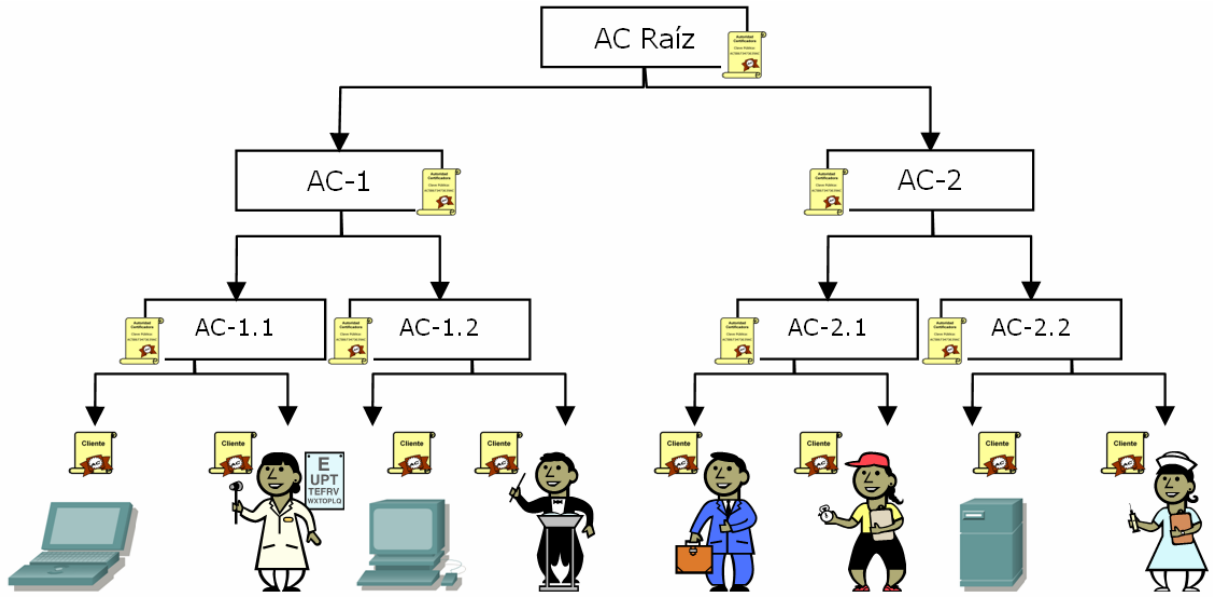

Figura 3.8 Arquitectura Jerárquica

Dentro de este tipo de arquitectura, todas las ACs miembros de la PKI mantienen relaciones de confianza conectadas por enlaces superior-subordinada, formando una estructura de árbol invertido como se muestra en la figura 3.8.

La estructura de árbol invertido mostrada en la figura 3.8 indica que la AC raíz emitió los certificados del segundo nivel de ACs subordinadas, las misma que a su vez emitieron los certificados de un tercer nivel; las ACs del tercer nivel solo emiten certificados de entidad destino.

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

La AC raíz por lo general emite certificados para otras ACs y no para entidades destino; en cambio, las ACs subordinadas, pueden emitir certificados de otras ACs o de entidad destino de acuerdo a la estructura de la PKI.

Este tipo de arquitectura introduce mejores condiciones de escalabilidad, debido a que se puede asignar una AC subordinada por locación geográfica y a su vez ésta puede mantener ACs subordinadas por departamento o área dentro de una empresa, lo que facilita el crecimiento de la estructura PKI.

La complejidad introducida por este tipo de arquitectura es aceptable, debido a que las verificaciones se realizan en forma unidireccional; es decir, todas las comprobaciones de confianza dentro de una PKI jerárquica se realizan tomando como punto común de confianza la AC raíz.

Si antes de llegar a la AC raíz se localiza un punto común de confianza no se requiere llegar a ésta; por ejemplo, en la figura 3.8, si un propietario de un certificado

emitido por la AC-1.1 requiere validar un certificado emitido por la AC-1.2, éste debe llegar a la AC-1 que es el punto común de confianza entre la AC-1.1 y la AC-1.2.

Si la PKI ha sido planeada cuidadosamente, las validaciones pasarán por pocos enlaces consumiendo pocos recursos; en todo caso, el mayor camino que se puede tomar para una validación de un certificado, es desde una entidad destino con un certificado emitido por una AC subordinada del nivel inferior hasta la AC raíz.

A pesar de todas sus ventajas, una arquitectura jerárquica mantiene el punto único de falla, debido a que la AC raíz controla toda la estructura de la PKI. En caso de compromiso de la clave de la AC raíz, toda la infraestructura pierde su funcionalidad. En cambio, el compromiso de la clave de una AC subordinada se puede resolver con mayor agilidad y sin afectar de gran manera al sistema.

Sin embargo, debido a que una AC raíz emite certificados y CRLs de ACs subordinadas y estos procedimientos están sometidos a planificación, la AC raíz puede mantenerse desconectada para guardar un alto nivel de protección del sistema, así el compromiso de su clave será un evento casi improbable.

Debido a todas sus ventajas y funcionalidades, puede ser implementada en instituciones gubernamentales y grandes corporaciones. Sin embargo, por el momento resulta complejo lograr una estructura jerárquica a nivel mundial, debido a que cada PKI establecida cuenta con su infraestructura y directivas; además, el emitir certificados digitales confiables reporta ganancias y muchas empresas no desean compartir sus ganancias.

3.3.2.3. Arquitectura Tipo Malla

Una PKI con arquitectura jerárquica es útil para el manejo interno de los certificados digitales dentro de grandes organizaciones o incluso entre organizaciones asociadas,

pero cuando se requiere establecer relaciones de confianza con otras organizaciones más distantes, esta arquitectura no es suficiente.

La arquitectura tipo malla permite que ACs que se encuentran dentro de organizaciones aisladas, logren interconectarse estableciendo relaciones de confianza sin modificar su infraestructura. Para esto se utilizan certificados cruzados, cada AC necesita certificados emitidos por las otras ACs que forman la malla.

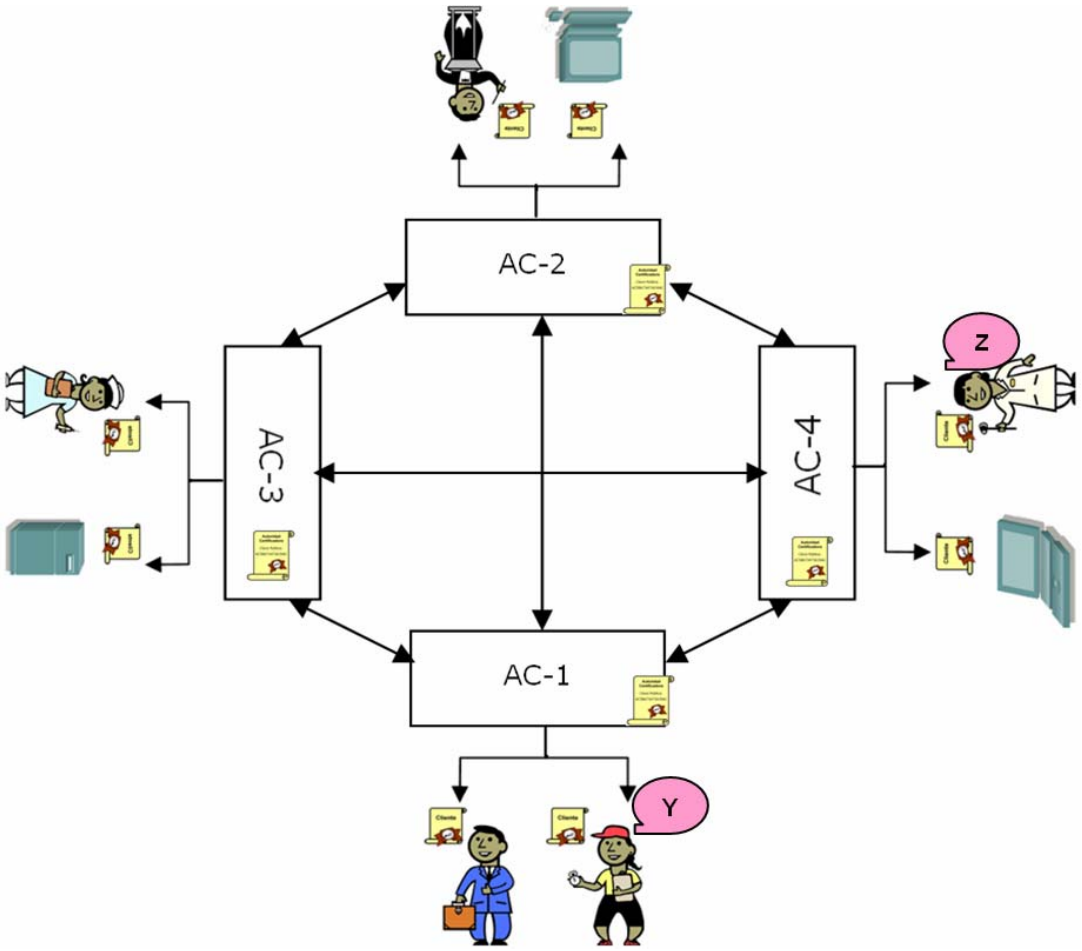

Figura 3.9 Arquitectura Tipo Malla

Como se ve en la figura 3.9, cada AC establece relaciones de confianza bidireccionales con las otras ACs dentro de la malla, manteniendo las relaciones

unidireccionales para las entidades destino. De esta manera, se cuenta con varios puntos de confianza para la validación de certificados.

Este tipo de arquitectura brinda escalabilidad y flexibilidad dentro de un sistema PKI, debido a que se puede añadir una AC fácilmente sin ser necesario que todas las ACs de la malla emitan un certificado para ésta; además, el compromiso de la clave de una AC afecta sólo a las entidades directamente relacionadas con ésta.

Debido a que no todas las ACs de la malla están obligadas a emitir certificados para las demás, el proceso de validación de certificados resulta más complejo, pues se debe establecer el camino que vincule al certificado con el punto de confianza de la entidad confiante, este camino puede tomar varias rutas y algunas rutas pueden presentar lazos; en el peor de los casos, el camino puede ser igual al número de ACs dentro de la malla.

El hecho de que las ACs posean certificados emitidos por cada AC miembro de la malla, aumenta la complejidad en la distribución de certificados y listas de revocación; adicionalmente, se debe considerar también el riesgo de que una AC emita un certificado para una AC no confiable.

Las arquitecturas jerárquica y tipo malla pueden trabajar dentro de modelos híbridos, de acuerdo a la conveniencia de las organizaciones participantes, de esta manera se puede tener una PKI jerárquica dentro de una organización y pertenecer a una PKI tipo malla formada por varias organizaciones.

3.3.3. RÉGIMEN LEGAL: ARQUITECTURA PKI

Dentro de la resolución 584 expedida por el CONATEL, se considera como elementos PKI: *software*, *hardware*, redes de información, políticas, procedimientos y

todo elemento que tenga como fin proporcionar soporte para la operación de los servicios de certificación o relacionados.

Como se dijo anteriormente, para el establecimiento de una PKI se debe obtener un título habilitante para la AC y AR, el mismo que será otorgado por la SENATEL[1], previa autorización del CONATEL; éste tiene una duración de 10 años y puede ser renovado. Está prohibido transferir de forma total o parcial los permisos para realizar certificaciones.

El título habilitante requiere que el subscriptor fije un domicilio en territorio ecuatoriano. Las instalaciones de la PKI deben basarse en las recomendaciones UIT-X.509, ETSI y CEN[2]; además, deben contar con niveles de seguridad adecuados, control de acceso, resguardo de documentos y protección contra siniestros.

Los certificados emitidos deben tener un identificador único y está prohibida la expedición de certificados de prueba o demostración. Los sistemas de encripción deben estar basados en algoritmos públicos.

Los contratos entre entidades destino y ACs o ARs acreditadas deben ser aprobados por el CONATEL antes de entrar en vigencia; en caso de terminación del título habilitante, el CONATEL tomará las medidas judiciales y extrajudiciales necesarias para garantizar la protección de la información presentada por los usuarios.

Finalmente, se señala que cualquier modificación en las condiciones técnicas de expedición de certificados u otro tipo de cambio debe ser comunicado al CONATEL, de lo contrario se anula el título habilitante.

---

[1] Secretaría Nacional de Telecomunicaciones.

[2] Comité Europeo de Normalización.

3.3.4. SITUACIÓN ACTUAL

Desde la publicación "*New Directions in Cryptography*" por *Diffie* y *Hellman* en 1976, la criptografía asimétrica ha evolucionado de manera lenta, debido a factores como falta de difusión en el uso de estándares, poco interés por parte de las empresas y gobiernos y escasa legislación.

Sin embargo, el interés en el comercio electrónico ha cambiado el panorama, la CNUDMI [1] creó en 1985 las recomendaciones sobre el valor jurídico de la documentación informática.

A partir de esto, publica en 1996 y 2001 las guías "Ley Modelo de la CNUDMI sobre Comercio Electrónico", y "Ley Modelo de la CNUDMI sobre las firmas electrónicas", respectivamente. En 2005 se efectuó una convención para formar un convenio sobre la utilización de las comunicaciones electrónicas para Contratos Internacionales.

Por otro lado, el Parlamento Europeo define en 1999 un compendio que incluye directrices para ambientes que utilicen firmas digitales, con el fin de estimular el uso de este tipo de ambientes y estandarizar los procesos de implementación y soporte; este compendio fue actualizado por última vez en Enero de 2002.

En Asia se creó en 2001 el Foro Asiático de PKI[2], formado por China, Japón, Corea del Sur, Singapur, Hong Kong, Taiwán y Macao, con el fin de fomentar el uso de tecnologías PKI para el comercio electrónico enfocado al turismo.

---

[1] Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. Comisión creada por la Asamblea General de las Naciones Unidas en 1966, con el fin de regularizar las leyes nacionales que regían el comercio internacional, y fomentar la armonización y unificación progresivas del derecho mercantil internacional. Ecuador se encuentra como país miembro hasta el año 2010. http://www.uncitral.org.

[2] http://www.asia-pkiforum.org/web/index.asp.

3.3.4.1. Situación de Gobiernos

País	Existe legislación	Posee institución que promueva el uso de PKI	PKI estatal acreditada	PKI privadas acreditada
Ecuador	SI	COMEXI[1]	NO	NO
Venezuela	SI	Ministerio de Ciencia y Tecnología mediante la Superintendencia de Servicios de Certificación Electrónica	NO	NO
Colombia	SI	Ministerio de Comunicaciones	Hasta el momento existen 4 entidades de certificación acreditadas bajo la modalidad de certificación cerrada.	Hasta el momento existen 2 entidades de certificación acreditadas, una bajo la modalidad de abierta, la otra funciona bajo la modalidad de certificación cerrada.
Perú	SI	Oficina Nacional de Gobierno Electrónico e Informática.	NO	NO
Bolivia	Anteproyecto	Agencia para el Desarrollo de la Sociedad de la Información en Bolivia	NO	NO
Argentina	SI	Infraestructura de Firma Digital de la República Argentina.	NO. Pero al momento Argentina cuenta con una autoridad certificadora que emite certificados para uso exclusivo de correo electrónico[2] de forma gratuita.	NO
Chile	SI	Ministerio de Economía	NO	Hasta el momento existen 5 PSC[3] acreditados.
Brasil	SI	ITI[4]	Actualmente cuenta con una AC raíz: ICP-BRASIL, ésta es la encargada de acreditar ACs.	NO
Uruguay	SI	Cámara Nacional de Comercio y Servicios del Uruguay	Administración Nacional de Correos, La Cámara Nacional de Comercio y Servicios del Uruguay emite CDEs[5].	NO
España	SI	Fábrica Nacional de Moneda y Timbre.	CERES (Certificación Española)	SI
Estados Unidos	SI	NSA[6], DoD[7], NIST[8] y CIOC[9].	FPKI[10] *infraestructura*, compuesta por la FBCA[11], CPFCA[12]; la C4CA[13] y la AC del *E-Governance*.	SI

Tabla 3.1 Situación de PKI en diferentes países

[1] Consejo de Comercio Exterior e Inversiones.

[2] Únicamente se verifica la existencia y disponibilidad de la cuenta de correo electrónico.

[3] Prestador de Servicios de Certificación.

[4] Instituto Nacional de Tecnologías de Información.

[5] Certificado Digital Empresarial, puede ser personal o para servidores.

[6] *National Security Agency*.

[7] *Department of Defense*.

[8] *National Institute of Standards and Technology*.

[9] *Chief Information Officers Council*.

[10] *Federal Public Key Infrastructure*.

[11] *Federal Bridge Certification Authority*.

[12] *Common Policy Framework Certification Authority*.

[13] *Citizen and Commerce Class Common Certification Authority*.

Actualmente, no todos los países cuentan con una legislación vigente; sin embargo, el uso de certificados digitales se hace presente tanto dentro de instituciones gubernamentales como en empresas particulares.

En la tabla 3.1 se muestra el estado de PKI en algunos países, como se puede observar, la mayoría de países cuenta con una legislación vigente o en proceso; sin embargo, pocos poseen una infraestructura que expida legalmente certificados digitales.

a. Situación en el Ecuador

El Ecuador cuenta con una legislación que brinda un soporte básico para la implementación de PKI. Se tiene la Ley 67 (Ley de comercio electrónico, firmas y mensajes de datos) y su Reglamento; además se cuenta con la Resolución 584 emitida por el CONATEL.

A pesar de que en la resolución del CONATEL se especifica que las instituciones públicas deben usar certificados emitidos por entidades acreditadas, hasta el momento, instituciones como el SRI[1] y el BCE[2] han decidido emitir sus propios certificados. El SRI emite certificados para la autenticación de sus servidores; por su parte el BCE ha implementado un PKI para el SNP[3].

Lamentablemente, existe poca voluntad por parte de las empresas públicas y privadas para el establecimiento de una PKI local que emita certificados acreditados. Hasta el momento, ante el CONATEL se han presentado cuatro[4] solicitudes para

---

[1] Servicio de Rentas Internas.

[2] Banco Central del Ecuador.

[3] Sistema Nacional de Pagos.

[4] Las cuatro empresas son nacionales; una de las cuatro empresas no cumple con los requisitos. Hasta el momento ninguna empresa internacional ha solicitado acreditar sus servicios de certificación en el Ecuador. Fuente: CONATEL.

obtener un título habilitante; estos procesos no han finalizado debido a que no se ha establecido la tasa que se debe cancelar al CONATEL.

3.3.4.2. Situación a nivel de Empresas

Al momento, los certificados digitales utilizados por la mayor parte de instituciones, son suministrados por empresas especializadas que gozan de confianza a nivel mundial.

Empresas como *Verising*, *Identrust, Thawte* y *Entrust*, presentan soluciones de seguridad basadas en certificados digitales; sus servicios van desde la emisión de un certificado personal hasta el soporte de toda la infraestructura PKI. El trabajo que realizan ha logrado el perfeccionamiento de PKI, debido a que promueven por una parte el desarrollo de estándares y por otro lado el uso de tecnologías PKI.

Hasta el momento, estas empresas han permitido la realización de transacciones en línea de manera segura en cuanto a tecnología; sin embargo, el uso de los certificados que expiden no se encuentra reconocido legalmente en muchos países, y aunque las soluciones que brindan mantienen niveles adecuados de seguridad, en muchos casos no son reconocidas como pruebas.

En Ecuador, la mayoría de instituciones financieras brindan a sus clientes la posibilidad de realizar transacciones a través de servidores *Web* seguros con certificados emitidos por estas empresas; además, servicios como Todo1 del Banco del Pichincha permiten que otras instituciones vendan sus servicios a través de Internet de manera segura.

3.3.5. PROBLEMAS CON PKI

PKI proporciona una infraestructura que permite autenticar a los usuarios de manera segura, soporta integridad de los mensajes e incluso garantiza la aceptación de

eventos o transacciones; además, introduce una connotación de legalidad a las transacciones realizadas electrónicamente.

Pero como toda alternativa posee falencias que se presentan cuando las directivas no se aplican correctamente; entre los principales problemas que se presentan dentro de un sistema PKI se puede mencionar:

- **Clave privada insegura**.- Todo el sistema de autenticación basado en certificados digitales sustenta su funcionamiento en la protección de las claves privadas; para lograr esto, se requiere que el acceso a cada clave esté limitado únicamente a su propietario[1].

  Esto implica que la clave debe estar protegida por otro sistema de autenticación; es decir, el propietario del certificado debe autenticarse ante el sistema para acceder a su clave privada.

  En la mayoría de los casos se utiliza las contraseñas para acceder a la clave, lo que introduce todos los problemas de los sistemas basados en autenticación por contraseña.

  Una mejor opción es almacenar la clave privada dentro de un *token* o una tarjeta inteligente; también se puede combinar el uso de certificados digitales con la biometría, en todo caso, el aumento de seguridad de la clave incrementa el valor de la inversión.

- **Certificado inseguro**.- Debido a que el tamaño de las claves tiene relación con el procesamiento requerido para su validación, algunos sistemas PKI generan claves con longitudes pequeñas, esto introduce vulnerabilidades en el sistema.

[1] Si se trata de un sistema que utiliza PKI para cifrar documentos, la clave privada puede ser duplicada y guardada en un almacén de claves.

- **Falta de Conciencia de los Usuarios**.- Los sistemas basados en criptografía asimétrica mantienen cierto nivel de complejidad; pero, no es necesario que los usuarios conozcan en detalle los algoritmos y procesos implícitos en el sistema, de ser posible, esta complejidad debe ser transparente para éstos.

  Sin embargo, todos los usuarios deben conocer y cumplir las CPs y CPS, esto implica la necesidad de planes de capacitación para que los usuarios se adapten al sistema, permitiendo que sean capaces de mantener su clave privada protegida y validar certificados.

  Incluso con un buen sistema de capacitación, no se puede garantizar que un certificado validado con éxito esté siendo utilizado por su propietario; por este motivo, es necesario incluir en los contratos de certificación cláusulas de responsabilidad, para conseguir un mayor compromiso por parte de los usuarios.

Todos los problemas son manejables, pero a medida que se incrementa el nivel de seguridad del sistema, la inversión se eleva también, y esto implica que el costo de los certificados se incrementa.

3.4. SERVICIOS DE UNA INFRAESTRUCTURA DE CLAVES PÚBLICAS

El objetivo de una infraestructura PKI es proveer confianza; para cumplir con este objetivo, la PKI debe brindar múltiples servicios a sus usuarios, y siendo la criptografía de clave pública su pilar fundamental, los servicios básicos que brinda están relacionados principalmente 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.
- Transmisión de claves simétricas para entablar comunicaciones seguras.
- Verificación de la integridad de mensajes o documentos electrónicos.

Para garantizar que todos estos servicios mantengan un nivel razonable de confianza, una infraestructura PKI se debe fundamentar en una generación de certificados digitales confiables.

3.4.1. EMISIÓN DE CERTIFICADOS DIGITALES CONFIABLES

Uno de los principales servicios que brinda PKI es obviamente la emisión de certificados digitales seguros; generar un certificado digital seguro implica llevar a cabo las siguientes etapas:

- **Identificación del usuario que solicita el Certificado**.- Es una de las responsabilidades de la AR, contiene las siguientes sub-etapas:

    - **Recepción de Solicitud**.- El usuario presenta una solicitud a la AR, 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 esta 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 a cumplir, la AC define qué tipo de información va

a 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 pública/privada**.- Esta etapa puede ser ejecutada por el usuario o por la AC; 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 AC 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 CP y las CPSs; además, se debe capacitar a los usuarios para que estén concientes del nivel de seguridad requerido en las etapas que requieren de su intervención.

3.4.2. SELLADO DE TIEMPO

Una firma digital se obtiene al aplicar una función *hash* a un documento digital y posteriormente cifrar el valor *hash* resultante con la clave privada del emisor, de esta manera se garantiza la integridad del mensaje y la autenticación del emisor.

Sin embargo, el uso de firmas digitales garantiza de manera limitada el servicio de aceptación en transacciones que resulten críticas para una empresa, debido a que los usuarios pueden argumentar compromiso de su clave privada o falsificación de la firma digital y negar la realización de la transacción.

PKI puede asegurar la aceptación de una transacción por medio del servicio de sellado de tiempo; para esto, PKI crea una entidad conocida como TSA (*Time Stamp Authority*), ésta es una entidad confiable que vincula el tiempo a un mensaje a través de un sistema seguro sincronizado con UTC (*Universal Time Coordinated*).

Para que la TSA resulte confiable, debe ser independiente de los sistemas que emiten o reciben los mensajes producto de las transacciones, debido a que actuará como testigo de la hora y fecha en que se realiza una transacción entre una pareja emisor/receptor.

En un sistema que utiliza el sellado de tiempo, todos los usuarios del sistema emisor envían sus mensajes o transacciones hasta la TSA, ésta verifica la firma digital del emisor; si la firma se confirma, adjunta al mensaje la fecha y hora exacta en la que recibió el mensaje y la fecha y hora en que se entregó el mensaje al destinatario.

La hora anexada al mensaje es firmada digitalmente por la TSA; esto garantiza que la hora no será adulterada. De esta manera, se tiene el respaldo de la firma digital del emisor con la fecha y hora en que se realizó la transacción.

El sellado de tiempo es independiente de la estructura de los documentos digitales, por lo tanto se puede anexar un registro de la fecha y hora a transacciones bancarias, formularios, correos electrónicos, documento de patentes, imágenes, etc.

La finalidad de este servicio es facilitar la realización de transacciones que normalmente requerirían de la presencia de los implicados y de un tercero que servía

de testigo; con el sellado de tiempo, este tipo de transacción se puede realizar ágilmente a través de Internet sin la necesidad de establecer una reunión.

3.4.2.1. Régimen Legal: Sellado de Tiempo

La Ley 67 establece dentro de sus disposiciones generales que las ACs acreditadas podrán prestar servicios de sellado de tiempo, servicio que deberá ser acreditado técnicamente por el CONATEL.

Su reglamento estipula que el mensaje debe ser enviado a través de la AC, para que ésta adjunte la hora y fecha exacta en que el mensaje de datos es recibido, y la fecha y hora exacta en que el mensaje es entregado al destinatario; el servicio de sellado de tiempo debe tener como referencia el uso horario del territorio continental Ecuatoriano.

Dentro de la resolución emitida por el CONATEL se establece que para prestar este servicio se debe presentar un anteproyecto técnico, éste debe contener un diagrama esquemático y descripción técnica detallada del sistema a emplear.

3.4.3. DISTRIBUCIÓN DE SERVICIOS PKI

Los servicios que brinda PKI pueden ser distribuidos de diferentes formas, de acuerdo a las entidades destino y al tipo de relación que exista entre la AC y éstas. Se pueden tener servicios de ACs públicas y corporativas; las ACs corporativas se pueden establecer dentro de una institución o por medio de un *outsourcing*.

- **ACs públicas**.- Una AC que brinda un servicio público está destinada a emitir certificados digitales para la población universal, sin el establecimiento de

límites institucionales; por lo tanto, las identidades establecidas son válidas en un entorno público.

Este sistema se utiliza generalmente para la emisión de certificados digitales, para correos electrónicos seguros (personales, no institucionales), servidores y clientes SSL, verificación de integridad de *software*, etc. En general, se utiliza para establecer autenticación e integridad de mensajes electrónicos emitidos por entidades relacionadas con ambientes públicos.

Cuando se expide certificados bajo este sistema, las ACs de la PKI establecen diferentes clases de certificados de acuerdo al nivel de seguridad empleado para la verificación de identidades; sin embargo, por tratarse de un sistema con una gran población, es complicado realizar verificaciones de manera personal.

Las ACs que brindan estos servicios pueden ser creadas por instituciones estatales o privadas; estas instituciones son conocidas ampliamente, lo que permite que el certificado de su AC raíz se encuentre almacenado en los navegadores y clientes de correo electrónico de los usuarios, por lo cual, la verificación de los certificados expedidos resulta cómoda para los usuarios.

- **ACs corporativas internas**.- Esta infraestructura PKI es creada para la emisión de certificados a nivel institucional; es decir, se emite certificados para empleados y equipos de una organización específica. También se puede emitir certificados para socios e incluso para clientes de acuerdo a la CP de la PKI.

  La principal característica de este sistema radica en que todos los procedimientos de administración del ciclo de vida de las claves y los certificados son manejados por entidades propias de la institución, esto permite una mayor flexibilidad para la implementación de CPs y CPSs.

Además, este sistema permite mantener el control total sobre la información relacionada con los usuarios del sistema y su registro, manteniendo niveles adecuados de seguridad en los procesos de establecimiento de las identidades.

El establecimiento de un PKI interno permite emitir certificados que se acoplen a las características de la institución, manteniendo costos aceptables en comparación con la contratación del servicio con terceros.

- **ACs corporativas por *outsourcing***.- Si una institución empieza a formarse en el campo de PKI, puede ser recomendable que subcontrate los servicios de PKI de una empresa especializada, de esta manera se asegura que el esquema PKI tendrá un nivel de seguridad acertado.

  No es necesario que se subcontrate toda la estructura PKI, en algunos casos se puede subcontratar elementos de ésta; por ejemplo, se puede mantener dentro de la organización la AR y tercerizar la emisión de certificados, con esto se garantiza el proceso de identificación de las entidades.

  Las CPs y CPSs dependerán de la empresa que contrate los servicios de *outsourcing*, de esta manera se puede garantizar la confiabilidad del sistema PKI. Esta etapa puede conservarse mientras la empresa gana experiencia, luego de lo cual puede pasar a estructurar su propia infraestructura.

La decisión de establecer un sistema de distribución de servicios PKI dependerá de las necesidades de una empresa, si se requiere niveles elevados de seguridad, lo más adecuado será manejar toda la infraestructura dentro de ésta; en cambio, si se va a utilizar PKI como una herramienta de trabajo, puede resultar atractivo la adquisición de certificados emitidos por ACs públicas o quizás tercerizar el servicio.

3.5. 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 PKI asegura que la clave pública asociada con una clave privada pertenece al usuario registrado en un certificado; sí la clave pública pertenece a otro usuario, no se cumple el propósito de PKI. Por este motivo es fundamental establecer procedimientos adecuados para los procesos de administración de claves y certificados.

3.5.1. ADMINISTRACIÓN DE LAS CLAVES

La administración de claves contempla todos los aspectos relacionados con el ciclo de vida de las parejas de claves pública/privada dentro de PKI; esto implica, las claves de las ACs y de todas las entidades destino.

3.5.1.1. Selección del Tipo Clave

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

Se puede generar dos tipos de claves, las claves que están destinadas para cifrar y las claves destinadas para firmar digitalmente un mensaje o documento electrónico; por supuesto, existen claves que cumplirán con 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 [1], ésta 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.

3.5.1.2. Generación y Entrega de Claves

Dentro de la generación de claves uno de los aspectos más importantes dentro de una PKI es la definición del algoritmo que se va a utilizar para cifrar y firmar digitalmente; éste determinará las longitudes de claves posibles, nivel de confiabilidad de las claves creadas, interoperatividad, 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 a 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.

---

[1] Permanecer bajo la custodia y protección exclusiva de su propietario.

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 AC la encargada de la generación de claves; esto resulta más amigable para el usuario y permite el almacenamiento[1] 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 generen 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.

3.5.1.3. 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.

3.5.1.4. Almacenamiento de Claves

El almacenamiento de las claves privadas va a depender de la entidad propietaria de éstas; por ejemplo, las claves pertenecientes a ACs de la PKI 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.

---

[1] En este caso se crea un punto único de falla, pues si un atacante logra tener acceso a la AC accederá también a todas las claves privadas.

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 almacenes de claves, éstos deben ubicarse en zonas restringidas y la información almacenada debe cifrarse.

3.5.1.5. Recuperación de Claves

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

3.5.2. ADMINISTRACIÓN DE CERTIFICADOS

En el caso de PKI, 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 las prácticas dentro de la PKI sean consistentes para lograr que el registro, renovación y revocación de certificados mantengan niveles razonables de confianza.

3.5.2.1. Registro de Certificados

Después de que la AR ha efectuado las verificaciones de identidad pertinentes y la AC ha sido notificada, los datos del usuario se registran en la PKI, 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 AR.

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 AR para que la AC 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 lo cual se le permite descargar su certificado.

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

3.5.2.2. 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 AR y AC 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 puede presentar en casos de cambios importantes de los datos del propietario del certificado.

3.5.2.3. 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 AC 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. CRLs

Un certificado digital deja de ser confiable si la clave privada relacionada con éste se ve comprometida. Además, debido a que los certificados son credenciales que indican la identidad de un usuario o entidad, éstos no serán válidos cuando el usuario o la entidad dejan de existir.

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 suspendido o revocado expira, se puede retirar de la lista.

El mantenimiento de una CRL y la revocación de certificados es responsabilidad de la AC que expide los certificados; ésta debe firmar digitalmente las CRLs para evitar adulteraciones. Al validar un certificado digital, se debe examinar la CRL pertinente para asegurar que el certificado no ha sido revocado; esta verificación toma algo de tiempo, por lo que resulta necesaria de acuerdo a la importancia de la transacción.

Existen dos modelos de distribución para una CRL: en el primero, un usuario descarga las CRLs de la AC cuando lo necesita; en el segundo, la AC envía periódicamente las CRLs a los usuarios. Los RFCs 3279 y 3280 contienen información de las especificaciones para el uso de CRLs; actualmente se cuenta con CRLs versión dos.

a.1. Formato de las CRLs

Una lista de revocación de certificados, de acuerdo a la norma, debe tener los siguientes campos:

- **Versión**.- Indica la versión de CRL; este campo puede tener registrada la primera o segunda versión del estándar. Si se requiere marcar extensiones críticas, se debe usar la versión 2.

- **Firma**.- Indica el tipo de función *hash* y el algoritmo de encripción con que se firmó la lista de revocación.

- **Expedidor**.- Indica el nombre de la AC que expidió y firmó la lista de revocación.

- **Actualización**.- Contiene la fecha y hora en que se publicó la lista de revocación.

- **Siguiente Actualización**.- Contiene la fecha y hora en que se publicará la siguiente lista de revocación.

- **Información de Certificados Revocados**.- Los certificados que han sido revocados se listan en el orden en que fueron ingresadas las revocaciones. En cada entrada se registra el número de serie del certificado, fecha de revocación y la razón de la revocación.

- **Extensiones**.- Este campo permite agregar información adicional manteniendo el formato del estándar.

a.2. Tipos de CRLs

Esta clasificación se basa en el tipo de contenido registrado en cada lista.

- **CRLs simples**.- Contienen información de todos los certificados revocados por una sola AC. Al igual que los certificados, las listas de revocación deben ser almacenadas en directorios. La AC debe informar a sus usuarios de la ubicación de los puntos de distribución de las CRLs.

- **CRLs indirectas**.- Tienen almacenada información de listas de revocación expedidas por múltiples autoridades certificadoras.

- **CRLs delta**.- Contienen información de actualizaciones de listas de revocación simples o indirectas; de esta manera, los usuarios no requieren descargar una CRL completa sino que pueden tener almacenada la CRL y descargar las siguientes actualizaciones sin consumir mayores recursos.

3.6. APLICACIONES QUE UTILIZAN PKI

PKI ofrece el ambiente ideal para cualquier aplicación que requiera proveer de los servicios de autenticación, confidencialidad, integridad y aceptación con niveles razonables de confianza y seguridad, esto incluye todas las aplicaciones que utilizan certificados digitales señaladas anteriormente.

Adicionalmente, existen aplicaciones desarrolladas para brindar servicios de seguridad a grandes poblaciones, en estos casos PKI ofrece las mejores condiciones de escalabilidad y administración.

3.6.1. EAP-TLS

Como se vio en el capítulo anterior, este protocolo fue creado por *Microsoft* y se encuentra registrado en el RFC 2716, provee autenticación con el más alto nivel de seguridad por medio de certificados digitales dentro de WLANs.

Durante el proceso de autenticación, todos los miembros de la WLAN utilizan certificados digitales para autenticarse mutuamente (clientes y servidor); por lo tanto el número de certificados a expedirse es elevado, por este motivo EAP-TLS necesita de una infraestructura que permita mantener una administración adecuada de éstos.

Además, a pesar de que la implementación de una PKI puede resultar compleja, introduce herramientas que permiten gestionar las credenciales de los usuarios dentro de la WLAN, manteniendo niveles adecuados de seguridad y escalabilidad.

EAP-TLS es necesario dentro redes corporativas con un gran número de usuarios móviles, distribuidos en distintas áreas geográficas u organizacionales, también es necesario para empresas que transmiten a través de medios inalámbricos información estratégica.

3.6.2. SECTOR FINANCIERO

En la actualidad, las transacciones realizadas por Internet no tienen aún la aceptación de todos los usuarios, debido a que no todos los sitios *Web* cuentan con la seguridad adecuada, y por otra parte no todos los usuarios se sienten cómodos o están capacitados para interactuar con este tipo de servicio.

Sin embargo, existe una tendencia por gran parte de los consumidores a aceptar la realización de transacciones por medios electrónicos; por este motivo, la mayoría de instituciones financieras ofrecen servicios como el pago en línea, transferencias de fondos, consulta de saldos, actualización de datos personales, etc.

El autoservicio conseguido no solo incrementa la agilidad en las transacciones, sino también ha logrado que las instituciones financieras ahorren dinero en la implementación de servicios y personal para la atención al cliente.

Internet está convirtiéndose en una entidad confiable mediante la cual se pueden realizar transacciones comerciales, las instituciones financieras incrementan día a día el nivel de seguridad de sus sitios *Web*, con el fin de darles legalidad a las transacciones realizadas a través de Internet, por medio de un sistema de autenticación y aceptación fiable.

En Estados Unidos según la *Mortgage Bankers Association*[1], en 1999 se realizaron transacciones a través de Internet por un valor de 4 billones de dólares, para el 2003 esta cifra se había incrementado a 250 billones de dólares.

Aunque en Ecuador no se tiene datos oficiales de los montos derivados de las transacciones realizadas a través de Internet, muchas instituciones han creado sitios *Web* que permiten la interacción con el usuario. Por ejemplo, gran parte de las instituciones bancarias ofrecen servicios en línea, las aerolíneas ofrecen precios promocionales para clientes que adquieran sus *tickets* a través de sus portales, instituciones públicas como el SRI aceptan pagos en línea, etc.

3.6.2.1. Soluciones

Debido a la creciente aceptación de los clientes y la disminución del costo de las transacciones realizadas por medios electrónicos, se generaliza el desarrollo y uso de aplicaciones que proporcionen autenticación, confidencialidad, integridad y aceptación, manteniendo la intimidad del individuo.

a. SET (Secure Electronic Transaction)

El protocolo SET fue creado en 1995 por *Visa* y *MasterCard*, en colaboración con *Microsoft*, *VeriSign*, *Netscape*, RSA e IBM. Este protocolo se desarrolló con el

---

[1] RAINA, *Kapil*. *PKI, Security Solutions for the Enterprise*. Primera Edición. *Professional Mindware*. Estados Unidos. 2002.

objetivo de lograr pagos seguros con tarjeta de crédito a través de Internet, reduciendo los costos de operación para el vendedor y aumentando el nivel de seguridad en las transacciones.

Los servicios de seguridad proporcionados por SET son:

- **Autenticación y Aceptación**.- Todas las entidades involucradas durante una transacción utilizan certificados digitales[1] para autenticarse mutuamente. La aceptación se garantiza de manera limitada por el uso de firmas digitales.

- **Confidencialidad**.- SET garantiza la confidencialidad del número de la tarjeta de crédito para evitar fraudes, esto se consigue cifrando los datos relacionados con la transacción financiera con la clave pública del Banco; de esta manera solo el cliente y la institución bancaria tienen acceso a esta información[2]. Por otro lado, se cifra los datos relacionados con el producto con la clave pública del vendedor.

- **Integridad**.- Para garantizar que la información intercambiada no se altere, se utiliza funciones *hash* y firmas digitales.

- **Intimidad**.- La institución bancaria que emitió la tarjeta de crédito no tiene acceso a la información de pedidos de sus clientes, de esta manera se protege al usuario, evitando el registro de sus hábitos de consumo; por otra parte, el vendedor no tiene acceso a la información de la tarjeta de crédito.

Para la realización de una transacción utilizando SET, se requiere de la intervención de las siguientes entidades: el banco emisor de la tarjeta de crédito, servidor adquiriente[3], cliente, vendedor, AC y *software* especializado.

---

[1] Los usuarios requieren un certificado digital por cada tarjeta de crédito.

[2] El vendedor no tiene acceso al número de tarjeta de crédito.

[3] Es el encargado de la validación de transacciones y autorizaciones de pago.

b. EMV (Europay, MasterCard, and Visa)

EMV es un estándar desarrollado por algunas de las firmas financieras de crédito más grandes del mundo; su desarrollo se inició en 1993, con el fin de proporcionar un método para el pago digital basado en tarjetas inteligentes. Los estándares de EMV están compuestos por las siguientes áreas:

- **Especificaciones para las tarjetas**.- Éstas cubren básicamente la plataforma de *software* requerido por la tarjeta inteligente universal EMV, incluyendo componentes PKI con el uso de algoritmos RSA. Las tarjetas pueden trabajar con múltiples aplicaciones, para esto se incluyeron especificaciones para la sincronización con los terminales de lectura.

- **Especificaciones de Terminal**.- Esta sección contiene todas las especificaciones de la estructura física del Terminal de lectura de tarjetas inteligentes. Este dispositivo debe soportar aplicaciones que provean manejo de riesgos y seguridad.

- **Especificaciones de Aplicaciones**.- Las tarjetas inteligentes pueden almacenar transacciones de pago y aplicaciones, para esto se definen estándares que determinan la manera en que las aplicaciones se escribirán para proporcionar compatibilidad.

c. Soluciones Institucionales

Existen varias empresas que trabajan por el desarrollo y aceptación de las transferencias financieras a través de Internet. A continuación se presenta información de dos de las instituciones pioneras en el desarrollo y promoción de transacciones en línea, *Indetrus* y GTA (*Global Trust Authority*).

c.1. *Identrus*

Identrus fue formada en 1999 por una asociación de instituciones financieras; su propósito fue estimular la confianza en sistemas B2B[1] para abrir el mercado del comercio electrónico. Actualmente, las instituciones financieras fundadoras de *Identrus* funcionan como proveedores de certificados digitales, obteniendo un alcance global con figuras locales.

Indentrus actúa como un ente neutral que proporciona validación de identidades por medio de sistemas basados en estándares PKI; la utilización de estándares ha conseguido que más instituciones se adhieran al sistema, logrando una disminución de los costos dentro del sistema B2B global.

c.2. *Global Trust Authority*

La GTA es una organización Europea formada por instituciones financieras que proporciona servicios similares a los de *Identrus*; GTA brinda servicios a sus miembros en varios países incluyendo: Bélgica, Francia, Italia, Países Bajos, Portugal y España.

Está compuesta por una AC raíz, ésta emite certificados para sus ACs subordinadas llamadas MTAs (*Master Trust Authorities*); también se encarga de proporcionar los servicios de revocación, establecimiento de políticas, cobros de garantías a sus miembros, etc.

Las MTAs, en cambio, emiten certificados para sus miembros llamados STAs (*Scheme Trust Authorities*), estableciendo una jerarquía de control para el mantenimiento de políticas y cumplimiento de garantías.

---

[1] *Business-to-Business*.

3.6.3. NOTARIZACIÓN ELECTRÓNICA

Un notario humano representa un ente de seguridad jurídica dentro de una sociedad, por lo que el servicio de notarización electrónica requiere de mecanismos y procedimientos que proporcionen niveles equivalentes de confianza y seguridad, ofreciendo las mismas garantías que su contraparte en papel.

La notarización electrónica está encargada de la certificación de documentos electrónicos por medio de firmas digitales y sellado de tiempo[1]; este servicio requiere de un Notario Público u otro tipo de autoridad, para dar fe de la realización o existencia de un documento, convenio o transacción realizados por medios electrónicos.

Entre las instituciones que promueven y proporcionan el uso de este tipo de aplicaciones se puede mencionar a la ABA[2] y *Surety Technology*; la ABA se ha enfocado desde 1996 en la legalización internacional de las transacciones de comercio electrónico, por medio de la creación de Cibernotarios[3].

Por su parte *Surety Technology* proporciona el servicio de notarización electrónica desde 1994 por medio de su sistema *AbsoluteProof*, éste funciona bajo un esquema de cliente/servidor.

En *AbsoluteProof* los clientes envían el valor *hash* del documento a certificarse al servidor por medio de una comunicación segura; el servidor combina el valor *hash* recibido, un registro de tiempo e información que identifica al cliente y documento. El

---

[1] Garantiza la autenticación, integridad y aceptación.

[2] *American Bar Association*.

[3] En Estados Unidos, hasta el momento se reconoce legalmente a la notarización electrónica solo en siete estados. http://www.nationalnotary.org/eNotarization/.

valor obtenido es enviado al cliente, y de esta manera el documento original nunca sale de la institución propietaria.

En Ecuador se está elaborando un proyecto para permitir que un usuario realice sus transacciones notariales, tales como escrituras públicas, declaraciones juramentadas, certificaciones de documentos, realización de testamentos, etc. a través de Internet[1]; para su ejecución se requiere de la existencia de una AC acreditada por el CONATEL y realizar reformas a la Ley Notarial.

3.6.4. FACTURACIÓN ELECTRÓNICA

Este tipo de aplicaciones es una solución para disminuir los costos ocasionados por las facturas físicas (papel); además, facilita el cumplimiento tributario minimizando la evasión y el fraude. Sin embargo, para su implementación hace falta voluntad por parte de los gobiernos y del sector privado.

El sistema de facturas electrónicas mantiene una complejidad considerable, debido a que requiere de la colaboración de las siguientes entidades: una AC acreditada, el cliente, el vendedor, la entidad de control tributario, entidades del sistema financiero y una legislación vigente.

Su implementación debe adaptarse a la legislación establecida en cada país; en general mantiene el siguiente esquema:

- La AC emite certificados para los vendedores y opcionalmente para los clientes.
- Cuando un cliente desea realizar una compra, el vendedor emite una factura y la firma digitalmente con un registro de tiempo.

---

[1] http://www.eluniverso.com/2006/03/01/10/ceb25996b6b0469d9ebc10a4c056e702.html?EUID=.

- El cliente verifica la firma del vendedor y envía una petición de validación para la entidad de control tributario, si la factura resulta ser lícita, el cliente confirma el pedido, en algunos sistemas es necesario que el cliente firme la factura electrónicamente.
- Después de confirmar el pedido, la transacción es registrada con la entidad de control tributario.
- Los montos involucrados son descontados de la cuenta[1] del cliente y se depositan en la cuenta del vendedor; si el monto involucra impuestos (IVA[2]), éstos son acreditados inmediatamente a la cuenta de la entidad de control tributario, de esta manera se elimina la evasión y el fraude.

Como se puede observar, se trata de un sistema complejo, que requiere de la interacción de varias entidades, pero que involucra a la vez varias ventajas entre las que se puede mencionar:

- Por tratarse de un sistema basado en PKI, se poseen los servicios de autenticación, integridad y aceptación, y de ser necesario se puede implementar adicionalmente mecanismos de confidencialidad.
- Este sistema no está limitado a la emisión de facturas electrónicas, también puede utilizarse para manejar todo tipo de cuentas por cobrar.
- No excluye el sistema de facturación física, si una de las partes desea mantener un registro físico puede imprimir las facturas emitidas o recibidas.
- Permite la verificación de documentos tributarios en línea.
- Reduce los costos en comparación con su contraparte en papel; según la AECOC[3] la reducción del costo estimado por factura es de 0,6 euros para un

[1] Esta cuenta puede estar relacionada con instituciones financieras como: bancos, cooperativas, mutualistas, proveedores de tarjetas de crédito, etc.

[2] Impuesto al Valor Agregado.

[3] Asociación Española de Codificación Comercial.

emisor, lo que ha logrado que las empresas que facturan digitalmente ahorren casi 60 millones de euros al año en gestión y tratamiento[1] de facturas.
- Por ser un sistema en línea, no se limita a un horario definido.
- Evita documentos tributarios extraviados y las multas eventuales por su pérdida.

Entre sus desventajas se puede mencionar su evidente complejidad y la falta de apoyo por parte de los organismos gubernamentales y privados. Esto ha causado que en las primeras etapas de su implementación en algunos países, la factura electrónica esté destinada solo para transacciones entre instituciones y que por el momento no esté al alcance de todo el público.

Para la implementación de un sistema de facturas electrónicas en Ecuador se requiere una reforma a la legislación básica de la Administración Tributaria Central y la acreditación de una entidad emisora de certificados digitales.

3.6.5. IMPLICACIONES GUBERNAMENTALES

El nivel de desarrollo y cultura de cada país determina la forma en que las tecnologías PKI deben implementarse y su respectiva evolución; por este motivo, el avance e implantación de las aplicaciones PKI requiere de la intervención directa del gobierno.

El gobierno debe establecer regulaciones que proporcionen un valor legal a las transacciones electrónicas; por otro lado, se requiere que éste tome un papel

[1] Esta disminución de costos está directamente relacionado con la emisión, verificación, distribución, seguimiento de pago y almacenamiento de las facturas, según el Código tributario vigente en Ecuador, los documentos tributarios deben guardarse por un período de 5 años desde su emisión.

protagónico en la emisión de certificados o en su lugar permita la acreditación de entidades de certificación confiables y establezca un ente de control neutral.

Muchos países se han dado cuenta de la importancia de una infraestructura PKI nacional, por este motivo han creado leyes que permiten de alguna manera el funcionamiento básico de ésta. La mayoría de regulaciones creadas hacen referencia a las firmas y certificados digitales, estableciendo medios para la creación y control de entidades de emisión de certificados.

Incluso en los países en que no existe una AC acreditada o una legislación vigente, instituciones de todo tipo hacen uso de los certificados emitidos por entidades reconocidas internacionalmente.

Este tipo de solución mantiene como sustento legal el acuerdo de las partes para el uso de determinada tecnología, esto pone en riesgo a los clientes, pues dependen únicamente de la seguridad de la infraestructura en la que confían, y en caso de que ésta falle, no se tendrá una base legal que contemple las particularidades y requerimientos de PKI.

Además del establecimiento de una legislación adecuada, la acreditación de ACs privadas o estatales y la creación de organismos de control y sus regulaciones, el gobierno puede intervenir en proyectos estatales como *e-Government* y el establecimiento de un Documento Nacional de Identidad (DNI) digital.

- **Proyectos *e-Government***.- Algunas aplicaciones de PKI se han diseñado para dar mayor acceso a servicios de gobierno a la población. El desarrollo de *e-Government* tiene varias etapas; en principio, todos los organismos del estado, incluidos ministerios, municipios, prefecturas, etc., ponen a disposición del público un portal[1] que brinde información referente a su desempeño.

[1] Estos portales deben ser sitios *Web* seguros.

En una segunda etapa, el gobierno pone a disposición de los ciudadanos un servicio de descarga de formularios y hablita el gobierno en línea, de esta manera, los ciudadanos pueden acceder a cualquier tipo de información desde su hogar o en su lugar de trabajo.

En una tercera etapa, se permite a los usuarios realizar pagos de impuestos o multas a través de los portales. Cuando se llega a una etapa más avanzada, los ciudadanos pueden incluso votar a través de Internet, para esto se requiere un sistema de autenticación robusto que mantenga el respeto a la intimidad del usuario.

La mayor parte de estos servicios pueden estar disponibles para los ciudadanos 24 horas al día y 7 días a la semana, brindando disponibilidad, agilidad y facilidad en la realización de los trámites y consultas.

En general, las soluciones *e-government* no requieren de la implementación de ambientes complejos, a excepción del voto electrónico en donde se requiere de una entidad capaz de emitir certificados para todo el electorado.

- **DIN digital**.- Es un método para crear credenciales para todos los ciudadanos de un país por medios electrónicos, manteniendo niveles adecuados de seguridad. De esta manera, los servicios *e-government* y otros pueden ser utilizados por medio de una credencial digital.

  Este esquema se basa en el uso de tarjetas inteligentes, éstas pueden contener la pareja de claves pública/privada, un sistema operativo, datos personales del usuario y hasta un chip de detección remota; esto logra que cada tarjeta se comporte como un dispositivo autónomo[1].

[1] No se requiere de un esquema cliente/servidor.

Un DIN digital tiene mayores funcionalidades que una credencial tradicional; por ejemplo, permite a un usuario identificarse y firmar un documento remotamente, esto conlleva la necesidad de capacitar a la población, pues el usuario debe estar protegido ante los posibles malos usos de la tecnología[1].

Las tarjetas inteligentes utilizadas como DIN, deben incorporar un sistema con resistencia a la falsificación. Además, debido a que se trata de una expedición masiva de credenciales, es necesario disponer de una interfaz basada en estándares de bajo costo, que permita la interacción con diferentes aplicaciones.

El establecimiento de un sistema de expedición de credenciales por medios electrónicos, no implica la eliminación del sistema tradicional; por el contrario, permite gran flexibilidad pues el usuario puede personalizar las funcionalidades de su DIN digital e incluso utilizarlo como una credencial tradicional.

3.7. MODELOS DE CONFIANZA

El establecimiento de una infraestructura PKI requiere en muchos casos de la intervención de varias ACs; para que los usuarios puedan confiar en los certificados emitidos por una AC diferente a la que expidió su propio certificado, las ACs emisoras de los certificados involucrados en la transacción deben establecer relaciones de confianza.

Las relaciones de confianza entre ACs se establecen mediante certificados cruzados, un certificado cruzado es un mecanismo para garantizar la vinculación de una AC

[1] http://www.votobit.org/articulos/dni.html.

subordinada dentro de una jerarquía o para reconocer a ACs externas a la organización como entes confiables dentro de un modelo distribuido de confianza.

3.7.1. EL PAPEL DE LA CONFIANZA

Debido a que la estructura PKI gira alrededor de la confianza, es necesario definir un significado apropiado para ésta. La definición de confianza expuesta en las especificaciones X.509 en su sección 3.3.59 es la siguiente: “En general, una entidad puede decir que confía en una segunda entidad cuando la primera entidad supone que la segunda se comportará exactamente como la primera entidad espera”[1].

Dentro de un entorno PKI el papel fundamental de la confianza es el establecimiento de un marco que describe la relación entre una entidad destino o confiante y la AC que emite sus certificados.

El marco de confianza le hará saber a una entidad destino que sus certificados son razonablemente seguros durante su período de validez; por otra parte, permitirá que una entidad confiante acepte los certificados reconocidos como válidos por la AC que emitió su certificado, incluso cuando estos certificados hayan sido emitidos por una entidad desconocida para el usuario.

3.7.2. ANCLA DE CONFIANZA

La decisión de confiar en una identidad registrada en un certificado va a depender de la AC que emitió la credencial; por ejemplo, en la figura 3.10, cuando A requiera validar los certificados de B, C y D, éste realizará las siguientes verificaciones:

---

[1] 3.3.59 *trust: Generally, an entity can be said to "trust" a second entity when it (the first entity) makes the assumption that the second entity will behave exactly as the first entity expects. X.509. 2005*.

- **Validación del certificado de B**.- A determina que el certificado de B está firmado por la AC-1.1, y debido a que ésta ha emitido su propio certificado digital (A confía en AC-1.1), éste decide confiar en el certificado de B.

- **Validación del certificado de C**.- A determina que el certificado de C está firmado por la AC-1.2; a su vez, el certificado de AC-1.2 fue emitido por la AC-1, y como ésta emitió el certificado de la AC-1.1 en quien confía, A decide confiar en el certificado de C.

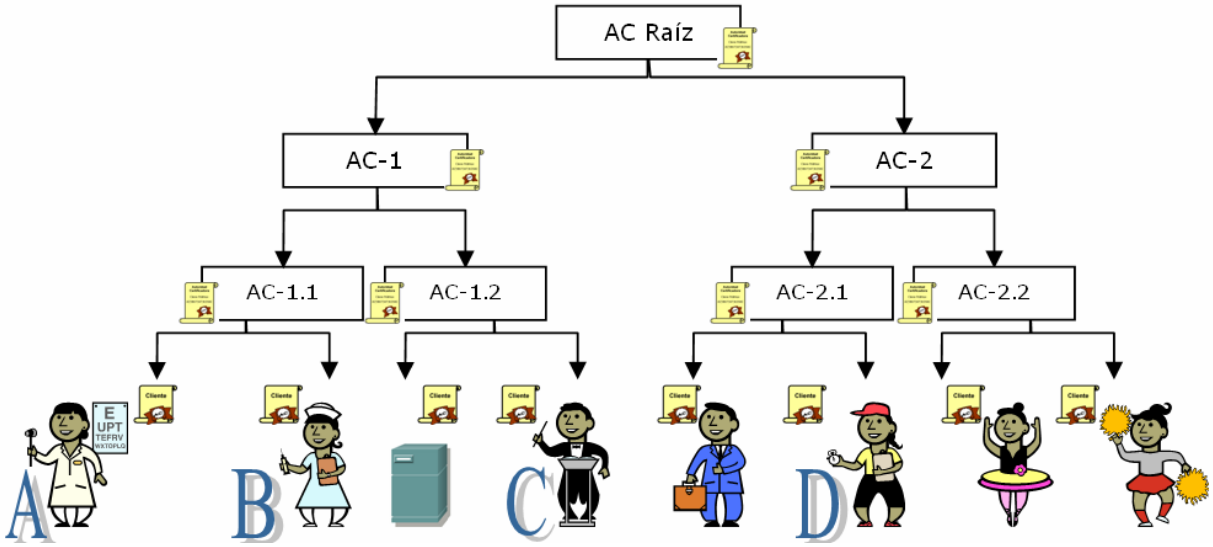

Figura 3.10 Ancla de Confianza

- **Validación del certificado de D**.- A determina que el certificado de D está firmado por la AC-2.1, el certificado de AC-2.1 fue emitido por la AC-2; luego A confirma que el certificado de AC-2 fue emitido por la AC-Raíz, y como ésta emitió el certificado de AC-1, y ésta última a su vez el certificado de A-1.1, A decide confiar en el certificado de D.

En otras palabras, para que una entidad confiante pueda aceptar un certificado, su propietario y/o la AC que emitió la credencial deben estar acreditados por una entidad en la que el usuario confía, esta entidad es el Ancla de Confianza del usuario; entonces, cada vez que el usuario requiera confiar en un certificado, éste se

asegurará [1] que su ancla de confianza haya garantizado la confiabilidad de la credencial.

El ancla de confianza puede localizarse tan cerca del usuario como se establezca en las directivas de la PKI; es común que se seleccione como ancla de confianza a la AC que emite el certificado del usuario; en el caso de las arquitecturas jerárquicas, el ancla de confianza es la AC raíz. También se puede establecer como ancla de confianza a una entidad que a pesar de estar muy separada del usuario, goce de buena reputación.

Debido a que los procesos de validación consumen recursos y tiempo, el ancla de confianza establece rutas válidas y se las entrega a los usuarios para que éstos no tengan que recorrer todo el trayecto desde la entidad que firmó un certificado hasta su Ancla de confianza; estas rutas son entregadas al usuario junto con su certificado digital.

3.7.2.1. Dominio de Confianza

Un dominio de confianza es la porción de una infraestructura PKI que opera bajo el mismo conjunto de directivas, puede estar formado por una o más ACs; además, dentro del dominio debe existir por lo menos un directorio.

Es importante establecer claramente los límites de un dominio de confianza; por ejemplo, dentro de una organización se pueden crear dominios de acuerdo a áreas de trabajo, zonas geográficas o mantener un único dominio.

Por otra parte, se debe considerar que los límites de un dominio están marcados por las relaciones de confianza de sus miembros y no por un conjunto de técnicas;

[1] Si es cuidadoso.

siendo así, cada miembro debe estar preparado para reconocer los límites del dominio y cumplir con las directivas vigentes.

3.7.3. TIPOS DE MODELOS DE CONFIANZA

Un modelo es el marco de referencia para crear y administrar relaciones de confianza[1]. Cuando se requiere que las relaciones de confianza se extiendan hasta ACs de otras organizaciones (o áreas), se requiere métodos que aseguren el cumplimiento de las directivas de las organizaciones involucradas.

Antes de asumir relaciones de confianza entre dos organizaciones, se debe revisar con detenimiento las directivas de éstas, pues si las directivas de una de las organizaciones involucradas tienen menores requerimientos de seguridad, pueden introducir vulnerabilidades a la infraestructura de la otra organización.

3.7.3.1. Modelo jerárquico

Este modelo establece como única ancla de confianza a la AC raíz[2], por lo tanto es la entidad que goza de mayor confianza dentro del sistema PKI. La AC raíz establece relaciones de confianza unidireccionales[3] con sus subordinadas.

En este modelo no es necesario establecer un camino desde la AC que emitió un certificado hasta la AC que emitió el certificado de la entidad confiante, debido a que todas las validaciones tienen como punto final el certificado de la AC raíz; por este motivo, el certificado de la AC raíz debe ser distribuido a todos los usuarios.

---

[1] NASH, Andrew. PKI-Infraestructura de Claves Públicas. Capítulo 8, página 244.

[2] La AC raíz crea su propio certificado (autofirmado).

[3] Solo una AC de jerarquía superior puede expedir certificados para sus subordinadas y éstas no pueden certificar a sus superiores.

Una de las debilidades de este modelo es que mantiene como punto crítico a la AC raíz, si su clave privada llega a comprometerse todos los usuarios se ven afectados, pues es necesario revocar su certificado y redistribuir el nuevo; además, deben revocarse todos los certificados emitidos por la AC desde el compromiso de su clave.

Sin embargo, el acceso a la AC raíz está restringido para la emisión de certificados para las ACs subordinadas bajo un ambiente planificado y controlado, por este motivo, el compromiso es un suceso que se presenta muy rara vez.

Este modelo es adecuado para la implementación de un ambiente PKI dentro de una organización, debido a que bajo estas circunstancias es fácil la determinación de un punto común de confianza, manteniendo las restricciones que implican la subordinación; en cambio, se torna inadecuado en ambientes compuestos por varias organizaciones, debido a que cada participante necesita establecer su propia ancla de confianza.

3.7.3.2. Modelo entre Iguales

Este modelo permite establecer relaciones de confianza bidireccionales entre ACs de diferentes organizaciones; por lo general, las ACs que intervienen en el establecimiento de las relaciones de confianza son el ancla de confianza local dentro de su organización.

Este modelo permite restringir las relaciones de confianza, permitiendo que éstas sean directas o distribuidas; en el caso de las relaciones directas, cada AC debe certificar a las demás ACs, esto asegura el cumplimiento de las directivas, sin embargo, es complicado.

Por otro lado, si se establece relaciones distribuidas, queda abierta la posibilidad para que se confíe en certificados reconocidos como válidos por una AC externa a la

organización; entonces el sistema se simplifica, pero se corre el riesgo de que la AC externa no verifique lo suficiente y permita el acceso a entidades peligrosas.

3.7.4. ADMINISTRACIÓN DE LA CONFIANZA

La administración de la confianza debe enfocarse en dos puntos claves: la administración de las anclas de confianza y el establecimiento de relaciones de confianza con ACs de otras áreas u organizaciones.

3.7.4.1. Administración de Anclas de Confianza

La administración de anclas de confianza involucra: la selección de un ancla de confianza adecuada, la distribución de listas de confianza local[1], capacitación de los usuarios, revisión de las entidades que las aplicaciones consideran confiables, etc. Todos estos procesos deben ser planificados cuidadosamente.

El ancla de confianza es una guía para que los usuarios puedan determinar en que entidades pueden confiar, esto se logra mediante la distribución de listas locales de confianza.

Sin embargo, los usuarios realizan transacciones en las que pueden encontrar entidades que no han sido reconocidas por su ancla de confianza, en estos casos es el usuario el que decide confiar o no en dicha entidad, siendo así, la capacitación de los usuarios es fundamental, pues la decisión final recaerá en sus manos.

Para hacer que el ambiente PKI no requiera de la intervención directa del usuario, muchas aplicaciones tienen almacenadas listas de expedidores reconocidos a nivel

[1] Se le llama local debido a que se instala en la estación de trabajo del usuario y solo él tiene acceso a ésta.

mundial, de esta manera la verificación no depende del usuario sino de la aplicación, por este motivo es necesaria una revisión de las entidades que determinada aplicación reconoce como confiables.

3.7.4.2. Administración de Relaciones de Confianza

La administración de las relaciones de confianza, empieza por el análisis de las CPs de cada organización que desea adherirse al PKI; debido a que cada CP maneja sus propios requerimientos de seguridad, se debe decidir qué puntos deben cumplirse estrictamente y cuáles son negociables. En algunos casos las relaciones de confianza serán inaplicables.

En el caso de los modelos de confianza jerárquicos, la administración de las relaciones de confianza se simplifica, debido a que una AC de jerarquía superior determina las directivas y su cumplimiento (no es necesario negociar); esto facilita la distribución de listas de confianza y la eliminación relaciones de confianza con entidades que se han visto comprometidas.

En el caso de los modelos entre iguales, la administración de relaciones de confianza se torna complicada, pues cada participante tiene definidas sus propias políticas y anclas de confianza.

Entonces es necesario constituir convenios en los que se establezca una nueva CP común, ésta debe incluir normativas bajo las cuales se mantienen las relaciones asumidas, soporte de varias anclas de confianza, distribución de listas de confianza y garantías en caso de incumplimiento de los acuerdos.

Dentro de un modelo entre iguales, el ancla de confianza de cada organización está encargada de distribuir las listas de confianza; por lo tanto el retiro de un ancla de

confianza en este entorno implica la distribución de listas de confianza en cada organización.

3.8. PKI DEL BANCO CENTRAL DEL ECUADOR (BCE)

La PKI del BCE se encuentra en funcionamiento desde Agosto de 2002; esta infraestructura brinda protección a las transacciones realizadas por el SNP[1] a través de su red privada, manteniendo un sistema de autenticación basado en certificados digitales para todas las instituciones que forma parte del SFN[2].

Mantiene una arquitectura plana; es decir, la AC de la PKI del BCE solo puede emitir certificados de entidad destino. Hasta el momento se han emitido 180 certificados de los 250 certificados que tiene disponibles para un período de 20 años contados desde Octubre de 2004.

Desde su implementación, se han realizado 18'084.195 transacciones, con un valor acumulado de 6.589'533.348,89 de dólares[3]. Se debe mencionar que al momento no todas las instituciones del SFN ofrecen los servicios del SNP a sus clientes; sin embargo, todas las instituciones reciben transferencias a favor de sus clientes.

El BCE mantiene información del funcionamiento del SNP en la página *Web* http://www.bce.fin.ec/contenido.php?CNT=ARB0000814; en este portal se puede encontrar información referente a tarifas, regulaciones, formularios, etc.

---

[1] Sistema Nacional de Pagos.

[2] Sistema Financiero Nacional.

[3] http://www.bce.fin.ec/contenido.php?CNT=ARB0000814, documento "Estadísticas".

3.8.1. ELEMENTOS DE LA PKI DEL BCE

Al igual que cualquier infraestructura de claves públicas, la PKI del BCE está conformada por: AC, directorio, AR, directivas, entidades destino y entidades confiantes. La figura 3.11 muestra un esquema general.

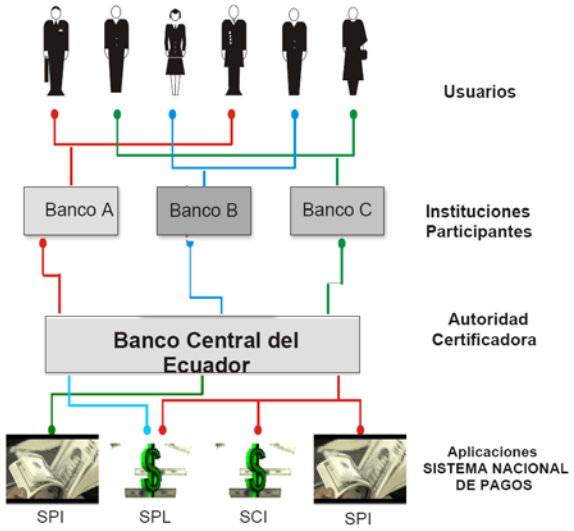

Figura 3.11 Esquema de la PKI del BCE[1]

3.8.1.1. AR de la PKI del BCE

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

Para lograr que el proceso de verificación de identidades sea seguro, cada institución debe asignar un responsable de certificados; éste trabajará conjuntamente con los administradores en el establecimiento de identidades auténticas. Para evitar

[1] BCE. Manual de Usuario.

conflictos de intereses, un responsable de certificados no puede solicitar un certificado para sí mismo.

El proceso de registro inicia con la descarga de un formulario de solicitud de certificado desde el sitio *Web* del SNP, este formulario es enviado posteriormente a los administradores de la PKI; uno de los administradores comprueba los datos consignados en el formulario con el responsable de la institución a la que pertenece el usuario, si los datos son correctos, el usuario queda registrado.

El proceso de registro finaliza mediante una interacción entre el usuario que ha solicitado un certificado, el responsable de su institución y la AC; para esto, el administrador entrega al usuario y al responsable sus códigos de activación[1], éstos permitirán que el usuario y el responsable se autentiquen durante el proceso de descarga del certificado.

3.8.1.2. AC de la PKI del BCE

La autoridad certificadora de la PKI del BCE es una AC raíz que puede expedir únicamente certificados de entidad destino, los usuarios pueden acceder a ésta a través de la página https://sas.bcepki.bce.fin.ec/enroll/.

Cuando el proceso de registro ha concluido, el usuario y el responsable deben ingresar al sitio *Web* de la AC y seleccionar la opción *"Zero footprint"* o ingresar directamente a la página https://sas.bcepki.bce.fin.ec/enroll/client-zf.html.

La opción *"Zero footprint"*, le permite al cliente acceder al sistema *Self-Administration Server*; este sistema está diseñado para crear y recuperar un certificado. Cada una

[1] Al usuario del certificado se entrega un número de referencia personal y al representante un código de autorización único para cada certificado.

de estas opciones se puede realizar ingresando el número de referencia del usuario y el código de autorización del responsable, como se muestra en la figura 3.12.

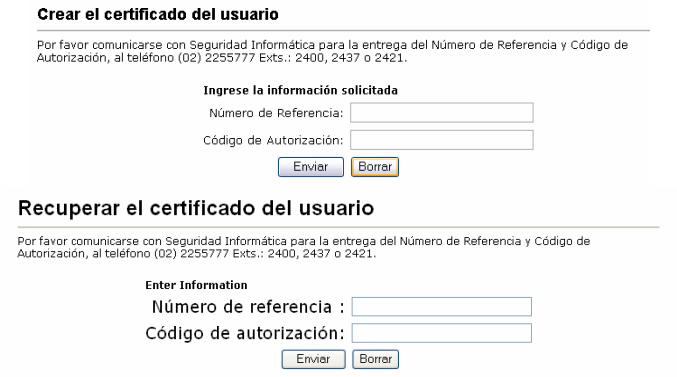

Figura 3.12 Creación de un certificado digital, ingreso de códigos de activación

Este proceso mantiene un nivel elevado de seguridad, pues el procedimiento recomendado indica que tanto el usuario como el responsable deben ingresar sus códigos de activación personalmente; de esta manera se garantiza que solo el usuario tendrá acceso al certificado digital que le permitirá posteriormente realizar transacciones dentro del SNP.

Una vez que se hayan ingresado los códigos de activación, el usuario continúa con el procedimiento haciendo clic en el botón Enviar. Si los códigos son correctos, se presenta la pantalla mostrada en la figura 3.13, en la cual el usuario debe ingresar el nombre del certificado, una contraseña personal y su confirmación.

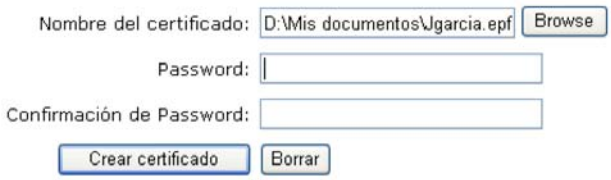

Figura 3.13 Creación de un certificado digital[1]

[1] BCE. Manual de Usuario.

El nombre del certificado de un usuario debe mantener el siguiente formato: la primera letra de su nombre en mayúscula seguido de su apellido completo en minúsculas; finalmente, se debe ingresar la extensión .epf. Por ejemplo, en el caso de Juan García, el nombre del certificado sería Jgarcia.epf.

Cuando se han llenado todos los datos el certificado es creado y almacenado en la ubicación seleccionada por el usuario.

3.8.1.3. Directorio de la PKI del BCE

El directorio de la PKI 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 almacenados, *Novell* usa su NDS (*Novell Directory Services*), el cual asocia a un certificado con su clave privada.

3.8.1.4. Directivas de la PKI del BCE

La PKI 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.

Adicionalmente, se posee un reglamento que especifica la forma en que se realizarán las transacciones entre instituciones, plazos para que cada institución acredite los montos pertinentes a sus respectivos clientes y sanciones a las instituciones en caso de incumplimiento.

También se ha determinado tarifas, obligaciones y responsabilidades del BCE y de las instituciones participantes dentro del SNP y sus distintas aplicaciones. El reglamento se encuentra actualizado al 20 de Mayo de 2004 en la página *Web* http://www.bce.fin.ec/frame.php?CNT=ARB0000817.

Por el momento no se ha establecido una CP o CPS, y la información que hace referencia a políticas y procedimientos está restringida para uso exclusivo de los usuarios del sistema.

3.8.1.5. Entidad Destino de la PKI del BCE

El SNP fue creado inicialmente para brindar servicios a las instituciones que forman parte del SFN, el sector público y las cámaras de compensación.

El SFN está conformado por 72 instituciones, incluyendo bancos nacionales y extranjeros, proveedores de tarjetas de crédito, mutualistas y cooperativas de ahorro y crédito; actualmente, todas estas instituciones realizan transacciones entre sí a través del SNP.

El sector público está compuesto por todas las instituciones del estado, éstas se hallan obligadas por el decreto ejecutivo 571, publicado en 2003 a realizar todos los pagos de remuneraciones a servidores públicos a través del SPI (Sistema de Pagos Interbancario).

Finalmente, las cámaras de compensación son instituciones que realizan procesos de compensación de pagos por diferentes conceptos y generan resultados netos bilaterales o multilaterales [1] . Los participantes en dichas transacciones deben

[1] BCE. REFORMAS DEL SISTEMA DE PAGOS. 2003.

mantener una cuenta corriente en el BCE, por medio de la cual se liquidan los valores resultantes de los procesos de compensación.

3.8.1.6. Entidad Confiante de la PKI del BCE

La PKI del BCE está destinada solamente para uso de instituciones que forman parte del SNP; siendo así, las entidades confiantes están constituidas por las mismas entidades destino y los servidores de la PKI. No existen terceros usuarios que tengan acceso a los certificados expedidos o que requieran hacer uso de éstos.

3.8.2. APLICACIONES DE LA PKI DEL BCE

El SNP está conformado por varios módulos o aplicaciones, entre los cuales se puede mencionar el SPL (Sistema de Pagos en Línea), SCI (Sistema de Cobros Interbancario), SPN (Sistema de Pagos por valores Netos) y el SPI (Sistema de Pagos Interbancarios).

Para utilizar estas aplicaciones, los usuarios pueden ingresar por la red privada que interconecta al SFN con el BCE, también se tiene acceso a través del portal de servicios bancarios https://publico.bce.fin.ec/.

El SPL y el SCI utilizan el esquema RTGS (*Real Time Gross Settlement*), que permite la transferencia inmediata de los montos involucrados en determinada transacción, esto hace que las transferencias sean irrevocables una vez realizadas.

El SPN permite que las diferentes instituciones realicen transacciones a través del SNP de los valores netos producidos durante un periodo de tiempo, las transacciones se realizan a una hora definida previamente entre los participantes.

Tipo	Nº de Instituciones Existentes	Nº de Instituciones que ofrece el Servicio SPI	Nº de Instituciones que recibe transacciones del SPI
BCE	1	1	1
Mutualistas	5	3	2
Bancos de desarrollo	2	0	2
Bancos extranjeros	2	2	2
Bancos nacionales	23	17	6
Proveedores de Tarjetas de Crédito	2	2	2
Cooperativas de Ahorro y Crédito	37	0	37
Total	**72**	**25**	**72**

Tabla 3.2 Distribución de Instituciones Participantes dentro del SPI[1]

El SPI es el más difundido, el 90,48 % de los usuarios activos del SNP lo utilizan; este servicio permite que una institución financiera transfiera recursos a otra entidad del SFN por medios electrónicos. En la tabla 3.2 se muestra una distribución del uso del SPI dentro del SFN.

3.8.3. ESTUDIO DE MERCADO

Este estudio de mercado pretende determinar las perspectivas de PKI en el Ecuador, enfocándose en el funcionamiento de la PKI del Banco Central, los servicios que brinda, y su inserción en el mercado.

Para la realización del estudio de mercado se han realizado encuestas a los responsables[2] de los certificados en cada institución participante dentro del SNP y

[1] Marzo 2006.

[2] El formato de la encuesta se encuentra registrado en el Anexo 3.

los usuarios[1] finales de certificados. Además se realizó una entrevista[2] al Ingeniero Marcelo Balarezo, uno de los Administradores de la PKI.

3.8.3.1. Etapas del Estudio de Mercado

Un estudio de mercado consta de seis etapas: planeación, recolección de datos, codificación, procesamiento, análisis e interpretación y finalmente publicación[3]. A continuación se detalla cada una de las etapas.

- **Planeación**.- Durante esta etapa se definieron los objetivos y estructura de la entrevista y encuestas[4]; además, se realizó el cálculo de la muestra manteniendo los criterios señalados por los administradores de la PKI del BCE.

- **Recolección**.- Después de obtener la aprobación por parte del Director de Informática del BCE el 30 de Noviembre de 2005, los responsables de los certificados digitales de cada institución fueron informados de la realización del estudio de mercado el 23 de Enero de 2006.

  En el caso de los responsables de certificados, las encuestas se realizaron utilizando como método de muestreo el censo; es decir, se encuestó a todos los responsables de certificados digitales (24) de las instituciones participantes dentro de la PKI del BCE. Estas encuestas se realizaron telefónicamente entre el 30 de Enero de 2006 y el 3 de Marzo de 2006.

  Las encuestas a usuarios se realizaron telefónicamente entre el 30 de Enero y el 17 de Febrero de 2006, utilizando como método el muestreo aleatorio

---

[1] El formato de la encuesta se encuentra registrado en el Anexo 4.

[2] El formato de la entrevista se encuentra registrado en el Anexo 2.

[3] CIRO, Martínez. Estadística y muestreo.

[4] Anexos 2, 3 y 4.

simple, debido a que este método es adecuado para poblaciones pequeñas, compuestas por elementos homogéneos como es el caso de los usuarios de certificados del SNP.

La entrevista se realizó personalmente al Ing. Marcelo Balarezo, administrador de la PKI del BCE el 18 de Noviembre de 2005. Los resultados de esta entrevista se encuentran registrados en el Anexo 2.

Sigla	Significado
B	Bóveda
BC	Bajo Custodia
C	Cuenca
CC	Cambio de Cargo (funciones del empleado)
CF	Caja fuerte
c / p	Depende de cada persona
D	Destruido
DE	Dispositivo extraíble
DU	Se desconfía del usuario
FT	Falla técnica en el Sistema de la PKI
G	Guayaquil
I	Indefinido
L	Loja
M	Memorizado
M1	Existe una persona del departamento de *helpdesk* encargada de instalar los certificados.
M2	Se reveló el código de autorización para la descarga de los certificados en las sucursales.
NC	No contesta
NE	No es estable
NR	No recuerda
NS	No sabe
PS	Personal de sistemas
Q	Quito
SCI	Sistema Cobros Interbancario
SPI	Sistema de Pagos Interbancario
SPL	Sistema de Pagos en Línea
SPN	Sistema de Pagos por valores Netos
# a	# años (# significa número de años; por ejemplo dos años)
# d	# días (# significa número de días; por ejemplo treinta días)
# m	# meses (# significa número de meses; por ejemplo dos meses)
	El encuestado no contestó la pregunta.

Tabla 3.3 Siglas utilizadas para la codificación de las encuestas realizadas

- **Codificación**.- La codificación es el proceso mediante el cual se establece acrónimos, representaciones de las respuestas y formatos que se van a utilizar durante el procesamiento de los datos encontrados. En la tabla 3.3 se detallan todas las siglas utilizadas dentro del estudio de mercado.

- **Procesamiento**.- Este proceso comprende la tabulación de los datos recogidos. La tabulación mantiene un formato que agrupa las preguntas dentro de cada una de las secciones planteadas en la entrevista y las encuestas.

  Los resultados de las tabulaciones se encuentran registrados en el Anexo 3 para los responsables de certificados y en el Anexo 4 en el caso de los usuarios de certificados.

- **Análisis e Interpretación**.- En la sección 3.8.3.2 se presenta con más detalle los resultados encontrados a partir de la tabulación de las encuestas. Los resultados se encuentran registrados en su totalidad en el Anexo 3 para los responsables de certificados y en el Anexo 4 en el caso de los usuarios de certificados.

- **Publicación**.- El Estudio de mercado fue presentado a los administradores de la PKI el 3 de Abril de 2006.

3.8.3.2. Análisis del Estudio de Mercado

Este estudio de mercado tiene como objetivo determinar la situación actual de la PKI del Banco Central, los servicios que brinda, su inserción en el mercado, con el fin de evaluar el progreso alcanzado; para lograr este objetivo se ha recolectado información relacionada con:

- El funcionamiento de la PKI.

- El desempeño de los Responsables[1] de los Certificados de cada institución que forma parte del SNP.
- El desempeño de los Usuarios de los Certificados de las instituciones que forman parte del SNP.

Al comparar los resultados obtenidos de los Responsables y Usuarios de certificados entre sí, y a su vez con la entrevista realizada al Administrador de la PKI del BCE, se puede determinar la situación actual de la PKI del BCE.

Los resultados encontrados se encuentran agrupados en distintas secciones; en los casos en los que se ha generado información adicional al realizar una encuesta, esta información se incluye como comentario.

a. Sección General

Esta sección tiene como objetivo, determinar el alcance y limitaciones de la PKI del BCE; para esto, se tomó en cuenta la infraestructura técnica de la PKI, arquitectura, plataformas, número de licencias, procedimientos para el registro de usuarios, aplicaciones del SNP, así como también el nivel de confiabilidad alcanzado por parte de la PKI del BCE.

Software* PKI / *Entrust	
Cantidad	Descripción
1	*Infrastructure Entrust Authority Security Manager* (AC)
1	*TruePass Server* (Autenticación robusta)
1	*Roaming Server* (Movilidad para el acceso de certificados)
1	*Self Administration Server* (Emisión de certificados vía *Web*)
1	*GetAccess Server* (Control de Acceso)
250	*Entrust TruePass ID's Funtions* (Licencias de Certificados Digitales)

Tabla 3.4 Productos de seguridad utilizados por la PKI del BCE

[1] Durante el proceso de encuestamiento, se detectó que el 4,76 % de los nombres de los Responsables no se encontraba actualizado.

- **Infraestructura Técnica.-** La PKI del BCE cuenta con una infraestructura técnica que utiliza productos de seguridad *Entrust*. Los productos utilizados se muestran en la tabla 3.4; éstos alcanzan un nivel satisfactorio de seguridad, creando certificados digitales que permiten la autenticación de usuarios ante las aplicaciones del SNP.

  Los productos utilizados por la PKI del BCE logran una autenticación segura[1], permitiendo a los usuarios acceder al sistema por medio de una red privada que conecta al PKI del BCE con cada institución, o a través de Internet, mediante una sección segura al ingresar al portal https://publico.bce.fin.ec/.

  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, manteniéndose cifrada la información almacenada.

---

[1] El 4,76 % de los Responsables de Certificados Digitales admite que las instalaciones existentes dentro de su institución mantienen un nivel menor de seguridad; señalan además que esto hace disminuir la seguridad de todo el sistema.

- **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.

- **Número de licencias**.- El certificado digital de la AC raíz tiene una duración de 20 años, contados a partir del 2004. Puede emitir en ese periodo 250 certificados digitales; hasta el momento se han expedido 180 certificados, de los cuales 175 fueron emitidos para usuarios del sistema y 5 para realización de pruebas.

- **Registro de Usuarios.-** La AR 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 FormularioDI-SI-0255, la información es validada por el Administrador de la PKI con la colaboración de los responsables de certificados de cada institución.

  El nivel de seguridad en este procedimiento alcanza un puntaje de 8 sobre 10 según los Administradores de la PKI. Al evaluar las encuestas realizadas a los Responsables de certificados, se obtuvo como resultado un promedio de 8,57 sobre 10; esto indica un nivel de eficacia satisfactorio en el procedimiento.

- **Aplicaciones.-** De los certificados creados, el 80 % han sido expedidos para ser utilizados dentro del SPI, el 15 % dentro del SPL y el 5 % para el SCI. Sin embargo, debido a que al autenticarse dentro del SNP con un certificado se puede acceder a varias aplicaciones, en la práctica el 90.48 % de los usuarios utiliza el SPI, el 19.05 % el SPL, el 14,29 % el SCI y el 9.52 % el SPN.

- **Nivel de Confiabilidad.-** La PKI del BCE está destinada a brindar servicios de certificación exclusivamente a las Instituciones que forman parte del SFN[1].

  Para estas instituciones; la PKI del BCE goza de un nivel elevado de confiabilidad; en el caso de los Responsables de certificados, alcanza un promedio del 9,08 sobre 10, mientras que los usuarios le otorgan un promedio de 9,38 sobre 10. Esto indica que la PKI del BCE tiene un alto nivel de confiabilidad dentro del sector al que debe proporcionar prestaciones.

b. Sección Manejo de Códigos de Autorización y Números de Referencia

Esta sección tiene como objetivo, determinar el nivel de seguridad existente dentro de los procesos involucrados en el ciclo de vida de los códigos de autorización y los números de referencia.

- **Nivel de Seguridad.-** El nivel de seguridad en la entrega de los Códigos de Autorización[2] y los Números de Referencia alcanza un puntaje de 8 sobre 10 según los Administradores de la PKI; al evaluar en las encuestas realizadas a los Responsables de certificados, se obtuvo como resultado un promedio de 8,61 sobre 10; esto indica un nivel de eficacia satisfactorio en el procedimiento.

- **Procedimientos.-** No se tiene definido un procedimiento específico para la entrega de estos códigos[3]. El 33,33 % de los usuarios obtuvo su número de referencia personalmente, otro 33,33 % mediante un correo electrónico, el 23,81 % lo obtuvo telefónicamente y el 9,52 % no recibió personalmente su

---

[1] Actualmente, 24 de las 25 instituciones que forman parte del SFN forman parte del SNP; sin embargo, no todas se encuentran utilizando regularmente el sistema. El 4,17 % de los usuarios, indica que como consecuencia las transacciones se realizan en un tiempo mayor al necesario.

[2] El 9,52 % de los Responsables cree que la entrega de los códigos de autorización es insegura.

[3] El 4,76 % de los responsables piensa que el proceso de generación de los códigos de autorización es lento. El 4,17 % de los usuarios piensa que el proceso de generación de los certificados digitales es lento.

número, debido a que es el personal de sistemas el encargado de la parte técnica.

Por otra parte, el almacenamiento de los códigos tampoco se encuentra definido, tanto los usuarios como los responsables, han almacenado su código según su propio criterio.

- **Caducidad.-** Existe un desconocimiento del período de duración de los Códigos de Autorización y Números de Referencia; apenas el 4.17 % de los Responsables conoce el periodo de duración de un código de autorización; en el caso de los usuarios solo el 9,52 % conoce el periodo de duración de su número de referencia.

- **Acceso.**- El 8,29 % de los Responsables han revelado sus códigos de autorización a otras personas; en algunos casos debido a que es el personal de informática el encargado de la instalación de los certificados; otro motivo es la delegación de funciones.

  En el caso de los usuarios el 14,29[1] % de los usuarios ha revelado su número de referencia a otra persona, específicamente al personal de informática, debido a que éste es el encargado de la instalación de los certificados.

c. Sección Manejo de Certificados Digitales

Esta sección tiene como objetivo, determinar el nivel de seguridad existente dentro de los procesos involucrados en el ciclo de vida de los certificados digitales generados por la PKI del BCE.

---

[1] Además del 14,29 % que respondió “si”, un 4,17 % (respondieron “no”) de los usuarios reveló su número de referencia dentro del proceso de encuestamiento; un 4,17 % de los usuarios se negó a proseguir con la encuesta hasta tener una autorización del departamento de seguridad e su institución.

- **Nivel de Seguridad.-** El nivel de seguridad en la generación de los certificados digitales es elevado, se requiere que el Responsable[1] de certificados y el usuario del certificado ingresen conjuntamente el código de autorización[2] y el número de referencia; este procedimiento se realiza utilizando una sesión *Web* cifrada. Finalmente, se tiene definidas normas estrictas para la aplicación de contraseñas para el acceso a los certificados.

  Al evaluar las encuestas realizadas a los Responsables de certificados, se obtuvo como resultado un promedio de 8,61 sobre 10, en el caso de los usuarios se alcanzó un 8.95 sobre 10; esto indica un nivel de eficacia satisfactorio en el procedimiento.

  En el caso de recuperación de certificados, el nivel de seguridad alcanza un puntaje de 8 sobre 10 según los Administradores de la PKI; para realizar este procedimiento, primero se realiza la verificación del requerimiento del usuario contactándose con el Responsable de certificados de la Institución en particular.

  Las CRLs son actualizadas cada 15 minutos lo que entrega un elevado nivel de confiabilidad de los certificados válidos.

- **Procedimientos.-** Existe un procedimiento establecido por la PKI del BCE para la generación y descarga de certificados digitales; sin embargo, no todos los certificados pasaron por este procedimiento, el 14,29 % de los usuarios reporta que es el personal de sistemas el responsable de la descarga e instalación de los certificados digitales.

---

[1] El 4,76 % de los Responsables de certificados admite que después de la generación de los certificados digitales, no se realiza un control del uso apropiado de éstos.

[2] El 19,05 % de los Responsables ha delegado sus funciones a un usuario de certificados y otro 4,76 % lo ha delegado a otro directivo de su institución cuando las instalaciones de certificados se han realizado en sucursales.

Por otra parte, el almacenamiento de los certificados no se encuentra definido; sin embargo, el 95.24 % de los usuarios han almacenado su certificado digital en su PC personal; el 4.76 % restante, tiene acceso restringido a su certificado, en este caso, el certificado digital se encuentra almacenado en Bóveda.

- **Caducidad.-** Existe un desconocimiento del período de validez de los certificados digitales; apenas el 4.76 % de los Usuarios conoce el periodo de validez de su certificado digital (2 años); en el caso de los responsables ninguno conoce el periodo de validez de un certificado digital.

- **Acceso.**- El 4,17[1] % de los Responsables admite que se permite que diferentes usuarios tengan acceso a los certificados dentro de su institución, debido a delegación de las funciones del usuario. En el caso de los usuarios el 9,52[2] % de los usuarios ha permitido que otra persona tenga acceso a su certificado digital.

- **Distribución Geográfica.**- El 62,5 % de los Responsables de certificados se encuentra registrado en la ciudad de Quito, el 29,17 % en la ciudad de Guayaquil y el 8.34 % restante se encuentra dividido entre las ciudades de Cuenca y Loja. Esto muestra que el sistema por el momento se encuentra centralizado.

d. Sección Cumplimiento de Políticas

---

[1] Además del 4,17 % que respondió “si”, un 23,81 % (respondieron “no”) de los responsables indico que se saca backups de los certificados, con el fin de permitir que otros usuarios reemplacen a los propietarios de certificados en caso de ser necesario.

[2] Además del 9,52 % que respondió “si”, un 8,33 % (respondieron “no”) indicó que ha permitido que otra persona tenga acceso a su certificado personal. Esto indica un 17,85 % de pérdida de la singularidad de los certificados.

Esta sección tiene como objetivo, identificar el nivel de seguridad de los procedimientos empleados dentro de la PKI del Banco Central del Ecuador, y su cumplimiento dentro de las Instituciones que forman parte del SNP.

- **Políticas de la PKI del BCE.-** El 87.5 % de los responsables de certificados asegura haber recibido recomendaciones sobre el manejo de códigos y certificados digitales; de este porcentaje el 85,72 % asegura que estas recomendaciones se están cumpliendo.

- **Políticas las Instituciones que forman parte del SNP.-** El 70,83[1] % de los responsables de certificados indica que dentro de sus instituciones se han creado normas y políticas de seguridad para el manejo de códigos y certificados; por otra parte, el 87,5 % de los usuarios asegura que las normas y políticas implementadas dentro de sus instituciones se está cumpliendo.

- **Reportes ante sucesos.-** Los responsables de certificados no tienen un conocimiento adecuado de los acontecimientos que deben ser reportados a los Administradores de la PKI; por ejemplo, el 20,83 % no reportaría la salida de uno de los usuarios de certificados de su institución y apenas el 50 % reportaría el compromiso de una contraseña para acceso al SNP.

e. Sección Soporte Técnico

Esta sección tiene como objetivo, determinar el tipo soporte técnico que se brinda a los clientes por parte de la PKI del BCE y el nivel de calidad percibido por los usuarios y responsables de las instituciones que forman parte del SNP.

- **Responsables.-** En el caso de los responsables de certificados, el 79.17 % ha utilizado el servicio de soporte técnico brindado por la PKI del BCE. Al encuestar a los responsables de certificados que han utilizado el soporte técnico, se

[1] Un 16,32 % del 29,17 % que no ha creado normas o políticas para el manejo de los códigos y certificados, mantiene políticas para el manejo de contraseñas.

encontró que el 21, 04 % considera que la información relacionada con el funcionamiento de la PKI es pública[1] (ésta es restringida[2]).

- **Usuarios.-** En el caso del soporte técnico brindado por la PKI del BCE, el 71,43 % de los usuarios asegura haber utilizado este servicio en algún momento; el 28,57 % restante, no lo ha utilizado debido a que es el personal de informática de sus instituciones el que soluciona cualquier incidente.

- **Disponibilidad[3].-** El 86,66 % de los usuarios y el 84,21 % de los responsables, conoce que la disponibilidad del soporte técnico se encentra dentro del horario de oficina[4] del BCE. Tanto los usuarios como los responsables han recibido soporte técnico dentro de las tres modalidades existentes: telefónicamente, por medio de correo electrónico o personalmente.

- **Calidad del Soporte Técnico.**- Al evaluar en las encuestas realizadas a los Responsables de certificados, se obtuvo como resultado un promedio de 8,61 sobre 10, en el caso de los usuarios se alcanzó un 8.95 sobre 10; esto indica un nivel de eficacia satisfactorio en el nivel de calidad del soporte técnico de la PKI.

3.8.4. SITUACIÓN LEGAL

La PKI del BCE no ha legalizado su situación como Autoridad Certificadora de acuerdo con la Resolución 584 emitida por el CONATEL, que obliga a las

---

[1] El 4,76 % de los responsables no maneja información relacionada con los certificados que se han expedido para su institución y otro 4,76 % no se encuentra bien informado.

[2] El 4,76 % de los Responsables de certificados piensa que se debería entregar documentación que contenga información acerca del funcionamiento del PKI y los procedimientos recomendados.

[3] El 4,76 % de los Responsables indica que no existe un monitoreo del sistema por parte del PKI del BCE.

[4] El 9,52 % de los Responsables de certificados señala que el horario destinado a brindar soporte técnico debería extenderse fuera del horario de oficina.

instituciones del sector público a acreditase con este organismo o trabajar con AC acreditadas.

Actualmente fundamenta su situación legal amparándose en el artículo 28 de la Ley 67, que establece que “Cuando las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas y certificados, se reconocerá que ese acuerdo es suficiente en derecho”.

Debido a que por el momento en el País no se han establecido ACs acreditadas por el CONATEL y que según el artículo 9 de su reglamento los certificados que no hayan sido emitidos por una de éstas son “certificados de firma electrónica no acreditados”; los usuarios del SPN y los miembros de la PKI del BCE asumen la responsabilidad por utilizar certificados no válidos como elementos de prueba.

A pesar de que las condiciones jurídicas no se encuentren totalmente favorables, la infraestructura de seguridad proporcionada por PKI hace que su uso sea indispensable dentro del SNP, debido a que se realizan transacciones con montos considerables y esta infraestructura proporciona niveles elevados de confiabilidad para la autenticación.

3.9. PKIX-X.509 EN INTERNET

El grupo de desarrollo de PKIX fue creado en 1995 por la IETF, con el propósito de crear estándares que permitan el funcionamiento de PKI con certificados X.509 sobre Internet, pero desde su creación su alcance se ha expandido y actualmente sus proyectos no se limitan a los estándares PKI de la UIT. Entre sus principales características se puede mencionar:

- **Arquitectura**.- La arquitectura PKIX es similar a la arquitectura general de PKI, incluye especificaciones que hacen referencia a la forma en que interactúan

sus elementos; por ejemplo, la forma en que se van a realizar las transacciones operativas[1] y administrativas, o la publicación de certificados y CRLs.

- **Elementos**.- Los principales elementos de PKIX son: clientes (entidad destino), autoridad certificadora, autoridad de registro y directorios.

- **Funciones PKIX.-** PKIX define dentro de sus funciones a las siguientes:

    - **Registro**.- Es el proceso mediante el cual un cliente se somete al proceso de identificación, el registro puede ser realizado por la AR o en su defecto por la AC.

    - **Iniciación**.- Es el proceso que abarca el inicio de la interacción entre una entidad destino y PKI, esto incluye la identificación de sus elementos, el intercambio de información inicial, entrega del certificado de la AC al cliente, etc.

    - **Generación de claves**.- El cliente puede generar la pareja de claves y enviárselas a la AR o AC en una solicitud; también contempla la posibilidad de que sea la AC la encargada de la generación de las claves, siempre y cuando éstas se envíen al cliente a través de una conexión segura.

    - **Certificación**.- Ésta es la etapa en la que la AC vincula el nombre del usuario y su pareja de claves en un certificado digital.

    - **Recuperación de la pareja de claves**.- Si se utiliza las claves públicas para cifrar, es necesaria la implementación de un almacén de claves; el

[1] Todo el ambiente operativo de PKIX funciona sobre los protocolos base de Internet: HTTP o FTP.

proceso de recuperación de claves se realiza en caso de pérdida de una clave privada.

- **Actualización de la clave**.- Este proceso puede ocasionarse bajo tres circunstancias: expiración de la pareja de claves, compromiso de la clave privada o una actualización del certificado.

- **Certificación cruzada**.- Un certificado cruzado es aquel que ha sido expedido por una AC para otra AC, se puede establecer relaciones de confianza unidireccionales o bidireccionales.

- **Revocación**.- La AC es responsable de la actualización del estado de los certificados emitidos, esto incluye la revocación y su respectiva notificación a los posibles afectados.

- **Distribución y publicación de certificados y CRLs**.- Los certificados son entregados a los clientes cuando se ha culminado el proceso de certificación, en ese momento, se puede entregar de forma simultánea información relacionada con las CRLs existentes.

  Las CRLs emitidas posteriormente, pueden ser publicadas en un directorio en un periodo de tiempo determinado o cuando la AC considere que es fundamental su actualización.

3.9.1. PROTOCOLOS PARA TRANSACCIONES ADMINISTRATIVAS

La IETF dentro del grupo de trabajo PKIX ha creado los protocolos CMP (*Certificate Management Protocol*-RFC 4210) y CMC (*Certificate Management Messages over CMS*[1]-RFC 2797), para los procesos de administración e intercambio de mensajes.

[1] *Cryptographic Message Syntax*.

3.9.1.1. CMP

Este protocolo define mensajes para la creación y administración de certificados X.509v3, su objetivo es conseguir que la estructura PKI sea consistente con los entes encargados de su administración.

CMP permite realizar un soporte en línea entre los componentes PKI, manteniendo compatibilidad con los estándares criptográficos existentes (RSA, DSA, MD5, y SHA-1); además, puede operar sobre protocolos de correo electrónico, HTTP, FTP y TCP/IP[1].

El protocolo define a la AC como la única entidad encargada de todo el proceso de emisión de certificados; es decir, la AR y el usuario del certificado no pueden intervenir en este proceso, de esta manera se asegura que los campos y las extensiones del certificado sean manipulados por la AC de acuerdo a la CP de la PKI.

Dentro de sus especificaciones se contempla todas las etapas del establecimiento de un sistema PKI, incluyendo el ciclo de vida de un certificado y de las claves relacionadas con éste; la administración de la PKI está basada en grupos operativos que definen el formato de los mensajes en cada etapa.

3.9.1.2. CMC

CMC define especificaciones para el intercambio de mensajes de administración, fue desarrollado para crear interfaces de productos PKI y servicios que soporten CMS y PKCS#10, con el fin de suministrar al protocolo S/MIMEv3 un medio para la obtención de certificados que manejen firmas DSA con el intercambio de claves *Diffie-Hellman*.

---

[1] *Transmission Control Protocol/Internet Protocol*.

El protocolo PKCS#10 es utilizado para el envío de solicitudes, éste define la sintaxis para solicitudes de certificación, incluyendo nombre distinguido, clave pública y otras opciones. Todo el contenido del mensaje debe ser firmado por la entidad que solicita el certificado; para las respuestas se utiliza el protocolo PKCS#7.

CMS emplea el mismo tipo de mensaje para solicitudes y respuestas [1], sus especificaciones establecen un formato que le permite anidar en el mismo mensaje información sobre el cifrado, datos firmados, valores *hash*, firmas digitales y registros de tiempo; los datos firmados pueden incluir información arbitraria, ésta es interpretada por la aplicación para los procesos de administración.

3.9.2. PROTOCOLOS PARA VALIDACIÓN DE CERTIFICADOS

El proceso de validación de certificados establece mecanismos que garantizan el uso seguro de un certificado dentro de un sistema PKI, que incluye las siguientes etapas:

- Verificación de la firma de la AC que emitió el certificado.
- Comprobación de la vigencia del certificado (¿ha caducado?).
- Verificación del uso adecuado del certificado.
- Verificación de las CRLs correspondientes.

El proceso de validación puede resultar complejo para algunos usuarios, con el fin de lograr que el entorno PKI sea transparente para el usuario. La IETF dentro del grupo de trabajo PKIX ha creado los protocolos OCSP (*Online Certificate Status Protocol*-RFC 2560) y el SCVP (*Standard Certificate Validation Protocol*-ID[2]), para los procesos de validación de certificados digitales.

---

[1] Utiliza codificación ASN.1.

[2] draft-ietf-pkix-scvp-23.

3.9.2.1. OCSP

Los servicios definidos por el protocolo OCSP, proporcionan a las entidades confiantes (usuarios y aplicaciones) un mecanismo eficiente para verificar el estado de un certificado de manera inmediata y actualizada, evitando que los usuarios descarguen las CRLs.

Los mensajes OCSP son transmitidos generalmente sobre HTTP y usan para su codificación ASN.1; cuando se recibe una solicitud de validación, OCSP responde con mensajes conocidos como "*responder*". Los valores de estos mensajes pueden tomar tres tipos de valores: bueno, revocado y desconocido; además, contienen un registro de tiempo que indica la hora en que el *responder* fue creado.

La validación realizada por OCSP solo confirma el estado del certificado, no establece una validación de la ruta de confianza ligada al certificado; otra limitación de OCSP es que dentro de las solicitudes no se envía el certificado sino un valor *hash* de éste con su identificador, por ese motivo no es posible verificar la firma de la AC que emitió el certificado.

3.9.2.2. SCVP

SCVP está diseñado para que los clientes deleguen a un servidor las tareas de validación de certificados y construcción de rutas de confianza, esto permite simplificar las aplicaciones cliente y mantener un sistema centralizado para el control del cumplimiento de directivas.

Este protocolo incluye los certificados dentro de los mensajes de solicitud de validación, debido a que el servidor posee toda la información del certificado, puede realizar el proceso de validación completo.

Cada solicitud enviada al servidor puede firmarse digitalmente por el cliente de manera opcional; en cambio, todas las respuestas de validación deben estar firmadas por la entidad que realizó la verificación. Los mensajes SCVP pueden ser enviados sobre HTTP o protocolos de correo electrónico.

3.9.3. AUTORIDAD NOTARIAL

El grupo de trabajo PKIX del IETF establece una sección de especificaciones para transacciones notariales, éstas definen una NA (*Notary Authority*[1]), la NA es una entidad de confianza que verifica y certifica la validez de los datos que son sometidos a su consideración, en otras palabras, su objetivo es la certificación de contenidos.

Los documentos certificados por la NA son firmados digitalmente por ésta después de la adición de un registro de tiempo, con esto se pretende asegurar la aceptación de las transacciones.

Las especificaciones notariales del grupo de trabajo PKIX fueron propuestas dentro de un I-D en 1997, éste no ha sido actualizado desde entonces, por lo que aun no se tiene claro el modelo y las funciones de la NA.

[1] IETF. draft-ietf-pkix-ipki6np-00.

Capítulo 4

IMPLEMENTACIÓN DE UNA PKI JERÁRQUICA SOBRE WINDOWS 2003 SERVER ENTERPRISE

4. IMPLEMENTACIÓN DE UNA PKI JERÁRQUICA SOBRE *WINDOWS 2003 SERVER ENTERPRISE*

Este capítulo presenta una guía para la implementación de una PKI jerárquica, la misma que será utilizada dentro de una solución de seguridad para WLANs con EAP-TLS en el siguiente capítulo. La PKI jerárquica está basada en la solución proporcionada por *Microsoft* con su sistema operativo *Windows 2003 Server Enterprise*.

4.1. GENERALIDADES DE LA SOLUCIÓN. VENTAJAS DE LA SOLUCIÓN BASADA EN *WINDOWS 2003 SERVER* FRENTE A OTRAS OPCIONES BASADAS EN *LINUX*

El esquema de la PKI jerárquica se muestra en la figura 4.1, en la que se puede observar, que la PKI está formada por dos niveles.

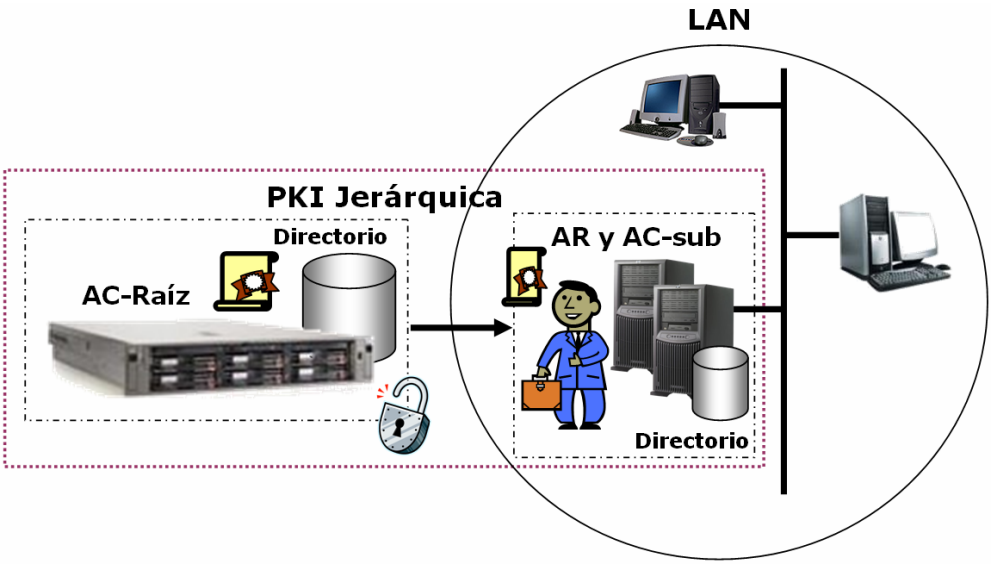

Figura 4.1 Esquema general: PKI Jerárquica

La AC-Raíz emite certificados para un nivel inferior de ACs subordinadas y no para entidades destino, lo que permite mantenerla desconectada de la red y almacenada bajo custodia para lograr un alto nivel de seguridad. En este nivel la AC está encargada del registro de entidades subordinadas y la administración del ciclo de vida de certificados y claves; estas funciones se realizan de manera manual.

Una AC subordinada dentro de la PKI solo podrá expedir certificados de entidad destino; estos certificados estarán vinculados a claves destinadas para el intercambio de claves simétricas con el fin de lograr comunicaciones seguras dentro de una WLAN.

La AR vinculada a una AC subordinada está compuesta por un servidor y personal de la empresa propietaria de la PKI; la identificación dentro del proceso de registro está a cargo del personal de la empresa. La etapa final del registro[1] se realiza en el controlador de dominio.

Cada AC dentro de la jerarquía cuenta con un directorio. En el caso del nivel subordinado, se implementa un directorio o punto de distribución de certificados, CRLs completas y *deltas*, el cual podrá ser accesado vía *Web*.

4.1.1. SOLUCIÓN BASADA EN *WINDOWS 2003 SERVER*

En el año 1997 los servidores basados en *Windows* mantenían el 59 %[2] de aceptación en el mercado mundial; para el año 2005 éstos habían alcanzado el 73 %[3] de aceptación a nivel mundial y hasta el 90 %[4] de preferencia a nivel de PYMES,

---

[1] La interacción con los clientes inalámbricos se configurará en el siguiente capítulo.

[2] Según IDC (*Internacional Data Corporation*). http://www.noticias3d.com/articulo.asp?idarticulo=450&pag=2.

[3] *Yankee Group 2005 North American Linux and Windows TCO Comparison Survey*.

[4] *Costs and Benefits Still Favor Windows Over Linux Among Midsize Businesses*. *Gartner*. 2005.

esto hace que la solución planteada sea aplicable dentro de una gran parte de la población de empresas.

El incremento en el uso de soluciones basadas en servidores *Windows* se debe a que su última versión (*Windows 2003 Server*) maneja mejores características de estabilidad y seguridad que las versiones anteriores de *Microsoft*, manteniendo un ambiente amigable y flexible.

Microsoft se ha enfocado a mejorar las características de seguridad para alcanzar plataformas confiables e interoperables; por este motivo *Windows 2003 Server* soporta todas las herramientas necesarias para la implementación de una PKI jerárquica, presentando ventajas al disponer de documentación en varios idiomas, soporte para actualizaciones y mantenimiento, etc.

4.1.1.1. Características de *Certificate Server*

Certificate Server está diseñado para la implementación de PKIs empresariales o independientes, proporcionando servicios de emisión y administración de certificados digitales seguros. A continuación se presenta una lista con las características soportadas por *Certificate Server*:

- Soporta todas las características y estándares de encripción asimétrica.
- Soporta los protocolos S/MIME, SSL, TLS, IPsec, EAP-TLS, PEAP, etc.
- Posee el sistema EFS[1] para el cifrado y descifrado de archivos.
- Maneja autenticación con certificados digitales en:
    - Inicio de sesión de usuarios en ambientes integrados con tarjetas inteligentes y *tokens*.
    - Sitios *Web* y correos seguros.

[1] *Encrypted File System*.

  - Redes inalámbricas con autenticación del lado del servidor o autenticación mutua entre cliente/servidor.
- Provee mecanismos para la administración de certificados, ésta se puede realizar a través de la consola MMC (*Microsoft Management Console*).
- Soporta para la emisión de certificados.
- Soporta inscripción automática de certificados.
- *Certificate Server* puede trabajar con IIS[1] para la inscripción de usuarios vía *Web*.
- No requiere de la implementación de un controlador de dominio (*Active Directory*); sin embargo, al trabajar conjuntamente con éste permite la distribución de certificados de confianza de forma transparente y la implantación de directivas de forma centralizada.
- Soporta diferentes tipos de entidades emisoras de certificados, permitiendo la inclusión de varias ACs dentro de una PKI.

4.1.1.2. Tipos de ACs para *Windows 2003 Server*

Windows 2003 Server soporta dos tipos de AC: ACs tipo empresarial y ACs independientes.

a. ACs de Empresa

Las ACs de empresa pueden emitir certificados dentro de ambientes que manejen *Active Directory*, esto le permite a la AC utilizar la directiva de grupo para distribuir su certificado a todos los usuarios y equipos que integran el dominio; además, pueden utilizar plantillas para la emisión de certificados digitales de acuerdo al perfil de usuario almacenado en *Active Directory*.

Los certificados digitales y CRLs emitidos por una AC de empresa son publicados en *Active Directory*, esta función se realiza de forma automática dentro del dominio en el

[1] *Internet Information Server*.

que se encuentra el servidor; si se desea publicar certificados o CRLs en otro dominio se debe expedir permisos especiales al servidor.

Para formar una PKI jerárquica empresarial, *Certificate Server* tiene definidos los siguientes roles:

- **AC-Raíz**.- Este tipo de AC forma parte del nivel superior de la jerarquía; para que ésta pueda emitir certificados requiere la configuración previa de *Active Directory*. La AC-Raíz firma su propio certificado y lo publica como ancla de confianza dentro del dominio.

- **AC-Subordinada**.- Cuando se ha instalado la AC-Raíz, ésta puede emitir certificados para ACs de jerarquía menor dentro del dominio, las ACs subordinadas pueden emitir a su vez certificados para otras entidades.

b. ACs Independientes

Una AC independiente funciona de manera autónoma, lo cual le permite emitir certificados para entidades que no forman parte de la empresa propietaria de la AC; el proceso de registro requiere que el usuario proporcione toda la información, debido a que no se cuenta con la base de datos almacenada en *Active Directory*.

Este tipo de AC no utiliza plantillas; cuando un usuario solicita un certificado, éste queda como pendiente hasta que el administrador de la AC verifique las condiciones bajo las cuales debe expedirse el certificado. Las ACs independientes pueden realizar los mismos roles que las ACs de empresa.

4.1.1.3. Roles para Administradores de PKI en Windows 2003 Server

Windows 2003 Server permite definir para entornos PKI diferentes tipos de perfiles para la administración, de acuerdo a las tareas que se requiera delegar a un

miembro del grupo de administradores con respecto a una AC de la PKI; esto permite establecer ACs por región o área y restringir las tareas administrativas y de configuración.

De acuerdo a los requerimientos de seguridad en la administración de PKI se puede definir los siguientes roles para la administración:

- **Administrador de AC**.- Responsable de la configuración de los servidores de certificados y registro; tiene potestad sobre la administración de certificados.

- **Oficial de AC**.- Responsable de la administración de certificados, esto incluye todos los procesos dentro del ciclo de vida de certificados y claves; cuando se maneja almacenes de claves. Encargado del proceso de recuperación de claves.

4.1.2. SOLUCIÓN BASADA EN *LINUX*

Linux está basado en licencias GPL[1] (*General Public Licence*), éstas fueron creadas por la *Free Software Foundation*.

Esta mejora permanente del código fuente por una comunidad compuesta por un gran número de programadores, ha logrado que varias herramientas provistas por *Linux* sean superiores a las entregadas por *Microsoft*, esto incluye todo lo referente a administración de tráfico IP, implementación de *firewalls*, restricción de ancho de banda, implementación de servidores *proxy*, etc.

---

[1] Una licencia GPL permite distribuir copias de software con su código fuente, pudiendo ser utilizado y modificado con la condición de que todas las modificaciones y mejoras realizadas sean distribuidas nuevamente para toda la comunidad.

Sin embargo, debido a que cada integrante de la comunidad realiza sus modificaciones o nuevas implementaciones de acuerdo a sus requerimientos e intereses, hasta el momento no se cuenta con una base especializada para la implementación de una PKI jerárquica dentro de la plataforma *Linux*.

En la documentación oficial de *Red Hat* [1], en el apéndice B del manual de personalización se encuentra una guía para la implementación de GPG (*GNU* [2] *Privacy Guard*), la versión de código abierto de PGP.

Por otra parte dentro de las guías oficiales *HowTo* de *Linux*, se puede obtener información para la implementación de un sistema basado en SSL; sin embargo, a pesar de que en el índice se muestran las opciones de generar ACs raíces y subordinadas, la guía no está terminada[3].

La fundación *SourceForge* ofrece una solución independiente del sistema operativo para la generación de ACs. La EJBCA[4] utiliza como ambiente de desarrollo J2EE[5]; este paquete soporta características que permiten la implementación de una PKI jerárquica, sin embargo, no forma parte del sistema operativo como *Certificate Server* en *Windows*.

Por lo expuesto anteriormente, *Linux* por si solo no presenta las facilidades para la implementación de una PKI jerárquica; sin embargo, tiene la capacidad de crear arquitecturas planas y administrar certificados de manera segura y confiable. Por otra parte, está abierta la posibilidad de la creación de nuevos proyectos que integren al sistema operativo la implementación de otro tipo de arquitectura PKI.

---

[1] *Red Hat* conserva el 45 % de preferencia en comparación con otras distribuciones *Linux*. *Yankee Group*.

[2] *GNU's not UNIX*.

[3] *Certificate Management*. http://howtos.linux.com/howtos/SSL-Certificates-HOWTO/c118.shtml.

[4] *Enterprise JavaBeans Certificate Authority*. http://ejbca.sourceforge.net/.

[5] *Java 2 Platform, Enterprise Edition*.

4.1.3. COMPARACIÓN ENTRE LA SOLUCIÓN BASADA EN *WINDOWS 2003 SERVER* FRENTE A LA SOLUCIÓN BASADA EN *LINUX*, VENTAJAS Y DESVENTAJAS

Existe una gran discusión a nivel mundial sobre las ventajas y desventajas que cada sistema operativo presenta frente a otros, está discusión se ha dividido en dos frentes, por un lado los sistemas propietarios encabezados por *Windows* y por otro los sistemas basados en *software* libre como es el caso de *Linux*.

En esta sección no se realiza una comparación del entorno total de cada sistema operativo, sino más bien del soporte que cada uno presenta para la implementación de una PKI; los puntos considerados se exponen en orden de prioridad para el aseguramiento de la infraestructura.

Además, se debe considerar que el éxito de una infraestructura PKI no depende solamente de la plataforma seleccionada, ésta es solo una parte de la solución; adicionalmente, se debe brindar una capacitación adecuada a los usuarios finales[1], crear CPs y CPSs apropiadas, verificar su cumplimiento y actualizarlas cuando sea necesario.

4.1.3.1. Alcance de la Solución

La plataforma *Windows 2003 Server* presenta un paquete especializado en modo gráfico para la implementación de PKI, éste permite crear PKIs con arquitectura plana o jerárquica de manera segura y eficiente; las PKIs pueden formar parte de un dominio o trabajar en forma autónoma lo que brinda flexibilidad para el diseño.

[1] Entidades destino o entidades confiantes.

Para la expedición de certificados cruzados con organizaciones fuera del dominio, *Windows* presenta un mecanismo que permite emitir certificados cruzados de forma manual o mediante la selección de nuevas plantillas.

Debido a que la implementación planteada requiere de la creación de una jerarquía de ACs dentro de una organización, la solución presentada por *Windows* resulta apropiada, pues contiene herramientas que permiten la generación de ACs raíces y subordinadas, establece mecanismos para la administración de certificados y CRLs; además, admite la distribución de certificados de confianza a través de *Active Directory* de manera transparente para los usuarios dentro del dominio.

En el caso de *Linux*, éste presenta una solución limitada al modo de consola; por el momento soporta arquitecturas planas que trabajan con protocolos como SSL, S/MIME, GPG, IPsec, etc. La generación de arquitecturas jerárquicas no está definida dentro de la documentación oficial.

A pesar de que *Linux* permite la adición de nuevas herramientas generadas de acuerdo a los requerimientos específicos de una organización, esto implica la contratación de personal con amplia experiencia y no asegura un funcionamiento óptimo para una PKI jerárquica.

4.1.3.2. Interoperabilidad

Microsoft implementa dentro de sus aplicaciones el soporte de estándares abiertos; sin embargo, introduce en forma paralela sus estándares propietarios, éstos trabajan mejor dentro de un entorno *Windows* y debido a que este sistema operativo se encuentra mayormente difundido, muchos fabricantes producen *software* y *hardware* basándose en los esquemas propietarios de *Windows* y no en estándares abiertos.

En el caso de *Linux* empresas como IBM y HP[1] han invertido en su mejora continua para lograr un mayor soporte de estándares para diversas aplicaciones; *Linux* no está limitado a restricciones de propiedad intelectual, por este motivo no implementa los estándares propietarios de *Microsoft*.

Actualmente existe una falta de interoperabilidad entre las dos plataformas debido a los estándares propietarios o la falta de cumplimiento de los estándares abiertos; pero, la necesidad de interconectar sistemas basados en diversas plataformas, ha motivado a *Microsoft* a cambiar su estrategia y crear un laboratorio en el que se prueba constantemente la compatibilidad entre el *software* libre y sus productos.

Para entornos PKI, los dos sistemas soportan estándares abiertos; sin embargo, *Microsoft* ofrece una plataforma con mayores capacidades, *Windows 2003 Server* ha sido valorado internacionalmente. La FBCA[2] después de rigurosas pruebas de seguridad, compatibilidad e interoperabilidad, certificó en el 2004 a *Windows 2003 Server* como una plataforma PKI confiable para todas las Agencias Federales de los Estados Unidos[3], *Linux* no cuenta con esta certificación.

4.1.3.3. Nivel de Seguridad

Esta sección hace referencia a la seguridad presentada por cada sistema operativo para la implementación de PKI; a continuación se trata algunos aspectos importantes para lograr el aseguramiento de una infraestructura.

- **Vulnerabilidades por Instalación**.- La instalación inicial de *Windows 2003 Server* provee los servicios mínimos; es el administrador el encargado de activar los servicios requeridos por su organización. Por parte de *Linux*, cada

[1] *Hewlett-Packard*.

[2] *Federal Bridge Certification Authority*.

[3] Hasta el momento existen 5 plataformas aprobadas. http://www.cio.gov/fbca/techio.htm.

paquete instalado es seleccionado por el administrador durante el proceso de instalación y es necesario activarlos luego para su funcionamiento.

Entonces, bajo las dos plataformas para evitar servicios habilitados innecesariamente, es obligatoria una planificación adecuada por parte del departamento de IT[1] de cada organización, las fallas ocurridas bajo este contexto no corresponden a defectos en las plataformas sino a un mal manejo de éstas.

- **Herramientas**.- *Linux* contiene paquetes para la implementación de *firewalls* y otras herramientas para la administración de una red, *Windows* requiere de un paquete adicional para implementar estos servicios (ISA[2]). Estas herramientas forman parte de un entorno general dentro de la política de seguridad de una empresa y deben funcionar de manera paralela a la PKI para asegurar su operación.

- **Alertas por vulnerabilidades**.- En el año 2002 *Windows* presentó el 44 %[3] de las vulnerabilidades localizadas, frente a un 29 % de *Linux*; por otra parte, el promedio de solución ante una vulnerabilidad de *Windows* es de 25 días[4] en comparación con los 31.1 días[5] presentados por *Linux*. El grupo *GNU/Linux* aclara que las vulnerabilidades críticas son resueltas en un promedio de 13,5 días.

  Un análisis realizado por el *Yankee Group* en 2005, muestra que los usuarios perciben que *Linux* entrega mejores niveles de seguridad en diferentes

---

[1] *Information Technology*.

[2] *Internet Security and Acceleration*.

[3] http://www.macuarium.com/macuarium/actual/noticias/2002_11_03_solidasanosx.shtml.

[4] *Forrester*.

[5] http://www.debian.org/News/2004/20040406.es.html.

entornos como se muestra en la figura 4.2.; por otro lado, reconocen que *Windows* es un 30 % más rápido para recuperarse después de un ataque exitoso como se muestra en la figura 4.3.

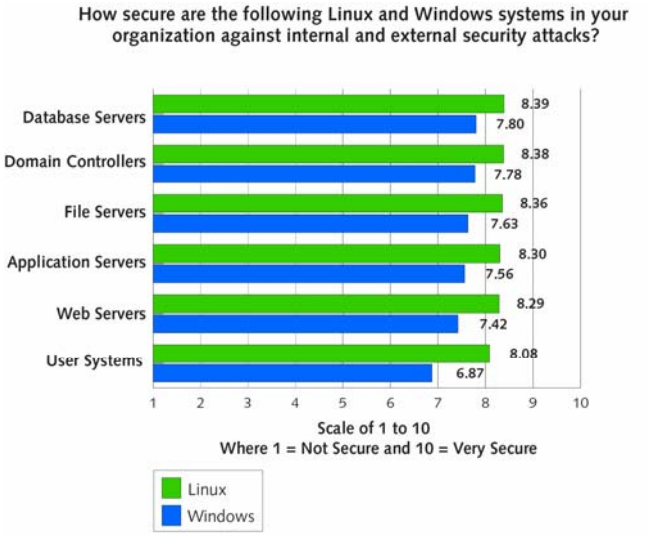

Figura 4.2 Comparación entre Windows y Linux: niveles de seguridad proporcionados[1]

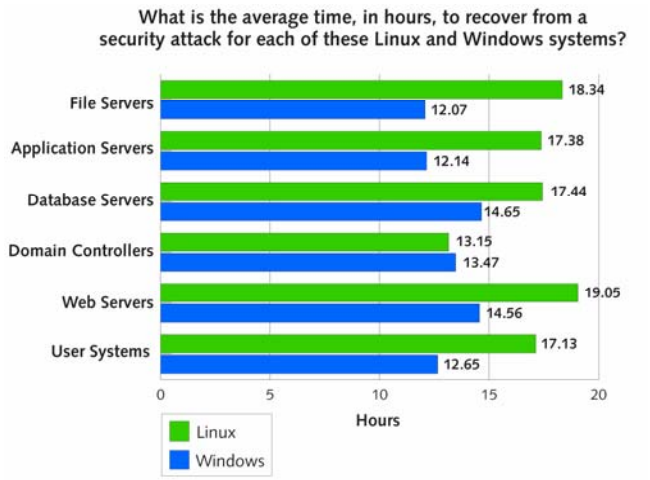

Figura 4.3 Comparación entre Windows y Linux: tiempo consumido en recuperarse después de un ataque exitoso[1]

[1] *Yankee Group 2005 North American Linux and Windows TCO Comparison Survey*.

- **Ataques recibidos**.- *Windows* recibió[1] en el 2002 el 47 % de los ataques mientras que *Linux* alcanzó el 36 %; en este punto se debe considerar que *Windows* posee una base instalada superior a la de *Linux*, por este motivo los atacantes se enfocan en hallar sus vulnerabilidades y exponerlas.

4.1.3.4. Estabilidad y Soporte de Actualizaciones

Windows 2003 Server está diseñado para trabajar con DLLs[2], éstas ejecutan acciones y rutinas que pueden ser invocadas por varios programas, por lo que en algunos casos la actualización de una DLL produce conflictos entre sus diferentes usuarios; sin embargo, para proteger las DLLs del sistema, *Windows* ha implementado en sus últimas versiones WFP[3].

WFP protege todos los archivos de sistema, como por ejemplo archivos con extensiones: .dll, .exe, .ocx y .sys, permitiendo su actualización en los siguientes casos:

- Instalación de SP (*Service Packs*) y *Hotfix*.
- Actualizaciones del sistema operativo con *Winnt32.exe*.
- Actualizaciones con *Windows Update*.

Si un programa reemplaza un archivo protegido, WFP utiliza el mecanismo *self-healing*, el cual restaura el archivo alterado a su versión original; si el sistema no tiene almacenados los archivos, WFP solicita el disco de instalación del sistema operativo. La protección de estos archivos evita conflictos críticos entre aplicaciones y el sistema operativo.

---

[1] Consultora británica de riesgos tecnológicos mi2g Ltd. http://www.mi2g.co.uk/cgi/mi2g/frameset.php?pageid=http%3A//www.mi2g.co.uk/cgi/mi2g/press/140802.php.

[2] *Dynamic Linking Library*.

[3] *Windows File Protection*.

Windows implementa además un sistema de fuentes de confianza, este mecanismo verifica si un controlador de *hardware* o una aplicación en particular es compatible con el sistema; de no ser así, presenta una advertencia que indica la condición del *software*, a partir de este momento la decisión de continuar con la instalación es responsabilidad del administrador[1].

En el caso de *Linux* las actualizaciones del sistema operativo o las instalaciones de *software* se realizan a partir de paquetes en código fuente o ya compilados; en general, se utilizan los paquetes conocidos como RPMs (*RPM Package Manager*).

Los RPMs están desarrollados bajo el formato establecido por la *Linux Standard Base*, esto les permite instalar, actualizar y desinstalar programas en diferentes distribuciones de *Linux*; para ejecutar un RPM u otro paquete, el usuario debe estar autenticado como *root* ante el sistema, esto protege al sistema contra instalaciones perjudiciales o innecesarias.

Las instalaciones de RPMs presentan en algunos casos problemas de dependencias; es decir, un paquete requiere que otro paquete sea instalado previamente para su ejecución. Estas dependencias entre paquetes generan inconvenientes debido a que un paquete puede estar desactualizado y por lo tanto no se encuentra disponible.

Por otra parte, se requiere que el Administrador maneje un nivel adecuado de conocimiento del sistema y sus dependencias, pues una instalación puede afectar a todo el sistema, ocasionando un daño irreparable.

Las dos plataformas contemplan sistemas de protección para asegurar la disponibilidad de operación: *Windows* a través de WFP y *Linux* a través de la estandarización de RPMs.

---

[1] Solo un usuario con perfil de Administrador puede instalar nuevos componentes.

En el caso de actualizaciones o parches de seguridad, *Windows* y *Linux* proporcionan a sus usuarios actualizaciones sin garantía de uso; por lo tanto, es responsabilidad del Administrador verificar los posibles efectos de éstas antes de instalarlas.

4.1.3.5. Costo

La inversión requerida para la implementación de una plataforma PKI no está atada a la compra de licencias, se debe considerar adicionalmente el costo del soporte técnico, capacitación del personal, mantenimiento, etc. En la figura 4.4 se muestra la comparación del costo entre una implementación basada en *Windows 2003 Server* y una basada en *Red Hat Enterprise Linux*.

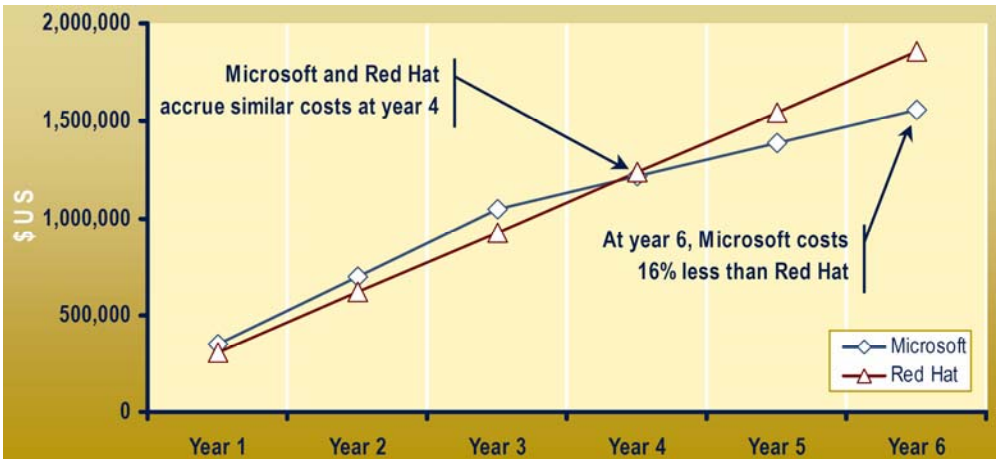

Figura 4.4 Comparación entre y Linux: costo por adquisición y soporte [1]

Los resultados mostrados en la figura 4.4 están basados en el siguiente ambiente: 500 licencias *Windows 2003 Server Enterprise* con 5000 CALs [2] (*Client Access*

---

[1] *IDEAS Custom Consulting Services*. *MICROSOFT WINDOWS SERVER VS. RED HAT ENTERPRISE LINUX*.

[2] Son licencias que proporcionan a los usuarios el derecho de acceder a los servicios de un servidor *Windows*, una CAL es requerida por cada usuario o dispositivo que use el *software* del servidor.

License) en comparación con una solución con 500 licencias *Red Hat Enterprise Linux*; en los dos casos se cuenta con un soporte de 24x7 en el 10 % de los servidores, el soporte es brindado por *Microsoft* o *Red Hat*, respectivamente.

Como se puede ver en la figura 4.4, *Windows* requiere de una inversión mayor hasta el cuarto año, a partir de este año, la solución basada en *Linux* requiere de mayor inversión[1].

El período de validez del certificado (servidor de certificación) de una AC-Raíz es generalmente superior a 10 años; en el caso de ACs subordinadas, éste puede encontrarse entre 1 y 10 años, por lo que en el caso de las ACs subordinadas la decisión puede enfocarse adicionalmente en otros aspectos.

Sin embargo, la solución planteada por *Microsoft* resulta más conveniente para una AC-Raíz, considerando su período de validez; en este punto se debe considerar también que la necesidad de actualización de un sistema operativo en el caso de PKI se puede presentar por la presencia de nuevos y mejores estándares criptográficos.

4.1.3.6. Disponibilidad de Información

Linux proporciona a sus usuarios información a través de sus guías *HowTo*[2], también dispone de manuales [3] para sus diferentes distribuciones; la documentación disponible varía de acuerdo al número de desarrolladores involucrados en cada proyecto. Los proyectos grandes entregan su propia documentación; adicionalmente, existen varios foros que ayudan a solventar problemas.

---

[1] Si bien es cierto que las licencias *Linux* son gratuitas, el soporte técnico anual estándar tiene un costo de 1499 dólares y el soporte *premiun* tiene un costo de 2499 $ (sin impuestos); estos costos generalmente están unificados para todos los distribuidores de soporte de *Linux*.

[2] http://howtos.linux.com/ **o** http://www.tldp.org/.

[3] http://www.europe.redhat.com/documentation/.

Microsoft por su parte, ha desarrollado el sitio *Web Windows Update*, éste proporciona enlaces a: boletines de seguridad, información sobre actualizaciones y descargas, etc.; por otra parte mantiene información del funcionamiento de sus productos en diferentes idiomas[1] en su biblioteca virtual *Microsoft TechNet*[2]. La base disponible de documentación de *Microsoft* es más extensa y diversa que la de *Linux*.

4.1.3.7. Facilidad de Uso

Linux no posee actualmente un entorno gráfico para la implementación de PKI, todos los procesos deben ser manejados bajo el modo de consola.

Por su parte *Windows* cuenta con un ambiente gráfico para la configuración de funciones básicas de PKI; para funciones especializadas, se debe utilizar MMC en modo de gráfico o de consola. Esto hace que un ambiente PKI bajo *Windows* entregue menores dificultades durante los procesos de configuración y operación.

4.2. PLANEACIÓN DE LA PKI JERÁRQUICA

4.2.1. PLANEACIÓN

Durante de la etapa de planeación de una PKI se debe tener en cuenta aspectos como: directrices de la empresa, arquitectura de la PKI, impacto en los usuarios, administración, contenido de los certificados, modelos de confianza y aspectos jurídicos.

---

[1] Las actualizaciones se emiten inicialmente en idioma inglés.

[2] http://technet.microsoft.com/en-us/default.aspx.

4.2.1.1. Directrices de la Empresa

Para adaptar la solución planteada a un ambiente real, se enfoca la implementación de la PKI en un entorno empresarial; para lograr esto, se toma como modelo la empresa ficticia ACSW (Autoridades Certificadoras *Wireless*). En la tabla 4.1 se presenta un perfil general de la empresa ACSW.

Perfil General de la Empresa ACSW[1]	
Característica	**Descripción**
Directrices	La empresa ACSW está dedicada a la investigación y desarrollo de nuevos productos. La información transmitida a través de sus redes está relacionada con datos de clientes y socios, estrategias comerciales, propiedad intelectual de carácter industrial y hasta patentes.
Valor de la Información	Sobre el 20% del capital total de la Empresa.
Usuarios WLAN que manejan información crítica.	Sobre el 20% del total de usuarios.
Servicios de Seguridad requeridos	Comunicaciones seguras a través de la WLAN.
Número de Sucursales	Mínimo 2.

Tabla 4.1 Perfil General de la Empresa ACSW

La inversión requerida para la implementación de un sistema de autenticación con EAP-TLS y una PKI jerárquica es superior a la requerida por otras soluciones; pero en compensación, brinda elevados niveles de seguridad.

En una empresa promedio, el valor de la información es equivalente a un 10 % del capital total[2], por lo tanto, no todas las empresas requieren asumir esta inversión, ésta sólo se justifica en empresas en las cuales el valor de la información es

[1] Los porcentajes asumidos en la tabla 4.2 para el valor de la información y usuarios WLAN que manejan información crítica, son sólo una referencia, éstos pueden variar de acuerdo a las particularidades de cada organización.

[2] Apuntes de Clase, Generación de Empresas, Ing. Jaime Cadena (Escuela de Ciencias – EPN).

equivalente o superior al 20 % del capital total. Este porcentaje puede disminuir en empresas con un gran número de usuarios.

En el caso de los usuarios WLAN, esta inversión no se justifica para un número limitado de usuarios, por ese motivo se toma como referencia el 20 %; sin embargo, en empresas con requerimientos elevados de seguridad, EAP-TLS brinda las mejores condiciones.

4.2.1.2. Arquitectura

Se escoge la arquitectura jerárquica pues ésta es la adecuada dentro del entorno planteado por los siguientes motivos:

- Manejo centralizado de directivas.
- Mejores condiciones de escalabilidad y administración, ya que se puede crear una AC subordinada por cada sucursal de la empresa; además, el compromiso de una AC subordinada no afecta a todos los usuarios de la PKI.
- Establecimiento claro del dominio de confianza.
- La AR relacionada con cada AC subordinada puede realizar la identificación de las entidades de manera personal.
- La infraestructura puede servir como base para nuevas aplicaciones que requieran de los servicios de PKI.

La PKI jerárquica está compuesta por dos niveles, esto permite crear una AC subordinada por cada sucursal de la empresa y se mantiene a la AC raíz desconectada para mantener niveles elevados de seguridad.

4.2.1.3. Impacto en los Usuarios

Antes de la implementación de una PKI, se deben definir sus alcances y limitaciones de acuerdo a los servicios requeridos; también se debe definir claramente el grupo

de usuarios que harán uso de los servicios. En la tabla 4.2 se presenta un resumen de estos aspectos.

La solución proporcionada no revela la complejidad real de la infraestructura; sin embargo, los usuarios y el personal del Departamento de IT de la empresa deben recibir una preparación que les permita entender y aplicar las CP y CPS, para lograr una interacción adecuada con el nuevo esquema de autenticación.

Impacto sobre los Usuarios	
Asunto	**Descripción**
Alcances de la PKI	La PKI debe funcionar como un proveedor de servicios de certificación para usuarios que utilizarán sus credenciales electrónicas para autenticarse mediante el protocolo EAP-TLS ante la red WLAN de ACSW. A partir de esta solución se garantiza los siguientes servicios: - Privacidad de la Información que se transmite a través de la WLAN. - Integridad de la Información que se transmite a través de la WLAN. - Autenticación de la Información que se transmite a través de la WLAN.
Límites de la PKI	Dentro de esta solución no se establecen mecanismos de seguridad de interconectividad de redes extremo a extremo. La solución tampoco está destinada a una aplicación específica, si no más bien al aseguramiento de las conexiones de la WLAN.
Usuarios Afectados	La implementación afectará a todo usuario que requiera intercambiar información por medios inalámbricos a través de la red LAN de ACSW.

Tabla 4.2 Impacto sobre los Usuarios

4.2.1.4. Administración

No se permite la administración remota de las ACs, todas las acciones relacionadas con el ciclo de vida de los certificados deben ser realizadas por el administrador en forma directa. La administración de la AC raíz está a cargo del Administrador de IT de la empresa.

En cada sucursal se cuenta con un servidor de certificados, éste debe ser gestionado por el Administrador de AC de la sucursal, debido a que los servicios de certificación están limitados al aseguramiento de la WLAN; los administradores de AC se encargarán de los procesos de administración, auditoría y *backup*.

4.2.1.5. Contenido de los Certificados

Los certificados expedidos respetan el formato X.509v3, los parámetros seleccionados se basan en las especificaciones ETSI SR 002 176 V1.1.1[1], éstos se encuentran registrados en la tabla 4.3.

Parámetros para la Emisión de Certificados		
ID	ETSI SR 002 176 V1.1.1: **002**	
Algoritmo de Firma Digital	RSA	
Parámetros Del Algoritmo (longitud de clave/*MinModLen*[2] = 1020)	**AC-RAÍZ**	4096 *bits*
	AC-SUB	2048 *bits*
	Usuarios	1024 *bits*
Algoritmo de Generación de Clave	rsagen1	
Función *hash*	SHA-1	

Tabla 4.3 Parámetros para la emisión de certificados

Las claves son generadas a partir del módulo RSA provisto por *Windows* para la generación de claves, éste está basado en *software*.

4.2.1.6. Modelos de confianza

Se establece el modelo de confianza jerárquico con dos niveles, por lo tanto la única ancla de confianza es la AC raíz, ésta goza de mayor confianza dentro del entorno PKI de la empresa ACSW. La AC raíz establece relaciones de confianza unidireccionales con sus subordinadas.

4.2.1.7. Aspectos Jurídicos

Debido a que en el Ecuador no se ha acreditado hasta el momento una AC con título habilitante, el funcionamiento de la PKI-ACSW se sustenta en el artículo 28 de la Ley 67, que establece que “Cuando las partes acuerden entre sí la utilización de

---

[1] ETSI: *Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures*.

[2] Longitud mínima de clave = 1020.

determinados tipos de firmas electrónicas y certificados, se reconocerá que ese acuerdo es suficiente en derecho".

Para legalizar el acuerdo entre ACSW y usuarios propietarios de certificados, estos últimos deben firmar un contrato en el que asume la responsabilidad del manejo de su certificado digital. En el Anexo 6 se proporciona un modelo para este contrato, éste puede manejarse de forma independiente al contrato de trabajo o incluirse como un anexo.

4.2.2. PREPARACIÓN DEL ENTORNO

Esta sección contiene los pasos preliminares requeridos para la implementación de la PKI jerárquica.

4.2.2.1. Preparación de los Equipos

a. Direcciones IP

El esquema de direccionamiento IP está resumido en la tabla 4.4.

Elemento	Dirección Asociada
Red	10.99.0.0
Máscara	255.255.0.0
AC-Raíz	10.99.30.1
AC-SUB	10.99.30.250
Usuarios	10.99.30.51/10.99.30.150

Tabla 4.4 Parámetros de Direccionamiento IP

b. Actualización de Servidores

Todos los servidores dentro de la PKI tendrán instalado el sistema operativo *Windows 2003 Server Enterprise* con *Service Pack 1* como se muestra en la figura 4.5; además, deberán tener instalados todos los parches de seguridad proporcionados por *Microsoft*.

Figura 4.5 Windows 2003 Server con Service Pack 1

4.2.2.2. Instalación de Servicios

La red debe contar con un controlador de dominio, éste es un requisito para la implementación de la PKI empresarial y el funcionamiento de EAP-TLS; durante la instalación de *Active Directory* se instalan todos los servicios relacionados con el servidor principal de la empresa.

Para la interacción entre un servidor de certificados y otras entidades dentro de la PKI, se requiere la instalación y configuración de IIS. Finalmente, para los eventos de auditoría de los servidores de certificados se requiere la instalación de las Herramientas de administración y supervisión. Los procedimientos requeridos para la instalación de servicios se encuentran registrados en el Anexo 8.

4.3. INSTALACIÓN Y CONFIGURACIÓN DE LA ENTIDAD RAÍZ

Durante el proceso de implementación de una PKI jerárquica, la configuración de la AC raíz determina el funcionamiento de toda la infraestructura, pues ésta será la encargada de limitar su alcance.

4.3.1. DETERMINACIÓN DEL OID DE LA CPS

Un OID está representado por una secuencia de números que identifica un objeto. Cada CP está ligada a un OID; sin embargo, el OID que se asocia con el certificado digital de la AC es el de la CPS, debido a que éste contiene información más detallada del funcionamiento de la PKI.

Cuando la PKI está diseñada para brindar servicios de certificación a una población universal, se debe adquirir un OID público a través de la IANA[1]. Todos los OIDs asignados por IANA para empresas comienzan con 1.3.6.1.4.1.x, esta secuencia representa: *iso.org.dod.internet.private.enterprise.x*. La *x* se modifica de acuerdo al nombre de la empresa propietaria del OID; por ejemplo 311 identifica a *Microsoft*.

Para PKIs que están diseñadas para brindar servicios de certificación dentro de organizaciones o empresas, se puede asignar OIDs privados. *Windows 2003 Server* tiene asignados tres segmentos dentro del árbol de OIDs de *Microsoft* para la configuración de PKIs empresariales:

- ***Low Assurance***.- Este grupo de identificadores representa certificados que son emitidos con requerimientos básicos de seguridad, este grupo puede utilizar la siguiente secuencia: 1.3.6.1.4.1.311.21.8.a.b.c.d.e.f.1.400[2].

- ***Medium Assurance***.- Este grupo representa certificados que requieren niveles adicionales de seguridad para su generación, este conjunto puede utilizar la siguiente secuencia: 1.3.6.1.4.1.311.21.8.a.b.c.d.e.f.1.401[3].

---

[1] *Internet Assigned Numbers Authority*.

[2] *iso.org.dod.intenet.private.enterprises.microsoft.certsrv.oidenterprisesroot.**a.b.c.d.e.f**.assurance.low*.

[3] *iso.org.dod.intenet.private.enterprises.microsoft.certsrv.oidenterprisesroot.**a.b.c.d.e.f**.assurance.medium*.

- ***High Assurance***.- Este grupo representa certificados que son generados con altos niveles de seguridad, puede utilizar la siguiente secuencia: 1.3.6.1.4.1.311.21.8.a.b.c.d.e.f.1.402[1].

Un OID privado se puede utilizar sólo dentro de su organización, debido a que éste se generará modificando la secuencia *a.b.c.d.e.f* de manera seudo-aleatoria a partir del GUID (*Globally Unique Identifier*) ligado al dominio.

Para obtener un OID privado relacionado con una organización, se da un clic en el **Inicio** de *Windows* y se selecciona **Ejecutar**. En el cuadro de diálogo que se presenta se ingresa el comando *certtmpl.msc*, como se muestra en la figura 4.6; luego se presenta un mensaje que sugiere la instalación de plantillas de certificados y se da un clic en **Aceptar**. *Certtmpl* maneja el grupo de plantillas instaladas en *Windows*.

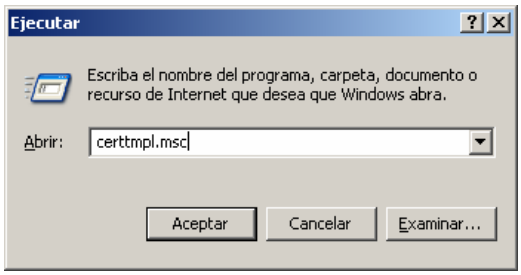

Figura 4.6 Ejecución de certtmpl

Para obtener el OID *High Assurance* relacionado con el dominio ACSW.com, se da un clic con el botón derecho del *mouse* sobre la opción **Plantillas de Certificado** y en el menú emergente se selecciona **Ver identificadores de objeto** como se muestra en la figura 4.7.

En la pantalla que presenta los OIDs disponibles, se selecciona el campo **Seguridad Alta** como se muestra en la figura 4.8; luego, se da un clic en el botón **Copiar**

[1] *iso.org.dod.intenet.private.enterprises.microsoft.certsrv.oidenterprisesroot.**a.b.c.d.e.f**.assurance.high*.

identificador de objetos, como resultado se obtendrá una secuencia semejante a la siguiente: 1.3.6.1.4.1.311.21.8.**2952412.15296278.215479.8911027.4677464.89**.1.402.

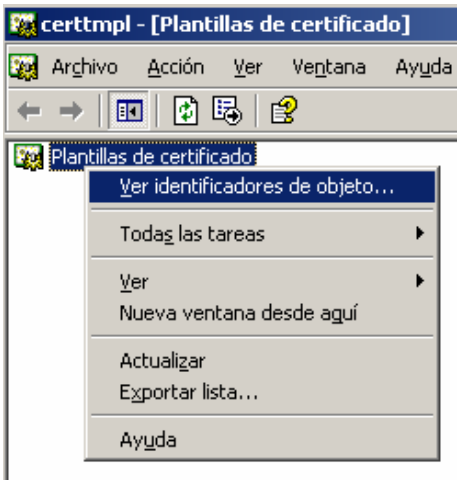

Figura 4.7 Ver OIDs relacionados con el GUID

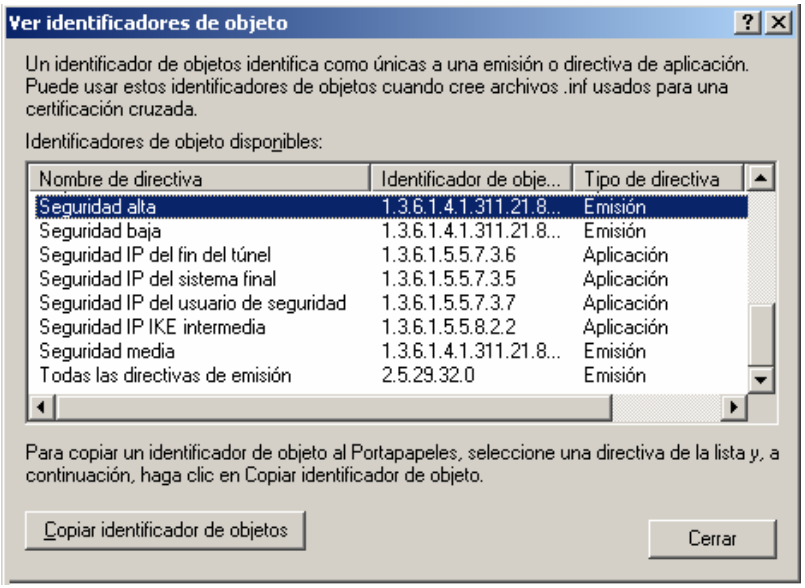

Figura 4.8 Copia de OIDs

El significado de estos OIDs durante la generación de certificados solo es válido dentro del dominio en que se generaron, otro dominio no podrá traducir la secuencia de números a su significado real como se muestra en la figura 4.9.

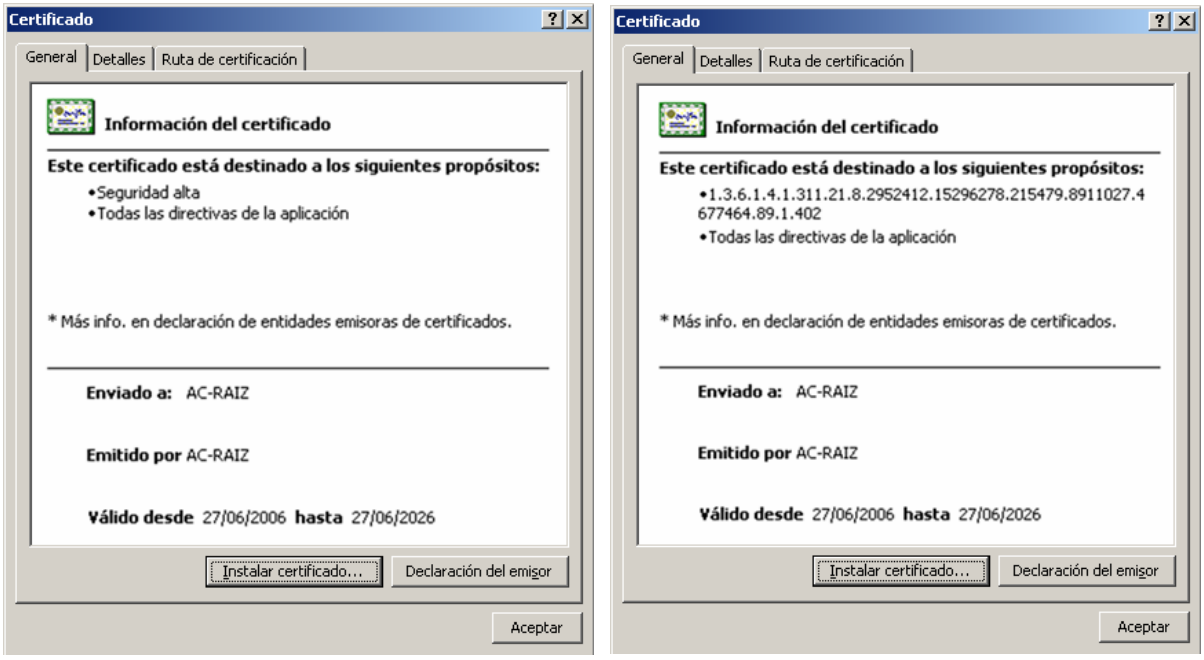

Figura 4.9 Traducción de OIDs

4.3.2. CREACIÓN DE *CAPolicy.inf*

Para modificar los valores registrados por defecto en las plantillas provistas por *Certificate Server*, antes de la instalación de la AC se debe crear el archivo *CAPolicy.inf* y copiarlo en la carpeta *%windir%* del sistema. Dentro de ésta implementación se utilizará el archivo *CAPolicy.inf* para cumplir con los siguientes objetivos:

- Proporcionar información de ACSW en el campo **Declaración del Emisor**.
- Proporcionar acceso a la CDS, CP y certificados de las ACs al seleccionar la opción **Más Información** en la **Declaración del Emisor**.
- Ligar el OIDs de seguridad alta al certificado.
- Restringir la longitud de ruta.
- Determinar los períodos de publicación de las CRLs completas y deltas.

A continuación se presentan los campos utilizados dentro del archivo *CAPolicy.inf*:

- **[*Version*]**.- Indica la versión que se utiliza para crear la *CAPolicy.inf* de ACs raíces o subordinadas; esta sección contiene los siguientes parámetros:

```
[Version]
Signature= "$Windows NT$"
```

- **[*RequestAttributes*]**.- Indica que el archivo contiene información relacionada con la creación de un certificado; esta sección contiene los siguientes parámetros:

```
[RequestAttributes]
```

- **[*PolicyExtension*]**.- Lista las políticas definidas por el usuario (OIDs); esta sección contiene los siguientes parámetros:

```
[PolicyExtension]
```

- **[*PolicyStatementExtension*]**.- Inicia la sección de información de los OIDs de la PKI. Aquí se indica qué OIDs están relacionados con el certificado de la AC; también permite modificar el campo de Declaración del Emisor con el comando *Notice* y agregar un acceso a la CP, CPS, CRLs, etc., mediante un URL[1]. Esta sección contiene los siguientes parámetros:

```
[PolicyStatementExtension]
Policies = HighAssurancePolicy
[HighAssurancePolicy]
OID = 1.3.6.1.4.1.311.21.8.2952412.15296278.215479.8911027.4677464.89.1.402
URL = http://acsw.com/
Notice = "Este certificado está restringido por política de certificación de la ACSW para
seguridad alta, para mayor información se da un clic en el botón Más Información y
accederá al sitio Web de la PKI-ACS."
```

- **[*AuthorityInformationAccess*]**.- Especifica los puntos de acceso de la información de la AC; esta sección contiene los siguientes parámetros:

---

[1] *Uniform Resource Locator*.

```
[AuthorityInformationAccess]
URL="http://acsw.com/
Empty = True
```

- **[*CRLDistributionPoint*]**.- Indica los puntos de distribución de las CRLs, se marca como *Empty* para evitar que en el certificado de la AC-Raíz se muestre información relacionada con el directorio LDAP utilizado por *Active Directory*; esta sección contiene los siguientes parámetros:

```
[CRLDistributionPoint]
Empty = true
Critical = true
```

- **[*BasicConstraintsExtension*]**.- Configura la máxima longitud de ruta; esta sección contiene los siguientes parámetros:

```
[BasicConstraintsExtension]
PathLength = 1
critical = true
```

- **[*certsrv_server*]**.- Utilizado para especificar los períodos de publicación de CRLs completas y deltas; esta sección contiene los siguientes parámetros:

```
[certsrv_server]
CRLPeriodUnits=1
CRLDeltaPeriod=weeks
CRLDeltaPeriodUnits=1
critical = trae
```

- **[*NewRequest*]**.- Utiliza el archivo .inf como un complemento de petición para la plantilla de certificado; esta sección contiene los siguientes parámetros:

```
[NewRequest]
Exportable = True
```

- **[*RequestAttribute*]**.- Usa a *NewRequest* para definir atributos adicionales asociados con la plantilla base para la petición de certificados; esta sección contiene los siguientes parámetros:

  [RequestAttribute]

En resumen, el archivo *CAPolicy.inf* tendrá el siguiente contenido:

```
[Version]
Signature= "$Windows NT$"
[RequestAttributes]

[PolicyExtension]
[PolicyStatementExtension]
Policies = HighAssurancePolicy
[HighAssurancePolicy]
OID = 1.3.6.1.4.1.311.21.8.10102129.11103354.12207488.3169803.4739320.75.1.402
URL = http://acsw.com/
Notice = "Este certificado está restringido por política de certificación de la ACSW para seguridad alta, para mayor información hacer clic en el botón Más Información y accederá al sitio Web de la PKI-ACS."

[AuthorityInformationAccess]
URL="http://acsw.com/
Critical = false

[CRLDistributionPoint]
Empty = true
Critical = true

[BasicConstraintsExtension]
PathLength = 1
critical = true

[certsrv_server]
CRLPeriod=years
CRLPeriodUnits=1
CRLDeltaPeriod=weeks
CRLDeltaPeriodUnits=4
critical = true
```

```
[NewRequest]
Exportable = True
critical = false

[RequestAttribute]
```

4.3.3. INSTALACIÓN DE LA AC-RAÍZ

Primero el equipo que funcionará como servidor de certificados debe agregarse al dominio, cuando éste se ha agregado correctamente se da un clic en el **Inicio** de *Windows* y se selecciona **Panel de control** y luego **Agregar o quitar programas**; en la pantalla que se presenta se da un clic sobre **Agregar o quitar componentes de *Windows***.

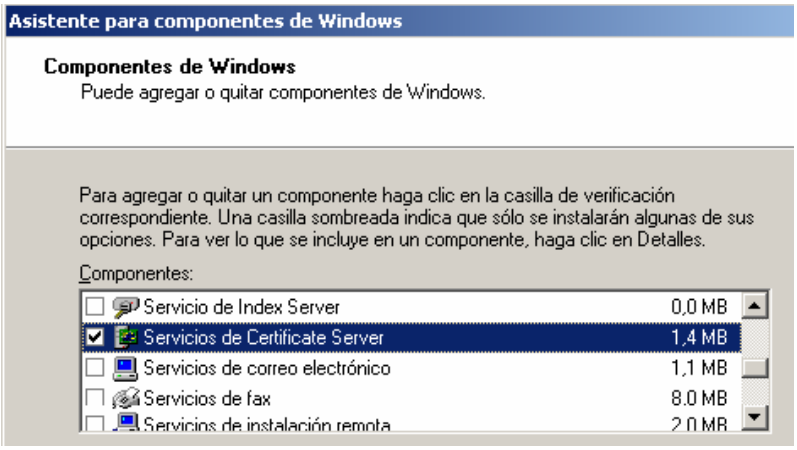

Figura 4.10 Selección de Certificate Server

En el **Asistente para componentes de *Windows*** se selecciona **Servicios de *Certificate Server*** como se muestra en la figura 4.10; ante la advertencia que se presenta indicando que después de la instalación no se podrá cambiar el nombre u otras características del equipo, se da un clic en **Sí** y en el cuadro de diálogo del Asistente se da un clic en **siguiente**.

En la pantalla siguiente se debe seleccionar el tipo de AC, se da un clic en la opción **Entidad emisora raíz de la empresa** y se selecciona **Usar la configuración**

personalizada para generar el par de claves y el certificado de la entidad emisora como se muestra en la figura 4.11, se da un clic en **siguiente**.

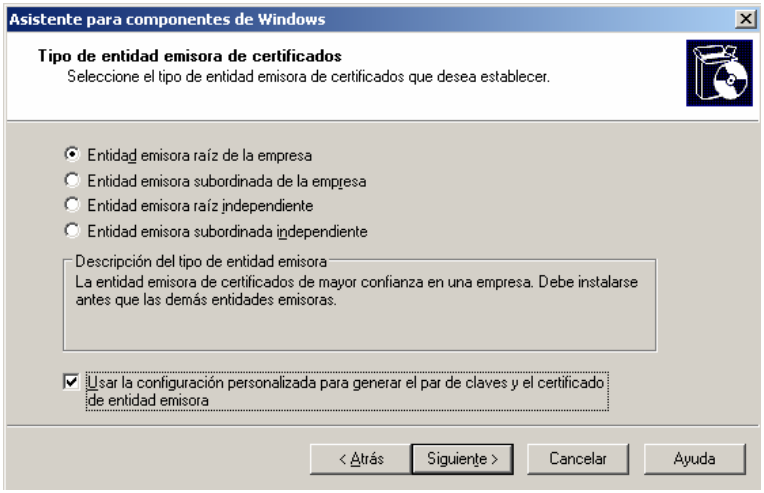

Figura 4.11 Selección del Tipo de AC

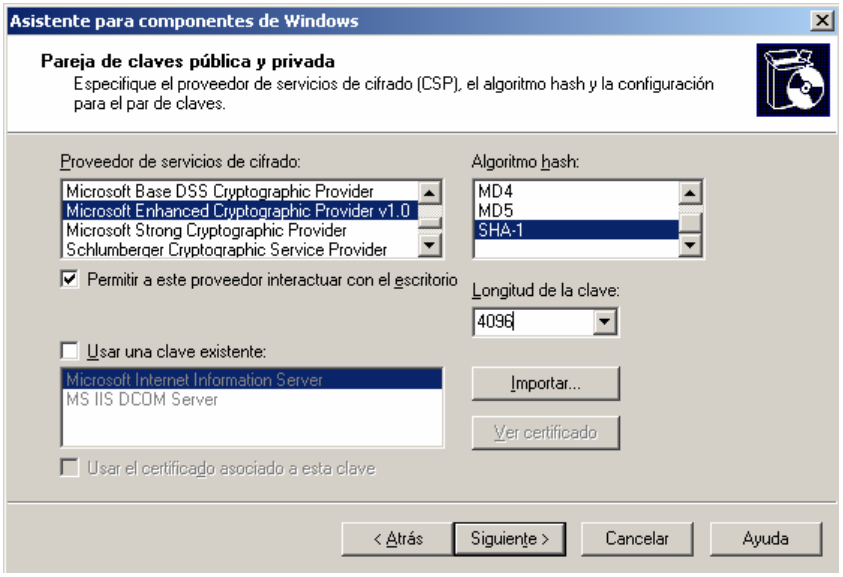

Figura 4.12 Parámetros de Generación de Claves

En la pantalla que se presenta se debe configurar los parámetros para la generación de la pareja de claves, se selecciona como longitud de clave 4096 *bits*; en la sección Proveedor de servicios de cifrado se selecciona ***Microsoft Enhanced Cryptographic Provider v1.0*** y se mantiene SHA-1 como algoritmo *hash*, como se muestra en la figura 4.12.

La pantalla que luego se presenta, se utiliza para configurar los datos de identificación de la AC; se ingresa en el **Nombre común para la entidad emisora de certificados** AC-RAIZ y en el **período de validez** se selecciona 10 años, como se muestra en la figura 4.13.

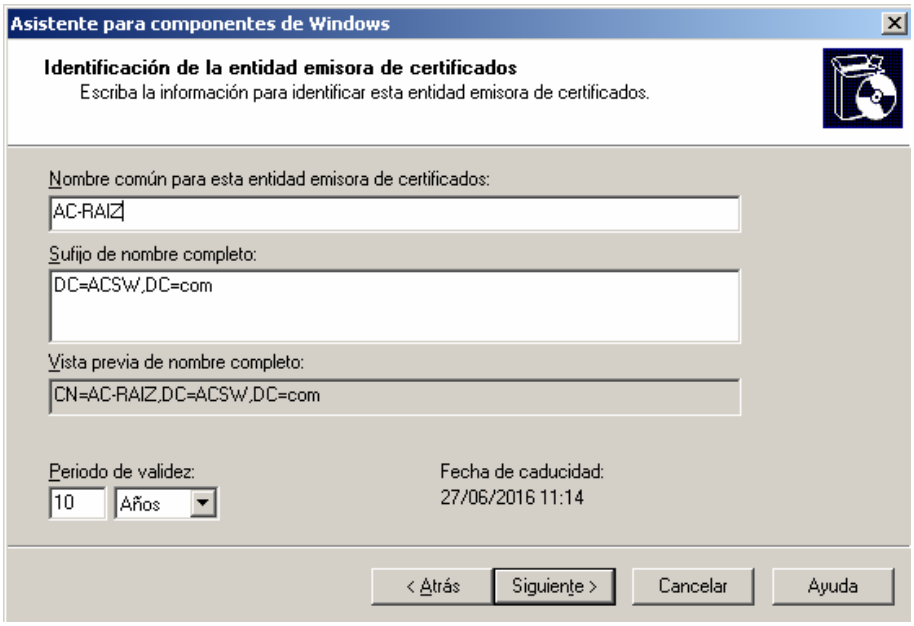

Figura 4.13 Datos de Identificación de AC

Se presenta la pantalla de información de la AC, en ésta se debe configurar la ubicación para la base de datos de los registros de la AC; se mantiene la configuración predeterminada pues ésta ofrece condiciones adecuadas de seguridad, luego se marca la opción **Almacenar la información de configuración en una carpeta compartida** y se da un clic en **Examinar** para proporcionar la ruta a la carpeta *CertRaiz* en la AC subordinada tal como se muestra en la figura 4.14, se da un clic en **siguiente**.

Finalmente se presenta un mensaje que indica que se deben detener los servicios de *Certificate Server* y luego otro mensaje que indica que para activar la inscripción por *Web* se requiere habilitar las páginas de ASP dentro de IIS, se da un clic en **Sí** en los dos mensajes. La instalación ha concluido, se da clic un en **finalizar**.

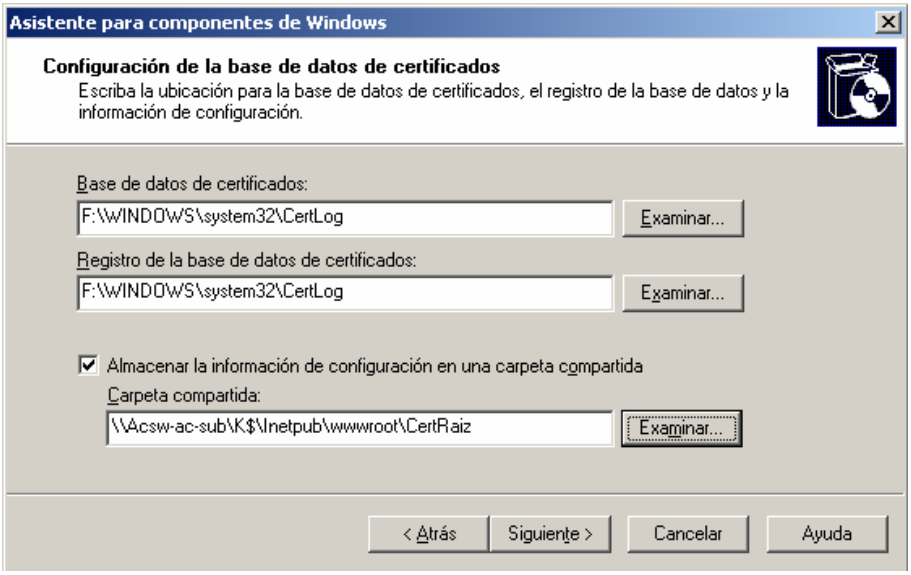

Figura 4.14 Almacén del certificado de la AC-Raíz

4.3.4. CONFIGURACIÓN DE LA AC-RAÍZ

Debido a que todo lo referente a la operación de la AC se incluye en la sección de pruebas de funcionamiento, en esta sección se tratará la configuración para limitar el alcance de la AC dentro de la PKI.

Para ingresar a la AC, se da un clic en el **Inicio** de *Windows* y se selecciona la opción **Herramientas Administrativas** y luego **Entidad emisora de certificados**, luego de lo cual se presenta la pantalla mostrada en la figura 4.15.

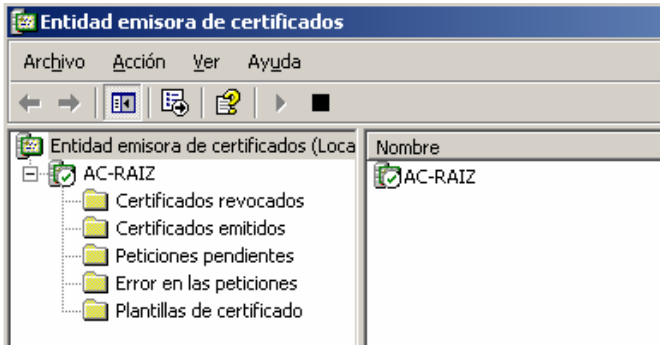

Figura 4.15 Entidad Emisora de Certificados

4.3.4.1. Solicitudes Pendientes

Las solicitudes enviadas por las ACs subordinadas no ingresan de forma automática a la AC-Raíz, debido a que son procesadas de forma manual; pero, si se envía una solicitud de manera automática, por defecto ésta se atiende de inmediato. Para evitar que usuarios ilícitos obtengan certificados emitidos por la AC-Raíz, es mejor marcar todas las peticiones como pendientes en la AC-Raíz.

Para marcar como pendientes las solicitudes se da un clic con el botón derecho del *mouse* sobre la AC-RAIZ y en el menú emergente se selecciona la opción **Propiedades** como se muestra en la figura 4.16.

Figura 4.16 Propiedades de la AC-Raíz

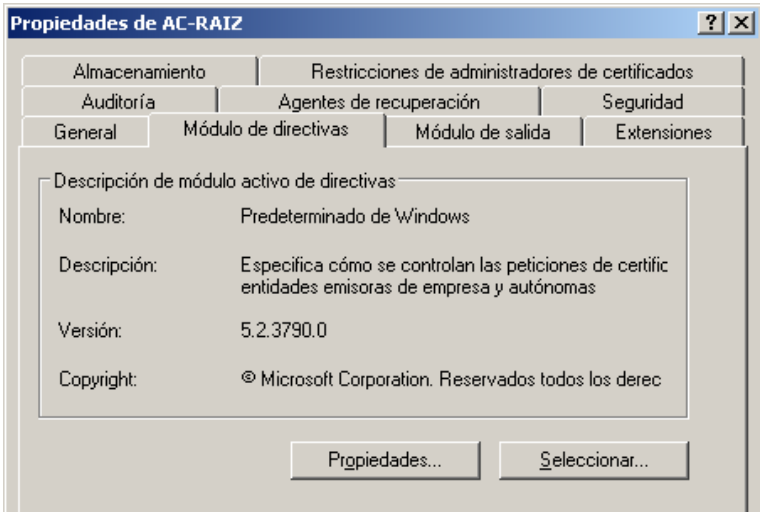

Figura 4.17 Propiedades de la AC-Raíz

En la pantalla de Propiedades se selecciona la pestaña **Módulo de directivas** mostrada en la figura 4.17, luego se da un clic sobre el botón **Propiedades**. En el cuadro de diálogo de **Propiedades** mostrado en la figura 4.18 se selecciona la opción **Establecer el estado de la petición de certificados como pendiente** y se da un clic en **Aceptar**.

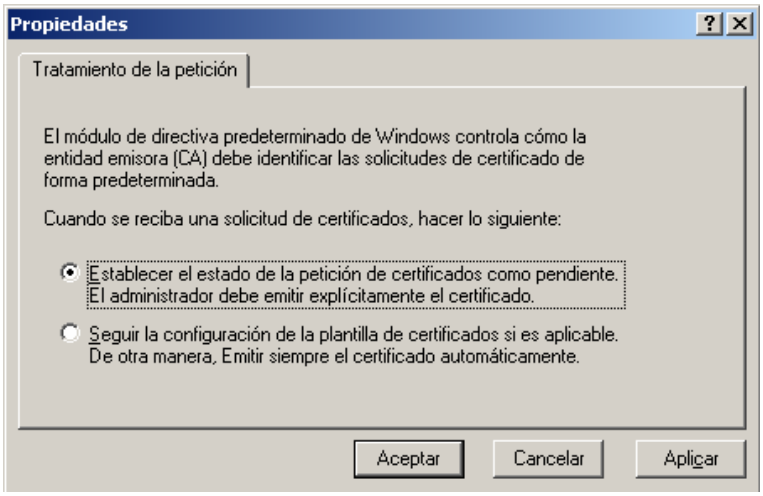

Figura 4.18 Peticiones Pendientes

4.3.4.2. Permisos de Usuarios

A pesar de que la mayor parte del tiempo la AC se encuentre desconectada, ésta debe conectarse a la red bajo ciertos eventos planificados. Por defecto la AC puede recibir y despachar solicitudes de cualquier entidad dentro del dominio, por este motivo se debe restringir la emisión de certificados para usuarios comunes dentro de la red. Para lograr esto se sigue el siguiente procedimiento:

- Se ingresa a las **Propiedades** de la AC-Raíz.
- En el cuadro de diálogo de Propiedades de la AC se selecciona la pestaña **Seguridad** y en la opción **Nombres de grupos o usuarios** se da un clic sobre **Usuarios autentificados**; en la opción **Permisos de usuarios**

autentificados en el campo **Permitir** se desactiva la opción **Solicitar certificados** como se muestra en la figura 4.19.

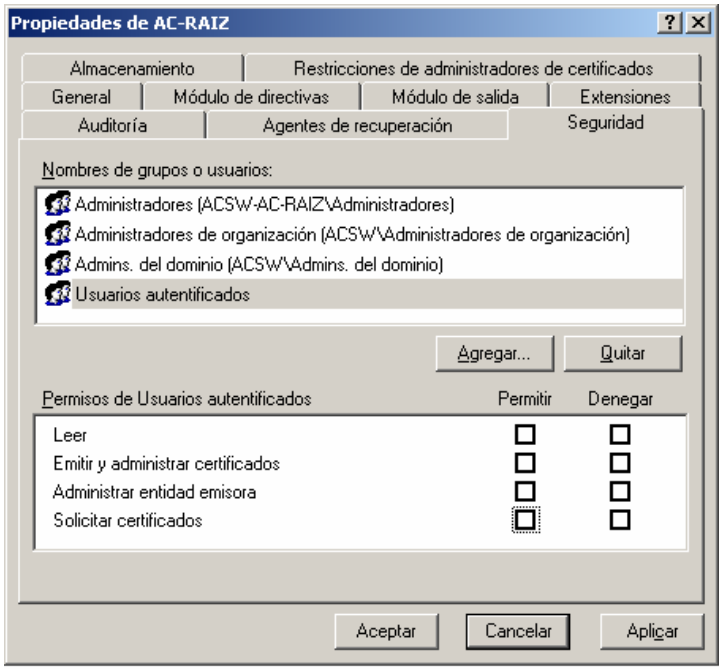

Figura 4.19 Cambio de permisos de emisión para Usuarios

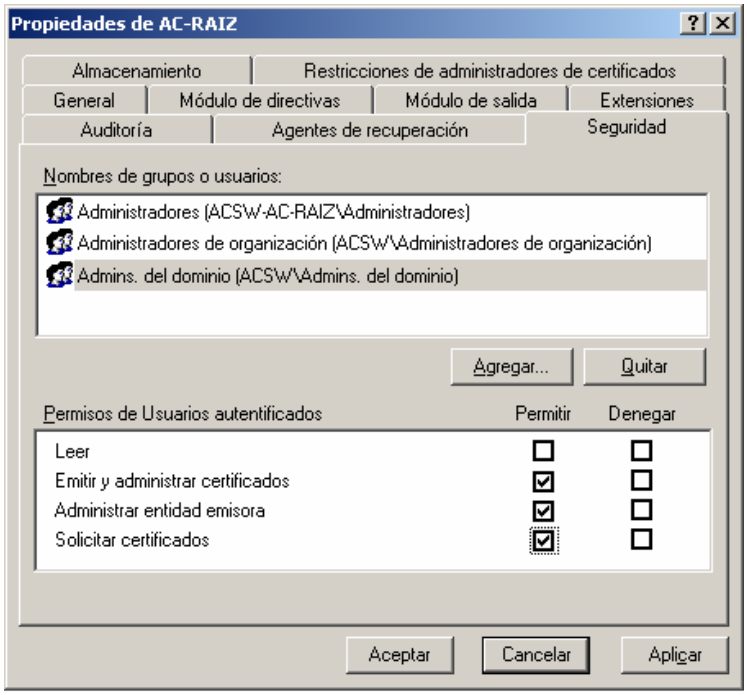

Figura 4.20 Cambio de permisos de emisión para Administradores

- El proceso anterior impedirá la emisión de todos los certificados; para habilitar la emisión de certificados para ACs subordinadas, se selecciona la opción **Admins. del dominio** y en la opción **Permisos de usuarios autentificados**, en el campo **Permitir**, se activa la opción **Solicitar certificados** como se muestra en la figura 4.20.
- Se realiza el procedimiento anterior con el grupo de los **Administradores de organización**.
- En el grupo de **Administradores** se elimina el permiso **Administrar entidad certificadora** y se da un clic en **Aceptar** para guardar todos los cambios, esto limita al grupo de Administradores la emisión de certificados.

Este procedimiento asegura que únicamente los Administradores del Dominio y de la Organización podrán administrar la AC-Raíz y los certificados. La restricción para la emisión de certificados únicamente para entidades subordinadas debe establecerse en la CP de la PKI; sin embargo, por seguridad, esta configuración debe activarse solo cuando se presente un evento planificado para la emisión se certificados de ACs subordinadas.

4.3.4.3. Determinación de Períodos de Publicación de CRLs

Para modificar los períodos de publicación establecidos en *CAPolicy.inf*, se da un clic con el botón derecho del *mouse* sobre la carpeta **Certificados revocados** y en el menú emergente se selecciona **Propiedades** como se muestra en la figura 4.21.

Figura 4.21 Propiedades Certificados revocados

En la pantalla de propiedades se selecciona la pestaña **Parámetros para la publicación de listas de revocación** como se muestra en la figura 4.22, si es necesario se modifica los parámetros de publicación de CRLs completas y delta.

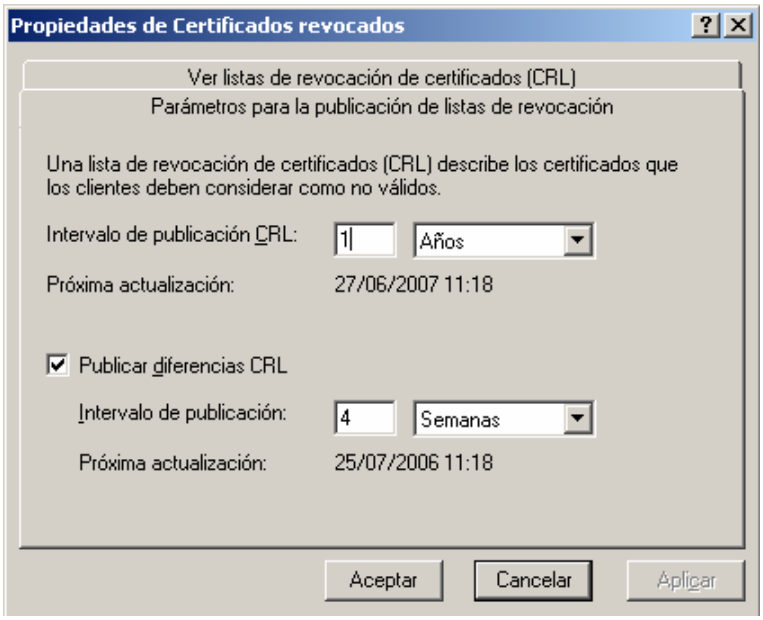

Figura 4.22 Cambio de períodos de Publicación de CRLs

4.3.4.4. Auditorías

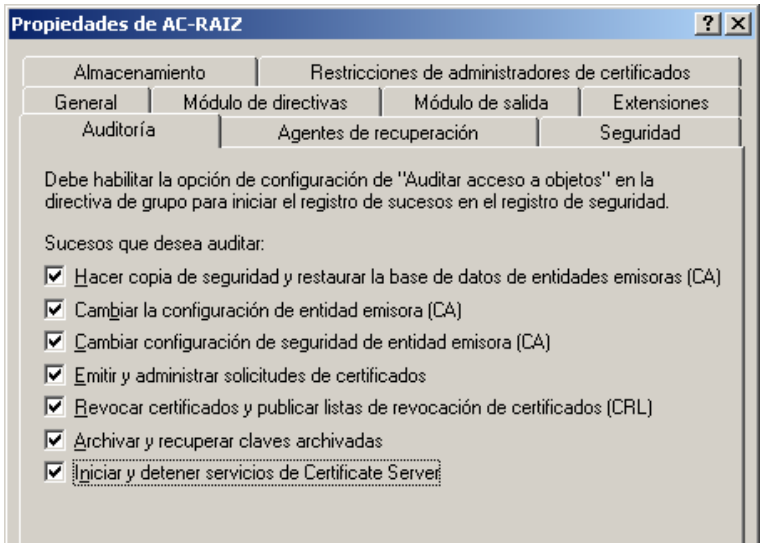

Figura 4.23 Configuración de eventos de Auditoría

Para establecer eventos de auditoría primero de debe activar **Auditar acceso a objetos** en los servidores de certificados como se indicó en la sección de planificación; entonces se ingresa a las propiedades de la AC, se selecciona la pestaña **Auditoría** y se elige los eventos que deben ser auditados como se muestra en la figura 4.23, luego se da un clic en **Aceptar**.

4.4. INSTALACIÓN Y CONFIGURACIÓN DE LA ENTIDAD SUBORDINADA

4.4.1. DETERMINACIÓN DEL OID DE LA CPS

Debido a que la AC-Raíz y las ACs subordinadas pertenecen al mismo dominio y por lo tanto tienen el mismo GUID, se mantiene el siguiente identificador de directiva: 1.3.6.1.4.1.311.21.8.**2952412.15296278.215479.8911027.4677464.89**.1.402

4.4.2. CREACIÓN DE *CAPolicy.inf*

Para modificar los valores registrados por defecto en las plantillas provistas por *Certificate Server*, antes de la instalación de la AC subordinada se debe crear el archivo *CAPolicy.inf* y almacenarlo en la carpeta *%windir%* del sistema. El archivo *CAPolicy.inf* para la creación del certificado de la AC subordinada tiene el siguiente contenido:

```
[Version]
Signature= "$Windows NT$"

[RequestAttributes]

[PolicyExtension]
[PolicyStatementExtension]
```

```
Policies = HighAssurancePolicy
[HighAssurancePolicy]
OID = 1.3.6.1.4.1.311.21.8.15992350.3977518.12537493.2069281.15878667.203.1.402
URL = http://acsw.com/
Notice = "Este certificado está restringido por política de certificación de la ACSW para seguridad alta, para mayor información hacer clic en el botón Más Información y accederá al sitio Web de la PKI-ACS."

[certsrv_server]
CRLPeriod=weeks
CRLPeriodUnits=4
CRLDeltaPeriod=weeks
CRLDeltaPeriodUnits=1
critical = true

[NewRequest]
Exportable = True
critical = false

[RequestAttribute]
```

No se utiliza todos los campos empleados para la creación de *CAPolicy.inf* en la sección relacionada con la AC-Raíz, debido a que la AC subordinada está supeditada a las restricciones impuestas por la AC-Raíz.

Por ejemplo, en el caso del campo *BasicConstraintsExtension* la AC-Raíz establece una longitud de ruta igual a cero para todas las ACs subordinadas; en cambio, en campos como *PolicyExtension*, se permite incluir información específica de la AC relacionada con el certificado.

4.4.3. INSTALACIÓN DE LA AC SUBORDINADA

El equipo que funcionará como servidor de certificados debe agregarse primero al dominio, luego se ingresa al **Asistente para componentes de *Windows*** y se selecciona **Servicios de *Certificate Server***; ante la advertencia que se presenta indicando que después de la instalación no se podrá cambiar el nombre u otras

características del equipo, se da un clic en **Sí** y en el cuadro de diálogo del Asistente se da un clic en **siguiente**.

En la pantalla siguiente se debe seleccionar el tipo de AC, se da un clic en la opción **Entidad emisora subordinada de la empresa** y se selecciona **Usar la configuración personalizada para generar el par de claves y el certificado de la entidad emisora** como se muestra en la figura 4.24, entonces se da un clic en **siguiente**.

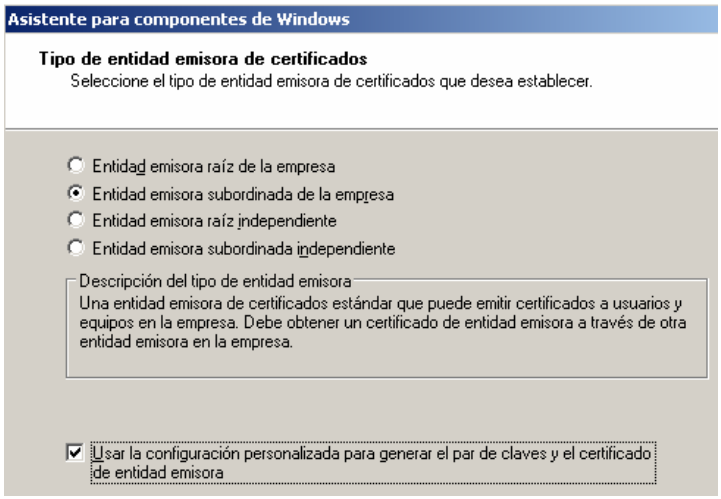

Figura 4.24 Instalación de la AC-SUB

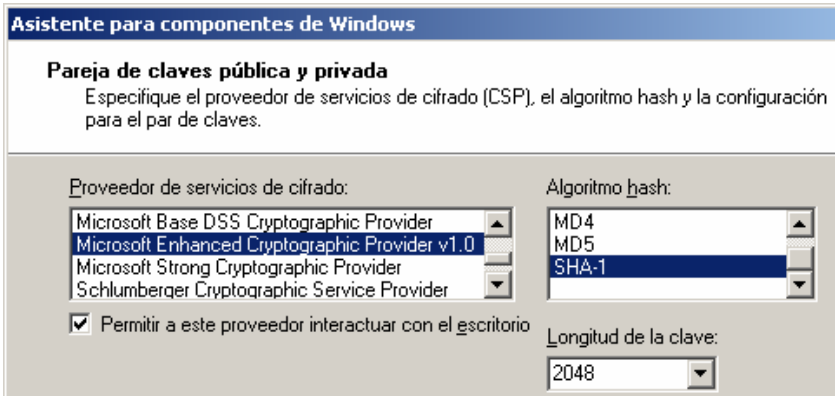

Figura 4.25 Parámetros de Generación de Claves

En la pantalla que se presenta se debe configurar los parámetros para la generación de la pareja de claves, se selecciona como longitud de clave 2048 *bits*. En la sección

Proveedor de servicios de cifrado se selecciona ***Microsoft Enhanced Cryptographic Provider v1.0***, se mantiene SHA-1 como algoritmo *hash*, como se muestra en la figura 4.25.

Se presenta la pantalla mostrada en la figura 4.26, en ésta se ingresa AC-SUB en el **Nombre común para la entidad emisora de certificados**. El **período de validez** está deshabilitado debido a que éste se determina por la AC-Raíz y es igual a 2 años.

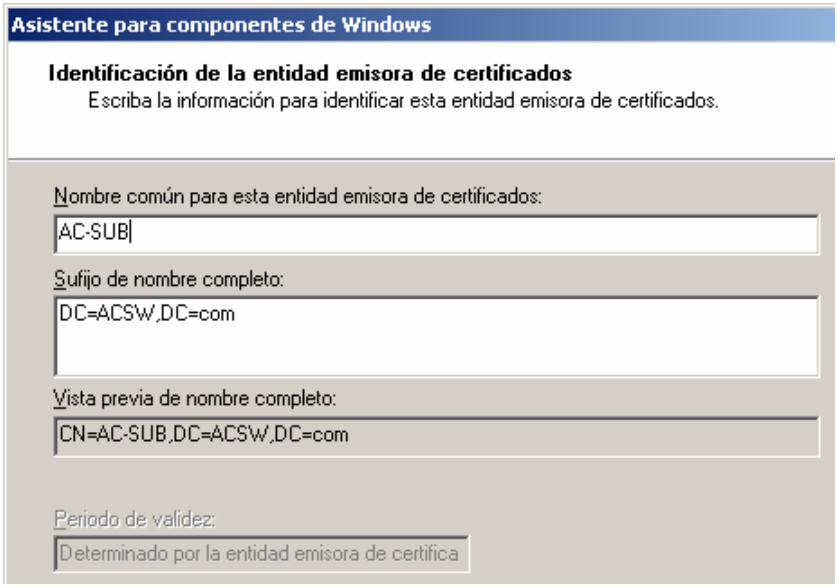

Figura 4.26 Datos de Identificación de AC

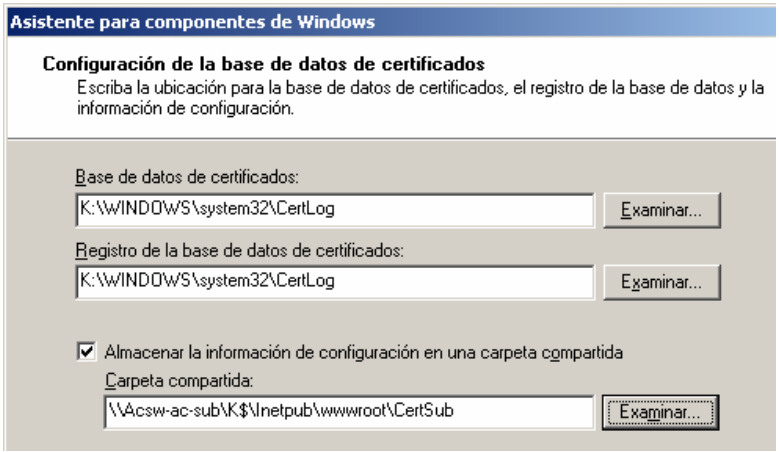

Figura 4.27 Almacén del certificado de la AC subordinada

En la pantalla siguiente se debe configurar la ubicación para la base de datos de los registros de la AC; se mantiene la configuración predeterminada pues ésta ofrece condiciones adecuadas de seguridad. Se marca la opción **Almacenar la información de configuración en una carpeta compartida** y se da un clic en **Examinar** para ingresar la ruta a la carpeta *CertSub* relacionada con IIS como se muestra en la figura 4.27, luego se da un clic en **siguiente**.

Para almacenar la solicitud de certificado se crea una carpeta con nombre *Req* en un directorio adecuado; luego, en la pantalla de solicitud de certificado se selecciona la opción **Guardar la petición en un archivo** y se da un clic en **Examinar** para ubicar la carpeta *Req*, se ingresa un nombre de solicitud; por ejemplo *AC-SUB.req* como se muestra en la figura 4.28. Cuando se ha concluido se da un clic en **siguiente**.

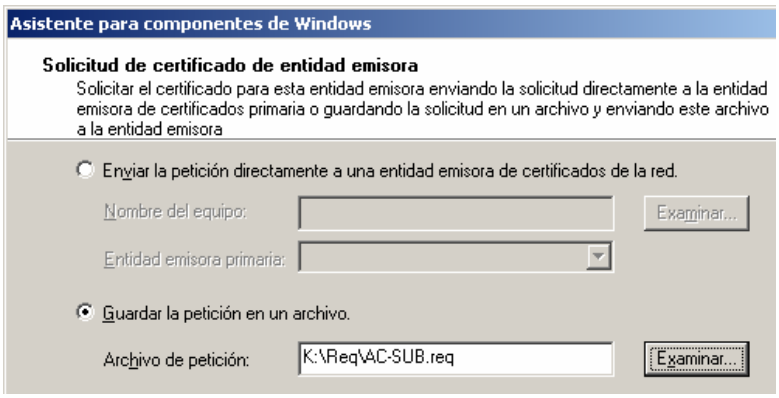

Figura 4.28 Solicitud para certificado de la AC subordinada

A continuación se presentan tres mensajes; el primero indica que se deben detener los servicios de *Certificate Server*; el segundo informa que para terminar el proceso se debe enviar la solicitud a la AC-Raíz de forma manual y el tercero indica que para activar la inscripción por *Web* se requiere habilitar las páginas de ASP dentro de IIS; se aceptan los tres mensajes. El proceso de solicitud ha concluido, se da un clic en **finalizar**.

Se almacena el archivo *AC-SUB.req* en un dispositivo extraíble para copiarlo en el servidor de certificados de la AC-Raíz. Se inician los servicios de la Entidad emisora

de certificados raíz y se da un clic con el botón derecho del *mouse* sobre la AC-Raíz, se selecciona **Todas las tareas** y en el menú emergente se selecciona **Enviar solicitud nueva**, como se muestra en la figura 4.29.

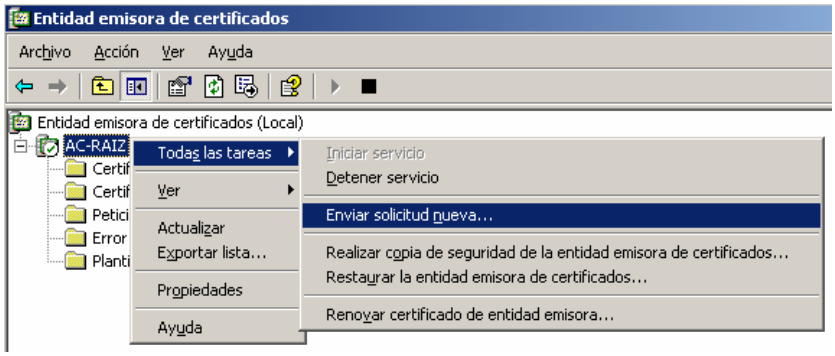

Figura 4.29 Solicitud de AC-SUB

En el cuadro **Abrir solicitud de archivo** se ubica la ruta en donde se almacenó la solicitud y se da un clic en **Abrir**; luego en el cuadro de diálogo **Guardar certificado** se ingresa el nombre AC-SUB.crt[1] y se da un clic en **Guardar**. Se copia el archivo AC-SUB.crt de servidor de certificados de la AC-Raíz y se lo almacena en la carpeta *Req* en la AC subordinada.

En el servidor de certificados de la AC subordinada se inicia los servicios de la Entidad emisora desde las **Herramientas administrativas** en el menú de **Inicio** de *Windows*, la AC está detenida como se observa en la figura 4.30.

Figura 4.30 AC-SUB detenida

[1] Como se verá en la sección de Pruebas de Funcionamiento, el nombre del certificado por defecto contiene información del equipo que funciona como servidor de certificados y de su dominio; el nombre AC-SUB solo se utiliza para la emisión del certificado, cuando éste se instala en la AC su nombre toma la estructura del nombre por defecto.

Para activar el servicio en la barra de herramientas se da un clic sobre el botón señalado con la flecha en la figura 4.30; entonces se presenta un mensaje en el que se pregunta si se desea instalar el certificado, se da un clic en **Sí**. En el cuadro de diálogo que se presenta se selecciona la ubicación del archivo AC-SUB.crt y se da un clic en **Abrir**.

A continuación se presenta un mensaje preguntando si se desea tener confianza en el certificado de la entidad Raíz, después de aceptar el certificado se instala y la AC subordinada queda habilitada como se indica en la figura 4.31.

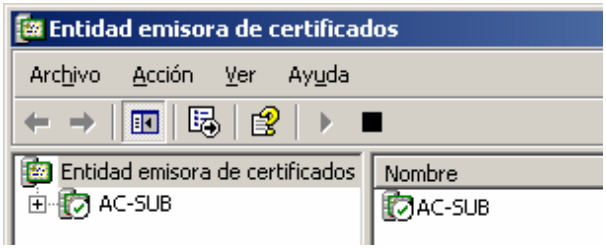

Figura 4.31 AC-SUB activada

4.4.4. CONFIGURACIÓN DE LA AC SUBORDINADA

Dentro del proceso de configuración de una AC subordinada se puede establecer las peticiones como pendientes, modificar los períodos de publicación de CRLs, activar la auditoría de eventos y restringir los permisos de usuarios de la misma manera que en el caso de la AC-Raíz.

Adicionalmente, se debe habilitar un sitio *Web* que servirá como directorio para la descarga de CP, CPS, CRLs y certificados de ACs raíz y subordinada. Para adecuar el sitio *Web* según las necesidades de la PKI, se debe realizar el siguiente procedimiento:

- Se da un clic en el botón de **Inicio** de *Windows* y luego en **Ejecutar**, en el cuadro de diálogo que se presenta se ingresa el comando *inetmgr* y se da un clic en **Aceptar** como se muestra en la figura 4.32.

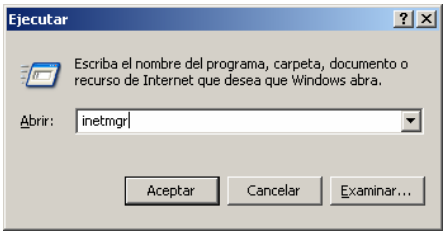

Figura 4.32 Ejecución de inetmgr

- En el **Administrador de IIS**, se selecciona **Sitio *Web* Predeterminado** como se muestra en la figura 4.33, se da un clic con el botón derecho del *mouse* sobre la carpeta CRL y en el menú emergente se selecciona **Propiedades**.

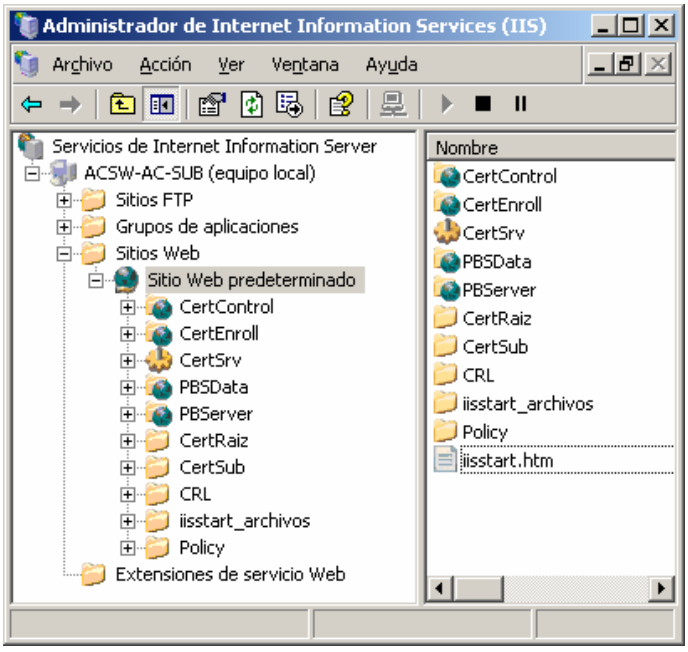

Figura 4.33 Sitio Web Predeterminado

- En el cuadro de diálogo se selecciona la pestaña **Directorio** y en la opción **Ruta de acceso local** se habilita el **Examen de Directorios** como se muestra

en la figura 4.34, esto permitirá que los usuarios puedan examinar las CRLs almacenadas en esta carpeta.

Figura 4.34 Propiedades de la Carpeta CRL en inetmgr

Las carpetas *CertSrv*, *CertControl* y *CertEnroll* mostradas en la figura 4.33 forman parte de la AC y sólo permiten accesos de lectura; la carpeta *CertSrv* contiene a *CertEnroll* y ésta a su vez contiene las listas de revocación y certificado de una AC; en otras palabras, el directorio de una AC está compuesto por la carpeta *CertEnroll*.

Sin embargo, para brindar un ambiente amigable para los usuarios y evitar accesos indebidos, se configuran las carpetas CRL, *CertRaiz* y *CertSub* de manera independiente para CRLs y certificados; las CRLs deben ser copiadas de forma manual y los certificados se copian durante la instalación de las ACs de forma automática.

Para configurar el sitio *Web* de ACSW mostrado en la figura 4.35, se da un clic con el botón derecho del *mouse* sobre el archivo *iisstart.htm* y se selecciona **Abrir con**, para seleccionar un procesador de texto como *WordPad* o el Bloc de notas, luego se puede copiar el código incluido en el Anexo 7.

En la figura 4.35 se encuentra incluida como opción de descarga de la Ruta de confianza. El archivo de la ruta de confianza contiene los certificados de la AC-Raíz y la AC subordinada; éstos se incluyen en un paquete PKCS#7.

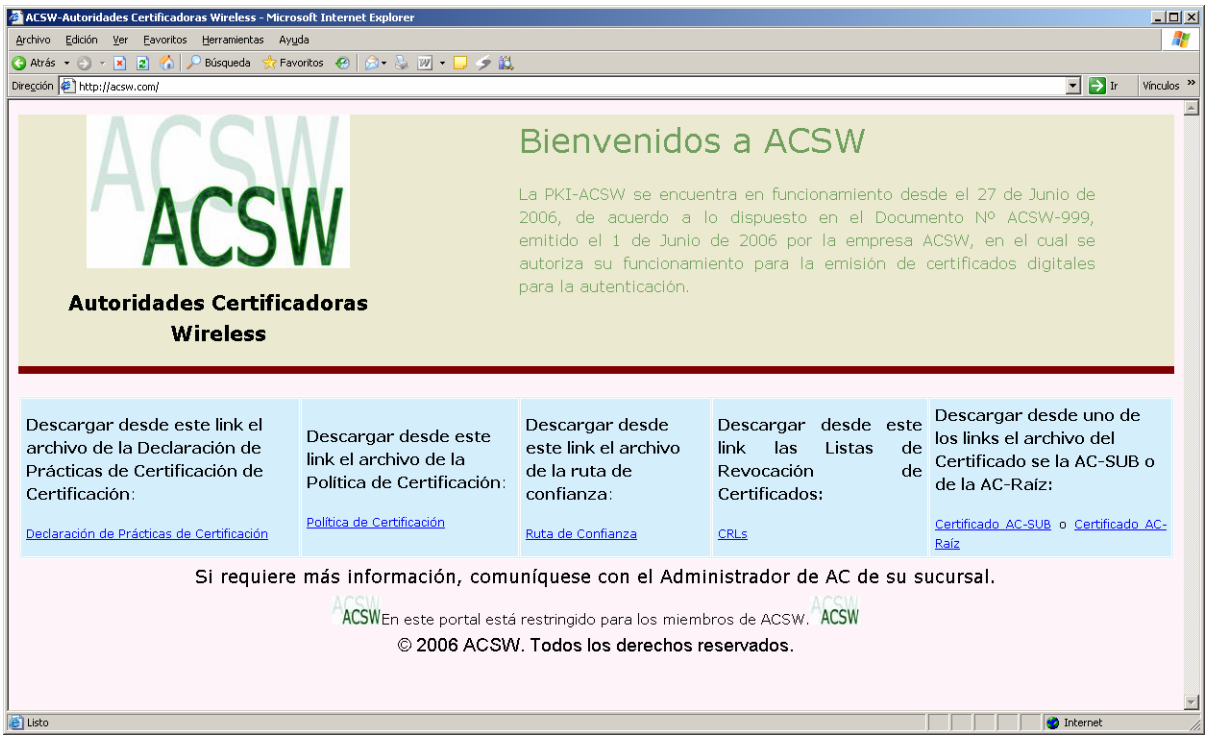

Figura 4.35 Sitio Web ACSW

Para obtener la ruta de confianza de una AC en particular, se ingresa al intérprete de comandos y se ejecutan los comandos *certutil -ca.chain ruta.p7b* como se muestra en la figura 4.36.

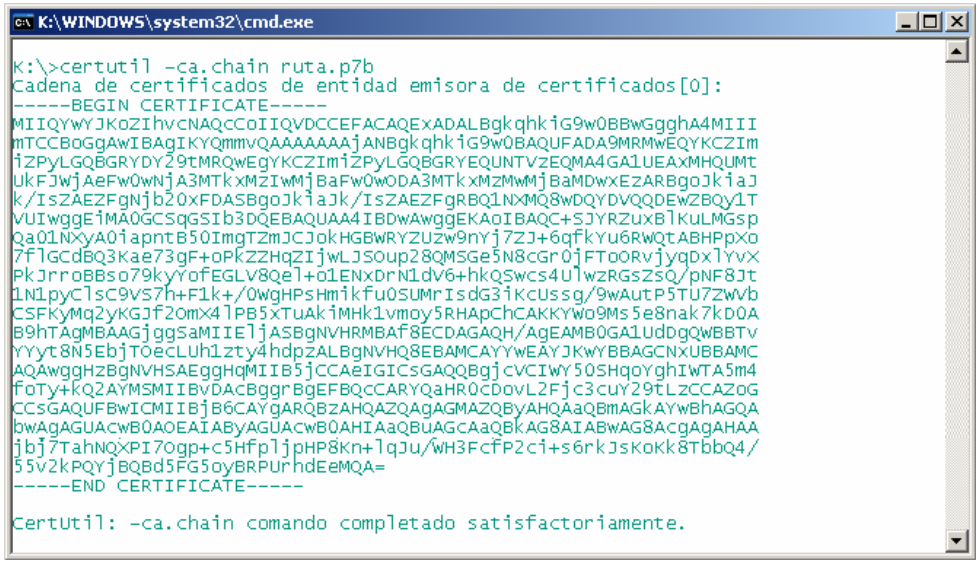

Figura 4.36 Obtención de la Ruta de Confianza de la AC-SUB

Figura 4.37 Archivo ruta.p7b

Si los comandos *certutil -ca.chain ruta.p7b* se ejecutan exitosamente, se genera el archivo *ruta.p7b* en el directorio en que se corrió el comando (K:\), como se muestra en la figura 4.37.

4.5. CONFIGURACIÓN DEL USUARIO PKI

Esta sección contiene información relacionada con la emisión de certificados digitales para usuarios dentro de la red LAN, estos certificados son emitidos con el único propósito de probar la interacción entre la AC-SUB creada en la sección anterior y usuarios convencionales dentro de la red cableada. Este proceso no forma parte de la solución planteada.

4.5.1. PROCESO DE EMISIÓN DE UN CERTIFICADO DIGITAL PARA UN USUARIO

Todo el proceso de emisión de certificados dentro de un entorno *Windows* está basado en su *CryptoAPI* [1], éste utiliza como directorio a *Active Directory*. A continuación se presentan los pasos seguidos durante la generación de un certificado digital en *Windows*.

- El proceso se inicia con una solicitud enviada por CMP (*Certificate Management Protocol*), a través de un paquete CMS[2], también se puede utilizar un paquete PKCS #10.

---

[1] *Cryptographic Application Programming Interface*.

[2] *Cryptographic Message Syntax*.

- Cuando un usuario envía una solicitud, *Xenroll.dll* utiliza el proveedor de servicios de cifrado CSP[1] para generar la pareja de claves del usuario y almacenarlas en su PC.
- Con la pareja de claves, *Xenroll* construye el paquete de solicitud de certificado en base a una plantilla.
- La clave pública es enviada junto con la información del usuario a *Certificate Server*, éste verifica si la solicitud cumple con las directivas establecidas en *Active Directory* y en la AC que emitirá el certificado.
- Después de que *Certificate Server* ha validado la solicitud del usuario, copia ésta en la base de datos de la AC añadiéndole un identificador.
- Para procesar la solicitud, *Certificate Server* verifica la correspondencia entre la clave privada utilizada para firmar la solicitud y la clave pública enviada; además, verifica que no se haya emitido previamente un certificado con esa pareja de claves, sí esto ha ocurrido, comprueba que el certificado no se haya revocado.
- De acuerdo al resultado de la validación de solicitud, la petición es aprobada, negada o permanece como pendiente[2].
- Si la petición es aprobada, durante la emisión del certificado se aplican las directivas relacionadas con la plantilla seleccionada. En este proceso se modifican los datos del certificado; por ejemplo: nombre de usuario, fecha de emisión y expiración, etc. Si se trata de una renovación, la información validada previamente se mantiene.
- El certificado creado es registrado en la base de datos de la AC y se envía a su propietario.
- Finalmente, el modulo *Xenroll* comunica al usuario que su certificado ha sido creado exitosamente; también puede presentarle un mensaje de error o de negación a su solicitud.

---

[1] *Cryptographic Service Provider*.

[2] Si se ha marcado la opción de establecer como pendientes las nuevas peticiones, el Administrador de AC deberá verificar cada solicitud y aprobar o negar la emisión del certificado.

4.5.2. CONFIGURACIÓN EN *WINDOWS XP*

Todo el proceso anterior es transparente para el usuario, pues el *CryptoAPI* de *Windows* brinda un ambiente que permite interactuar al usuario con *Certificate Server* de manera amigable, sin revelar los detalles criptográficos correspondientes. Para que un usuario pueda solicitar un certificado digital necesita estar registrado dentro del dominio.

Para iniciar el proceso de solicitud se da un clic en el botón de **Inicio** de *Windows* y luego se selecciona **Ejecutar**; en el cuadro de diálogo que se presenta se ingresa el comando *certmgr.msc* y se da un clic en **Aceptar** como se muestra en la figura 4.38.

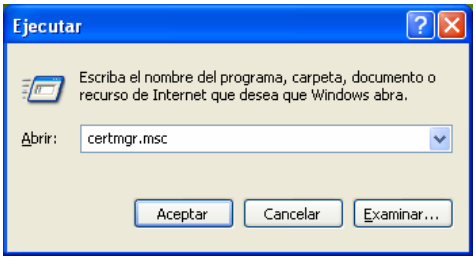

Figura 4.38 Ejecución de certmgr.msc

Al ejecutar el comando *certmgr.msc* se abre la aplicación mostrada en la figura 4.39, ésta contiene el perfil de administración de certificados del usuario actual; en la carpeta **Personal**, se almacenan todos los certificados emitidos para el usuario.

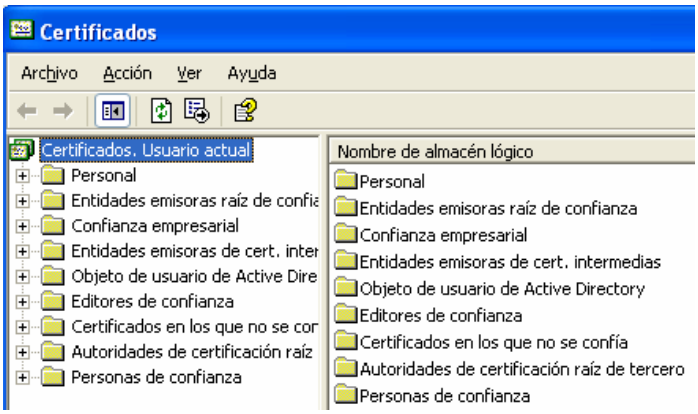

Figura 4.39 Perfil de certificados: Usuario Actual

Para solicitar un nuevo certificado se da un clic con el botón derecho del *mouse* sobre la carpeta **Personal**, en el menú emergente se selecciona **Todas las tareas** y luego **Solicitar un nuevo certificado**, como se muestra en la figura 4.40; entonces se presenta una pantalla con el asistente para instalación de certificados dentro de un dominio, se da un clic en **siguiente**.

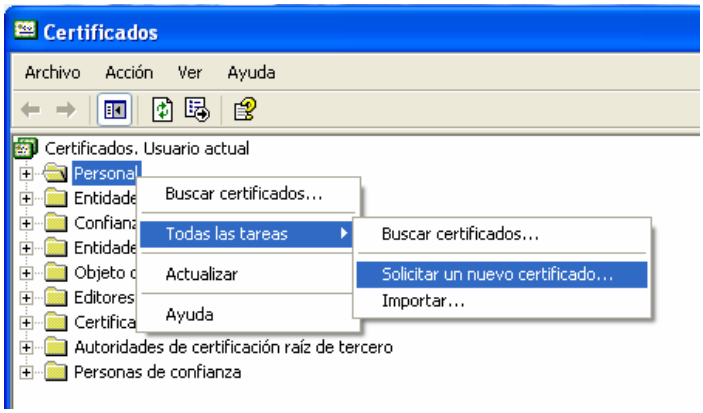

Figura 4.40 Solicitar un Certificado Personal

La pantalla que se muestra indica los tipos de certificado que puede solicitar el usuario, los tipos existentes son: Administrador, Agente de recuperación de EFS, EFS básico y Usuario como se muestra en la figura 4.41. Los cuatro tipos están disponibles solo para perfiles de Administrador, un usuario normal puede acceder únicamente a los últimos dos tipos.

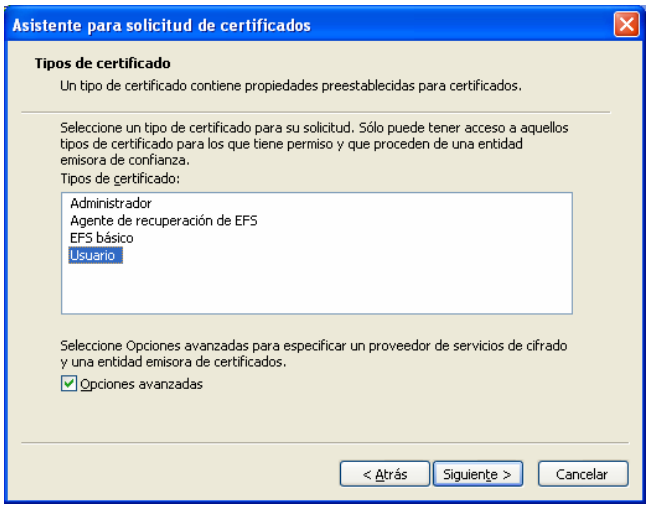

Figura 4.41 Tipos de Certificado

Se selecciona el tipo de certificado, en este caso **Usuario**; para definir las características del certificado, se selecciona **Opciones Avanzadas** y se da un clic en **siguiente**.

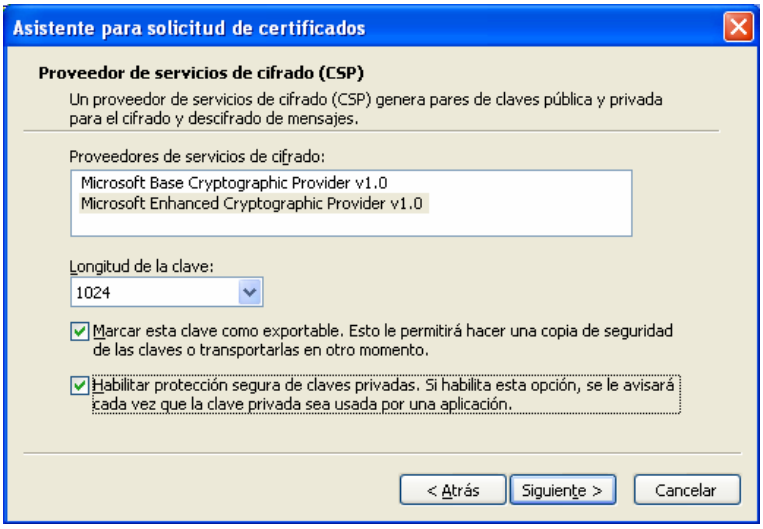

Figura 4.42 Características del Certificado

La pantalla mostrada en la figura 4.42 permite definir el proveedor de servicios de cifrado, es recomendable seleccionar la versión *enhanced* pues provee mejores características de seguridad; luego, de acuerdo a los requerimientos del certificado se selecciona la longitud de clave y se marca las opciones de **clave exportable** y **protección de claves**. Cuando se ha concluido se da un clic en **siguiente**.

Figura 4.43 AC seleccionada

En la pantalla que se presenta a continuación se debe seleccionar la AC que debe atender la solicitud, para esto se da un clic en **Examinar** y se elige la AC-SUB como se muestra en la figura 4.43; luego se da un clic en **siguiente** para continuar con el proceso.

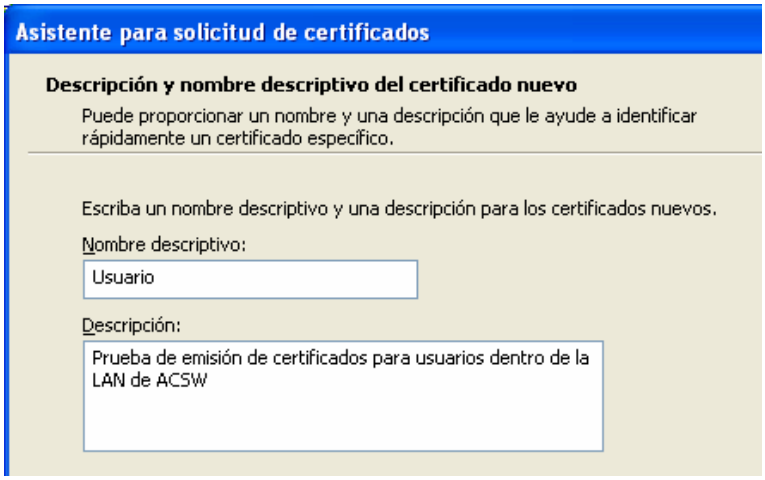

Figura 4.44 Nombre Alternativo del Certificado

El proceso continúa con un cuadro de diálogo que solicita el nombre alternativo del certificado y opcionalmente una descripción de éste; se llenan los datos como se indica en la figura 4.44 y se da un clic en **siguiente**.

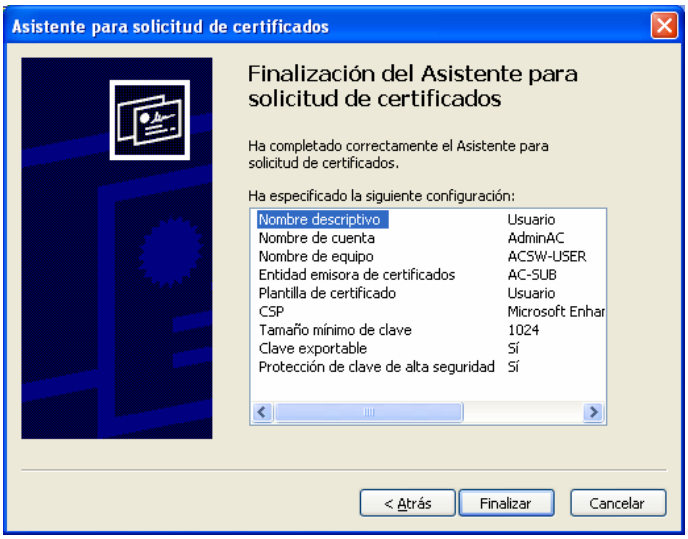

Figura 4.45 Características del Certificado Solicitado

La configuración de las características del certificado termina con un cuadro de diálogo que indica todas las características seleccionadas como se observa en la figura 4.45; estas características serán enviadas dentro del paquete de solicitud después de dar un clic en el botón **Finalizar**.

Debido a que se habilitó la protección de claves, se presenta el cuadro de diálogo para la generación de claves mostrado en la figura 4.46, éste permite seleccionar el nivel de seguridad; por defecto se establece un nivel medio. Para cambiar esta característica se da un clic en **Nivel de seguridad** y en el cuadro de diálogo que se presenta se selecciona **Alto** y se da un clic en **siguiente**.

Figura 4.46 Asistente para Seguridad de la Clave

El nivel de seguridad Alto requiere del establecimiento de mecanismos de seguridad para proteger la clave privada, para esto el asistente de generación de claves solicita una contraseña; después de ingresar y confirmar la contraseña se da un clic en **finalizar** en el cuadro de diálogo de protección de clave y se selecciona **Aceptar** en el cuadro de diálogo de generación de claves.

Figura 4.47 Certificado de Usuario Creado

Si la generación del certificado tuvo éxito, se presenta un mensaje indicando que el certificado ha sido creado como se muestra en la figura 4.47, caso contrario se comunica al usuario que su solicitud fue rechazada.

4.5.3. ENTIDADES DE CONFIANZA DEL USUARIO

Al ejecutar el comando *certmgr.msc* se puede verificar las entidades registradas como ACs de confianza para un usuario. En la figura 4.48 se localiza dentro de las ACs raíz de confianza a la AC-RAIZ y en la figura 4.49 se encuentra a la AC-SUB dentro de las ACs intermedias de confianza.

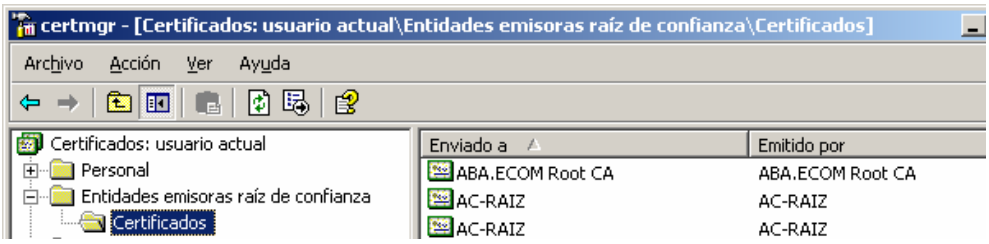

Figura 4.48 Certificados de ACs raíz de confianza de Usuario

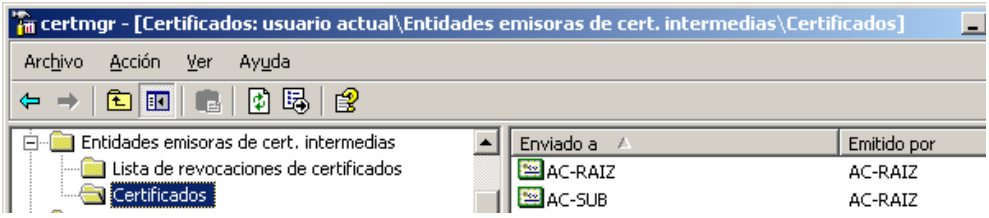

Figura 4.49 Certificados de ACs intermedias de confianza de Usuario

4.6. PRUEBAS DE FUNCIONAMIENTO

4.6.1. PRUEBAS DE CONTENIDO DE CERTIFICADOS

En esta sección se verificará el contenido de los certificados de la AC-Raíz y de la AC subordinada de acuerdo al archivo *CAPolicy.inf*.

4.6.1.1. Certificado de la AC-RAÍZ

En la figura 4.50 se muestra el certificado digital de la AC-Raíz. Como se puede observar, la ficha general muestra en la directiva de Seguridad alta configurada en el archivo *CAPolicy.inf*; además, el botón de Declaración del Emisor se encuentra habilitado.

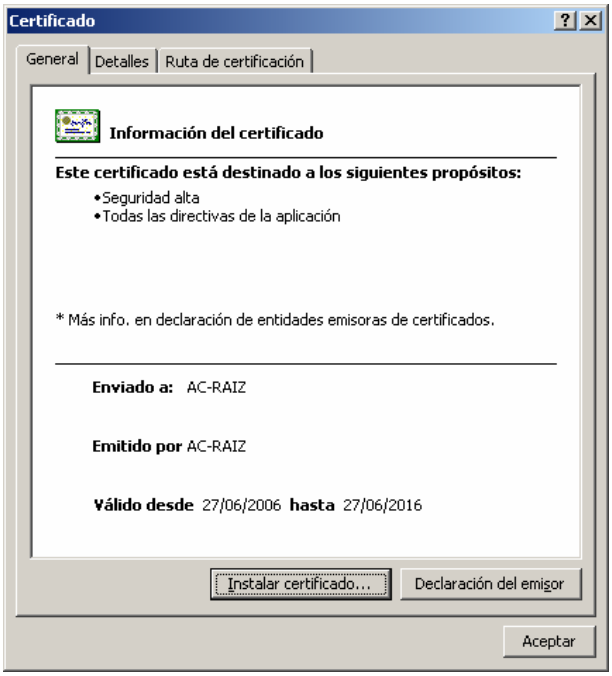

Figura 4.50 Certificado AC-RAIZ

Para acceder a la información se da un clic en el botón **Declaración del emisor** y se presenta la pantalla mostrada en la figura 4.51; si se da un clic en el botón **Más información** se accederá al sitio *Web* http://acsw.com.

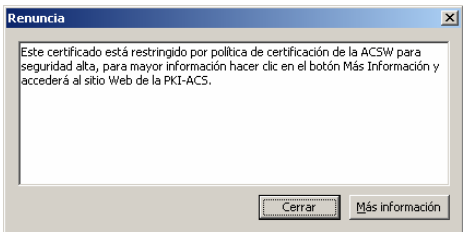

Figura 4.51 Declaración del Emisor

a. Pestaña Detalles

Cuando se selecciona la pestaña Detalles de la figura 4.50, se puede identificar cada campo del certificado. Para verificar los parámetros de configuración del certificado se da un clic en la opción **Mostrar** y se selecciona **Solo campos versión 1** como se muestra en la figura 4.52.

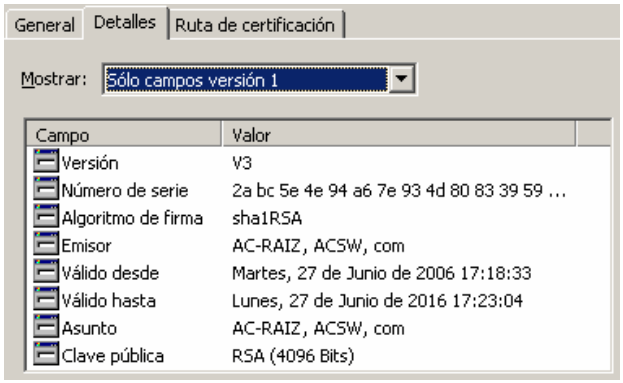

Figura 4.52 Parámetros del Certificado

En la opción **Sólo campos versión 1** mostrada en la figura 4.52 se pueden verificar los siguientes parámetros:

- Versión X.509: v3.
- Número de serie: 2a bc 5e 4e 94 a6 7e 93 4d 80 83 39 59 16 74 33.
- El algoritmo *hash*: SHA-1.
- El algoritmo de firma digital: RSA.
- El emisor del certificado: AC-RAIZ, ACSW, com[1].
- El propietario del certificado: AC-RAIZ, ACSW, com.
- Fecha de emisión del certificado: 27 de junio de 2006.
- Fecha de expiración del certificado: 27 de junio de 2016.
- Longitud de la clave: 4096 *bits*.

[1] Nombre común: AC-RAIZ dentro del dominio ACSW.com.

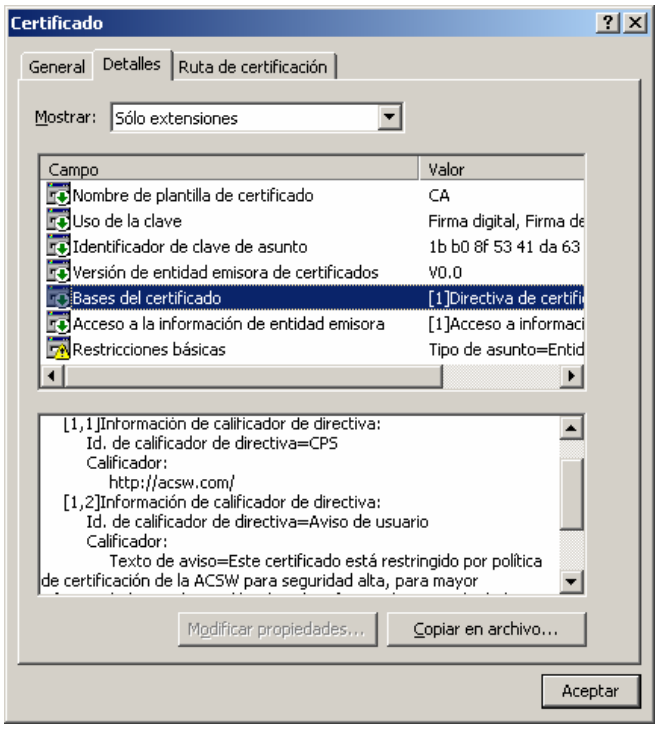

Figura 4.53 Extensiones del Certificado

Para verificar los parámetros relacionados con las extensiones del certificado se da un clic en la opción **Mostrar** de la pestaña **Detalles** y se selecciona **Solo extensiones** como se muestra en la figura 4.53.

Cuando se selecciona la extensión Bases del certificado de la figura 4.53, en la parte inferior de la pantalla se encuentra en el primer calificador la ubicación de la CPS en http://acsw.com; en el segundo calificador se encuentra el texto del campo *Notice* ubicado en [*PolicyExtension*] en el archivo *CAPolicy.inf*.

En la figura 4.54 se observa una descripción relacionada con la información de la AC; el OID 1.3.6.1.5.5.7.48.2[1] está relacionado con el RFC 2459, para determinar el acceso a la información de la AC. Por otro lado se encuentra como nombre

[1] *iso.org.dod.internet.security.mechanisms.pkix.ad.caIssuers*.

alternativo el sitio *Web* definido dentro del campo [*AuthorityInformationAccess*] en el archivo *CAPolicy.inf*.

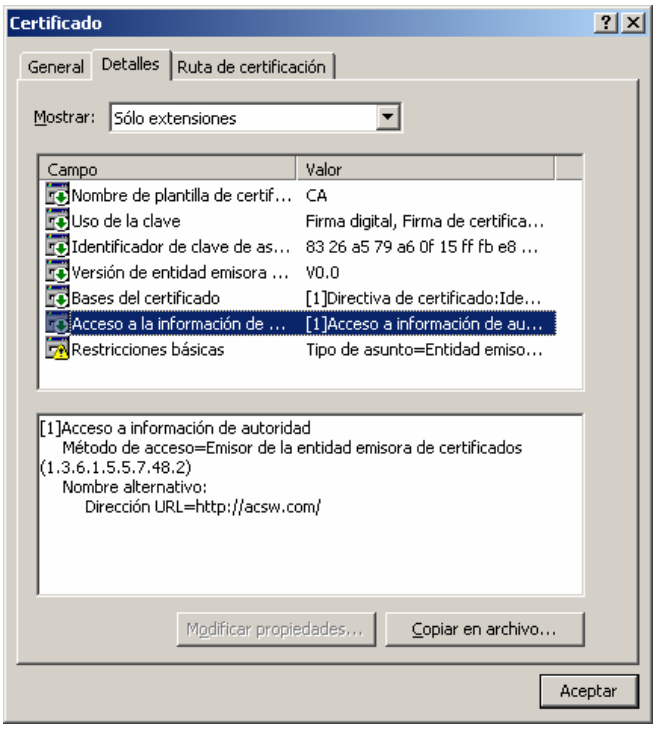

Figura 4.54 Extensión AuthorityInformation

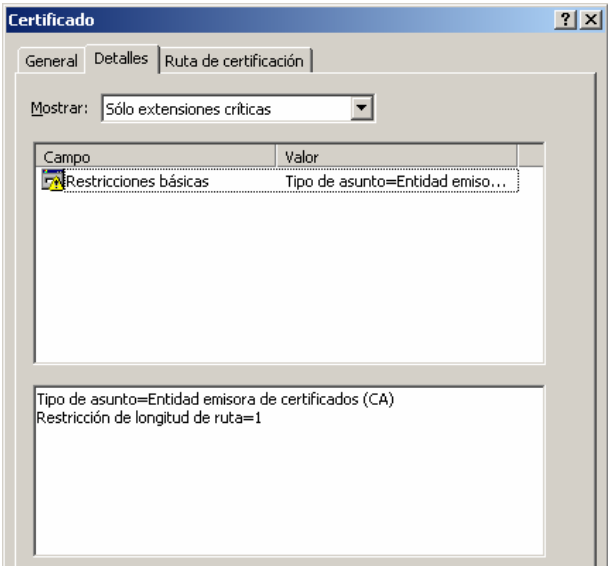

Figura 4.55 Extensiones Críticas

Las extensiones críticas del certificado se muestran en la figura 4.55. Como se puede observar, la única extensión crítica es la longitud de ruta configurada en el campo [*BasicConstraintsExtension*] del archivo *CAPolicy.inf*; en la figura 4.55 se observa que la longitud de ruta de la AC-Raíz es igual a 1.

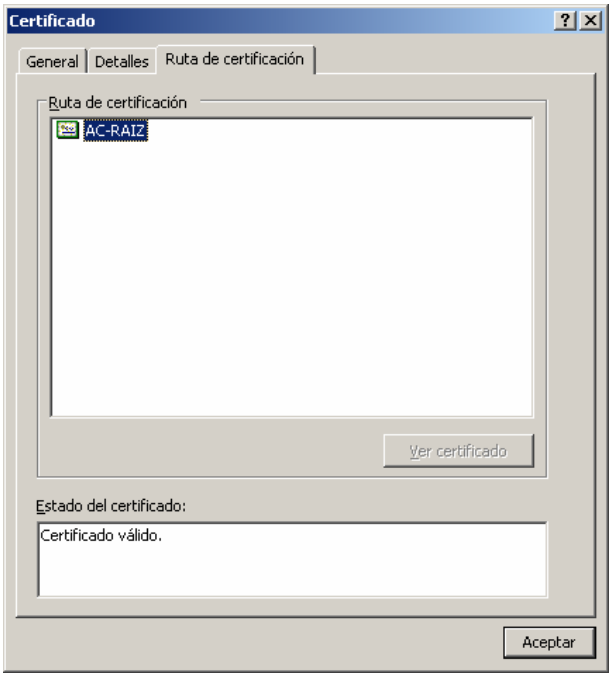

Figura 4.56 Ruta de Certificación

Finalmente, en la pestaña **Ruta de certificación** mostrada en la figura 4.56, se observa que se trata del certificado de una entidad raíz y en la parte inferior de la pantalla se comprueba que el certificado es válido.

4.6.1.2. Certificado de la AC-SUB

En la figura 4.57 se muestra el certificado digital de la AC-SUB. Como se puede observar, la ficha general muestra en la directiva de Seguridad alta configurada en el archivo *CAPolicy.inf*; además, el botón de Declaración del Emisor se encuentra habilitado de la misma manera que en el caso de la AC-Raíz.

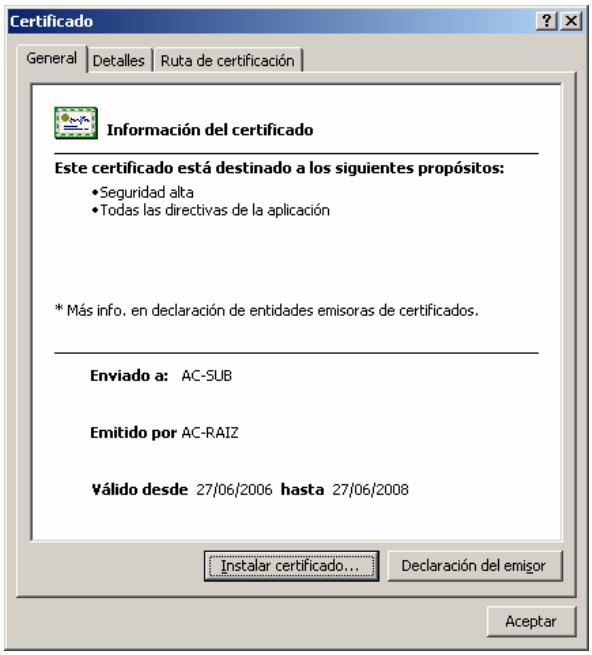

Figura 4.57 Certificado AC-SUB

a. Pestaña Detalles

Cuando se selecciona la pestaña **Detalles** se puede identificar cada campo del certificado. Para verificar los parámetros de configuración del certificado se da un clic en la opción **Mostrar** y se selecciona **Solo campos versión 1** como se muestra en la figura 4.58.

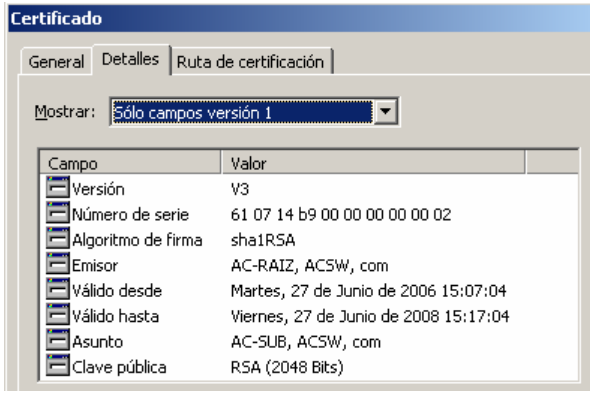

Figura 4.58 Parámetros del Certificado

En la opción **Sólo campos versión 1** mostrada en la figura 4.58 se pueden verificar los siguientes parámetros:

- Versión X.509: v3.
- Número de serie: 61 07 14 b9 00 00 00 00 00 02.
- El algoritmo *hash*: SHA-1.
- El algoritmo de firma digital: RSA.
- El emisor del certificado: AC-RAIZ, ACSW, com.
- El propietario del certificado: AC-SUB, ACSW, com.
- Fecha de emisión del certificado: 27 de junio de 2006.
- Fecha de expiración del certificado: 27 de junio de 2008.
- Longitud de la clave: 2048 *bits*.

Las extensiones relacionadas con los campos [*PolicyExtension*] y [*AuthorityInformationAccess*], contienen la misma información que en el caso del certificado de la AC-Raíz.

Para verificar los parámetros relacionados con las extensiones del certificado de la AC-SUB se da un clic en la opción **Mostrar** de la pestaña **Detalles** y se selecciona **Solo extensiones** como se muestra en la figura 4.59.

Figura 4.59 Extensiones del Certificado

El certificado de la AC-Raíz no contenía la extensión Puntos de distribución CRL encontrada en la figura 4.59, esto se debe a que dentro del archivo *CAPolicy.inf* en este campo se configuró la variable *Empty* = *true*; sin embargo, el certificado de la AC subordinada contiene esta extensión debido a que la AC-Raíz demanda informar a las entidades confiantes la ubicación de la CRL relacionada con el certificado.

Figura 4.60 Extensiones Críticas

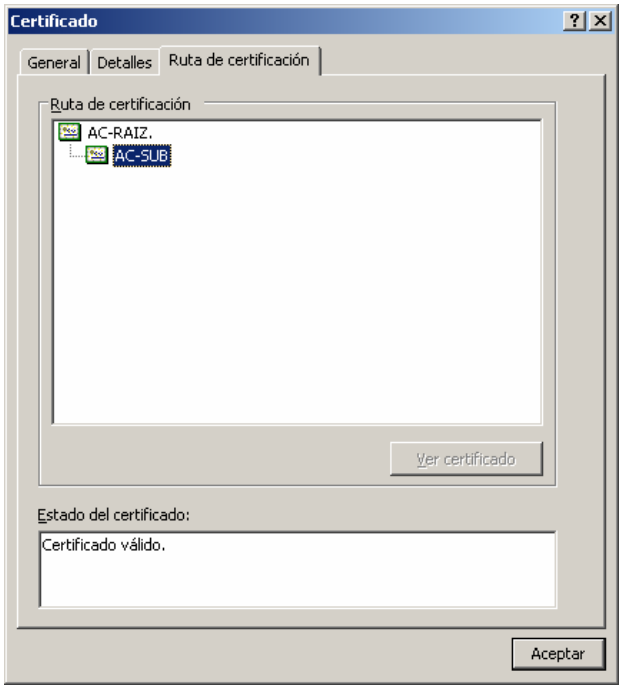

Figura 4.61 Ruta de Certificación

Las extensiones críticas del certificado se muestran en la figura 4.60. Como se puede observar a pesar de que el campo [*BasicConstraintsExtension*] no se incluyó dentro del archivo *CAPolicy.inf* de la AC-SUB, la AC-Raíz restringió la longitud de ruta de la AC-SUB a cero.

Finalmente, en la pestaña **Ruta de certificación** mostrada en la figura 4.61, se observa que se trata del certificado de una entidad subordinada a la AC-Raíz y en la parte inferior de la pantalla se comprueba que el certificado es válido.

4.6.2. PRUEBAS DE OPERACIÓN

Las pruebas de operación se exponen de manera general; es decir, cuando se hace referencia a una AC, el proceso es aplicable para la AC-Raíz o para la AC subordinada. Solo la revocación del certificado de la AC-Raíz requiere de un tratamiento especial.

4.6.2.1. *Certconfig* y *Certenroll*

CertConfig y *CertEnroll* son carpetas compartidas utilizadas como directorio local dentro del servidor de certificados, éstas sirven para almacenar diferentes archivos relacionados con una AC. Si durante la instalación de la AC se selecciona la opción **Almacenar la información en una carpeta compartida**, la información de *CertConfig* se almacena también en la carpeta seleccionada.

En la tabla 4.5 se presenta un resumen de los archivos almacenados en estas carpetas y su finalidad.

Ubicación/Archivo	Finalidad
CertConfig\Certsrv.txt	Este archivo contiene información general de la AC.
CertConfig\Certsrv.bak	Cuando la AC es reinstalada, la información registrada en Certsrv.txt es almacenada en este archivo.
\CertConfig\AC-SUB(#).req	Archivo de solicitud para la generación de un certificado, el campo (#) indica la versión del archivo y se omite cuando se trata de la primera petición (0); si se llega a realizar una nueva petición toma el valor de (1) y así incrementalmente en cada versión.
\Req\AC-SUB(#).req	Si durante el proceso de solicitud de un certificado, se modifica la ubicación por defecto; por ejemplo la carpeta *Req* que se creó durante la instalación de la AC subordinada.
AC-SUB(#).crt Se incluye en las dos carpetas.	Es el certificado de la AC, el campo (#) indica la versión del archivo y se omite cuando se trata de la primera versión del certificado (0), todas las siguientes versiones modifican incrementalmente este campo.
CAname(*n*-*k*)[1].crt CAname(*k*-*n*).crt Se incluyen en las dos carpetas.	Si durante la renovación del certificado de una AC raíz se requiere renovar la pareja de claves, se crean certificados cruzados para generar confianza en el nuevo certificado, (*n*-*k*) significa que se utilizó la versión *n* de clave privada para firmar la versión *k*. Los certificados cruzados no se crean cuando se presentó un compromiso de clave, en este caso se elimina el certificado relacionado con la clave comprometida y se crea un certificado con una nueva versión.
AC-SUB(#).crl Se incluye en las dos carpetas.	Este archivo pertenece a la CRL, el campo (#)[2] indica la versión del archivo y se omite cuando se trata de la primera versión de CRL (0), todas las siguientes versiones lo modifican incrementalmente.
AC-SUB+.crl Se incluye en las dos carpetas.	Archivo de CRL delta, el campo (#) indica la versión del archivo.

Tabla 4.5 Archivos generados por Certificate Server

4.6.2.2. Detener y Activar *Certificate Server*

Cuando no se requieren los servicios de certificación dentro de la red, se deben detener los servicios de *Certificate Server* hasta que sean requeridos nuevamente.

Para desactivar los servicios de *Certificate Server* se da un clic con el botón derecho del *mouse* sobre la AC y en el menú emergente se selecciona la opción **Detener**

[1] $k = n+1$.

[2] Este argumento es incluido en el nombre del archivo solo si la renovación implica cambio de claves.

servicio; también se puede se dar un clic sobre el botón señalado en la figura 4.62 en la barra de herramientas.

Figura 4.62 Detener la AC

Para activar los servicios de *Certificate Server* se da un clic con el botón derecho del *mouse* sobre la AC y en el menú emergente se selecciona la opción **Iniciar servicio**; también se puede se da un clic sobre el botón señalado en la figura 4.63 en la barra de herramientas.

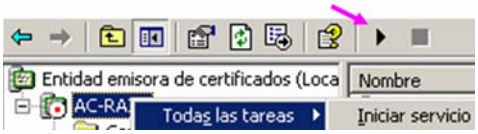

Figura 4.63 Activar la AC

4.6.2.3. *Backup*

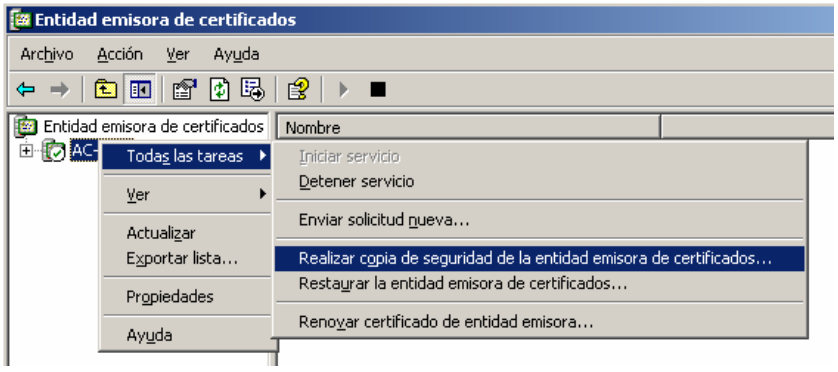

Figura 4.64 Realizar copia de seguridad

Certificate Server permite sacar respaldos de la base de datos de la AC y de sus claves. Para realizar un respaldo se da un clic con el botón derecho del *mouse* sobre

la AC, se selecciona **Todas las tareas** y luego **Realizar copia de seguridad de la entidad emisora de certificados**, como se muestra en la figura 4.64.

A continuación se presenta el Asistente para copia de seguridad, y se da un clic en **siguiente**. En la siguiente pantalla se selecciona la opción **Clave privada y certificado de la entidad emisora** y/o **Base de de datos de certificados emitidos**; en la opción **Ubicación para copia de seguridad** ingresar la localidad donde se almacenarán los archivos de respaldo como se muestra en la figura 4.65, entonces se da un clic en **siguiente**.

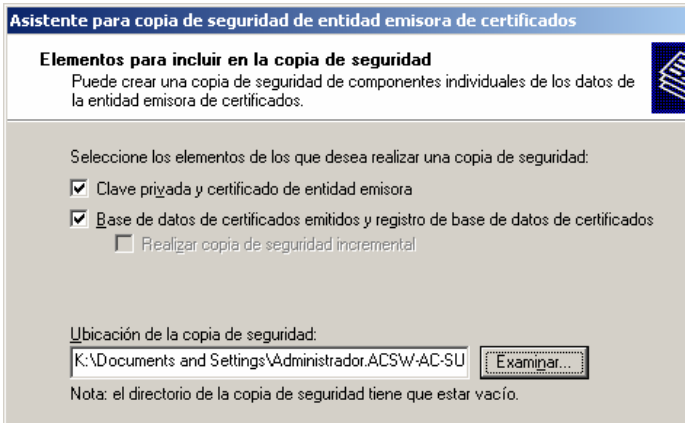

Figura 4.65 Selección de archivos para copia de seguridad

En el siguiente cuadro de diálogo se ingresa y confirma una contraseña para cifrar la clave privada y el certificado de la AC; se da un clic en **siguiente** y en la siguiente pantalla se da un clic en **finalizar**.

Como se muestra en la figura 4.66, los archivos relacionados con la base de datos de certificados se almacenan en la carpeta *DataBase*; para almacenar la pareja de claves y el certificado se generó un archivo PKCS#12[1].

[1] Estándar diseñado por RSA *Laboratories*, define la sintaxis general para mensajes de intercambio de información personal que incluyen elementos criptográficos como: información personal, claves, certificados, extensiones, etc.

Figura 4.66 Archivos de Respaldo

4.6.2.4. Restaurar la AC

Para restaurar la información de una AC, se debe sacar respaldos previamente. Para iniciar con el proceso se da un clic con el botón derecho del *mouse* sobre la AC, se selecciona **Todas las tareas** y luego **Restaurar la entidad emisora de certificados**, como se muestra en la figura 4.67.

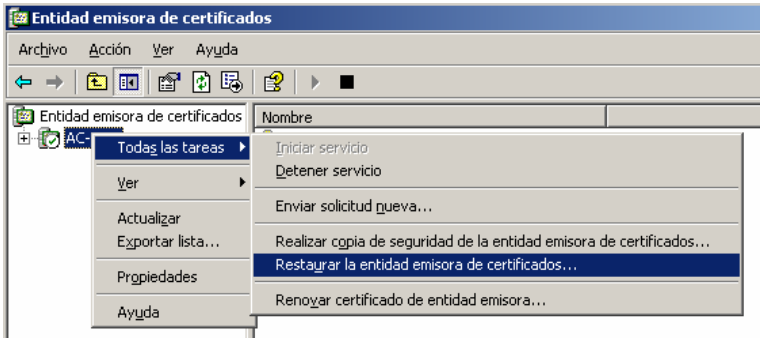

Figura 4.67 Restaurar la AC

A continuación se presenta un mensaje indicando que deben detenerse los servicios de *Certificate Server* durante el proceso, se da un clic en **Aceptar**. En la pantalla de inicio del asistente de restauración se da un clic en **siguiente**.

En la pantalla siguiente se selecciona la opción **Clave privada y certificado de la entidad emisora** y/o **Base de de datos de certificados emitidos** según el caso; en la opción **Ubicación para copia de seguridad** se ingresa la localidad donde se almacenaron los archivos de respaldo como se muestra en la figura 4.68; se da un clic en **siguiente**.

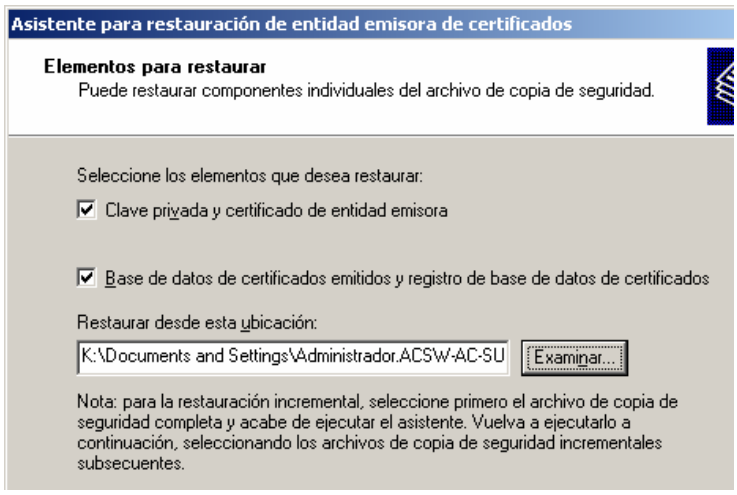

Figura 4.68 Selección de archivos para copia de seguridad

En el cuadro de diálogo siguiente se ingresa la contraseña y se da un clic en **siguiente**. En la pantalla final del asistente de restauración se da un clic en **finalizar**.

4.6.2.5. Renovar el Certificado de una AC

El certificado de una AC se puede renovar cuando su período está por finalizar o cuando se requiere actualizar el certificado manteniendo el mismo par de claves; en el primer caso, es necesario renovar el certificado antes de cumplir con su período de validez, con el fin de mantener un lapso de sobreposición en el cual los dos certificados sean válidos.

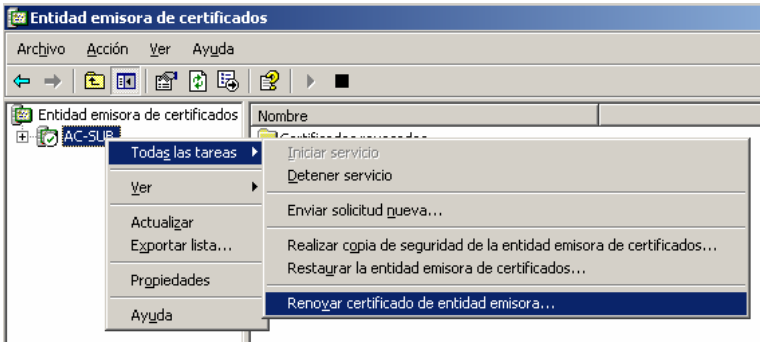

Figura 4.69 Renovar certificado de AC

Para renovar el certificado de una AC se da un clic con el botón derecho del *mouse* sobre la AC, se selecciona **Todas las tareas** y luego **Renovar certificado de entidad emisora**, como se muestra en la figura 4.69.

Se presenta un mensaje indicando que deben detenerse los servicios de *Certificate Server* durante el proceso, se da un clic en **Aceptar**.

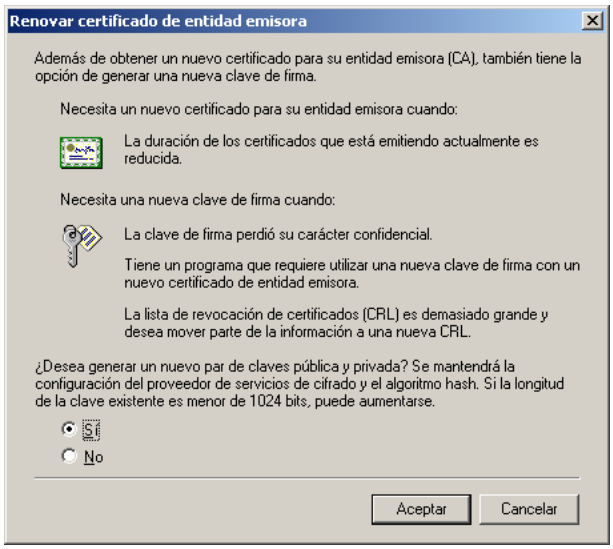

Figura 4.70 Renovar la pareja de claves de la AC

En la pantalla **Renovar certificado** mostrada en la figura 4.70, se selecciona **Sí** en caso de requerir la generación de una nueva pareja de claves y **No** para mantener las actuales, luego se da un clic en **siguiente**. Cuando el certificado se ha renovado se reactivan los servicios de *Certificate Server*.

Cuando se renueva un certificado de AC su período de validez se reestablece desde el día de renovación y no se aplica el campo [*PolicyExtension*] del archivo *CAPolicy.inf*. Todos los certificados de una AC se registran dentro del directorio del dominio hasta que su período de validez se cumpla, excepto en caso de revocación.

4.6.2.6. Revocar, Suspender y Reactivar Certificados

Las causas para la revocación de un certificado se exponen en la tabla 4.6, esta tabla incluye también el código y nombre relacionado con cada una.

Código	Nombre	Causa de Revocación
0	*CRL_REASON_UNSPECIFIED*	No especificado (predeterminada).
1	*CRL_REASON_KEY_COMPROMISE*	Compromiso de la clave privada.
2	*CRL_REASON_CA_COMPROMISE*	Compromiso de la clave privada de la AC.
3	*CRL_REASON_AFFILIATION_CHANGED*	Afiliación modificada (Cambio de funciones del propietario de certificado).
4	*CRL_REASON_SUPERSEDED*	Reemplazado.
5	*CRL_REASON_CESSATION_OF_OPERATION*	Cese de la operación de la AC.
6	*CRL_REASON_CERTIFICATE_HOLD*	Retención de certificado (suspensión).
8	*CRL_REASON_REMOVE_FROM_CRL*	Quitar de la CRL (reactivación).

Tabla 4.6 Revocación de Certificados

a. Revocar, Suspender y Reactivar Certificados de Entidad Destino

Para revocar o suspender un certificado se ingresa a la carpeta de **Certificados Emitidos** dentro de la AC como se muestra en la figura 4.71; se da un clic con el botón derecho del *mouse* sobre el certificado o certificados, en el menú emergente se selecciona **Todas las tareas** y luego **Revocar certificado**.

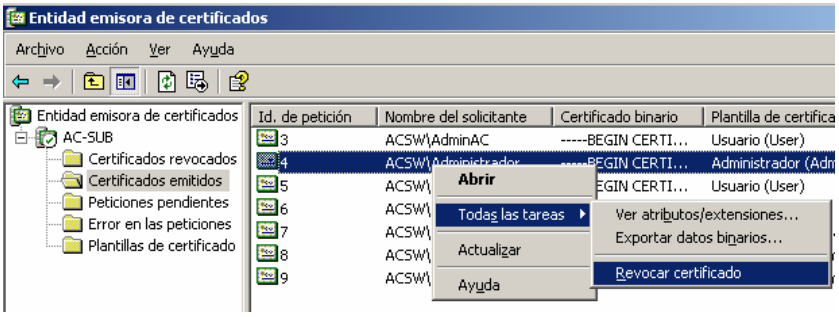

Figura 4.71 Revocación de Certificados

A continuación se presenta el cuadro de diálogo mostrado en la figura 4.72, en éste se debe seleccionar el motivo de la revocación del certificado; luego se da un clic en **Sí**. Todas las razones revocan el certificado permanentemente excepto **Certificado retenido**, esta opción produce la suspensión temporal del certificado.

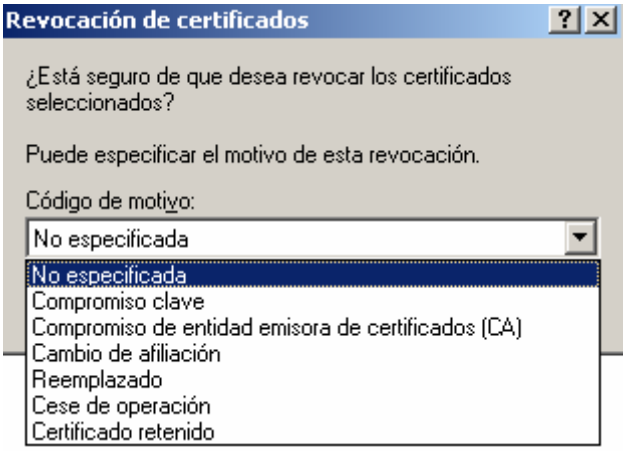

Figura 4.72 Razones de Revocación

Cuando se trate de la revocación del certificado de una AC subordinada, es necesario realizar el proceso de renovación de certificado de manera inmediata, debido a que mientras no se renueve el certificado la revocación no se publica en *Active Directory*.

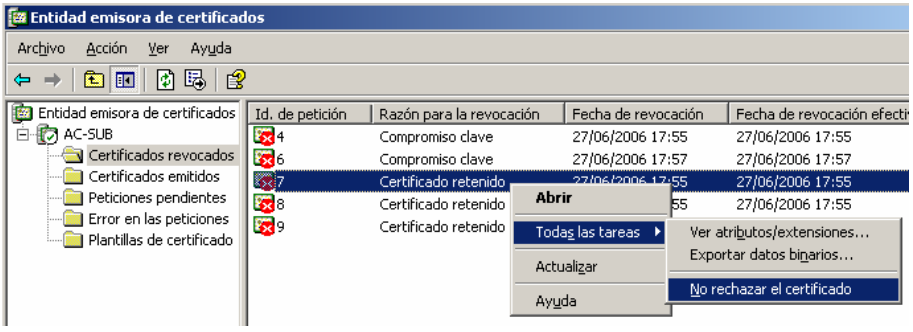

Figura 4.73 Reactivación de Certificados

Para reactivar un certificado suspendido se ingresa a la carpeta de **Certificados Revocados** dentro de la AC como se muestra en la figura 4.73, se da un clic con el

botón derecho del *mouse* sobre el certificado o certificados, en el menú emergente se selecciona **Todas las tareas** y luego **No rechazar certificado**.

b. Revocar el certificado de una AC-Raíz

El certificado de la AC raíz no se registra dentro de los certificados emitidos, por lo tanto, para revocar su certificado se debe utilizar el comando *certutil* en la interfaz de comandos como se indica a continuación:

- Se da un clic sobre el botón **Inicio** de *Windows* y se selecciona **Ejecutar**, en el cuadro de diálogo que se presenta se ingresa el comando *cmd*, como se muestra en la figura 4.74 y se da un clic en **Aceptar**, este comando permite ingresar a la interfaz de comandos de *Windows*.

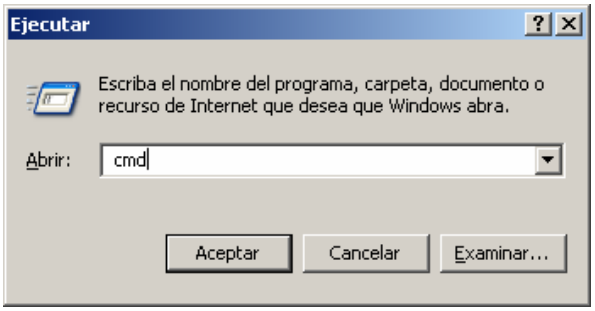

Figura 4.74 Ejecución del Comando cmd

- En la interfaz de comandos se ingresa el comando *certutil* siguiendo la siguiente sintaxis: *certutil -revoke número _ de _ serie razón*.

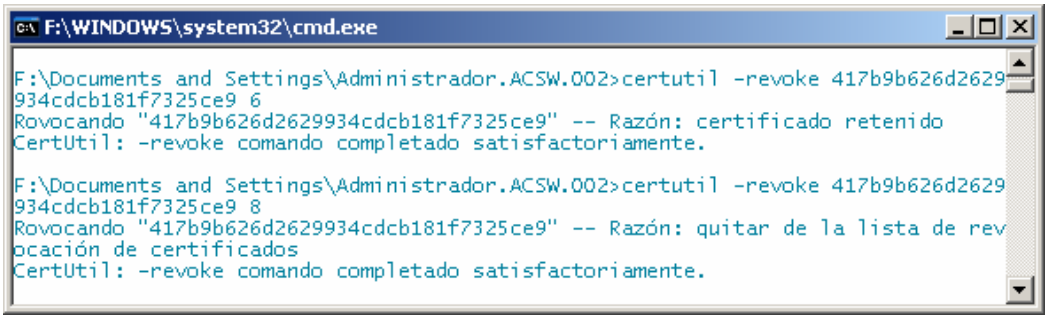

Figura 4.75 Suspensión por Interfaz de comandos

En la figura 4.75 se muestra la suspensión y reactivación del certificado de la AC-Raíz; este procedimiento funciona siempre y cuando los servicios de *Certificate Server* estén activados, de no ser así, se presenta un error durante la reactivación del certificado.

En la figura 4.76 se muestra la revocación de un certificado por compromiso de clave; como se puede observar, es necesario apagar los servicios de *Certificate Server* para que la revocación se complete.

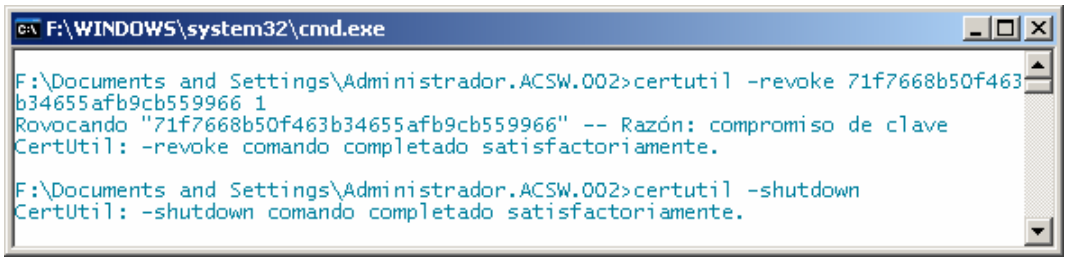

Figura 4.76 Revocación por Interfaz de comandos

Si se intenta acceder a los servicios de *Certificate Server* después de una revocación, la AC-Raíz se encuentra desactivada y se presenta el mensaje de certificado revocado mostrado en la figura 4.77.

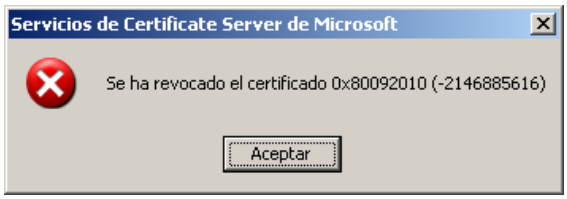

Figura 4.77 Mensaje Error: Certificado Revocado

4.6.2.7. Publicar CRLs

Para publicar CRLs se da un clic con el botón derecho del *mouse* sobre la carpeta **Certificados revocados**, se selecciona **Todas las tareas** y luego **Publicar**, como se muestra en la figura 4.78.

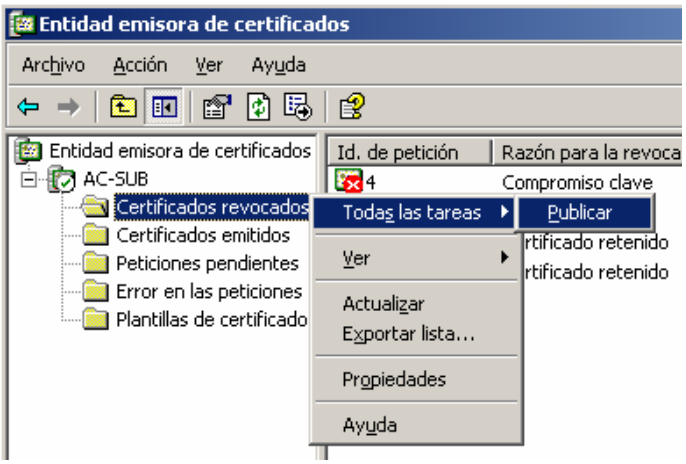

Figura 4.78 Publicación de CRLs

En el cuadro de diálogo que se presenta se selecciona la opción **Lista de revocación de certificados nueva** si se desea publicar una CRL completa, caso contrario se elige la opción **Sólo diferencias entre listas CRL** para publicar una versión delta, luego se da un clic en **Aceptar**.

Para publicar una CRL mediante la interfaz de comandos, se ingresa la siguiente línea: *certutil -CRL* para CRLs completas y *certutil -CRL delta* para actualizaciones.

4.7. PRESUPUESTO REFERENCIAL

La implementación de una PKI jerárquica requiere de la adquisición de un servidor de certificados por cada AC dentro de la PKI, y cada servidor requiere la compra de una licencia del sistema operativo *Windows 2003 Server Enterprise*.

La solución planteada contempla la instalación de una PKI jerárquica de dos niveles; la AC-Raíz puede emitir certificados a 25 (CALs) entidades subordinadas y la AC subordinada puede generar certificados para 25 (CALs) entidades destino.

El presupuesto referencial planteado contempla la adquisición de un servidor tipo *rack* para la AC-Raíz, debido a que éste permanecerá bajo custodia; para la AC subordinada se elige un servidor tipo torre.

Proveedor[1]	Servidor tipo Torre		Servidor tipo *Rack*	
	Modelo	Costo [$]	Modelo	Costo [$][2]
HP	*ProLiant* ML350 G4	2634[3]	DL320 G4 SATA	1866[4]
IBM	IBM *xSeries* 236 8841MC1	3222[5]	*xSeries* 306m 8491MC1	2118[6]
Sun	SUN *Netra* 210 *Small*	4126[7]	SUN *Fire* 4100 1 *Model* 248	2182[8]

Tabla 4.7 Comparación de Costos: HP, IBM y Sun Microsystems[9]

Para la compra de los servidores se escoge como proveedor a HP (*Hewlett-Packard*), debido a que al comparar los costos entre servidores de características semejantes, HP presenta una ventaja en comparación con sus competidores *Sun Microsystems* e IBM, tal como se muestra en la tabla 4.7.

Las características de los dos servidores han sido seleccionadas para que éstos puedan atender hasta 75[10] usuarios a la vez; sin embargo, el servidor tipo torre posee mejores características debido a que la AC subordinada brindará servicios de

---

[1] Las características de los servidores HP e IBM son las registradas en la tabla 4.9; en el caso de los servidores *Sun* se ha seleccionado servidores con capacidades equivalentes.

[2] Estos precios no incluyen la fuente redundante.

[3] http://h71016.www7.hp.com/dstore/MiddleFrame.asp?view=all&oi=E9CED&BEID=19701&SBLID=&AirTime=False&BaseId=14289&FamilyID=2105&ProductLineID=431.

[4] http://h71016.www7.hp.com/dstore/MiddleFrame.asp?view=all&oi=E9CED&BEID=19701&SBLID=&AirTime=False&BaseId=17998&FamilyID=2296&ProductLineID=431.

[5] http://www-03.ibm.com/systems/x/tower/index.html.

[6] http://www-03.ibm.com/systems/x/rack/index.html.

[7] http://store.sun.com/CMTemplate/CEServlet?process=SunStore&cmdViewProduct_CP&catid=146679.

[8] http://store.sun.com/CMTemplate/CEServlet?process=SunStore&cmdViewProduct_CP&catid=138712.

[9] Estos precios no incluyen impuestos ni transporte.

[10] http://www.hp.com/cgi-bin/sbso/buyguides/tsg_product_select.cgi.

certificación de manera continua. Los dos servidores poseen adicionalmente un sistema de fuente redundante para garantizar un nivel elevado de disponibilidad.

PKI JERÁRQUICA[1]					
#	Tipo	Descripción	Cantidad	Precio Unitario	Precio Total
1	Sistema Operativo	***Windows 2003 Server Enterprise R2*** **Edition**: Versión 32-bit. Incluye 25 CALs.	2	$ 3999[2]	$ 7998
2	AC-Raíz	**HP ProLiant DL320 G4 SATA[3] Tipo *Rack*** **# Usuarios**: 75 **Procesador**: Intel® Pentium® D 930 3.00GHz **Disco Duro**: HP 160 GB SATA 7,200 rpm **RAM**: 1GB **NIC**[4] : NC324i Dual Port 10/100/1000T Gigabit **Floppy drive**: 1.44MB **Monitor**: HP s7540 17'' **DVD-RW**: HP **Fuente**: Redundante **Garantía**: 3 años en partes, 1 año mano de obra y 1 año soporte en sitio.	1	$ 2119	$ 2119
3	AC-Sub.	**HP ProLiant ML350 G4p Tipo Torre** **# Usuarios**: 75 **Procesador**: Intel® Xeon™ 3.40GHz **RAM**: 2GB **Disco Duro**: HP 72.8 GB SCSI 15,000 rpm **NIC** (2): PCI 10/100/1000T Gigabit **CD-ROM/DVD**: 48X IDE (ATAPI) **Floppy drive**: 1.44MB **Monitor**: HP s7540 17'' **Fuente**: Redundante **Garantía**: 3 años en partes, mano de obra y soporte en sitio.	1	$ 2634	$ 2634
4	Instalación de Equipos	Instalación de servidores.	1 HT[5]	$ 50	$ 50
5	Configuración	Configuración AC-Raíz y AC-Subordinada.	4 HT	$ 50	$ 200
					$ 13001

Tabla 4.8 Presupuesto final para una PKI Jerárquica: AC-Raíz y AC-Subordinada[6]

En la tabla 4.8 se muestra un desglose del presupuesto referencial final de la solución de una PKI jerárquica de dos niveles; el presupuesto considera la compra de licencias, servidores y los costos de mano de obra por la instalación y configuración de los servidores de certificados.

---

[1] Este presupuesto no incluye los equipos clientes.

[2] http://www.microsoft.com/windowsserver2003/howtobuy/licensing/pricing.mspx.

[3] *Serial Advanced Technology Attachment*.

[4] *Network Interface Card*.

[5] Horas técnicas.

[6] Este presupuesto no incluye impuestos ni transporte.

Como se puede observar, en el caso de las garantías, HP proporciona para los dos servidores una garantía de 3 años en partes. El servidor tipo torre posee además una garantía de 3 años en mano de obra y soporte en sitio.

Para el servidor tipo *rack*, HP entrega un año de garantía en mano de obra y soporte en sitio. No se adquiere un soporte técnico adicional para este servidor debido a que el mantenimiento de la AC-Raíz no requiere de personal externo a la empresa.

Cada AC subordinada adicional incrementa el presupuesto en $ 6758; por otro lado, si se requiere que más clientes accedan a los servicios del servidor de certificados de la AC subordinada, un paquete adicional con 20 CALs, tiene un costo de 799 dólares.

4.8. POLÍTICAS Y PROCEDIMIENTOS PARA EL CONTROL DE LA OPERACIÓN DE LA AUTORIDAD CERTIFICADORA RAÍZ

En una empresa, el control de la operación de los servidores debe estar contemplado dentro de su política de seguridad; sin embargo, las CP y CPS de la PKI empresarial, deben incluir regulaciones específicas para el aseguramiento del servidor de certificados de la AC-Raíz.

La CP y CPS se han desarrollado de forma independiente en los Anexos 5 y 6, respectivamente, con el objetivo de mantener el formato establecido en el RFC 3647 para el desarrollo de CPs y CPSs; sin embargo, en esta sección se exponen los puntos relacionados con el control de la operación del servidor de certificados de la AC-Raíz.

4.8.1. CONTROLES DE SEGURIDAD FÍSICA

Los controles de seguridad física expuestos en esta sección están relacionados con el control de acceso al servidor de certificados de la AC-Raíz.

- **Ubicación, Construcción y Acceso Físico**.- El servidor de la AC-RAÍZ debe almacenarse bajo custodia en la bóveda de la empresa y su disponibilidad está supeditada a eventos planificados. La construcción de la bóveda debe mantener niveles adecuados de solidez en la cimentación, manteniendo un sistema a prueba de incendios.

- ***Backup***.- El respaldo de la base de datos y las claves de la AC-RAÍZ deben realizarse después de cada evento planificado; este procedimiento está a cargo del Administrador de IT de la empresa propietaria de la PKI.

4.8.2. CONTROLES DE PROCEDIMIENTOS

El administrador del departamento de IT es el encargado de la operación de la AC-RAÍZ, esto implica la planificación de eventos de emisión de certificados y CRLs para las ACs subordinadas.

- **Alteración de los Recursos *Hardware*, *Software* y/o Datos**.- En caso de percibir comportamientos anómalos del *software* o *hardware* que solventan el funcionamiento del servidor de certificados de la AC-RAÍZ, se debe respaldar la base de datos y las claves de la AC.

  Cuando todos los respaldos estén protegidos, se debe realizar una inspección para localizar la falla y corregirla. Si luego de las reparaciones se considera necesaria la reinstalación de la AC, se debe proceder de inmediato.

- **La Clave Privada se Compromete**.- Si se llega a revocar el certificado de la AC-Raíz por compromiso de clave, el certificado se debe retirar de la lista de ACs raíz de confianza del dominio, luego se debe detener la ejecución de la AC y se realiza una nueva instalación.

Todos los certificados emitidos por la AC o sus subordinadas deben revocarse antes de revocar el certificado de la AC; la AR correspondiente es la responsable de notificar a todos los usuarios afectados.

Las CRLs publicadas por la AC-Raíz eliminada deben permanecer en el directorio hasta que todos los certificados registrados en éstas hayan cumplido su período de validez, luego de esto se pueden retirar del directorio.

4.9. POLÍTICAS Y PROCEDIMIENTOS PARA EL MANEJO DE CERTIFICADOS DIGITALES IMPLEMENTACIÓN RAÍZ

Las políticas de certificación de la AC-Raíz se incluyen en la CP de la PKI; por otro lado, los procedimientos concernientes al manejo de certificados digitales están registrados en la CPS relacionada con la CP.

La CP y CPS se han desarrollado de forma independiente en los Anexos 5 y 6, respectivamente, con el objetivo de mantener el formato establecido en el RFC 3647 para el desarrollo de CPs y CPSs.

En los Anexos 5 y 6 se encontrará que la sección variable (a.b.c.d.e.f) del OID de la CPS no coincide con el OID generado a partir del GUID; este cambio se ha realizado con el afán de facilitar su lectura. En el caso de la CP se ha asignado el OID: 1.3.6.1.4.1.311.21.8.**0.0.0.2.1.0.**1.402 [1] y para la CPS se ha asignado el OID: 1.3.6.1.4.1.311.21.8.**0.0.0.3.1.0.**1.402 [2]. La CP y CPS poseen nueve temas, a continuación se presenta un resumen de cada uno.

---

[1] *iso.org.dod.intenet.private.enterprises.microsoft.certsrv.oidenterprisesroot.0.0.0.**cp-acsw.v1.0**.assurance.high*.

[2] *iso.org.dod.intenet.private.enterprises.microsoft.certsrv.oidenterprisesroot.0.0.0.**cps-acsw.v1.0**.assurance.high*.

- **Introducción**.- En esta sección de exponen las definiciones de cada elemento de la PKI e información de los usos permitidos para los certificados emitidos dentro de la PKI.

- **Publicación de información y directorio**.- Esta sección contiene información relacionada con la publicación y actualización de CP, CPS, CRLs y certificados de las ACs de la PKI.

- **Identificación y Autenticación**.- Esta sección especifica los métodos utilizados para la identificación y registro de las entidades destino y ACs subordinadas dentro de la PKI.

- **Ciclo de Vida de los Certificados**.- Esta sección contiene información sobre los procesos de solicitud, emisión, renovación, revocación y suspensión de certificados.

- **Controles de: Seguridad Física, Gestión y Operación**.- Esta sección define mecanismos de control de acceso y administración de los servidores de certificados.

- **Controles de Seguridad Técnica**.- Esta sección contiene información de los parámetros utilizados para la generación de los certificados digitales, incluyendo longitudes de claves, algoritmos y aspectos relacionados con la administración de la pareja de claves.

- **Perfiles de Certificados y CRLs**.- Esta sección hace referencia a los estándares y versiones utilizadas para la generación de certificados digitales y listas de revocación de certificados.

- **Auditoría de Conformidad**.- Esta sección contiene información sobre los parámetros a considerar para la realización de una auditoría a la PKI por una entidad externa a la empresa propietaria de la PKI.

- **Requisitos Comerciales y Legales**.- Esta sección está relacionada con tarifas, clasificación de documentos confidenciales y no confidenciales, propiedad intelectual, obligaciones de las entidades de la PKI y legislación aplicable a los certificados emitidos.

4.10. POLÍTICAS Y PROCEDIMIENTOS PARA EL CONTROL DE LA OPERACIÓN DE LA AUTORIDAD CERTIFICADORA SUBORDINADA

Como se dijo anteriormente, en una empresa el control de la operación de los servidores debe estar contemplado dentro de su política de seguridad; sin embargo, las CP y CPS de la PKI empresarial, deben incluir consideraciones específicas para el aseguramiento del servidor de certificados de una AC-SUB.

La CP y CPS se han desarrollado de forma independiente en los Anexos 5 y 6, respectivamente, con el objetivo de mantener el formato establecido en el RFC 3647 para el desarrollo de CPs y CPSs; sin embargo, en esta sección se exponen los puntos relacionados con el control de la operación del servidor de certificados de una AC-SUB.

4.10.1. CONTROLES DE SEGURIDAD FÍSICA

Los controles de seguridad física expuestos en esta sección están relacionados con el control de acceso al servidor de certificados de la AC-SUB.

4.10.1.1. Ubicación, Construcción y Acceso Físico

Los servidores de certificados de las ACs subordinadas deben ubicarse en el Centro de Seguridad Informática de cada sucursal de la empresa propietaria de la PKI; la

construcción de estos locales debe mantener niveles adecuados de solidez en la cimentación y un régimen de vigilancia.

La red de cada sucursal debe dividirse en diferentes perímetros de seguridad; cada perímetro debe tener niveles razonables de seguridad de acuerdo a sus características y requerimientos.

El servidor de certificados de una AC-SUB, debe ubicarse en el perímetro con mayor nivel de seguridad, para acceder a éste se puede establecer un sistema de autenticación factor 2 para permitir que sólo los administradores tengan acceso al servidor.

4.10.1.2. Alimentación Eléctrica y Aire Acondicionado

La instalación de los sistemas de alimentación debe diseñarse para brindar servicio de manera ininterrumpida; además, debe incluir un sistema de puesta a tierra para proteger los equipos frente a fluctuaciones eléctricas.

El sistema de ventilación debe tener la capacidad de suministrar niveles de temperatura y humedad óptimos para la operación de los sistemas las 24 horas del día durante los 365 días del año. Los niveles de temperatura deben mantenerse entre 64 y 75 grados Fahrenheit. Por otra parte, se debe mantener entre 30% y 55% de humedad[1].

4.10.1.3. Exposición al Agua

Los centros de seguridad informática deben estar dotados de detectores de inundación, si éstos detectan anomalías en el medio, deben activar una alarma.

---

[1] ANSI/TIA/EIA (*American National Standards Institute /Telecomunications Industries Association/ Electronics Industries Association*). *Technical Information*: ANSI/TIA/EIA-569-A. 2005.

4.10.1.4. Protección y Prevención de Incendios

Todos los centros de seguridad informática deben contar con armarios ignífugos y un sistema a prueba de incendios; de presentarse un siniestro, el sistema debe activar una alarma.

4.10.1.5. *Backup*

El respaldo de las bases de datos y claves de las ACs subordinadas debe guardarse una vez por mes, este procedimiento está a cargo del Administrador de AC de cada sucursal.

4.10.2. CONTROLES DE PROCEDIMIENTOS

El administrador de AC de cada sucursal es el encargado de la operación de la AC-SUB, éste hace las funciones de solicitante ante el Administrador de IT cuando se requiere la generación de un certificado para la AC-SUB a su cargo. Por otro lado, debe realizar parte de las funciones de registro de los usuarios finales.

Adicionalmente, un administrador de AC está encargado de los procedimientos relacionados con la alteración de los recursos y el compromiso de la clave privada de la AC-SUB.

4.11. POLÍTICAS Y PROCEDIMIENTOS PARA EL MANEJO DE CERTIFICADOS DIGITALES IMPLEMENTACIÓN SUBORDINADA

Las políticas de certificación de la AC-SUB se incluyen en la CP de la PKI; por otro lado, los procedimientos concernientes al manejo de certificados digitales están registrados en la CPS relacionada con la CP.

Como se indicó anteriormente para mantener el formato establecido en el RFC 3647 para el desarrollo de CPs y CPSs, éstas se han desarrollado de forma independiente en los Anexos 5 y 6, respectivamente, los temas tratados en la CP y CPS fueron expuestos en la sección 4.9 de este capítulo.

En el Anexo 6 se incluye un formulario para la solicitud de certificados digitales, este formulario debe ser llenado por la entidad destino y presentado a la AR correspondiente durante el proceso de registro.

Finalmente, para definir un acuerdo entre la PKI-ACSW y el usuario propietario de un certificado, en el Anexo 6 se incluye un contrato de certificación relacionado con la CPS formulada.