ESCUELA POLITECNICA DEL EJÉRCITO

FACULTAD DE INGENIERIA EN SISTEMAS E INFORMATICA

ESTUDIO TECNICO PARA LA IMPLEMENTACIÓN DE UNA AUTORIDAD CERTIFICADORA PARA EL CTT – ESPE CECAI

Previa a la obtención del titulo de:

INGENIERO EN SISTEMAS E INFORMATICA

POR: **WILLIAM RAUL GARCIA MUÑOZ**
ANDRES VARGAS JURADO

SANGOLQUI, 18 ABRIL de 2005

INDICE DE CONTENIDOS

CAPITULO II

CAPITULO III

RESUMEN

En el documento de investigación que a continuación se desarrolla, se tratan temas fundamentales sobre las Autoridades emisoras de certificados, su implementación y administración acorde con los estándares internacionales. Brindando de esta manera una tercera parte de confianza que garantice la seguridad de la transacción.

El comercio electrónico, firmas de contratos virtuales, elaboración electrónica de documentos y demás figuras que impliquen transacción o negocio, toman como medio el uso de los certificados digitales como herramienta de validación.

Un mercado globalizado funcionando sobre Internet debe permitir la integridad de la información para prevenir la modificación deliberada o accidental de los datos firmados digitalmente durante su transporte, almacenamiento o manipulación.

Los certificados digitales y la firma electrónica son los instrumentos adecuados para evitar los fraudes en las operaciones electrónicas a través de Internet. El uso de estas tecnologías garantiza integridad, autenticidad y no repudio de la información, tanto de las entidades involucradas como de sus usuarios.

En este contexto, el CTT ESPE CECAI por medio de este proyecto toma la iniciativa con el fin de brindar soluciones de seguridad mediante la implementación de una Autoridad emisora de certificados digitales, generando de esta manera una oportunidad de negocio y prestando servicios al desarrollo del país en materia de seguridad informática.

CAPITULO I

MARCO TEORICO

1.1- Seguridades en la Web

1.1.1- Complejidad de las medidas de seguridad

La seguridad de redes y comunicaciones alcanza actualmente niveles de alta complejidad. La mayor parte de los requisitos que se le exigen a la seguridad parecen resultar muy claros, y se los designa con términos que por sí solos darían la explicación de su contenido: confidencialidad, autenticación, no repudio, integridad. A pesar de estos términos casi descriptivos alcanzar dichos requerimientos puede ser muy complejo, y su comprensión requiere de razonamientos especiales.

Para todo nuevo mecanismo de seguridad debemos considerar una potencial amenaza o medida en contra. En la mayoría de los casos la forma de descubrir fallas es simulando ataques, explotando alguna debilidad no contemplada o simplemente enfocando el problema de diferente manera.

Debemos considerar que la existencia de un requerimiento no implica el diseño de una contramedida. El hecho de que exista un determinado requerimiento no implica que se necesite la elaboración de una medida que lo satisfaga. Sólo cuando las diversas contramedidas tienen una entidad suficiente como para ser consideradas, se entiende que las medidas utilizadas tienen sentido.

Con tanta diversidad de mecanismos de seguridad, se hace necesario decidir dónde utilizarlos.

Se debe determinar ubicación física (por ejemplo, en qué puntos de una red se necesitan ciertos mecanismos de seguridad), y de lógica (por ejemplo, en qué capa - layer o layers - de una arquitectura como TCP/IP deberían ubicarse los mecanismos).

1.1.2- Information Security

Comprende tres aspectos fundamentales, de los cuales se desprenden los productos de seguridad:

- Servicios
- Mecanismos
- Ataques

1.1.2.1- Servicios

Son aquellos que procuran la seguridad de los sistemas de procesamiento de datos y la transferencia de información.

1.1.2.1.1- Confidencialidad

Es un servicio de seguridad que tiene como meta asegurar que el contenido del mensaje no ha sido revelado a terceros, es decir que se oculta los datos frente a accesos no autorizados. La confidencialidad, a veces denominada secreto o privacidad, se refiere a la capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él.

En áreas de seguridad gubernamentales el secreto asegura que los usuarios pueden acceder a la información que les está permitida en base a su grado o nivel de autoridad,

normalmente impuestas por disposiciones legales o administrativas. En entornos de negocios, la confidencialidad asegura la protección en base a disposiciones legales o criterios estratégicos de información privada, estableciendo acceso a datos tales como: las nóminas de los empleados, documentos internos sobre estrategias, nuevos productos o campañas, etc. Este aspecto de la seguridad es particularmente importante cuando hablamos de organismos públicos, y más concretamente aquellos relacionados con la defensa.

Algunos de los mecanismos utilizados para salvaguardar la confidencialidad de los datos son:

- El uso de técnicas de control de acceso a los sistemas.
- El cifrado de la información confidencial o de las comunicaciones.

Un objetivo primario en la administración de cualquier sistema de Seguridad de PCs y Redes es la conservación de la confidencialidad.

Extensos estudios han demostrado el peligro que sufre la información que proviene de las personas que la utilizan, esto puede deberse a personal insatisfecho, el mismo que altera la información o atenta contra su contenido causando perdidas económicas e impacto en la productividad. Es este contexto es de vital importancia identificar a los usuarios y restringir el acceso, mediante claves, tokens electrónicos, tarjetas inteligentes o medios biométricos.

Entonces surge la pregunta. ¿Cuánto tiempo deberá protegerse la información? Un principio de seguridad informática determina que *"Los datos confidenciales deben protegerse sólo hasta que ese secreto pierda su valor".* Se habla, por tanto, de la

caducidad del sistema de protección, es decir tiempo en el que debe mantenerse la confidencialidad o secreto del dato.

1.1.2.1.2- Autenticación

Autenticación es un servicio que permite verificar que dos personas que intervienen en el proceso de comunicación son las que dicen ser. Se trata de proporcionar los medios para verificar que el origen de los datos es el correcto, quién los envió y cuándo fueron enviados y recibidos.

En el campo de la criptografía hay diversos métodos para mantener o asegurar la autenticidad de los mensajes y la precisión de los datos recibidos. Se usan para ello códigos o firmas añadidos a los mensajes en origen y recalculadas o comprobadas en el destino.

El método más usado para proporcionar autenticidad es la firma digital, basada, en la criptografía.

La autenticación permite que usuarios se autentiquen a sí mismos y comprueben la autenticidad de otros, pero también debe permitirse que sistemas informáticos (servidores) se autentiquen entre sí y ante una petición de un usuario.

La autenticación mediante contraseña es el sistema más común ya que viene incorporado en los sistemas operativos modernos de todos los ordenadores, y en tal virtud aquellos ordenadores que estén preparados para la autenticación mediante dispositivo, sólo

reconocerán al usuario mientras mantenga introducida una "llave", que normalmente una tarjeta con chip. [1]

Los dispositivos biométricos son un caso especial del anterior, en los que la "llave" es una parte del cuerpo del usuario, huella dactilar, voz, pupila o iris. [2]

En resumen, con el servicio de autenticación se busca:

- Protección contra agresiones activas
  - Falsificación de datos y transacciones
- Funciones que proporcionan autenticación
  - Encriptación de mensajes
  - Códigos de autenticación de mensajes (MAC)
  - Funciones hash
- Protocolos
  - Kerberos
  - X509

1.1.2.1.3- Integridad

Es otro servicio de seguridad que garantiza que la información pueda ser modificada, creada y eliminada sólo por personal autorizado, teniendo por objetivo asegurar que la información almacenada o circulante no pueda ser corrompida ni falseada ya sea intencional o accidentalmente.

[1] Hay sistemas de generación de claves asimétricas que introducen la clave privada en el chip de una tarjeta inteligente.

[2] Existen ya en el mercado a precios relativamente económicos ratones que llevan incorporado un lector de huellas dactilares

El concepto de integridad significa que el sistema no debe modificar o corromper la información que almacene, o permitir que alguien no autorizado lo haga. Esta propiedad permite asegurar que no se ha falseado la información, es decir, que los datos recibidos o recuperados son exactamente los que fueron enviados o almacenados, sin que se haya producido ninguna modificación, adición o borrado. De hecho el problema de la integridad no sólo se refiere a modificaciones intencionales, sino también a cambios accidentales o no intencionados.

En el entorno financiero o bancario, este aspecto de la seguridad es el más importante. En los bancos cuando se realizan transferencias de fondos u otros tipos de transacciones, normalmente es más importante mantener la integridad y precisión de los datos que evitar que sean interceptados o conocidos.

1.1.2.1.4- Disponibilidad

Disponibilidad significa que el sistema, tanto hardware como software, se mantienen funcionando eficientemente y que es capaz de recuperarse rápidamente en caso de fallo, manteniendo la información disponible para los usuarios.

1.1.2.1.5- No Repudio

También llamada “imposibilidad de rechazo”. Este servicio permite asegurar que cualquier entidad que envía o recibe información, no puede alegar ante terceros que no la envió o la recibió. Esta propiedad es especialmente importante en el entorno bancario y en el uso del comercio digital.

1.1.2.1.5.1- Detalle Técnico

Tres partes están involucradas en el esquema actual de "No repudio": El emisor, el receptor y el certificador del mensaje.

a) El emisor crea un mensaje y agrega una encriptación de llave pública al mensaje.
b) El emisor transmite el mensaje en la red hacia el certificador.
c) El certificador verifica la firma del emisor e identifica los datos.
d) El certificador incorpora una estampilla de tiempo al mensaje y lo firma.
e) Posteriormente el mensaje es enviado al emisor y al receptor.
f) El receptor verifica la firma del certificador y la del emisor.
g) El emisor verifica el mensaje transmitido por el certificador con la copia originalmente enviada.
h) El certificador guarda los eventos de caducidad o claves secretas usadas en el proceso de verificación.

Esta tecnología asegura al receptor, que el mensaje vino de la fuente indicada y graba un evento de tiempo que indica cuando se envío dicha información. El emisor no puede negar el envío del mensaje ni tampoco asumir pérdida o robo de la clave criptográfica.

1.1.2.1.5.2- Costos y limitaciones

El uso de esta tecnología requiere conocimiento de algoritmos de firma digital, encriptación de llave publica, algoritmos hash y formas de proteger las claves de posible robo o uso malintencionado.

1.1.2.1.5.3- Dependencias

El uso exitoso de esta tecnología requiere la generación y distribución de llaves públicas y generación y protección de llaves secretas o privadas.

1.1.2.2- Mecanismos y tipos

Los mecanismos de seguridad son aquellos que se emplean para detectar, prevenir o recuperarse de un ataque activo o pasivo.

Cada mecanismo puede proveer uno o varios de los servicios de seguridad requeridos por un usuario, pero un solo mecanismo no puede proveer todos los servicios al mismo tiempo, salvo las técnicas criptográficas.

Los tipos de mecanismos son los siguientes:

- Intercambio de autenticación
- Cifrado
- Firma digital
- Control de acceso
- Tráfico de relleno
- Control de encaminamiento
- Unicidad

1.1.2.2.1.- Intercambio de autenticación

Es un mecanismo que corrobora que una entidad, origen/destino, es la deseada, existen dos grados en el mecanismo de autenticación:

- *Autenticación simple*- El emisor envía su nombre distintivo y una contraseña al receptor, quien los comprueba.
- *Autenticación fuerte*- Utiliza las propiedades de los criptosistemas de clave pública. Cada usuario se identifica por un nombre distintivo y por su clave secreta. Cuando un segundo usuario desea comprobar la autenticidad de su interlocutor, habrá de asegurarse que aquel está en posesión de su clave secreta, para lo cual deberá obtener su clave pública. Para que un usuario confíe en el procedimiento de autenticación, la clave pública de su interlocutor se tiene que obtener de una fuente de confianza, a la que se denomina Autoridad de Certificación. La Autoridad de Certificación utiliza un algoritmo de clave pública para certificar la clave pública de un usuario produciendo así un certificado. [3]

El mecanismo de intercambio de autenticación se utiliza para soportar el servicio de autenticación de entidad par.

[3] Un certificado es un documento firmado por una Autoridad de Certificación, válido durante el período de tiempo indicado, que asocia una clave pública a un usuario

1.1.2.2.- Cifrado

1.1.2.2.1- Introducción

El cifrado es una técnica que autentifica un documento o usuarios aplicando algoritmos criptográficos, es decir que sin una clave no se podrá tener acceso a dicho documento.

Sea cual sea el medio de transmisión (enlace, red telefónica, red de datos, disco magnético, disco óptico, etc.) éste será siempre y por definición inseguro y habrá que adaptarse a este medio. Esto podría dejar de ser cierto en los futuros sistemas con criptografía cuántica.[4]

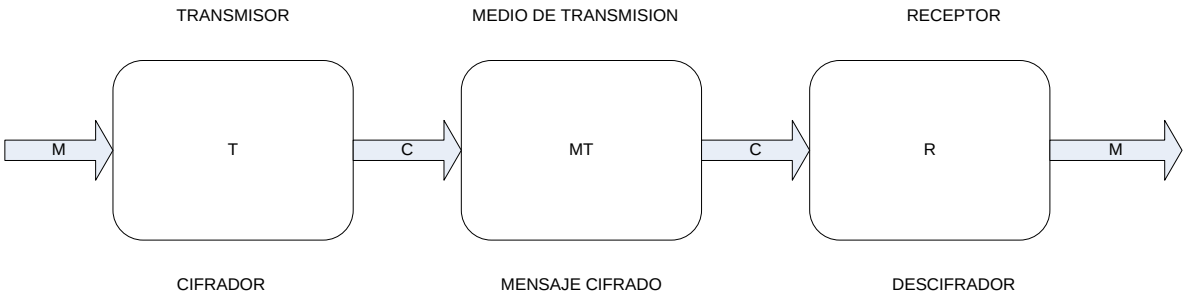

Figura 1.1: Sistema de cifrado

[4] La criptografía cuántica se basa en el principio de incertidumbre de Heisenberg, que de forma básica, dice que no se puede conocer con exactitud la posición y la velocidad de una partícula. Cuanto más exactamente se conoce una variable, menos concretamente se sabe el valor de la otra. Según este principio, es imposible saber en cuál de las cuatro direcciones posibles (vertical, horizontal, diagonal izquierda o diagonal derecha) está polarizado un fotón (partícula de luz), base de la criptografía cuántica

1.1.2.2.2.2- Tipos

1.1.2.2.2.2.1- Cifrado en bloque

El mismo algoritmo de cifra se aplica a un bloque de información (grupo de caracteres, número de bytes, etc.) repetidas veces, usando la misma clave. El bloque será normalmente de 64 ó 128 bits.

1.1.2.2.2.2.2- Cifrado en flujo

El algoritmo de cifra se aplica a un elemento de información (carácter, bit) mediante un flujo de clave en teoría aleatoria y mayor que el mensaje. La cifra se hace bit a bit.

Cuadro 1.1: Ventajas y desventajas del cifrado por bloques y cifrado por flujo

TIPO DE CIFRADO	VENTAJAS	DESVENTAJAS
CIFRADO EN BLOQUE	▪ Alta difusión de los elementos en el criptograma ▪ Inmune: Imposible traducir bloques extraños sin detectarlo	▪ Baja Velocidad de cifrado al tener que leer antes el bloque completo. ▪ Propenso a errores de cifra. Un error se propagará a todo el bloque
CIFRADO EN FLUJO	▪ Alta velocidad de cifra al no tener en cuenta otros elementos	▪ Baja Difusión de elementos en el criptograma ▪ Vulnerable. Puede alterarse los elementos por separado.

1.1.2.2.2.3- Cifrado por capa

1.1.2.2.2.3.1- Cifrado de enlace

En este caso el cifrado se realiza en la capa física. Para ello se utiliza una unidad de puesta en clave o cifrado entre cada ordenador, participante de la comunicación, y el medio físico, de manera que cada bit que sale de la máquina emisora sufre un proceso de cifrado, y a cada bit que entra en la máquina receptora se le practica el proceso inverso.

La ventaja del cifrado de enlace es que tanto las cabeceras como los datos se cifran.

1.1.2.2.2.3.2- Cifrado en transporte

Si introducimos el cifrado en la capa de transporte el efecto inmediato es que el cifrado se realice en la sesión completa. Se entiende que este cifrado tan general, conlleva una sobrecarga de trabajo de cifrado y que en muchas ocasiones será innecesario para algunos de los datos cifrados.

1.1.2.2.2.3.3- Cifrado en presentación

Es quizás una solución más elaborada ya que el cifrado es sufrido sólo por aquellas partes de los datos que sean consideradas necesarias, consiguiendo de este modo que la sobrecarga del proceso de cifrado sea menor.

1.1.2.2.2.4- Cifrado con claves privadas

Esta técnica convierte el texto normal en algo ininteligible, por medio de algún esquema reversible de codificación desarrollado en torno a un clave privada que sólo conocen el emisor y el receptor.

El proceso inverso es el descifrado, mediante el cual el texto en clave vuelve a convertirse en texto legible. El cifrado suele tener lugar en el emisor, mientras que el descifrado suele realizarse en el receptor.

El cifrado con claves públicas se clasifica en dos tipos: Cifrado por sustitución y cifrado por transposición.

1.1.2.2.2.4.1- Sustitución

Es la forma más sencilla de cifrado. Consiste en reemplazar una letra o un grupo de letras del original por otra letra o grupo de letras.

Uno de los esquemas más sencillos es el *Cifrado De César*, en este mecanismo cada letra del alfabeto es sustituida por otra.

Cuadro 1.3: Ejemplo de cifrado por sustitución

Texto legible	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Letras de sustitución	FGQRASEPTHUIBVJWKLXYZCONMD

Este tipo descifrado se conoce como *sustitución mono alfabética*, ya que cada una de las letras se sustituye por otra del mismo alfabeto.

Aunque este método ofrece 4x1026 claves distintas, la propia clave puede revelar bastante sobre la inteligibilidad del mensaje. Si no se conocen las claves, o si éstas no presentan ninguna regularidad, se calcula que un ordenador tardaría 1013 años en probar con todas las claves, si se dedica un microsegundo a probar con cada clave. Sin embargo, los lenguajes presentan ciertas propiedades que permiten descifrar mucho más rápido.

La principal desventaja de todas las estructuras basadas en una clave privada es que todos los nodos de la red han de conocer cuál es la clave común. La distribución y confidencialidad de las claves acarrea algunos problemas administrativos y logísticos, si se considera que los nodos de la red cambian la clave periódicamente; por ejemplo, cada 24 horas, o incluso, si es necesario, cada pocos minutos.

Hasta hace poco, la idea de una clave privada era el esquema de cifrado predominante en las redes.

1.1.2.2.2.4.2- Transposición

Es un método criptográfico más sofisticado, en él que las claves de las letras se reordenan, pero no se disfrazan necesariamente.

Ejemplo: La clave utilizada: "SEGURIDAD"

Texto a Cifrar: "*compra barato vende caro y hazlo hoy"*

Tabla 1.1: Ejemplo de texto cifrado por el método de transposición

S	**E**	**G**	**U**	**R**	**I**	**D**	**A**	**D**
8	4	5	9	7	6	2	1	3
C	O	M	P	R	A	B	A	R
A	T	O	V	E	N	D	E	C
A	R	O	Y	H	A	Z	L	O
H	O	Y	A	B	C	D	E	F

Y el texto cifrado será el siguiente:

AELEBDZDRCOFOTROMOOYANACREHBCAAHPVYA

1.1.2.2.2.5 Cifrado con claves públicas

Muchos sistemas comerciales emplean métodos de cifrado/descifrado basados en claves públicas. Este sistema está basado en el uso de claves independientemente para el cifrado y para el descifrado de los datos. La particularidad y enorme ventaja es que la clave y el algoritmo de cifrado pueden ser de dominio público, siendo la clave de descifrado la que se mantiene en secreto. Este método elimina los problemas logísticos y administrativos relacionados con la distribución y gestión de las claves públicas.

Los métodos inventados en la Universidad de Stanford y en el MIT incluyen la generación de un par de enteros positivos **"E y N"** que se usan para cifrar los datos, según la fórmula $\boldsymbol{textolegible^{E}/N = textocifrado}$.

El mismo proceso que genera E y N da como resultado el valor D, que se emplea para descifrar, según la fórmula: $\boldsymbol{textocifrado^{D}/N = textolegible}$.

Los enteros E, N y D se calculan generando dos grandes números aleatorios primos.

Los sistemas basados en claves públicas no son tampoco infalibles ya que también pueden romperse. En cualquier caso, y para evitar que la clave pueda ser detectada, es posible generar una clave distinta para cada transmisión, o de una forma más realista, a intervalos periódicos o aleatorios. El cambio de clave frecuente aumenta la seguridad de las transmisiones, ya que el posible intruso deberá intentar romper la clave cada vez que ésta cambia. Puede incluso añadirse otro nivel de seguridad, utilizando un sistema de claves privadas para cifrar las claves públicas, es decir, pueden emplearse dos niveles de cifrado para los datos más delicados.

1.1.2.2.3- Firma digital

Esta técnica es utilizada tanto para la autenticación como para el mantenimiento de la integridad y la auditoria.

Las firmas digitales son métodos de cifrado que tienen dos propósitos:

- **Validar el contenido:** de un mensaje electrónico y se puede utilizar posteriormente para comprobar que un emisor envió de hecho ese mensaje.
- **Probar que no se ha falsificado un mensaje durante su envío**. Las firmas digitales respaldan la autenticidad del correo electrónico, transacciones de contabilidad, órdenes de empresa, documentos para grupos de trabajo y otros mensajes y archivos que se trasladan entre sistemas, usuarios u organizaciones.

Las firmas digitales se basan en el hecho de que dos grupos pueden autentificarse el uno al otro para el intercambio seguro de documentos, pero la relación entre ellos no se basa en una confianza total. [5]

Las firmas digitales autentifican los mensajes y se usan para validar compras, transferencias de fondos y otras transacciones de negocios. Un formulario con una firma digital debe incluir el nombre del emisor, la fecha y hora, junto con una secuencia numérica o identificación que identifique positivamente a la persona o a la transmisión.

---

[5] Una persona podría enviar un mensaje para apostar a un caballo de carreras, si el caballo pierde, la persona puede negar haber enviado dicho mensaje. Aunque se sabe a través del proceso de autenticación que esta persona realmente envió ese mensaje, sin una firma digital no se podría probar técnicamente que el mensaje no se modificó. El emisor podría decir, "sí, yo le mandé un mensaje, pero usted lo cambió"

Procedimiento que usa cifrado de clave pública con firma digital:

a) El emisor crea la firma digital con el uso de su clave privada, con la que cifra la información de identificación en el documento.
b) Antes de enviar el mensaje, el emisor cifra todo el documento de nuevo con el uso de la clave pública del receptor. Ahora el mensaje original cifrado se incrusta en el documento nuevamente cifrado.
c) El mensaje se envía al receptor que lo descifra con su clave.
d) El primer cifrado protege la firma y la información que identifica al emisor de la falsificación y proporciona una forma de autentificar el mensaje. El segundo cifrado protege la parte del texto o la información del documento que se transmite y permite que el receptor descifre y lea la información recibida.

La seguridad de una firma digital, como otros métodos de cifrado, se basa en un algoritmo matemático que asegura que dos firmas nunca son iguales.

Con los algoritmos de cifrado proporcionados por RSA Data Security la probabilidad de que por casualidad diferentes documentos tengan el mismo código es menor de 1 entre un billón de billones.

1.1.2.2.4- Control de Acceso

Este mecanismo se utiliza para autenticar las capacidades de una entidad, con el fin de asegurar los derechos de acceso a recursos que posee. El control de acceso se puede realizar en el origen o en un punto intermedio, y se encarga de asegurar si el emisor está autorizado a comunicar con el receptor y/o a usar los recursos de comunicación requeridos.

Si una entidad intenta acceder a un recurso no autorizado, o intenta el acceso de forma impropia a un recurso autorizado, entonces la función de control de acceso rechazará el intento, al tiempo que puede informar del incidente, con el propósito de generar una alarma y registrarlo.

Existen tradicionalmente dos tipos básicos de controles de acceso con filosofías diametralmente opuestas:

En el modelo de control de acceso discrecional (DAC), un usuario bien identificado (típicamente, el creador o 'propietario' del recurso) decide cómo protegerlo estableciendo cómo compartirlo, mediante controles de acceso impuestos por el sistema.

En el modelo de control de acceso mandatorio (MAC), es el sistema quién protege los recursos. Todo recurso del sistema, y todo principal (usuario o entidad del sistema que represente a un usuario) tienen una etiqueta de seguridad. Esta etiqueta de seguridad sigue el modelo de clasificación de la información militar, en donde la confidencialidad de la información es lo más relevante, formando lo que se conoce como política de seguridad multinivel. Una etiqueta de seguridad se compone de una clasificación o nivel de seguridad (número en un rango, o un conjunto de clasificaciones discretas, desde DESCLASIFICADO hasta ALTO SECRETO) y una o más categorías o compartimentos de seguridad (CONTABILIDAD, VENTAS, I+D...).

En este tipo de sistemas, todas las decisiones de seguridad las impone el sistema, comparando las etiquetas del usuario frente al recurso accedido.

Los modelos DAC y MAC son inadecuados para cubrir las necesidades de la mayor parte de las organizaciones.

El modelo DAC es demasiado débil para controlar el acceso a los recursos de información de forma efectiva, en tanto que el MAC es demasiado rígido. Desde los 80 se ha propuesto el modelo de control de accesos basado en roles (RBAC), como intento de unificar los modelos clásicos DAC y MAC, donde el sistema impone el control de accesos, pero sin las restricciones rígidas impuestas por las etiquetas de seguridad.

En la actualidad lo más visible y novedoso quizá sea el fenómeno PKI. En los negocios electrónicos se requiere controlar la seguridad en los accesos de usuarios bajo los que no se tiene control administrativo, como proveedores, clientes, consumidores.

La tecnología de clave pública ofrece grandes ventajas en cuanto a autenticación fuerte de usuarios (su combinación con dispositivos como las tarjetas inteligentes, de hecho, constituye el estado del arte en cuanto a autenticación de usuarios). Protocolos como SSL o IPSEC se apoyan en la PKI para ofrecer servicios añadidos de confidencialidad e integridad en las comunicaciones, aquí surge la pregunta ¿Que ofrecen las PKI en cuanto al control de accesos?.

La respuesta son los certificados de atributos. La idea es simple, los certificados de clave pública X.509 proporcionan evidencia de la identidad de una persona, pero en entornos de comercio electrónico, se precisa más información, en especial cuando las partes involucradas en una transacción no han tenido contacto previo.

En este caso, la información sobre los atributos de privilegio de una persona por ejemplo, su capacidad de firmar un contrato, o su límite de crédito es mucho más relevante que su mera identidad.

X.509 v3 introdujo el útil concepto de extensión. Lo más lógico pareció en ese momento añadir al certificado de identidad extensiones que recogieran estos atributos. Pero es como mezclar agua y aceite. Los atributos de privilegio cambian mucho más a menudo que la identidad de los individuos, lo cual obliga a revocar el certificado antiguo y emitir uno nuevo, esto se evidenciaba por ejemplo cuando se otorga un certificado al director de compras, y a continuación se le despide. Las extensiones dedicadas al control de accesos son propietarias, y dificultan la interoperabilidad.

La respuesta a estas dificultades es inmediata: ¿Por qué no dividir el certificado X.509 en dos, uno para la información de identidad (Certificado de identidad), y el otro para la información ligada con el control de accesos (Certificado de atributos)?. Esto simplifica el proceso de emisión ya que los certificados de atributos se emiten con una duración limitada, podría no ser necesaria su revocación, simplemente expiran.

¿Cuáles pueden ser los atributos encerrados en un certificado de esta clase?. Pueden ser roles, grupos, identidades de acceso o auditoria, restricciones, etc.

Por ejemplo, un atributo puede expresar el límite de crédito concedido a un determinado suscriptor a un servicio de tienda virtual. Las posibilidades son ilimitadas. Podemos contemplar así los certificados de atributos como un 'manojo de llaves' que se añaden a un certificado de identidad para abrir determinadas puertas.

Ejemplos de aplicaciones de esta tecnología son:

- *Servicios de suscripción:* Los usuarios se registrarían de forma gratuita, pero sólo obtendrían un certificado de atributos tras el pago de una cuota de suscripción. La duración del certificado correspondería a la de disfrute del servicio subscrito.

- *Control de accesos basado en roles a servicios en red cuya autenticación se realiza usando una PKI (Web, FTP, SMTP).* El protocolo SSL autentica al cliente; un certificado de atributos permite al servicio determinar qué puede hacer el usuario dentro del mismo.
- *Control de accesos a redes privadas virtuales (RPV).* Piénsese en los usuarios 'itinerantes' de una gran organización. En vez de mantener controles de acceso replicados en cada puerta de acceso RPV, mediante un servicio centralizado se concede al usuario un certificado de atributos que le franquee el acceso a través del puerto de acceso.
- *Sign-on único basado en autenticación fuerte mediante tarjeta* inteligente. Las credenciales necesarias para el acceso a aplicaciones (usuario / password) pueden ir cifradas en el certificado de atributos concedido al usuario tras el proceso de autenticación basado en la posesión de la clave privada en tarjeta inteligente.

1.1.2.3- Ataques

Todos los elementos de un sistema informático son vulnerables. Algunos tipos de vulnerabilidad pueden ser:

- *Natural:* Desastres naturales o ambientales.
- *Física:* Acceso físico a los equipos informáticos, a los medios de transmisión.
- *Lógica:* Programas o algoritmos que puedan alterar el almacenamiento, acceso, transmisión.
- *Humana:* Las personas que administran y utilizan el sistema constituyen la mayor vulnerabilidad del sistema.

1.1.2.3.1- Ataques Activos

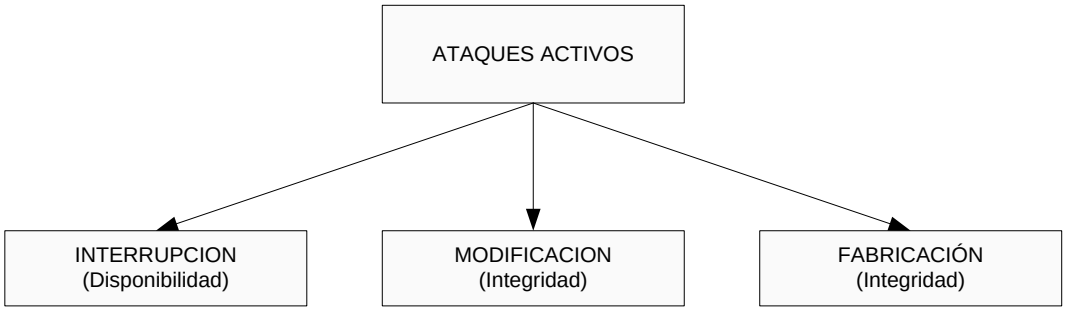

Figura1.2: Ataques activos

1.1.2.3.1.1- Interrupción

Destruye información o la inutiliza. Ataca la accesibilidad o disponibilidad

Ejemplo: Destruir algún dispositivo. Saturar la capacidad del procesador.

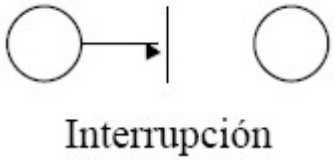

Figura1.3: Ataque (Interrupción)

1.1.2.3.1.2- Modificación

Una parte no autorizada modifica el bien. Ataque a la integridad.

Ejemplo: Cambiar contenidos de bases de datos, cambiar líneas de un programa, datos de una transferencia.

Figura1.4: Ataque (Modificación)

1.1.2.3.1.3- Fabricación

Falsificar la información: Ataca la autenticidad.

Ejemplo: Añadir campos y registros en una base de datos, añadir líneas de un programa (virus).

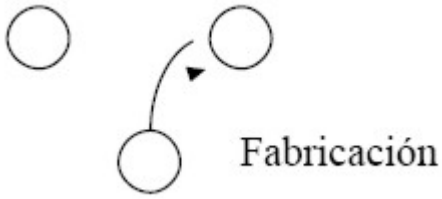

Figura1.5: Ataque (Fabricación)

1.1.2.3.2- Ataques Pasivos

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante

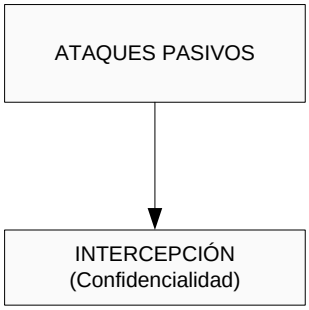

Figura1.6: Ataques Pasivos

1.1.2.3.2.1- Intercepción

Una parte no autorizada gana el acceso a un bien. Ataca la confidencialidad. Entre las técnicas para obtener información de la comunicación, puede consistir en:

- Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitorizados.
- Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.
- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Ejemplo: Escuchas en línea de datos. Copias no autorizadas.

Figura1.7: Ataque (Intercepción)

CAPITULO II

ANALISIS DE LA INFRAESTRUCTURA DE SEGURIDADES

2.1- Firmas Digitales

2.1.1- Definición

Es el medio por el cual los autores de un mensaje, archivo u otro tipo de información codificada digitalmente, enlazan su identidad a la información. El proceso de firmar información digitalmente implica la transformación de la misma y de ciertos datos secretos que guarda el remitente en una etiqueta denominada firma. Las *Firmas Digitales* se utilizan en entornos de claves públicas y permiten mantener la integridad y evitar el rechazo.

Una F*irma Digital* es una forma de asegurar la integridad y el origen de los datos. Proporciona una evidencia de que los datos no se han sido modificados desde que se firmaron y confirma la identidad de la persona o entidad que los firmó. Esto posibilita las importantes características de *seguridad*, de *integridad* y *aceptación*, que resultan esenciales para asegurar las transacciones de comercio electrónico.

La *Firma Digital* normalmente se utiliza cuando los datos se distribuyen en formato de texto simple o sin cifrar. En estos casos, aunque la propia confidencialidad del mensaje puede no garantizar el cifrado, podría haber un motivo convincente para asegurar que los datos se encuentran en su formato original y no han sido enviados por un impostor, debido a que en un entorno informático distribuido, es posible que cualquier persona en la red con los recursos adecuados lea o modifique el texto simple, esté autorizado o no.

2.1.2- Requisitos

Se entiende por *Firma Digital* a los datos expresados en formato digital, utilizados como método de identificación de un firmante y de verificación de la integridad del contenido de un documento digital, que cumpla con los siguientes requisitos:

a) Pertenecer únicamente a su titular.
b) Encontrarse bajo su absoluto y exclusivo control.
c) Ser susceptible de verificación.
d) Estar vinculada a los datos del documento digital de modo tal que cualquier modificación de los mismos ponga en evidencia su alteración.

2.1.3- Proceso de creación y verificación

La *Firma Digital* es un sistema que va a garantizar que:

a) El mensaje no ha sido alterado en su transmisión (integridad).
b) El emisor es realmente quien dice ser (autenticación).
c) El mensaje necesariamente ha sido enviado por el emisor y no por otro (no repudio).

La *Firma Digital* se basa en el cifrado, con la clave privada del emisor, de un resumen del mensaje, que acompañará a dicho mensaje, ya se transmita éste, cifrado o en claro.

El siguiente es un resumen de los pasos a seguir para la generación de la Firma digital y Autenticación de usuario:

a) El emisor genera un resumen del mensaje a través de una función *Hash* [6] conocida.
b) A continuación cifra ese resumen con su clave privada (por lo tanto solo será posible descifrarlo con su clave pública), y envía tanto el mensaje como el resumen cifrado al receptor.
c) El receptor a la llegada del mensaje, utilizando la función *Hash* conocida, generará, a su vez, otro resumen a partir del mensaje.
d) Por otra parte, descifrara el resumen enviado, con la ayuda de la clave pública del emisor.
e) Finalmente, se comparara ambos resúmenes, y si existe igualdad, se puede asegurar que el contenido no ha sido alterado en ningún momento de la transmisión (integridad), y que además el emisor solo puede ser el poseedor de la clave privada que correspondiese a la clave publica con la que se descifro el resumen (autenticación y no repudio).

[6] Una función Hash es el resultado de la aplicación de un algoritmo matemático unidireccional no único que genera un resumen del texto al cual es aplicado que se utiliza como medio de identificación, esta cadena de caracteres será siempre la misma de forma tal que se aplique la misma función sobre el texto. El objetivo de la función Hash es el de verificar la integridad de la información; al ser aplicado en una instancia sin efectuar cambios sobre el texto producirá un valor, y otro diferente si se realizan cambios.

Se puede definir la creación de la *Firma Digital* en los siguientes pasos:

PASO 1: Crear la Firma Digital

A quiere enviar un mensaje firmado a B. Lo primero que se debe hacer es escribir el mensaje y luego proceder a firmarlo. El proceso de firmar incluye dos pasos:

- Se calcula el resultado de aplicar una función "hash" al mensaje, lo cual se llamará *digest*
- El *digest* se encripta con la clave privada de A y se adjunta al mensaje original

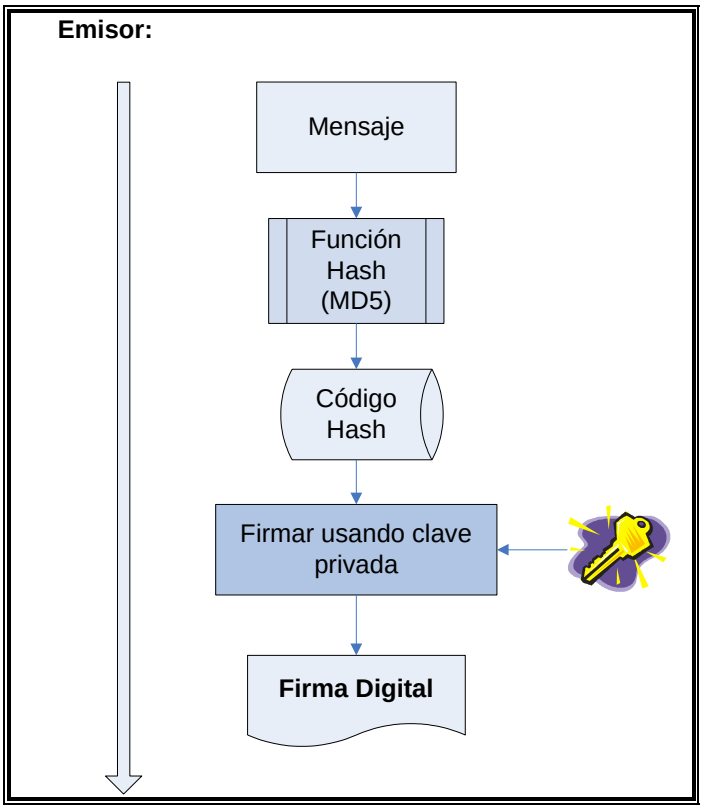

Figura 2.1: Creación de la Firma Digital

PASO 2: Crear un Mensaje seguro para ser enviado

El mensaje más la firma se encriptan para ser enviados, la encriptación puede ser realizada de dos maneras:

- Con una clave de una única vez, si se usa un algoritmo simétrico (Esta clave debe ser comunicada al receptor por otra vía para poder desencriptarlo)
- Con la llave pública de destinatario, si se usa algoritmo asimétrico.

Al resultado de esta operación simplemente resta enviarlo al destinatario.

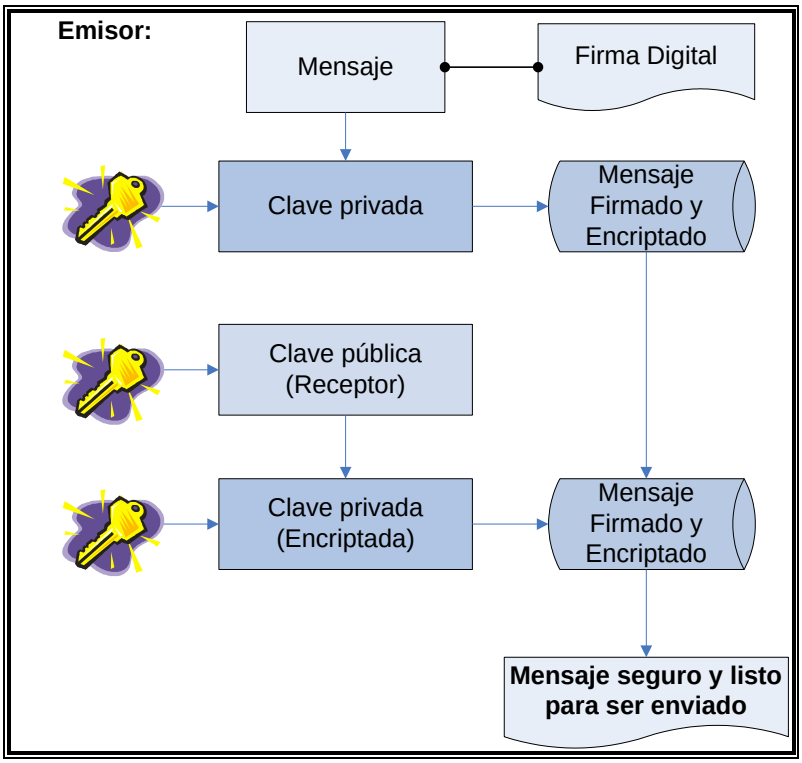

Figura 2.2: Creación de un mensaje seguro

PASO 3: Desencriptar el mensaje seguro recibido

B recibe el mensaje de A, dependiendo de cómo se encriptó procederá a:

- Desencriptarlo con la llave de única vez
- Desencriptarlo con la llave privada de B

El resultado obtenido es el mensaje y la firma digital.

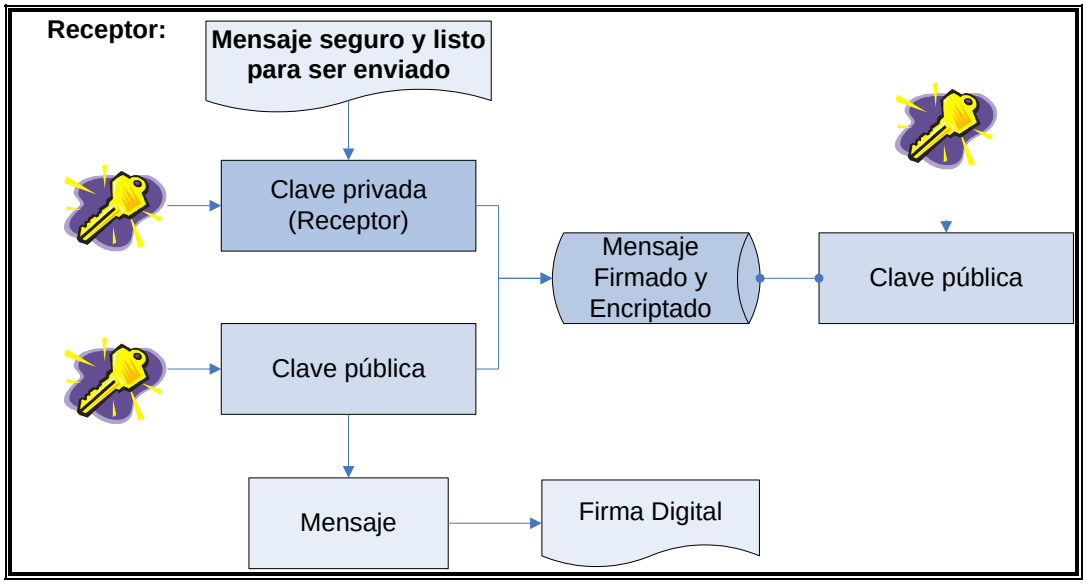

Figura 2.3: Recepción segura y desencriptado del mensaje

PASO 4: Verificar autenticidad / integridad del mensaje

Resta verificar que realmente el mensaje fue firmado por A, para esto debemos:

- Desencriptar la firma con la clave pública de A, obteniendo el *Digest*
- Calcularle al mensaje recibido (mediante la misma función "hash" que utilizo A) el *digest*

Una vez terminada las acciones anteriores, simplemente comparamos los resultados obtenidos y de esta manera, en caso de ser iguales, verificaremos la identidad del emisor.

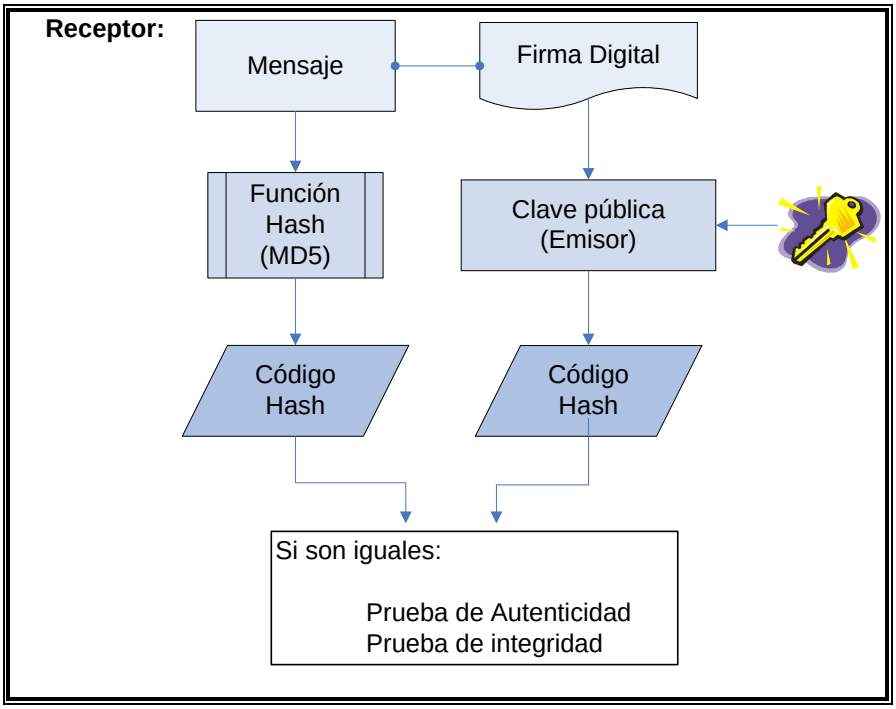

Figura 2.4: Verificación de Autenticidad e integridad del mensaje

2.1.3.1- Estándares para la generación y utilización de Firma Digital

La firma es un número natural de mas o menos 300 dígitos si se usa el sistema RSA, que tiene las mismas propiedades que la firma convencional, es decir, es posible asociar un número único a cada persona o entidad, existe un método de firma y un método de verificación de la firma. Esta *Firma Digital* resuelve satisfactoriamente el problema de autenticación y no repudio.

Los siguientes son algunos estándares y métodos utilizados para la generación de *Firmas Digitales*:

a) El estándar más usado para firmar digitalmente es el conocido como RSA, lo importante de este método es que es el más usado actualmente y por lo tanto es conveniente usarlo para poder ser compatible. Para que sea segura la longitud de sus claves (una pública y otra privada) debe de ser de 1024 bits, es decir un número de un poco más de 300 dígitos.
b) Otro estándar reconocido para *Firma Digital* es el llamado DSA, que es oficialmente aceptado para las transacciones oficiales en el gobierno de USA. Este estándar usa también claves del mismo tamaño que RSA, pero esta basado en otra técnica. En mediciones comparativas es casi equivalente en seguridad a RSA.
c) Una tercera opción es el estándar que usa curvas elípticas, este método tiene la ventaja a los dos anteriores a reducir hasta en 164 bits, es decir como 45 dígitos las claves, manteniendo la misma seguridad. Por lo que es más apropiado para ser usado donde existen recursos reducidos como en Smart Cards, PDAs, etc. Actualmente este método se ha integrado como el reemplazo oficial de DSA para el gobierno de USA.

2.2- Criptografía

2.2.1- Definición

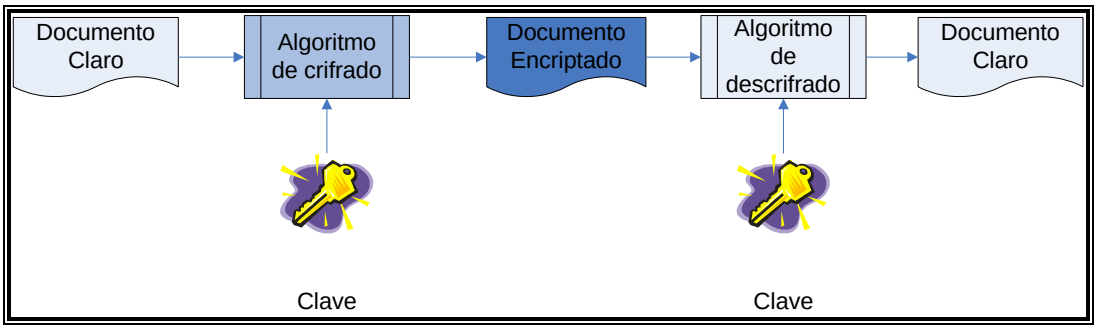

Figura 2.5: Esquema de cifrado

Es la ciencia que trata del enmascaramiento de la comunicación de modo que sólo resulte inteligible para la persona que posee la clave, o método para averiguar el significado oculto, mediante el criptoanálisis de un texto aparentemente incoherente. En su sentido más amplio, la criptografía abarca el uso de mensajes encubiertos, códigos y cifras. Los mensajes encubiertos, como los ocultos en textos infantiles o los escritos con tinta invisible, cifran todo su éxito en no levantar ninguna sospecha; una vez descubiertos, a menudo no resultan difíciles de descifrar. Los códigos, en que las palabras y las frases se representan mediante vocablos, números o símbolos preestablecidos, por lo general resultan imposibles de leer si no se dispone del libro con el código clave.

La criptografía moderna, sin embargo, se encarga de la construcción de esquemas eficientes para los cuales es inviable (no imposible) recuperar el texto original a partir del texto cifrado.

2.2.2- Clases de criptografía

La palabra criptografía se limita a veces a la utilización de cifras, es decir, métodos de transponer las letras de mensajes (no cifrados) normales o métodos que implican la sustitución de otras letras o símbolos por las letras originales del mensaje, así como a diferentes combinaciones de tales métodos, todos ellos conforme a sistemas predeterminados. Hay diferentes tipos de cifras, pero todos ellos pueden encuadrarse en una de las dos siguientes categorías: transposición y sustitución.

En las claves de transposición, el mensaje se escribe, sin separación entre palabras, en filas de letras dispuestas en forma de bloque rectangular. Las letras se van transponiendo según un orden acordado de antemano, por ejemplo, por columnas verticales, diagonales o espirales, o mediante sistemas más complicados. La disposición de las letras en el mensaje cifrado depende del tamaño del bloque utilizado y del camino seguido para inscribir y transponer las letras. Para aumentar la seguridad de la clave o cifra se puede utilizar una palabra o un número clave. Las cifras de transposición se pueden reconocer por la frecuencia de las letras normales según el idioma utilizado. Estas cifras se pueden desentrañar sin la clave reordenando las letras de acuerdo con diferentes pautas geométricas, al tiempo que se van resolviendo anagramas de posibles palabras, hasta llegar a descubrir el método de cifrado.

2.2.2.1- Función Hash

Una función Hash es una función matemática compleja unidireccional que aplicada a un conjunto de caracteres de cualquier longitud obtiene un pequeño resultado de largo fijo, y cualquier cambio al conjunto de caracteres origen, producirá un cambio en el resultado.

Se estima que para lograr un conjunto de caracteres diferente al anterior pero que genere el mismo resultado después de la aplicación de la función requeriría un esfuerzo incalculable.

El objetivo de los códigos *Hash*, es el de mantener la integridad en la información asegurado que los datos no hayan sido alterados, por error o intencionalmente durante la transmisión o el almacenamiento.

2.2.2.1.1- Integridad de datos con funciones Hash

Los códigos Hash de autenticación de mensajes (HMAC) firman paquetes para comprobar que la información recibida se corresponde exactamente con la enviada. Esto se denomina integridad de los datos y es fundamental cuando la información se transmite a través de un medio no protegido.

La función *Hash* se describe normalmente como una firma en el paquete, sin embargo, una función hash es diferente de una *Firma Digital* pues utiliza una clave secreta compartida, mientras que la firma utiliza la tecnología de claves públicas y la clave privada del equipo remitente.

La *Firma Digital* proporciona el no incumplimiento, mientras que la función *Hash* no. Las funciones *Hash* también se denominan funciones unidireccionales, en las funciones unidireccionales es sencillo determinar la función *Hash* a partir del mensaje, pero es matemáticamente inviable determinar el mensaje a partir de la función hash. Por el contrario, en las funciones bidireccionales, el mensaje original puede determinarse a partir de su forma convertida. Los sistemas de cifrado y descifrado son ejemplos de funciones bidireccionales.

La función *Hash* es una suma de comprobación criptográfica o un código de integridad de mensaje (MIC) que ambos interlocutores deben calcular para comprobar el mensaje. Por ejemplo, el equipo remitente utiliza una función hash y una clave compartida para calcular la suma de comprobación del mensaje, y la incluye en el paquete.

El equipo receptor debe calcular la misma función hash sobre el mensaje recibido con la clave compartida y comparar el resultado con el original (que se incluye en el paquete del remitente). Si el mensaje ha cambiado durante el trayecto, los valores de hash serán diferentes y se descartará el paquete.

Para la integridad, es posible elegir entre dos funciones hash al configurar la directiva:

a) MD5, Síntesis del mensaje 5 (MD5) se basa en RFC 1321. Se diseñó como respuesta a un punto débil detectado en MD4. MD5 realiza cuatro pases sobre los bloques de datos (MD4 daba tres pases) y utiliza una constante numérica distinta para cada palabra del mensaje en cada pase. El número de constantes de 32 bits que se utilizan durante el cálculo de MD5 es 64, lo que produce una función hash de

128 bits que se utiliza para comprobar la integridad. Aunque MD5 requiere más recursos que MD4, también ofrece una integridad más efectiva.

b) SHA1, Secure Hash Algorithm 1 (SHA1, Algoritmo de hash seguro 1) fue diseñado por el National Institute of Standards and Technology, como se describe en Federal Information Processing Standard (FIPS, Estándar federal de procesamiento de información) PUB 180-1. El proceso de SHA se basa en gran medida en el de MD5. El cálculo de SHA1 produce una función hash de 160 bits que se utiliza para comprobar la integridad. Las mayores longitudes de hash suponen una mayor seguridad, por lo que SHA es más efectivo que MD5.

c) RIPEMD-160, Maneja claves muy robustas, normalmente de 160 bits, aunque existen versiones de 128 y se están planteando nuevas de 256 y 320 bits. Es muy rápido, no está patentado y su código fuente es abierto, de libre acceso.

2.2.2.2- Criptografía Asimétrica

Se utiliza la criptografía de claves públicas para la autenticación (firma de certificados) y el intercambio de claves. La criptografía de claves públicas ofrece toda la funcionalidad de la criptografía de claves secretas, pero en general es más segura, ya que requiere dos claves: una para firmar y cifrar los datos, y otra para comprobar la firma y descifrar los datos. Este principio se denomina criptografía asimétrica, que denota la necesidad de disponer de dos claves.

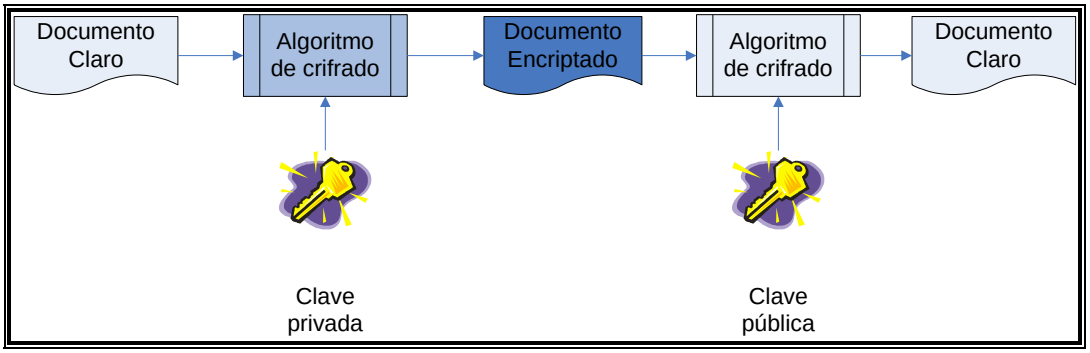

Figura 2.6: Esquema de cifrado por criptografía asimétrica

Cada usuario tiene una clave privada (también llamada clave secreta) que nadie más conoce y una clave pública que se distribuye ampliamente.

Las claves pública y privada tienen características matemáticas especiales, de tal forma que se generan siempre a la vez, por parejas, estando cada una de ellas ligada intrínsecamente a la otra, de tal forma que si dos llaves públicas son diferentes, entonces sus llaves privadas asociadas también lo son, y viceversa.

Los algoritmos asimétricos están basados en funciones matemáticas fáciles de resolver en un sentido, pero muy complicadas de realizar en sentido inverso, salvo que se conozca la clave privada, como la potencia y el logaritmo. Ambas claves, pública y privada, están relacionadas matemáticamente, pero esta relación debe ser lo suficientemente compleja como para que resulte muy difícil obtener una a partir de la otra. Este es el motivo por el que normalmente estas claves no las elige el usuario, si no que lo hace un algoritmo específico para ello, y suelen ser de gran longitud.

Mientras que la clave privada debe mantenerla en secreto su propietario, ya que es la base de la seguridad del sistema, la clave pública es difundida ampliamente por Internet, para que esté al alcance del mayor número posible de personas, existiendo servidores que guardan, administran y difunden dichas claves.

El problema fundamental al que se enfrenta la criptografía asimétrica es al de la autenticidad de las claves públicas, es decir, el método para garantizar que la clave pública de un interlocutor, que se obtiene libremente en la red, es realmente de quien dice ser.

2.2.2.3- Criptografía Simétrica

Se caracteriza por que usa *la misma clave* para encriptar y para desencriptar, motivo por el que se denomina simétrica.

Toda la seguridad de este sistema está basada en la llave simétrica, por lo que es misión fundamental tanto del emisor como del receptor conocer esta clave y mantenerla en secreto. Si la llave cae en manos de terceros, el sistema deja de ser seguro, por lo que habría que desechar dicha llave y generar una nueva.

Para que un algoritmo de este tipo sea considerado fiable debe cumplir dos requisitos básicos:

- Conocido el criptograma (texto cifrado) no se pueden obtener de él ni el texto en claro ni la clave.
- Conocidos el texto en claro y el texto cifrado debe resultar más caro en tiempo o dinero descifrar la clave que el valor posible de la información obtenida por terceros.

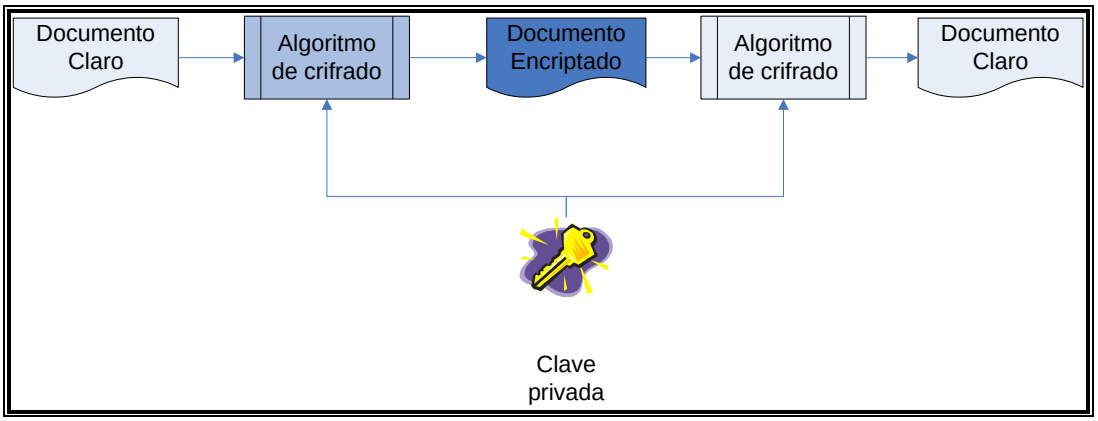

Figura 2.7: Esquema de cifrado por criptografía simétrica

Generalmente el algoritmo de encriptación es conocido, se divulga públicamente, por lo que la fortaleza del mismo dependerá de su complejidad interna y sobre todo de la longitud de la clave empleada.

Los algoritmos simétricos encriptan bloques de texto del documento original, y son más sencillos que los sistemas de clave pública, por lo que sus procesos de encriptación y desencriptación son más rápidos.

Todos los sistemas criptográficos clásicos se pueden considerar simétricos, y los principales algoritmos simétricos actuales son *DES, IDEA y RC5*. Actualmente se está llevando a cabo un proceso de selección para establecer un sistema simétrico estándar, que se llamará *AES* (Advanced Encryption Standart), que se quiere que sea el nuevo sistema que se adopte a nivel mundial.

Las principales desventajas de los métodos simétricos son la distribución de las claves, el peligro de que muchas personas deban conocer una misma clave y la dificultad de almacenar y proteger muchas claves diferentes.

2.3- Certificado digital

2.3.1- Definición

Para solucionar el problema de la Autenticación en las transacciones por Internet se buscó algún sistema identificador único de una entidad o persona. Anteriormente existían los sistemas criptográficos de clave asimétrica, mediante los cuales una persona disponía de dos claves, una pública, al alcance de todos, y otra privada, sólo conocida por el propietario. Cuando deseamos enviar un mensaje confidencial a otra persona, basta pues con cifrarlo con su clave pública, y así estaremos seguros de que sólo el destinatario correcto podrá leer el mensaje en claro.

Un certificado de clave pública, al que se hace referencia normalmente como un certificado, es una declaración firmada digitalmente que enlaza el valor de una clave pública con la identidad de una persona, dispositivo o servicio que posee la clave privada correspondiente.

El problema era estar seguro de que efectivamente la clave pública que nos envían sea de la persona correcta, y no de un suplantador. Entonces se pensó en implementar una especie de documento de identidad electrónica que identificara sin dudas a su emisor.

La solución a este problema la trajo la aparición de los *Certificados Digitales* o *Certificados Electrónicos*, documentos electrónicos basados en la criptografía de clave pública y en el sistema de *Firmas Digitales*). La misión principal de un *Certificado Digital* es garantizar con toda confianza el vínculo existente entre una persona, entidad o servidor Web con una pareja de claves correspondientes a un sistema criptográfico de clave pública.

Un *Certificado Digital* es un documento electrónico que contiene datos identificadores de una persona o entidad (empresa, servidor Web, etc.) y la llave pública de la misma, haciéndose responsable de la autenticidad de los datos que figuran en el certificado otra persona o entidad de confianza, denominada *Autoridad Certificadora*.

El usuario o servicio que recibe el certificado es el *sujeto* del certificado. El emisor y firmante del certificado es una entidad emisora de certificados.

Normalmente, los certificados contienen siguiente la información:

a) Valor de la clave pública del sujeto
b) Información del identificador del sujeto, como el nombre y la dirección de correo electrónico
c) Período de validez (el período durante el que el certificado se considera válido)
d) Información del identificador del emisor
e) La *Firma Digital* del emisor, que da fe de la validez del enlace entre la clave pública del sujeto y la información del identificador de sujeto.

Un certificado es válido sólo para el período especificado en éste; cada certificado contiene las fechas *Válido desde* y *Válido hasta*, que marcan el límite del período de validez. Una vez que el período de validez del certificado ha transcurrido, el sujeto del certificado actual caducado debe solicitar un certificado nuevo.

En los casos en que sea necesario deshacer el enlace confirmado en un certificado, el emisor puede revocarlo. Cada emisor mantiene una lista de revocación de certificados que los programas pueden utilizar al comprobar la validez de un certificado determinado.

Uno de las ventajas principales de los certificados es que los *Host* [7] ya no tienen que mantener ningún conjunto de contraseñas para sujetos individuales que necesiten como requisito previo autenticarse para tener acceso. Por el contrario, el *Host*, simplemente, establece la confianza en un emisor de certificados.

Cuando un *Host*, como un servidor Web seguro, designa a un emisor como entidad raíz de confianza, el *Host* confía de forma implícita en las directivas que el emisor utiliza para establecer los enlaces de los certificados que emite. En efecto, el *Host* confía en que el emisor ha comprobado la identidad del sujeto del certificado. Para designar a un emisor como entidad raíz de confianza, un *Host* coloca el certificado firmado por el propio emisor que contiene la clave pública del emisor en el almacén de certificados de la entidad emisora de certificados raíz del equipo *Host*. Se confía en las entidades emisoras de certificados subordinadas o intermedias sólo si disponen de una ruta de acceso de certificación de una entidad emisora de certificados raíz de confianza.

2.3.2- Usos de los certificados

Dado que los certificados se utilizan generalmente para establecer identidades y crear confianza para intercambios seguros de información, las entidades emisoras de certificados (CA) pueden emitir certificados para personas, dispositivos (como equipos) y servicios que se ejecutan en equipos.

[7] Un *Host* es considerado como el sistema invitado, es decir, el que solicita los servicios a los que se puede tener acceso en una red o dominio, es suma puede ser cualquier equipo que acceda a servicios que se encuentran distribuidos en una red.

En algunos casos, los equipos tienen que poder intercambiar información con un alto grado de confianza en la identidad del otro dispositivo, servicio o persona que participa en la transacción.

Las aplicaciones y los servicios que se ejecutan en equipos también necesitan comprobar frecuentemente que tienen acceso a información de un origen de confianza.

En circunstancias en las que dos entidades (como dispositivos, personas o aplicaciones o servicios) intentan establecer identidad y confianza, el hecho de que ambas entidades confíen en la misma entidad emisora de certificados permite establecer el enlace de identidad y confianza entre ellas. Una vez que el sujeto de un certificado presenta un certificado emitido por una CA de confianza, la entidad que intenta establecer la confianza puede proseguir con el intercambio de información almacenando el certificado del sujeto del certificado en su propio almacén de certificados y, si procede, utilizar la clave pública contenida en el certificado para cifrar una clave de sesión de forma que todas las siguientes comunicaciones con el sujeto del certificado sean seguras.

Cuando el software está firmado con un certificado válido de una entidad emisora de certificados de confianza, sabe que el software no ha sido interceptado y se puede instalar en el equipo sin problemas. Durante la instalación del software, se le pide que acepte si confía en el fabricante del software.

También se le puede ofrecer la opción de confiar siempre en el software de dicho fabricante de software concreto. Si decide confiar en el contenido del fabricante, su certificado va a al almacén de certificados y otras instalaciones software de productos de dicho fabricante tienen lugar con confianza predefinida. En el caso de confianza

predefinida, puede instalar el software del fabricante sin que se le pida si confía en él; el certificado almacenado en su equipo indica que confía en el fabricante del software.

De igual forma que con otros certificados, aquellos certificados utilizados para comprobar la autenticidad de software y la identidad de un fabricante de software pueden tener otros propósitos. Por ejemplo, cuando el complemento Certificados está establecido para ver los certificados por su propósito, la carpeta Firma del código podría contener un certificado emitido a Compatibilidad de hardware con Microsoft Windows por la Entidad emisora raíz de Microsoft. Dicho certificado tiene tres propósitos:

a) Asegura que el software viene del fabricante de software.
b) Protege el software para que no sea alterado después de su publicación.
c) Proporciona la comprobación del controlador de hardware de Windows.

2.3.3- Requisitos

Los certificados, debido a su propia naturaleza y al papel que desempeñan, no son documentos imperecederos, al igual que sucede con el resto de documentos de autenticación de otros tipos. [8]

En primer lugar, al estar basados en el uso de claves no conviene que sean válidos por periodos de tiempo largos, ya que uno de los principales problemas del manejo de claves es que cuanta más vida tienen más fácil es que alguien extraño se apodere de ellas. Además, con el paso del tiempo los equipos informáticos van teniendo cada vez más poder de cálculo, facilitando con ello la labor de los criptoanalístas, por lo que es conveniente que cada cierto tiempo se vaya aumentando el tamaño de las claves criptográficas.

[8] Los Documentos imperecederos son aquellos no expiran en el tiempo.

Por este motivo los Certificados Digitales tienen estipulado un periodo de validez, que suele ser de un año.

En segundo lugar, es posible que un certificado convenga anularlo en un momento dado, bien porque se crea que las claves estén comprometidas, bien porque la persona o entidad propietaria haya caído en quiebra o delito. Es por esto que existe la posibilidad de revocar o anular un certificado, y esta revocación puede llevarla a cabo el propietario del mismo, la Autoridad Certificadora o las autoridades judiciales.

Para llevar un control de los certificados revocados (no válidos) las Autoridades de Certificación han implementado unos servidores especiales que contienen bases de datos en las que figuran los certificados anulados, que se conocen con el nombre de Lista de Certificados Revocados, CRL.

Un CRL es un archivo, firmado por la Autoridad Certificadora o emisor de certificados digitales, que contiene la fecha de emisión del mismo y una lista de certificados revocados, figurando para cada uno de ellos su número de identificación y la fecha en que ha sido revocado.

La solución a estos problemas la dan los Servicios de Directorios o de Consulta de Certificados, servicios ofrecidos por personas o entidades de confianza aceptada, por el que al recibir una petición de validez de un certificado responde al instante si en esa fecha y hora concreta el mismo es válido o si por el contrario está revocado, en cuyo caso proporcionará también la fecha UTC de revocación. Para dar validez a la respuesta, el Servicio de Directorios firma con su llave privada la misma, con lo que el usuario estará seguro de la Autenticidad de la respuesta recibida.

Los Certificados Digitales son emitidos por las *Autoridades de Certificación*, entidades consideradas de confianza probada. Al hacerse responsables estas entidades de los certificados que emiten, dando certeza de la relación existente entre los datos que figuran en un certificado y la persona o entidad que lo solicita, una de las tareas más importantes de las mismas en ejercer un control estricto sobre la exactitud y veracidad de los datos incorporados en el certificado.

Para solicitar un certificado a una *Autoridad de Certificación* la persona o entidad interesada debe cumplir unos procedimientos previos, confeccionando un documento, denominado Requerimiento de Certificación, en el que deben figurar los datos representativos del solicitante (nombre personal o de empresa, domicilio personal o social, dominio asociado a la empresa y al servidor seguro, etc.) y su llave pública.

También debe manifestar su voluntad de aceptar dicha llave pública y demostrar que es el propietario real de la llave privada asociada, mediante el firmado digital de un mensaje.

La presentación de todos estos datos ante la Autoridad Certificadora puede acarrear problemas, al estar éstas normalmente muy distantes de los solicitantes. Para solventar esto se han creado unas entidades intermedias, conocidas como Autoridades Registradoras, autorizadas por las AC, y cuya misión es comprobar la validez de los datos presentados en el Requerimiento de Certificación. Una vez comprobados, las AR envía la aprobación a las AC, que emiten el correspondiente *Certificado Digital*.

Para que se pueda obtener con facilidad el *Certificado Digital* de cualquier persona o entidad las Autoridades de Certificación disponen de servidores de acceso público que

realizan la función de depósito de certificados, en los que se puede buscar el deseado y descargarlo a nuestro ordenador. Es ésta una forma más segura que la de usar directamente un certificado recibido por correo o descargado de una página Web, ya que la Autoridad de Certificación responsable del servidor es la encargada de verificar constantemente la validez y autenticidad de los certificados que distribuye.

Además de las Autoridades de Certificación reconocidas existen otras entidades que también pueden expedir certificados. Estos certificados se suelen usar para empleados de la propia compañía que deben hacer negocios para ella

2.3.4- Revocación

La solicitud de revocación de un certificado digital debe hacerse en forma personal, o por medio de un documento digital firmado digitalmente. Si la revocación es solicitada por el titular, ésta debe concretarse de inmediato. Si la revocación es solicitada por un tercero, debe ser realizada dentro de los plazos mínimos necesarios para realizar las verificaciones del caso. La revocación debe indicar el momento desde el cual se aplica, precisando minutos y segundos, como mínimo, y no puede ser retroactiva o ser aplicada a futuro. La revocación del certificado digital debe ser notificada a su titular y a toda parte que el certificador tenga conocimiento que confíe en el mismo. Asimismo debe ser incluido inmediatamente en la lista de certificados digitales revocados y la lista debe estar firmada por el certificador licenciado. Dicha lista debe publicarse en forma permanente e ininterrumpida en Internet. El certificador licenciado debe emitir una constancia de la revocación para el solicitante y proveer, opcionalmente, el servicio de sellado digital de fecha y hora de documentos digitales.

2.4- Terceras partes de confianza

La validez de un certificado es la confianza de que la clave pública contenida en el certificado pertenece al usuario indicado en dicho certificado. La validez del certificado en un entorno de clave pública es esencial ya que se debe conocer si se puede confiar o no en que el destinatario de un mensaje será o no realmente la persona el que esperamos.

La manera en que se puede confiar en el certificado de un usuario con el que nunca hemos tenido ninguna relación previa es mediante la confianza en terceras partes.

La idea consiste en que dos usuarios puedan confiar directamente entre sí, si ambos tienen relación con una tercera parte ya que ésta puede dar veracidad de la fiabilidad de ambos.

La necesidad de una Tercera Parte Confiable (TPC ó TTP, Trusted Third Party) es fundamental en cualquier entorno de clave pública de tamaño considerable debido a que es impensable que los usuarios hayan tenido relaciones previas antes de intercambiar información cifrada o firmada. Además, la mejor forma de permitir la distribución de las claves públicas (o *Certificados Digitales*) de los distintos usuarios es que algún agente en quien todos los usuarios confíen se encargue de su publicación en algún repositorio al que todos los usuarios tengan acceso.

2.4.1- Autoridades de certificación

2.4.1.1- Funciones

Se puede tener confianza en el *Certificado Digital* de un usuario del que previamente no tenemos conocimiento si dicho certificado está avalado por una tercera parte de confianza bilateral. La forma en que esa tercera parte avalará que el certificado es a través su *Firma Digital* sobre el certificado. Por tanto, es posible confiar en cualquier *Certificado Digital* firmado por una tercera parte sobre la cual se tiene conocimiento de veracidad en el funcionamiento. La Tercera parte de confianza se encarga de la *Firma Digital* de los certificados de los usuarios en un entorno de clave pública se conoce con el nombre de Autoridad de Certificación [9].

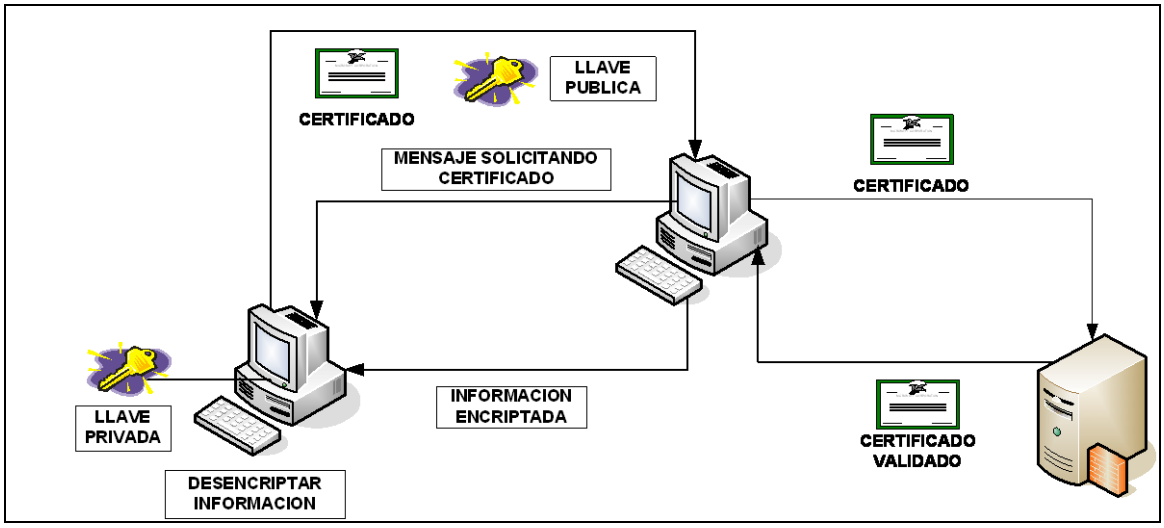

Figura 2.8: Esquema de funcionamiento de una Autoridad Certificadora

[9] El CONATEL emitió el reglamento para la acreditación, registro y regulación de entidades habilitadas para prestar Servicios de Certificación de Información y Servicios relacionados, que regula el funcionamiento de las Autoridades de Certificación en el país. (Ver ley de comercio electrónico)

El modelo de confianza basado en Terceras Partes Confiables es la base de la definición de las Infraestructuras de Clave Pública (ICPs o PKIs, Public Key Infrastructures).

Una infraestructura de Clave Pública es un conjunto de protocolos, servicios y estándares que soportan aplicaciones basadas en criptografía de clave pública.

Algunos de los servicios ofrecidos por una ICP son los siguientes:

a) Registro de claves públicas: emisión de un nuevo certificado para una clave pública.
b) Revocación de certificados: cancelación de un certificado previamente emitido.
c) Selección de claves: publicación de la clave pública de los usuarios.
d) Evaluación de la confianza: determinación sobre si un certificado es válido y qué operaciones están permitidas para dicho certificado.
e) Recuperación de claves: posibilidad de recuperar las claves de un usuario.

Las ICPs están compuestas por distintas terceras partes en los que todos los demás usuarios de la infraestructura confían:

a) Autoridad de Certificación
b) Autoridad de Registro
c) Otras Terceras Partes Confiables.

La Autoridad Certificadora debe emitir *Certificados Digitales* de acuerdo a lo establecido en sus políticas de certificación, para lo cual debe:

a) Recibir una solicitud de emisión de Certificado Digital, firmada digitalmente con los correspondientes datos de creación de Firma Digital del solicitante.
b) Identificar inequívocamente los Certificados Digitales emitidos.
c) Mantener copia de todos los Certificados Digitales emitidos, consignando su fecha de emisión, y de sus correspondientes solicitudes de emisión.
d) Revocar los Certificados Digitales por él emitidos en los siguientes casos:
    - A solicitud del titular del *Certificado Digital*.
    - A solicitud justificada de un tercero y bajo su responsabilidad.
    - Si determinara que un *Certificado Digital* fue emitido en base a una información falsa, que en el momento de la emisión hubiera sido objeto de verificación.
    - Si determinara que el procedimiento de seguridad de los datos de verificación de *Firmas Digitales* contenidos en los *Certificados Digitales* emitidos ha dejado de ser seguro o si la función utilizada para crear la *Firma Digital* del *Certificado Digital* dejara de ser segura.

2.4.1.2- Responsabilidades y garantías

Son responsabilidades del Certificador:

a) Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a los datos de creación de firma digital de los titulares de certificados digitales por él emitidos.

b) Mantener el control exclusivo de sus propios datos de creación de firma digital e impedir su divulgación

c) Operar utilizando un sistema técnicamente confiable.

d) Notificar al solicitante las medidas que está obligado a adoptar para crear firmas digitales seguras y para su verificación confiable y de las obligaciones que asume por el solo hecho de ser titular de un certificado digital.

e) Recabar únicamente aquellos datos personales del titular del certificado digital que sean necesarios para su emisión, quedando el solicitante en libertad de proveer información adicional.

f) Mantener la confidencialidad de toda información que no figure en el certificado digital.

g) Poner a disposición del solicitante de un certificado digital toda la información relativa a su tramitación.

h) Incorporar en las condiciones de emisión y utilización de sus certificados digitales los efectos de la revocación de su propio certificado digital y de la licencia que le otorgara la autoridad de aplicación.

i) Publicar en Internet en forma permanente e ininterrumpida los certificados digitales que ha emitido, la lista de certificados digitales revocados, las condiciones de emisión y utilización de sus certificados digitales, los informes de las auditorias de que hubiera sido objeto, su manual de procedimientos y toda información que determine la autoridad de aplicación.

j) Publicar en el Boletín Oficial aquellos datos que la autoridad de aplicación determine.

k) Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas.

l) Informar en las condiciones de emisión y utilización de sus certificados digitales si éstos requieren la verificación de la identidad del titular.

m) Solicitar inmediatamente a la autoridad de aplicación la revocación de su propia licencia, cuando tuviera sospechas fundadas de que los datos de creación de firma digital que utiliza hubiesen sido comprometidos o cuando el uso de los procedimientos de aplicación de los datos de verificación de firma digital en él contenida haya dejado de ser seguro.

n) Informar inmediatamente a la autoridad de aplicación sobre cualquier cambio en los datos relativos a su licencia.

CAPITULO III

ANALISIS DE PLATAFORMAS TECNOLOGICAS

3.1- Plataforma Linux

3.1.1- Seguridad como Autoridad Certificadora

El kernel de Linux se halla desarrollado de modo que se protege el funcionamiento de los procesos; sin descuidar la multitarea Linux tiene un alto soporte para procesamiento en paralelo y soporte para varios procesadores, por lo que su funcionamiento en servidores es de muy alto rendimiento

En cuanto a su utilización en la red, Linux posee Firewall y Proxy[10] a nivel de red e incluido como parte del sistema; ambas aplicaciones trabajan de forma muy fuerte impidiendo las conexiones no autorizadas hacia el servidor o los terminales que se encuentren como parte de la red.

En este contexto, se puede afirmar categóricamente que Unix es el sistema operativo más seguro que existe. Linux posee la capacidad de permitir una configuración muy particularizada de las seguridades en el sistema residente, esto se debe a que la seguridad en Unix viene implementada desde el kernel, de modo que es posible configurarla al nivel de sistema de archivos, de servicios de red, de facilidades en el host y de capacidades de usuario.

[10] La mayoría de las distribuciones que se encuentran disponibles, incluyen las aplicaciones, de no ser así existen las versiones disponibles desde Internet de forma gratuita.

3.1.2- Análisis Costo – Beneficio

En cuanto al análisis Costo – Beneficio y debido en su gran mayoría a que se trata de software de libre distribución la primera variable en nuestro marco de referencia posee valores muy bajos o en determinadas circunstancias tiende a valores muy bajos por lo que la segunda variable Beneficio crece vertiginosamente.

El proyecto enteramente se puede implementar en la plataforma en mención por una fracción del costo, pero con una complejidad realmente alta, pues como se mencionó anteriormente existen complicaciones subsecuentes, como es la generación de las solicitudes y los certificados en forma manual a través de scripts.

El punto fuerte radica en que el precio del sistema puede ser cero y solo sería necesario asumir el precio del hardware, pero la desventaja es el mantenimiento y soporte, debido a que no es posible obtener ayuda profesional de primera línea por no existir una licencia.

3.1.2.1- Administración

En cuanto a la generación y tratamiento de los certificados, la plataforma posee una desventaja que radica en que las operaciones con certificados deben realizarse manualmente a través de scripts, lo que resta funcionalidad y eficiencia al tratamiento de la información.

Generalmente, los avances tecnológicos en el campo de la autenticación y la encriptación se dan en el ambiente Unix, donde son adoptados en primera instancia y luego implementados por otros sistemas operativos.

3.1.2.2- Confiabilidad

Probablemente una de las características de los sistemas operativos, a la que mayor importancia le dan los administradores de sistemas, es la confiabilidad. Linux tiene tras de sí 30 años de desarrollo en Unix, el cual tiene la reputación de ser el más confiable de todos, y no es una reputación gratuita, pues muchos servidores han estado en operación durante años sin tener que ser arrancados de nuevo por alguna falla.

3.1.2.3- Escalabilidad

Entre las características mínimas que debe poseer un sistema operativo se puede mencionar: la capacidad para trabajar en un ambiente de red, comunicarse con diversos tipos de equipos, proporcionar servicios seguridad y autenticación para mantener segura la información, etc.

Facilidad de configuración y la posibilidad de hacerlo sin tener que reiniciar el servidor es otra característica de funcionalidad importante, la cual posee Unix.

Existen también ciertas aplicaciones cuya migración es limitada o simplemente se podría considerar inexistente, esto es sin duda un problema, sobre todo cuando ciertas empresas utilizan determinados paquetes de software que obviamente se encuentran desarrollados para una sola plataforma.

Un punto fuerte es el soporte multiplataforma de Linux sobre cualquier otra plataforma, esto implica la capacidad para correr aplicaciones diseñadas en otras plataformas así como también determinados servicios estándares.

3.1.2.4- Disponibilidad

En definitiva la instalación, configuración y mantenimiento de determinados servicios requiere indiscutiblemente de conocimiento avanzado debido en la mayoría de los casos, a que las aplicaciones necesarias para el funcionamiento de ciertos servicios no se encuentran desarrolladas en cuanto a facilidad, más sí en cuanto a estabilidad y código limpio de errores.

La disponibilidad del sistema ha sido tratada como un costo oculto, debido a que el monto de la información disponible con respecto a las cifras de tiempo en funcionamiento no permite un cálculo de costo real.

Sin embargo, la estabilidad del sistema operativo es únicamente un aspecto de la disponibilidad. Junto con otros factores, la plataforma de hardware juega un papel significativo.

3.1.2.5- Rendimiento

En este respecto es muy importante resaltar el hecho de que el hardware es responsable en gran medida, del desempeño del sistema. Este punto radica en la capacidad del sistema operativo para correr sobre plataformas de hardware poderosas y escalables. Tradicionalmente Unix ha mantenido el liderazgo en este campo, es por eso que las empresas con grandes necesidades de procesamiento ejecutan sus sistemas en alguna versión de este sistema.

La plataforma Linux se encuentra diseñada para proporcionar el mayor rendimiento sobre las aplicaciones y sobre los servicios de forma que los recursos necesarios para la ejecución del sistema son en la mayoría de los casos reducidos.

3.1.2.6- Soporte

El soporte está estrechamente ligado a la distribución y a la adquisición de la licencia por parte del usuario final; como en la mayoría de los casos y en pro del software de libre distribución el paquete es copiado informalmente y aplicado de forma particular a un sistema por lo que no existe soporte activo.

Esto conlleva de igual manera a mantener un mantenimiento informal y a una dependencia a expertos, sin duda la documentación sobre la plataforma Linux es muy amplia y todos los aspectos relacionados con la configuración y desarrollo constituyen una seudo especie de soporte.

3.1.2.7- Costo de propiedad

Tal vez este sea el factor más determinante en la adopción de Linux como plataforma de trabajo, pero no es el único debido a que el hecho de que la plataforma sea de libre distribución no implica directamente que su funcionalidad o aplicabilidad vayan a ser las mejores o que se puedan acoplar a los requerimientos completamente.

Linux es la plataforma más económica de instalar y operar. Aún cuando algunos costos iniciales son altos, la habilidad de escalar masivamente al sistema de forma horizontal sin pagar cargos adicionales por licencias, puede representar ahorros significativos a largo plazo.

3.1.3 Ventajas y desventajas

Cuadro 3.1: Ventajas Plataforma Linux

Ventajas	Descripción
Seguridad	Linux Se ha mantenido inmune del ataque de los virus que constantemente asedian a otras plataformas. Además, Linux ha sido utilizado en ambientes donde la seguridad es una necesidad a priori: instalaciones militares, plantas nucleares, oficinas federales, etc.
Estabilidad	Linux posee un modo de protección de memoria denominado Dumping, que libera procesos que poseen un funcionamiento sospechoso o que ocupan demasiados recursos, pero debido a que su actividad está reportada en segundo plano se permite un adecuado funcionamiento de todas las aplicaciones. Este sistema también evita el desbordamiento de memoria lo que ayuda a evitar que una aplicación inestable colapse todo el sistema.
Escalabilidad	• Las actualizaciones en Linux son totalmente gratuitas de igual manera que el paquete inicial, por lo que el mantenimiento de los servidores en el caso de que se publiquen revisiones de seguridad para los paquetes que se están utilizando es completamente sencillo. • La escalabilidad horizontal[11] es Linux es muy sencilla y económicamente conveniente al no existir precio por licencias adicionales.

[11] La escalabilidad horizontal es la capacidad que posee una plataforma para crecer añadiendo nuevos equipos de similares características al sistema inicial.

Precio	Puede copiarse y distribuirse libremente. Incluso las distribuciones preparadas para facilitar la instalación y el acceso a las funciones, como SuSE Linux, Red Hat, Linux y Mandrake Linux por mencionar algunas, pueden obtenerse por poco dinero.

Cuadro 3.2: Desventajas Plataforma Linux

Desventajas	Descripción
Compatibilidad	Únicamente ciertas casas comerciales desarrollan controladores y aplicativos para Linux junto con sus elementos de hardware, lo que limita la capacidad de los desarrolladores al momento de liberar una versión del kernel de Linux. Es por tal motivo que se considera limitada la compatibilidad de hardware sobre todo en los sistemas nuevos.
Soporte directo	Linux carece completamente de soporte directo para los sistemas implantados informalmente debido a que este tipo de servicios son adquiridos en la mayoría de los casos con la compra de una licencia
Variedad de distribuciones	Se han liberado un gran número de distribuciones de Linux, algunas estables otras no, lo que definitivamente confunde al consumidor potencial.
Migración	Existen también ciertas aplicaciones cuya migración es limitada o simplemente se podría considerar inexistente, esto es sin duda un problema, sobre todo cuando ciertas empresas utilizan determinados paquetes de software que obviamente se encuentran desarrollados para una sola plataforma.
Generación de certificados	Las operaciones sobre los certificados son realizadas en su mayoría de forma manual, de igual manera la administración y seguimiento de los mismos.

3.2- Plataforma Microsoft

Windows Server 2003 proporciona una arquitectura de llave publica probada a nivel empresarial, de fácil integración con otras plataformas y con una administración insuperable. A continuación se detalla las características de la plataforma.

3.2.1- Seguridad como autoridad certificadora

Windows Server 2003 facilita la implementación de una infraestructura de claves públicas, junto con tecnologías asociadas como las tarjetas inteligentes. Esto se traduce en una entidad certificadora robusta que implementa una variedad de servicios, incorporando de una manera intrínseca las siguientes medidas de seguridad.

Cuadro 3.3: Características de seguridad para una CA (Fuente Microsoft)

CARACTERÍSTICA	DESCRIPCIÓN
Renovación automática e inscripción automática de certificados	Windows Server 2003 posibilita la inscripción e implementación automática de certificados para los usuarios, y cuando el certificado caduque, podrá renovarse de forma automática. La renovación automática e inscripción automática de certificados facilita la implementación más rápida de tarjetas inteligentes y mejora la seguridad de las conexiones inalámbricas (IEEE 802.1X) mediante la caducidad y renovación automática de certificados.
Compatibilidad de Windows Installer con la firma digital	La compatibilidad con la firma digital permite que los paquetes y contenedores externos de Windows Installer se firmen digitalmente. Esto permite proporcionar a los administradores de tecnologías de la información unos paquetes de Windows Installer más seguros, lo cual resulta especialmente importante si el paquete se envía a través de Internet.

Mejoras en las listas de revocación de certificados (CRL)	El servidor de certificados incluido en Windows Server 2003 ahora es compatible con las CRL delta. Una CRL hace que la publicación de certificados X.509 revocados sea más eficaz y facilita que un usuario pueda recuperar un certificado nuevo. Y como ahora se puede especificar la ubicación en la cual se encuentra almacenada la CRL, resulta más fácil moverla para albergar las necesidades de seguridad y empresariales específicas.
Servidor de seguridad de conexión a Internet	Windows Server 2003 proporciona seguridad de Internet mediante el uso de un servidor de seguridad basado en software llamado Servidor de seguridad de conexión a Internet (ICF).
Servidor IAS/RADIUS seguro	El Servidor de autenticación de Internet (IAS) es un Servidor de usuario de acceso telefónico de autenticación remota (RADIUS) que administra la autorización y la autenticación del usuario.
Seguridad aumentada para servidores Web	Las características de seguridad avanzada de IIS 6.0 incluyen: servicios criptográficos seleccionables, autenticación de síntesis avanzada y control configurable de la obtención de acceso de los procesos.
Compatible con FIPS, modo de núcleo, módulo criptográfico	Este módulo criptográfico se ejecuta como un controlador en modo de núcleo e implementa algoritmos criptográficos aprobados por el Estándar federal de procesamiento de información (FIPS). Entre estos algoritmos cabe incluir: SHA-1, DES, 3DES y un generador de número aleatorio aprobado. El módulo criptográfico, compatible con FIPS, de modo de núcleo permite que las organizaciones gubernamentales implementan implementaciones de Seguridad de Protocolo Internet (IPSec) compatibles con FIPS 140-1
Administrador de credenciales	El administrador de credenciales de Windows Server 2003 proporcionará un almacén seguro para las credenciales del usuario, incluyendo contraseñas y certificados X.509. Estas credenciales proporcionan una experiencia sólida de inicios de sesión únicos para los usuarios, incluidos los usuarios móviles.

3.2.2- Costo Beneficio

3.2.2.1- Administración

Windows Server 2003 posee características avanzadas de administración con el fin de tener un control adecuado del servidor. Se cuenta con asistentes simplificados que facilitan la configuración de funciones de servidor y de las tareas habituales de administración de servidores, de tal forma que incluso los servidores que no disponen de un administrador dedicado son fáciles de administrar.

Las herramientas de implementación mejoradas, como los servicios de instalación remota, ayudan a los administradores a crear rápidamente imágenes del sistema y a implementar servidores. El servicio de instantánea de volumen mejora las tareas de copia de seguridad, restauración y capacidad de administración de redes de área del sistema.

La nueva Consola de administración de directivas de grupo (GPMC), permite a los administradores implementar y administrar mejor las directivas que automatizan las áreas de configuración de claves, como los perfiles móviles, la seguridad, la configuración y los escritorios de los usuarios.

Un nuevo conjunto de herramientas de línea de comandos permite a los administradores crear secuencias de comandos y automatizar las funciones de administración, permitiendo que la mayoría de tareas de administración se realicen desde la línea de comandos, si lo desean.

3.2.2.2- Confiabilidad

Windows Server 2003 proporciona confiabilidad gracias a una infraestructura integrada que le permite garantizar la seguridad de la información empresarial

Microsoft ha mejorado la manera en que Windows Server 2003 maneja los controladores de dispositivos, una de las principales causas del tiempo improductivo inesperado. Windows Driver Protection bloquea los controladores que presentan problemas al instalarse y dirige a los clientes a una versión actualizada, mientras que el Driver Rollback permite restablecer rápidamente Windows Server 2003 a un estado de trabajo cuando los controladores defectuosos llegan a afectar el desempeño.[12]

Otras mejoras que Windows 2003 Server a implementado son:

- Aislamiento de proceso de aplicaciones, que separa las aplicaciones para que una aplicación dañada no interrumpa el rendimiento de los servicios Web de las demás aplicaciones
- Réplica de memoria, que permite la recuperación veloz de los servidores tolerantes a fallas.
- Nuevas capacidades de agrupamiento, que simplifican la instalación y reconfiguración remotas de Windows Server 2003 sin la necesidad de reiniciar

[12] "Con más de 200 redes VPN empresariales administradas por nuestra plataforma de centro de datos y debido a la demanda de nuestros clientes de contar con disponibilidad 24x7, la confiabilidad es un tema muy crítico para nosotros", dijo Greg Moore, CEO y presidente de SmartPipes Inc. "Las innovaciones y mejoras de ingeniería que Microsoft ha integrado en Windows Server 2003 demuestran que la compañía toma muy en serio la confiabilidad de los sistemas de sus clientes".

3.2.2.3- Escalabilidad

Windows Server 2003 ofrece escalabilidad a través de "Scale-up", habilitado por multiprocesamiento simétrico (SMP) y "Scale-out", habilitado por clustering. Pruebas internas indican que, comparado con Windows 2000 Server, Windows Server 2003 da hasta un 140 por ciento de mejor desempeño en la administración de archivos y un rendimiento más significativo en varias otras características incluyendo servicio Microsoft Active Directory, servidor Web y componentes Terminal Server así como servicios de red. Windows Server 2003 abarca desde soluciones de procesador únicas hasta sistemas de 32 vías. Esto soporta procesadores tanto de 32-bits como de 64 bits.

El almacenamiento conectado a la red ayuda a consolidar los servicios de archivo. Otras mejoras serían la compatibilidad con la tecnología Hyper-Threading de Intel y la entrada-salida (E/S) por diversas vías de acceso, que colaboran al escalado de los servidores.

3.2.2.4- Disponibilidad

Windows Server 2003 ofrece una disponibilidad mejorada de soporte a clustering. Los servicios de clustering han llegado a ser esenciales para las organizaciones en cuanto a implementación de negocios críticos, comercio electrónico y aplicaciones de negocios en línea, porque proporcionan mejoras significativas en disponibilidad, escalabilidad y manejabilidad. La instalación y configuración de clustering es más fácil y más robusta en Windows Server 2003, mientras que algunas características de red mejoradas en el producto ofrecen mejor recuperación de fallos y un tiempo productivo alto del sistema.

Windows Server 2003 soporta clusters de servidor de hasta 8 nodos. Si uno de los nodos en un cluster no se puede usar debido a un fallo o por mantenimiento, inmediatamente otro nodo empieza a dar servicio, un proceso conocido como recuperación de fallos. Windows Server 2003 también soporta balanceo de carga de red, el cual nivela el tráfico de entrada dentro del Protocolo de Internet (IP), a través de los nodos en un cluster.

3.2.2.5- Rendimiento

- Como servidor Web es de un 100% a un 165% más rápido que Windows 2000 Server.
- Las características mejoradas del Directorio Activo permiten realizar tareas más fácilmente, entre las que destacan la habilidad de renombrar dominios, la posibilidad de redefinir el esquema y una replicación más eficiente.
- Mayor disponibilidad a través del Windows System Resource Manager, de las actualizaciones del sistema automáticas y gracias a un servidor cuyos parámetros le confieren la máxima seguridad por defecto.
- Ofrece la mejor conectividad, facilitando al máximo la configuración de enlaces entre delegaciones, acceso inalámbrico seguro y acceso remoto a aplicaciones a través de los Terminal Services, así como en su integración mejorada con dispositivos y aplicaciones.
- Combinado con Visual Studio .NET 2003, se convierte en la plataforma más productiva para implementar, ejecutar y gestionar aplicaciones conectadas mediante la nueva generación de servicios Web basados en XML.

3.2.2.6- Soporte

Las organizaciones tienen acceso a una amplia gama de soluciones y personal con experiencia en todo el mundo, incluyendo los 750.000 asociados que proporcionan hardware, software y servicios, así como los 450.000 profesionales certificados de Microsoft (MCP).

3.2.2.7- Costo de propiedad (TCO)

Microsoft diseñó Windows Server 2003 para ayudar a las compañías a darle valor añadido a sus negocios al mantener costes bajos. La alta fiabilidad de Windows Server 2003 ayuda a controlar costes al reducir fallos y tiempo de inactividad. Windows Server 2003 tiene la flexibilidad de escalar según la demanda.

Las herramientas poderosas de administración y configuración en Windows Server 2003 le permiten a los negocios implementar y administrar sistemas tan fácil y eficientemente como sea posible. La compatibilidad con aplicaciones heredadas y productos de otras compañías hará que las organizaciones no pierdan su inversión de infraestructura existente. Con la familia de Windows Server 2003, las organizaciones se benefician de una plataforma poderosa y robusta que ayuda a darle a los negocios valor hoy en día y en el futuro.

En conclusión con Windows Server 2003 se tiene menor TCO gracias a la consolidación de la tecnología más moderna, Windows Server 2003 proporciona muchos avances técnicos que ayudan a las organizaciones a disminuir el costo total de la propiedad (TCO).

3.2.3- Ventajas y Desventajas

Windows Server 2003 proporciona cuatro ventajas y 3 desventajas fundamentales

Cuadro 3.4: Ventajas Windows Server 2003

Ventaja	Descripción
Confiable	Windows Server 2003 proporciona confiabilidad gracias a: • Proporcionar una infraestructura integrada que le permite asegurar la seguridad de la información empresarial. • Proporcionar confiabilidad, disponibilidad y escalabilidad para que pueda proporcionarse la infraestructura de red que los usuarios requieren.
Productivo	Windows Server 2003 proporciona las herramientas que le permiten implementar, administrar y utilizar la infraestructura de red para obtener la máxima productividad. Windows Server 2003 lo consigue gracias a: • Proporcionar herramientas flexibles que permiten que el diseño y el desarrollo se adapten a las necesidades organizativas y de red. • Facilitar la administración proactiva de la red, mediante el establecimiento de políticas, la automatización de tareas y la simplificación de las actualizaciones. • Facilitar la disminución de la sobrecarga de los servicios de soporte técnico, aumentando la autosuficiencia de los usuarios.
Conectado	Windows Server 2003 ayuda a crear la infraestructura de soluciones empresariales para mejorar la conexión entre empleados, asociados, sistemas y clientes. Windows Server 2003 lo consigue gracias a: • Proporcionar un servidor Web y un servidor de multimedia de transmisión

	por secuencias integrados para facilitar la creación rápida, fácil y segura de sitios Web dinámicos para Internet e intranet. • Proporcionar un servidor de aplicaciones integrado para facilitar una administración, implementación y desarrollo sencillos de servicios Web XML. • Proporcionar las herramientas para permitir la conexión de servicios Web XML con aplicaciones internas, proveedores y asociados.
Ahorro de costos	Windows Server 2003, en combinación con los productos y servicios de la mayoría de asociados de hardware, de software y de canal, proporciona las opciones que facilitan la obtención de la máxima amortización de las inversiones en infraestructura. Windows Server 2003 lo consigue gracias a: • Proporcionar facilidad de uso y directrices para soluciones completas que permitan que la tecnología esté disponible con rapidez. • Facilitar la consolidación de los servidores, aprovechando las ventajas de las metodologías, el hardware y el software más actuales para optimizar las implementaciones de los servidores. • Disminuir el costo total de la propiedad (TCO) para obtener una rápida amortización de la inversión.

Cuadro 3.5: Desventajas Windows Server 2003

Desventaja	Descripción
Hardware	Como desventaja principal de Windows 2003 server es la necesidad de contar con equipos potentes para ejecutar las aplicaciones y servicios de una manera eficiente. Sin embargo teniendo la infraestructura física instalada la inversión se paga por si sola.
Preferencia en Ataques	Existe preferencia hacia ataques a servidores Microsoft por parte de hackers, se tiene la errónea idea de que atacar un servidor Microsoft Server 2003 es fácil debido a experiencias con otras líneas Microsoft de sistemas operativos. Por el contrario este sistema operativo es completamente nuevo e incorpora medidas de seguridad superiores. El mayor numero de ataques no significa mayor numero de ataques efectivos, es decir que un servidor bien configurado con todos los parches instalados es poco probable que se vea comprometido en un ataque
No es software libre	El código fuente de Windows 2003 Server no esta disponible para manipulación del usuario.

3.3- Benchmark

El siguiente test fue realizado por VeriTest, una división de Lionbridge Technologies. El test se realiza con diferentes configuraciones de hardware y configuraciones de procesador.

Para estos test Hewlett-Packard proveyó de 3 servidores.

- Un servidor HP ProLiant DL760 con 4 procesadores 900MHz Pentium III Xeon, 4GB de RAM y 4 adaptadores de servidor Intel PRO/1000 MF.
- Un servidor HP ProLiant DL760 con 8 procesadores 900MHz Pentium III Xeon, 4GB de RAM y 8 adaptadores de servidor Intel PRO/1000 MF.
- Un servidor HP ProLiant DL380 G2 con 2 procesadores 1.4GHz Pentium III, 2GB de RAM y 2 adaptadores de servidor Intel PRO/1000 MF.

Nota: Red Hat Linux 8 no es un sistema operativo soportado por el servidor HP DL760, como resultado no existe valores para este servidor

Las figuras 3.1 y 3.2 indican los picos de rendimiento en Mbps obtenidos en todos los test con las configuraciones antes mencionadas y los porcentajes de mejoramiento que se obtuvieron sobre Red Hat Linux

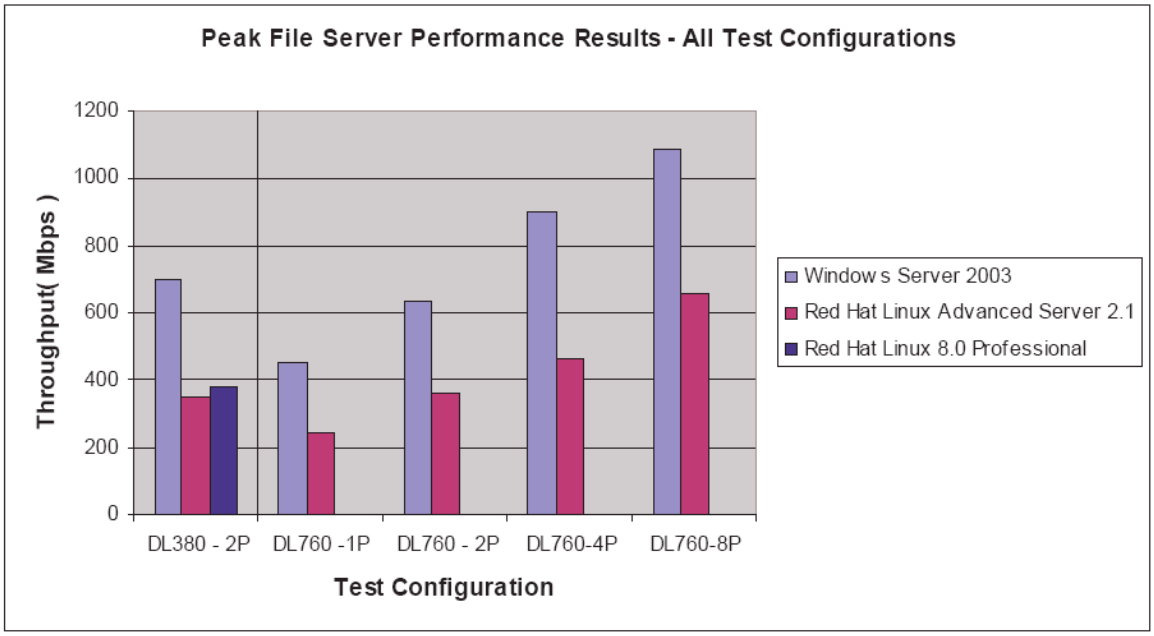

Figura 3.1 Benchmark realizado por VeriTest en servidores Windows 2003 Server y Red Hat Linux 8

Operating System	DL380 - 2P	DL760 -1P	DL760 - 2P	DL760-4P	DL760-8P
Windows Server 2003	700 Mbps	453 Mbps	632 Mbps	901 Mbps	1088 Mbps
Red Hat Linux Advanced Server 2.1	350 Mbps	244 Mbps	365 Mbps	462 Mbps	657 Mbps
Percent Improvement with Windows Server 2003 over Red Hat Linux Advanced Server 2.1	100%	86%	73%	95%	66%

Figura 3.2 Rendimiento del sistema operativo (Fuente: VeriTest)

La figura 3.3 muestra la curva de rendimiento obtenida en una prueba de carga de usuarios, como vemos Windows Server 2003 se comporto de una manera superior, esto se debe a que el sistema de Archivos Ext3 de Linux no maneja adecuadamente el arreglo de disco RAID 0, los servidor a utilizar en la entidad certificadora en un principio serán RAID 0 +1 de lo cual se concluye que Windows Server 2003 es la mejor opción.

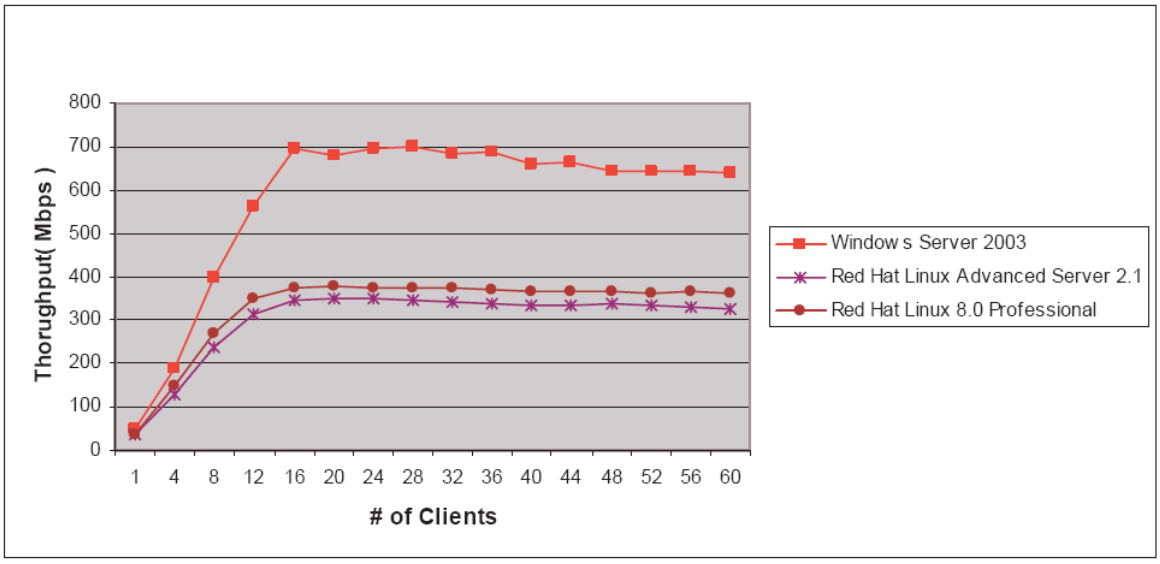

Figura 3.3 Test de rendimiento en configuración RAID (Fuente: NetBench)

3.3.1 Diagramas de red para las pruebas de servidor

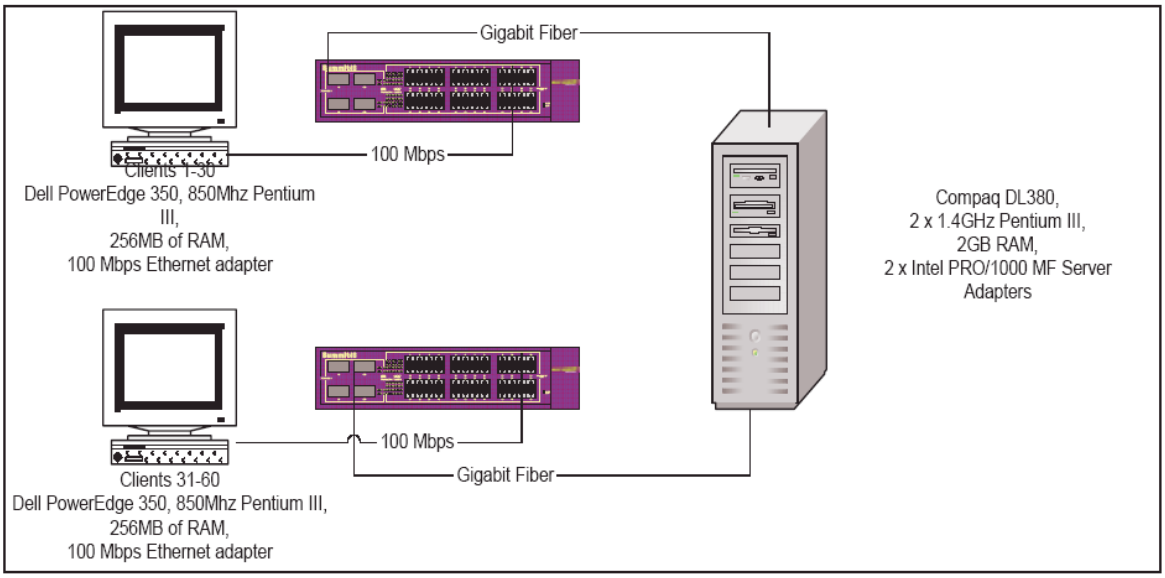

Figura 3.4 Configuración de prueba para servidor HP DL380 (Fuente HP)

La figura 3.5 indica el diagrama de red para un servidor HP ProLiant DL760 con 4 procesadores 900MHz Pentium III Xeon, 4GB de RAM y 4 adaptadores de servidor Intel PRO/1000 MF

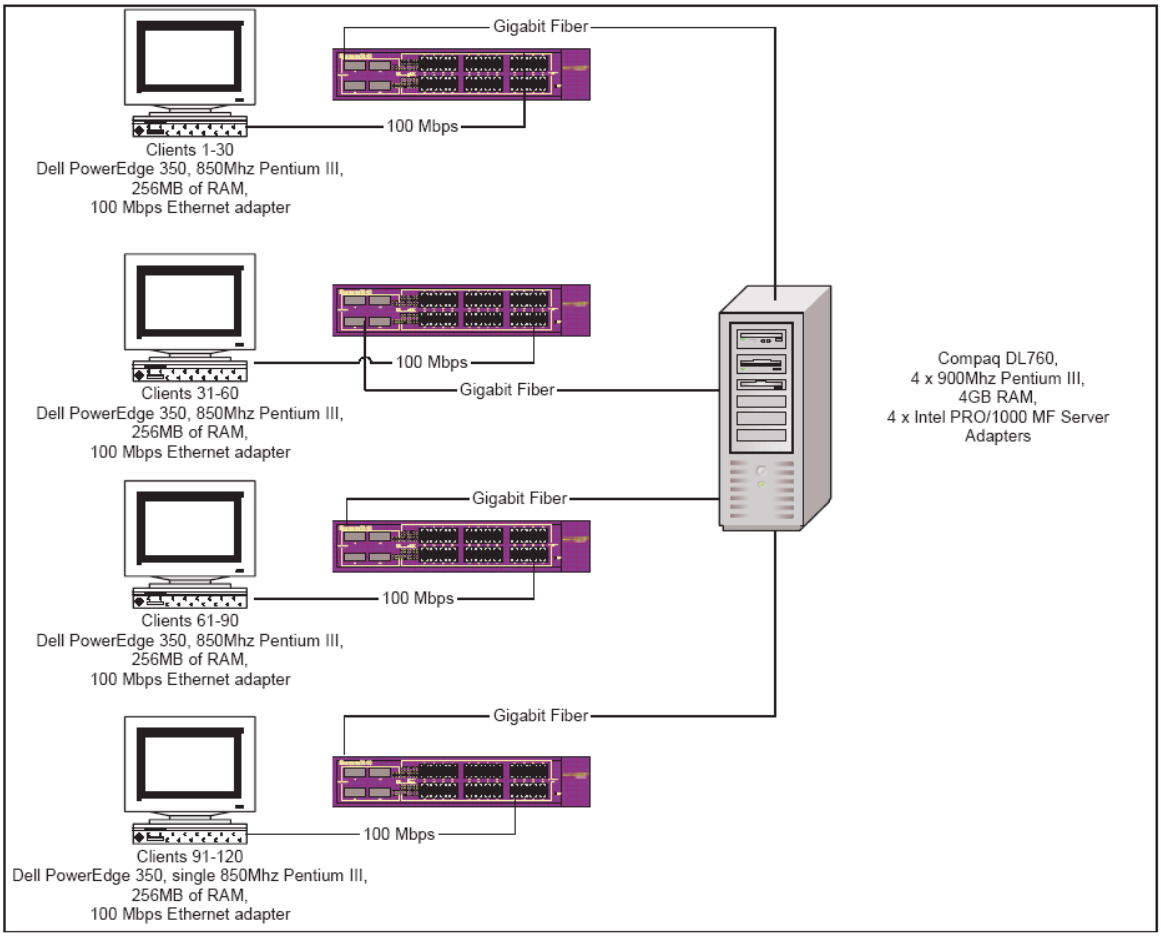

Figura 3.5 Configuración de prueba para servidor HP DL760 usando 4 procesadores

(Fuente HP)

La figura 3.6 indica el diagrama de red para un servidor HP ProLiant DL760 con 8 procesadores 900MHz Pentium III Xeon, 4GB de RAM y 8 adaptadores de servidor Intel PRO/1000 MF

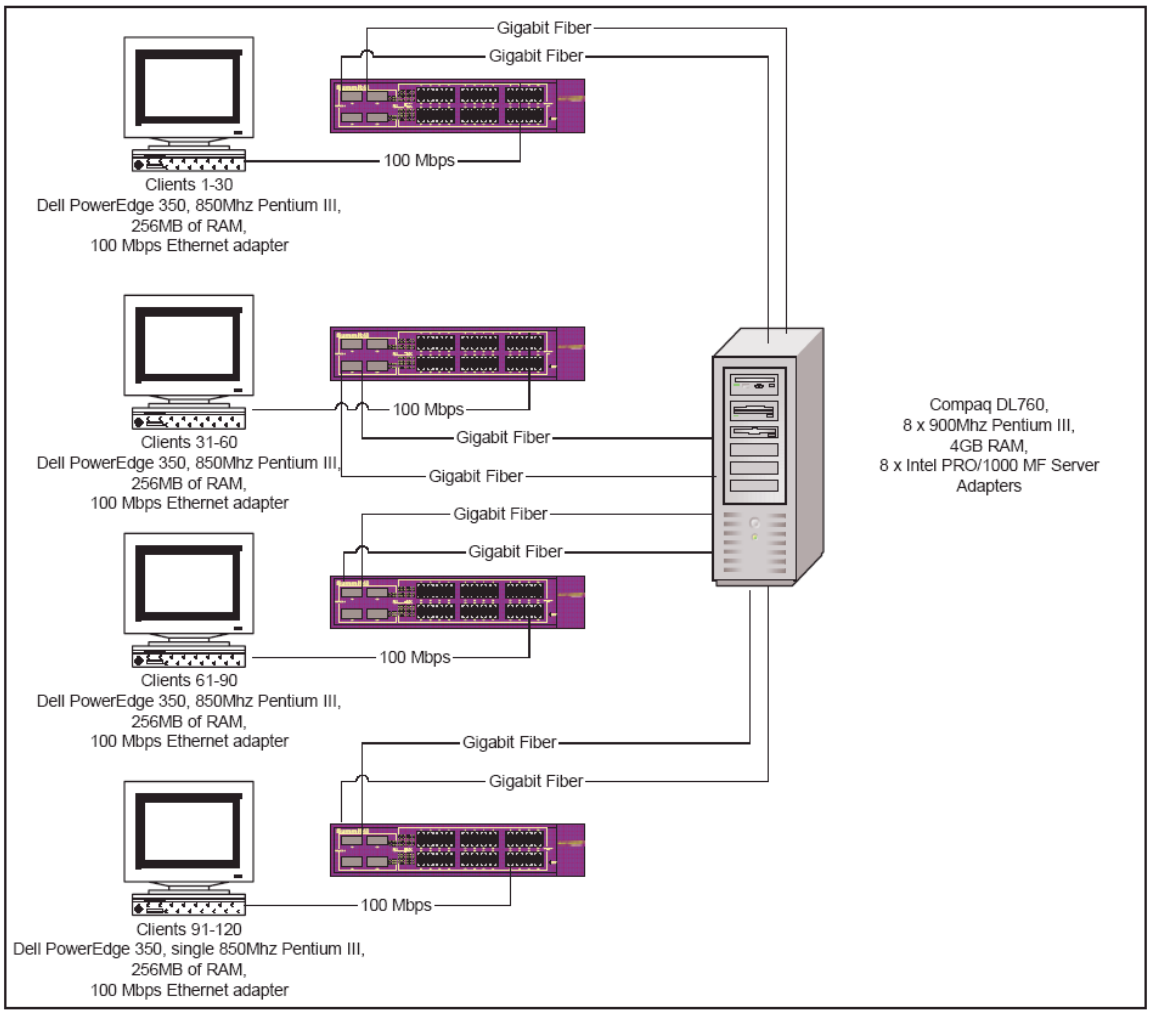

Figura 3.6 Configuración de prueba para servidor HP DL760 usando 8 procesadores

(Fuente HP)

CAPITULO IV

IMPLEMENTACION DE LA INFRAESTRUCTURA

4.1- Situación Actual CTT ESPE CECAI

4.1.1- Seguridades Físicas

- En el área que actualmente esta destinada para servidores se pudo observar que no se cuenta con los requerimientos mínimos de seguridad. No se cuenta con acceso físico seguro, el área esta totalmente expuesta.
- No se cuenta con un procedimiento de acceso al área segura y no están identificados los usuarios por roles y nivel de acceso administrativo. Los respaldos deberían ser guardados en una caja fuerte en un área diferente en donde reside el servidor, dicha seguridad no esta implementada.
- El área de servidores no posee medidas contra incendio o robo, así como protección eléctrica (UPS) que aseguren la disponibilidad del servicio, por lo que la inversión tecnológica esta en riesgo permanente.

4.1.2- Seguridades lógicas

- Los servidores deben estar tras un firewall para impedir ataques, dicho firewall no esta implementado.
- Cuentan con Active Directory para el manejo de Exchange, lastimosamente las características de seguridad que posee Active Directory están deshabilitadas en el servidor.

- No están implementadas políticas de seguridad, a tal punto que todos los usuarios poseen privilegios de administrador. Esta manera de operar en la entidad emisora de certificados implicaría una brecha de seguridad con implicaciones impredecibles.

4.1.3- Infraestructura tecnológica

- No poseen equipos adecuados para cumplir las funciones de servidores emisores de certificados
- No existe dispositivos de generación de claves y almacenamientos de las mismas
- No existe dispositivos que permitan realizar backup.
- El cableado que actualmente tiene el CTT ESPE CECAI no se encuentra bajo los estándares de conectividad, por que el rendimiento bajo condiciones de trabajo pueden ser comprometido creando un cuello de botella entre peticiones de usuario y servidor.

4.2- Diseño de la jerarquía de certificación

Diseñar la jerarquía de certificación es la primera tarea a realizar antes de implantar una infraestructura de llave pública. Esto es de vital importancia ya que de esto depende la emisión de certificados para las diferentes aplicaciones o usuarios que los requieran.

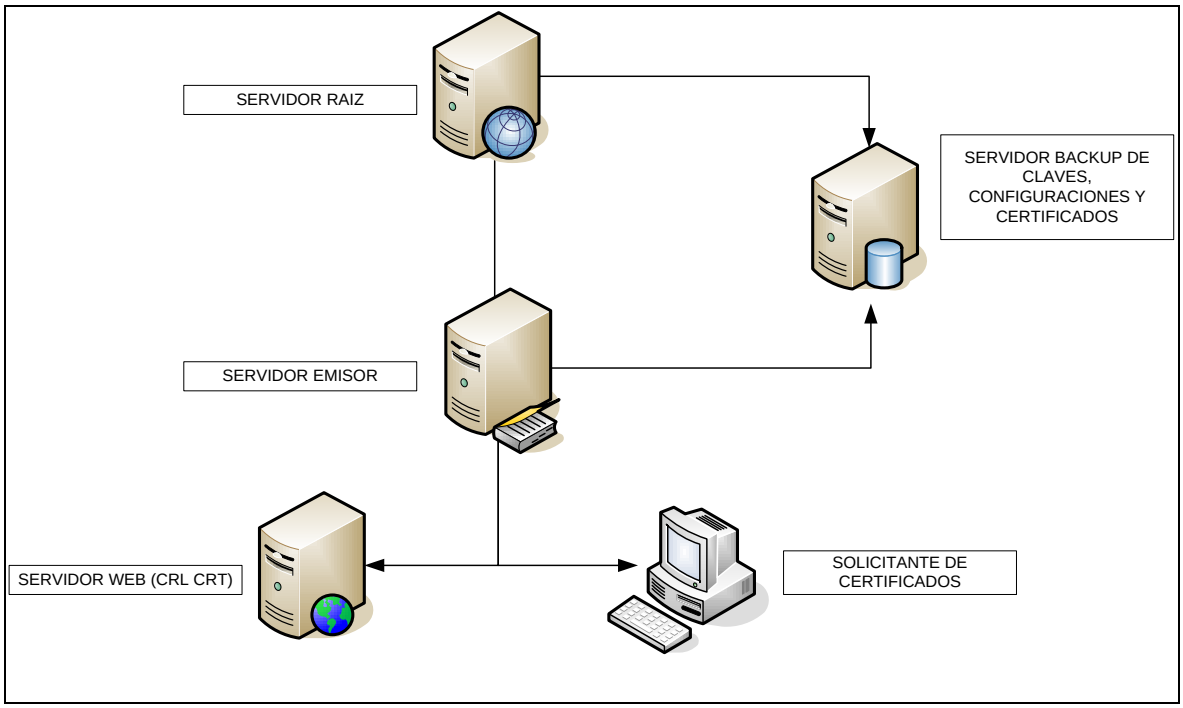

Figura 4.1: Jerarquía de la infraestructura de certificación

4.2.1- Pasos para identificar los requerimientos de diseño

4.2.1.1- Alcance del proyecto

El diseño de la infraestructura puede abarcar la jerarquía completa o una parte de la jerarquía si la infraestructura PKI ya existe. En el caso de la entidad emisora de certificados CTT ESPE CECAI, se necesitará una infraestructura completa con una

estrategia de administración centralizada en la cual el equipo de administración definirá las políticas.

4.2.1.2- Aplicaciones que usarán PKI

Es importante identificar la información que se desea proteger y el costo de implementación de un sistema de seguridad sólido en la organización. La entidad emisora de certificados CTT ESPE CECAI debe iniciar una etapa de prueba, en la cual por factores como costo elevado, recurso tecnológico de punta y área física segura se limitará a la emisión de certificados a las siguientes aplicaciones:

- Firma Digital
- Correo Seguro
- Servidor Web Seguro
- IPSec (Transmisión segura por redes inseguras)

4.2.1.3- Identificación de requerimientos técnicos

Los requerimientos técnicos influyen en el diseño en relación a cómo se debe implantar la tecnología. Los requerimientos técnicos que afectan el diseño son: seguridad, y disponibilidad.

4.2.1.3.1- Requerimientos de seguridad

El diseño de la jerarquía debe hacer cumplir las políticas y requerimientos de seguridad. Si fuera necesario tomar medidas adicionales de seguridad se debe adquirir dispositivos de almacenamiento de claves públicas y privadas como los HSM.

4.2.1.3.2- Requerimientos de disponibilidad

Este requerimiento es de suma importancia en razón de que según las aplicaciones que se establezcan en la organización y lo crítico que sea su uso se evaluará cuantas CA se necesitarán. Para la entidad emisora de certificados CTT ESPE CECAI en su primer año de funcionamiento se necesitará un servidor raíz y un servidor emisor como infraestructura básica.

Posteriormente cuando la entidad crezca se deberá incorporar servidores de alta capacidad, se implantarán módulos seguros de almacenamiento y una granja de servidores a fin de proveer redundancia y balanceo de carga, finalmente se delegará la administración a entidades subordinadas geográficamente distantes.

Este requerimiento puede afectar el diseño de dos maneras.

- Si se necesita que el servicio esté disponible 24 horas, los 7 días de la semana, se deberá contar con al menos dos entidades emisoras en la jerarquía, de tal manera que si una no está disponible, la segunda pueda seguir emitiendo.
- Si los certificados se emiten localmente la entidad debe ser colocada en los segmentos locales y de esta manera se reduce la cantidad de trafico WAN.

4.2.1.4- Identificación de Requerimientos de negocio

Establecer como funciona la entidad a nivel empresarial impacta en el diseño y en el costo de operación, para ello se debe identificar los requerimientos de acceso y requerimientos de administración.

4.2.1.4.1- Requerimientos de acceso externo

La entidad emisora de certificados está en la capacidad de emitir certificados por Internet, el diseño también debe incluir la publicación de la lista de revocación de certificados en un sitio público. La entidad emisora de certificados CTT ESPE CECAI recibirá solicitudes y emitirá certificados por medio del portal Web, pero la aprobación de certificados se lo hará manualmente por el administrador.

4.2.1.4.2- Requerimientos de administración

Estos requerimientos también afectan el diseño, debido a que el modelo centralizado requiere una sola entidad emisora de certificados. Se debe tomar en cuenta que la Entidad emisora de certificados CTT ESPE CECAI funciona bajo un criterio de administración centralizada, pero en un futuro se puede crear entidades emisoras subordinadas bajo la administración de un proyecto den Centro o de una facultad o departamento específico de la ESPE.

4.2.2- Pasos para diseñar los requerimientos legales

El objetivo es definir los requerimientos legales en la organización con el fin de usar los certificados que son emitidos por la entidad. Para ello se definen los siguientes pasos:

a) **Creación de una política de certificados.** Es un documento escrito que define como la organización emitirá los certificados, que medidas de validación del sujeto y los requerimientos legales que debe cumplir con el uso del certificado.

b) **Creación de la declaración de prácticas de certificación (CPS)**. Es una declaración de prácticas que la CA usa para emitir, revocar y manejar certificados.

c) **Publicación de la CPS**. Es aplicar lo escrito a políticas de servidor.

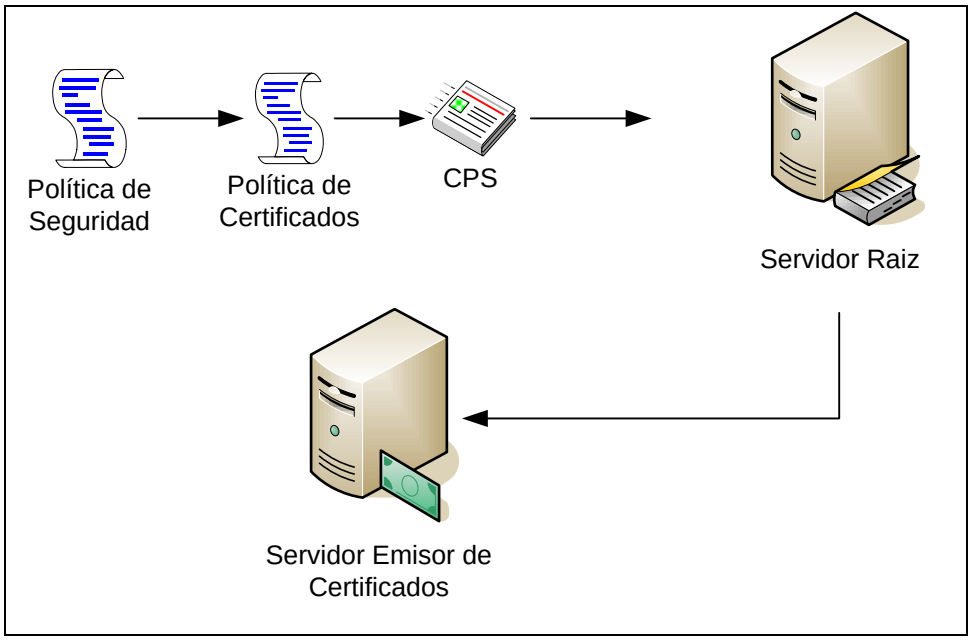

Figura 4.1 Diseño de los pasos legales

4.2.2.1- Políticas de Certificados

Define como es verificada la identidad del usuario antes de que se emita un certificado a este usuario, también explica como usar el certificado y sus llaves en transacciones.

Las políticas de certificados debe incluir:

- **El proceso de identificación del usuario:** Entrevista o credenciales
- **Requerimientos para el manejo de llaves privadas** Donde se almacena: tarjeta inteligente, dispositivo de almacenamiento, computador o si se puede exportar o archivar

- **Proceso de respuesta ante perdida o compromiso de llave privada***:* Determina quien es responsable y como responder ante una catástrofe
- **Requerimiento de registro y renovación**: Que identificación debe presentar un usuario y en que caso es necesaria una entrevista
- **Máximo valor de una transacción**.

Ver Anexo A (Políticas de Certificación para CTT ESPE CECAI)

4.2.2.2- Declaración de prácticas de certificación (CPS).

El CPS son lineamientos acerca de las prácticas que la CA usa cuando emite certificados, define como la política de certificado es aplicada a la arquitectura de llaves publica y a sus procesos operativos. El CPS traduce las políticas de certificado en procedimientos operacionales a nivel de CA. [13]

El CPS debe incluir:

- **Introducción:** Identifica al usuario que pide un certificado, también provee información de contacto con la organización.
- **Cláusula General**: Provee información de las obligaciones y responsabilidades legales y financieras.
- **Identificación y Autenticación**: Detalla como la autoridad identifica al usuario para la emisión y renovación de certificados.
- **Requerimientos Operacionales:** Describe requerimientos operacionales como emisión, revocación y auditoria de certificados, almacenamiento de llaves y recuperación ante un desastre.

[13] El CPS aborda la administración de la autoridad certificadora, la política de certificado se dirige hacia la administración y manejo del certificado en si

- **Control técnico de seguridad:** Describe las medidas de seguridad para la protección de la llave privada de la autoridad emisora.
- **Especificaciones de Administración:** Describe el mantenimiento del CPS, incluye procedimientos de publicación.

Ver Anexo B (Declaración de prácticas de certificación)

4.3.- Creación de la jerarquía

4.3.1- Creación de la entidad raíz fuera de línea

Como primer nodo de la jerarquía tenemos la entidad raíz, este servidor debe estar fuera de línea o desconectado de la red. Uno de los primeros pasos es la definición del archivo CAPolicy.inf.

4.3.1.1- Archivo CAPolicy.inf

Es un archivo opcional que provee información básica acerca de la entidad emisora de certificados y provee también información acerca del proceso de renovación de los certificados.

El archivo CAPolicy.inf se lo puede obtener de la página de Microsoft y modificarlo antes de instalar la entidad raíz.[14]

Ver Anexo C

[14] El documento en el cual se encuentra el archivo CAPolicy.inf es "Planning and Implementing Cross Certification and Qualified Subordination using Windows Server 2003".

4.3.1.1.1- Campos del archivo CAPolicy.inf

Los campos a definir en este archivo son:

- CPS
- Intervalo de publicación de los CRL
- Configuración para renovación
- Tamaño de la clave
- Período de validez para la entidad Raíz
- Punto de distribución para las CRL y AIA

Es importante considerar que el archivo CAPolicy.inf que es usa en la entidad raíz los campos “CRLDistributionPoint” y “ AuthorityInformationAccess” deben ir vacíos, ya que esto asegura que el chequeo de revocación no se lo haga a nivel de entidad raíz.

4.3.1.1.2- Identificador OID

Es un número que identifica un objeto, se puede obtener este identificador gratuitamente y con reconocimiento público a través de la IANA. Este identificador puede ser parte de la definición del archivo CAPolicy.inf

4.3.2- Definición de configuración para una entidad fuera de línea

Es importante documentar la configuración después de la instalación exitosa de la entidad, de esta manera en el caso de un desastre se pueda reconstruirla. A continuación se detalla las configuraciones a tomar en cuenta.

- ***CA Policy:*** Se debe instalar la entidad como standalone o independiente de esta forma puede ser removida de la red
- ***Nombre de Computador***: No puede ser cambiado una vez que se instala en servicio de certificaos.
- ***CA Name:*** El nombre de la Entidad describe el propósito de la misma. Puede usar un sufijo en el caso de que pertenezca a un bosque o dominio.
- ***CSP:*** Es el proveedor de servicios criptográficos, es importante definirlos en esta etapa ya que en ellos se basa la generación de las claves y certificados. Las llaves privadas que el CPS genera se guardan y encriptan en un almacenamiento seguro.

4.3.3- Seguridad para las claves privadas

La seguridad es primordial para la entidad emisora de certificados, para ello es altamente recomendable que se use HSM (Módulos de seguridad por hardware)[15]. Si las claves se guardan en un disco duro o sistema de memoria están expuestos a robo por parte de un hacker, que puede incluso tomar el control del servidor. Esto obliga a la generación de nuevas claves privadas y el reemplazo de todos los certificados emitidos, causando pérdidas irreparables en costo y tempo. Por lo tanto se debe proceder de la siguiente manera:

- La generación, almacenamiento y administración de claves se las debe hacer a través de HSM´s.
- Las operaciones de firma de certificados son realizadas exclusivamente por el HSM.

[15] Los módulos de hardware de seguridad están diseñados para proteger y gestionar datos clave de forma segura. Su característica principal es que el algoritmo de cifrado se encuentra diseñado por hardware y no por software, ofreciendo velocidad en la generación de claves y el proceso de cifrado.

- Usar HSM para las operaciones de encriptación libera de carga al procesador del servidor.

4.3.4- Prácticas seguras de negocio

- La administración de la entidad se la debe hacer solo por personal de alta confianza.
- Una vez que se obtenga las CRL´s del servidor, estas deben ser propagadas manualmente a un punto de distribución fuera del área segura.
- Realice la publicación de las CRL varias días antes, esto permite detectar fallas y garantiza la propagación correcta de las CRL´s.

4.3.5- Guía para el despliegue de una Entidad Raíz Fuera de Línea

Esta guía tiene el fin de ayudar al despliegue exitoso de una CA fuera de línea, también reduce el tiempo de rediseño si fuera el caso.

- No conecte la CA raíz a la red
- Las extensiones CSP y AIA para la entidad raíz deben ir vacías.
- Implemente seguridad con HSM
- Escoja la longitud de la clave de tal manera que permita a los protocolos y aplicaciones manejar la clave
- Use un nombre distintivo para la CA de tal manera que identifique el propósito y permita reconocerla ante los usuarios.
- Implemente periodos largos de validez, normalmente 10 a 20 años, esto reduce carga administrativa al renovar frecuentemente los certificados.

4.3.6- Puntos de Publicación

Es importante que los usuarios puedan acceder a la información de revocación de los certificados. La Autoridad emisora de certificados CTT ESPE CECAI posee los servicios de Active Directory pero a un nivel de uso exclusivo, de forma tal que no podemos hacer uso del mismo para las operaciones con certificados por lo tanto se debe buscar otro mecanismo de publicación, para ello se usara servidores Web, FTP o Servidor de archivos, los cuales estarán ubicados tanto en la Intranet como en la extranet.

4.4- Administración de una infraestructura de clave pública

4.4.1- Introducción

Los certificados y autoridades de certificación (CA) son los dos componentes principales de una infraestructura de clave pública (PKI) esto requiere una planificación detallada para el diseño y la implementación de la PKI. Es necesario manejar estos dos componentes para asegurar que una PKI funciona adecuadamente durante su operación normal y en caso de un desastre.

Para reforzar la seguridad de la PKI, es necesario dividir la administración de CA y los certificados entre los distintos grupos de usuarios. De esta manera, se asegura que ningún usuario maneje todos los aspectos de la PKI.

La administración de certificados y CA incluyen varias tareas de dirección. Individuos en roles específicos de administración de la PKI realizan estas tareas. El administrador de la CA decide cuales usuarios o grupos asignar a los roles predefinidos.

4.4.2- Administración de tareas de infraestructura de clave publica.

La administración de un ICP consiste en dos categorías de tareas de administración:

a) Administración de certificados
b) Administración de autoridad certificadora

4.4.2.1- Administración de certificados

La administración de certificados incluye las siguientes tareas:

- **Emite o niega las peticiones de certificados pendientes**. De esta manera el administrador de certificados puede evaluar la solicitud del certificado, asegurar que pertenece a un usuario autorizado, computadora o servicio y emitir o denegar la solicitud del certificado.
- **Revocar los certificados emitidos.** El administrador de certificados debe revocar un certificado si el recipiente del mismo rompe las reglas que se encuentran definidas en la declaración de prácticas de certificados o si la clave asociada por el certificado se encuentra comprometida. La revocación termina la validez del certificado antes de que su periodo de validez expire.
- **Determinar los agentes de recuperación de llaves (KRA).** Un administrador de certificados determina cuales KRA definidas pueden descifrar una llave privada almacenada desde la base de datos de la CA.

4.4.2.2- Administración de autoridad certificadora.

La administración de la CA incluye las siguientes tareas:

- **Instalar CA**. Cuando se define una CA, se designa una persona para realizar la instalación y la configuración inicial de la CA.
- **Renovar certificados de CA**. Es necesario renovar el certificado de la CA periódicamente para asegurar que su validez continúa.
- **Definir agentes de recuperación de llaves**. Un administrador de certificados determina uno o más KRA cuyas llaves publicas cifran las llaves privadas almacenadas en una CA. Las KRA pueden entonces usar sus llaves privadas para recuperar las llaves privadas almacenadas en la base de datos de la CA.

- **Definir administradores de certificados**. Se designan administradores de certificados para emitir y denegar las solicitudes de certificados y para extraer llaves privadas cifradas de la base de datos de la CA como recuperación de llaves.
- **Respaldar y recuperar la CA.** Respaldar la información de la base de datos de la CA y su posterior recuperación asegura que se puede disponer del contenido de la base de datos en caso de falla de la CA.
- **Auditar los servicios de certificados.** Es necesario auditar todas las tareas de administración de servicios de cerificados para asegurar que las personas que ejecutan esas tareas están siguiendo todas las reglas definidas en las políticas de seguridad de la organización

4.4.3- Roles de criterio común en la administración de una infraestructura de clave pública

Se utiliza una administración basada en roles[16] para organizar la administración de la CA en varios roles basados en tareas definidos previamente. Para asignar un rol a un usuario o un grupo, se aginan permisos de seguridad, membresías de grupo o derechos de usuario asociados con el role.

Distribuir roles de administración entre varios individuos en la organización para asegurar que una sola persona no pueda comprometer los servicios de PKI. La separación de roles capacita a una persona para verificar las acciones de otra.

El criterio común de administración de roles en PKI incluye:

- **Administrador de CA**. Configura y mantiene la CA, designa administradores alternos, administradores de certificados y se encarga de la renovación de los certificados de la CA.
- **Administrador de certificados.** Aprueba o deniega los registros para las solicitudes y la revocación de los certificados emitidos.
- **Operador de respaldos**. Realiza un backup de la base de datos de la CA, la configuración de la CA y del par de llaves pública y privada de la CA (Conocido también como par de llaves).
- **Auditor.** Define que eventos van ha ser auditados en los Servicios de Certificación y las revisiones de los registros de seguridad de un adecuado funcionamiento de los eventos relacionados con Servicios de Certificación.

[16] La separación de roles es soportada únicamente en Autoridades de Cerificados independientes sobre plataformas Windows Server 2003.

Se definen los roles de administrador de CA y administrador de certificados en cada CA en toda la jerarquía establecida. Los roles de operador de respaldos y de auditor no son definidos explícitamente en ningún grupo de políticas local directamente relacionado con un computador en la CA.

4.4.4- Tareas del administrador de certificados

Un administrador de certificados es responsable de todas las funciones de dirección del certificado que ha sido emitido por una CA. Las funciones de administración incluyen la emisión o denegación de certificados pendientes (sujeto de la declaración de prácticas de certificados de la CA), eliminación de certificados de la base de datos de la CA así como también la revocación de certificados previa la expiración de su periodo de validez.

Un usuario al cual se le asignan permisos de Administración y Emisión de certificados mantiene el criterio común de Administrador de certificados. Un administrador de certificador realiza las siguientes tareas:

- **Emisión de certificados**. Un administrador de certificados puede emitir un certificado únicamente si la solicitud del mismo es válida.
- **Eliminación de certificados**. Un administrador de certificados puede eliminar un certificado de la base de datos de la CA si el certificado ha sido revocado o ha espirado.
- ***Denegar solicitudes de certificados***. Si el certificado se encuentra en un estado pendiente el administrador de certificados puede denegar la solicitud del certificado si dicha solicitud no es valida.

- **Revocar un certificado**. Si el recipiente del certificado rompe las reglas establecidas en las políticas de seguridad de la organización o si la llave privada de un certificado se encuentra comprometida, un administrador de certificados puede revocar un certificado y terminar la validez del mismo antes de la finalización de su periodo de validez.
- **Determinación de los Agentes de Recuperación de Llaves**. Un administrador de certificados puede verificar las propiedades de un certificado usando una llave privada almacenada para determinar cual KRA puede recuperar la llave privada almacenada. El administrador de certificados recupera la llave privada almacenada de la base de datos de la CA y provee la información extraída a los KRA para su recuperación.

4.4.5- Restricciones del administrador de certificados

A pesar de que algunas políticas de seguridad organizacionales permiten al administrador de certificados administrar todos los certificados que se encuentran emitidos por una CA, otras organizaciones requieren que el administrador de certificados maneje únicamente un subconjunto de los certificados emitidos.

Las restricciones para el administrador de certificados permiten al administrador de CA limitar a los administradores de certificados para que manejen solamente los certificados emitidos por un grupo de seguridad específico. Si una computadora no pertenece a un grupo de seguridad que el administrador de certificados esté habilitado para manejar, las funciones del administrador de certificados se ven completamente limitadas.

Para restringir un administrador de certificados, el administrador de la CA debe asignar permisos hacia la cuenta del administrador de certificados. Si se asignan permisos para Emitir y Administrar Certificados a un grupo no se pueden asignar restricciones individuales para los administradores de certificados que sean miembros del grupo.

4.4.6- Otras tareas del administrador de certificados

Adicionalmente a las tareas que realizan en el rol de Administrador de Certificados, existen otras tareas relacionadas con la administración de certificados como son la publicación de la lista de revocación de cerificados información que no esta incluida en el rol de Administrador de Certificados (CRL).

4.4.6.1- Publicación CRL

Por defecto, usuarios y grupos que tienen asignados los permisos de Administración de CA pueden publicar CRL y CRL delta en la CA.

Adicionalmente para la publicación de CRL, un usuario o grupo que tiene permisos de Administración de CA pueden modificar el intervalo de de publicación de CRL. Intervalos de publicación separados están definidos para las CRL y las CRL delta.

4.4.7- Definición global de roles

Cuando se implementa la separación de roles solamente ciertos roles específicos pueden ejecutar las tareas de instalación y configuración. Ver Anexo E

Se pueden dividir las responsabilidades de la CA entres tareas generales:

- *Instalación*. Solamente los administradores locales de una computadora pueden instalar Servicios de Certificación para crear una CA. Si la CA es una empresa, el instalador debe ser también un miembro del grupo de administradores empresariales, entonces el instalador puede cambiar la configuración nombrando al contexto con el nuevo nombre y la información de la CA.
- *Ver*. Cuando se habilita la separación de roles solamente los titulares de los roles de criterio común pueden ver la configuración actual de la CA. Los miembros de los grupos de Administradores locales no pueden ver la configuración de la CA a menos que sean asignados a un rol simple de administración de PKI.
- *Modificar*. Únicamente los administradores de la CA pueden modificar la configuración actual de la CA cuando la separación de roles esta implementada. La única excepción a esta regla es cuando el certificado de la CA es renovado. Únicamente los miembros del grupo de administradores locales pueden renovar el certificado de una CA empresarial. Para poder renovar el certificado es necesario deshabilitar la separación de roles temporalmente[17].

[17] Un administrador local puede ver y modificar la configuración de la CA en cualquier momento deshabilitando la separación de roles. Es necesario asegurarse de auditar los eventos en la CA para determinar si un administrador local está modificando la configuración de la CA.

Tabla 4.1: Roles y ejecución

Rol o grupo	Instalar	Ver	Modificar
Administrador de la CA		✓	✓
Administrador de Certificados		✓	
Auditor		✓	
Operador de respaldos		✓	
Administrador Local	✓		
Administrador Corporativo	✓		

4.4.8- Renovación de un certificado de CA

La renovación de un certificado de CA re realiza cuando ocurre un cambio en las políticas de certificados o cuando el certificado emitido para la CA expira. Como cualquier cuenta cada CA emite un certificado también. Una CA raíz emite un certificado para si misma. Una CA subordinada obtiene su certificado de su CA padre. Cada CA tiene un periodo de validez definido, durante el cual la CA puede emitir certificados. Después que la CA alcanza la fecha de expiración. La CA no tiene un certificado válido para si mismo.

Cuando se renueva un certificado para una CA, se puede reutilizar su par de llaves existente o se puede generar un par nuevo. No es posible rehusar un par de llaves más de dos veces debido a que es matemáticamente posible derivar la clave privada a través de la clave pública. Si se genera un nuevo par de claves para la CA, la CA crea una CRL separada para ese par de llaves.

Cuando se escoge el tamaño del par de llaves para la CA, es necesario que la clave no sea ni muy grande ni muy pequeña. Claves muy pequeñas pueden comprometer la clave privada. Si se implementa una clave muy grande, puede tomar mucho tiempo para el Proveedor de Servicios de Criptografía (PSC) para generar el par de llaves. Cuando se renueva un certificado de CA, se puede implementar una clave más grande si la primera fue muy pequeña. Para proteger a la CA contra atacantes que intentan determinar la llave privada en función de la llave pública es recomendable implementar una clave entre 1024 y 4096 bits.

4.4.9- Auditar Servicios de Certificación

Es posible habilitar la auditoria en una CA para proveer un registro para todas las CA y las tareas de administración de certificados. Todos los Servicios de Certificación auditados son reportador en el Visor de Eventos del sistema.

Se pueden habilitar auditorias para los siguientes eventos para Servicios de Certificados en una CA. Esos eventos registran quien ejecuta las tareas de auditoria:

- Respaldos y recuperación de la base de datos de la CA.
- Cambios en la configuración de la CA.
- Cambios en los valores de la configuración de seguridad.
- Emitir y administrar solicitudes y certificados.
- Revocar certificados y publicar CRL.
- Guardar y recuperar claves guardadas.
- Iniciar y detener servicios de certificados.

Para habilitar la auditoria en para Servicios de Certificación:

- Configurar el servidor para auditar fallos y aciertos para acceso a objetos.
- Habilitar todos los eventos de Auditoria para la CA.
- Definir quien puede realizar las auditorias asignando a un usuario o grupo los permisos de Administración de Auditoria y de registros de seguridad. Definiendo quien puede realizar la auditoria se habilita al usuario o al grupo para auditar todos los eventos en la CA, no solo los eventos relacionados con CA[18].

4.5- Recuperación de desastres

4.5.1- Plan para recuperación de desastres

El uso de recuperación de desastres para restaurar el sistema si el disco duro falla y es necesario reemplazarlo o reformatearlo. Es posible restaurar el sistema si archivos críticos del sistema son accidentalmente borrados o corrompidos[19].

Recuperación de desastres incluye preparación para resolver problemas del sistema y recolectar la información acerca del sistema y las opciones de reparación y recuperación. Para Servicios de Certificación, se implementa un plan de recuperación de desastres cuando:

[18] Para poder asegurar que se mantiene la separación de roles no se deben asignar los permisos de Administración de Auditoria y registros de seguridad a los miembros los grupos de Administradores de CA y Administradores de Certificados.

[19]Es posible utilizar recuperación de desastres después de que se ha intentado reparar el sistema usando Modo Seguro, Consola de recuperación, y Proceso de Reparación de Emergencia.

- *Los Servicios de Certificación fallan*...Los Servicios de Certificados no inician cuando existen versiones incorrectas de los Servicios de Certificados en la CA, o cuando un aplicación o librería esta dañada en la CA.
- *La CA esta configurada incorrectamente.* Una configuración incorrecta de la CA puede causar un fallo en el inicio de los Servicios de Certificación, se puede configurar la CA a sus valores previos realizando el proceso de recuperación de desastres.

En el plan de recuperación de desastres debe constar la siguiente información:

- *Recuperación desde un fallo de hardware*. Se basan en las políticas de seguridad de la organización, determina la solución para recuperar un fallo de hardware. Es posible mantener hardware duplicado para la recuperación de una CA o mantener dispositivos duplicados para los componentes principales de la CA, como el CPU o la Tarjeta madre.
- *Recuperación de una CA comprometida*. Si una CA se encuentra comprometida el plan de recuperación de desastres debe incluir un plan para la reconstrucción de la CA y las acciones a tomar para los certificados emitidos. Típicamente se pueden revocar los certificados emitidos y generar nuevos.
- *Minimizar el riesgo de fallo de una CA*. Administrar el riesgo de un fallo de hardware implementando hardware redundante.

4.5.2- Métodos para respaldar una CA

Es posible respaldar un Servidor de Certificados utilizando dos métodos: Un respaldo automático de sistema o un respaldo manual. Se puede planear respaldar de forma regular, independientemente de si la CA en una CA fuera de línea o una CA emisora. Se utilizan respaldos completos para proveer la recuperación más rápida y la más confiable redundancia de datos.

4.5.2.1.- Respaldo automático de sistema

El método adecuado para respaldar una CA sobre Windows Server 2003 es un respaldo automático de sistema. Se utiliza este método en la computadora que actúa como Servidor de Certificados para respaldar la base de datos, archivos de registro, el par de llaves y toda la configuración de registro de la CA

Este tipo de respaldo no incluye únicamente la configuración del Servidor de certificados y los archivos, este también incluye los componentes principales del sistema operativo. Cuando se restaura la CA utilizando este método se recuperan todos los aspectos de la computadora que almacena el Servidor de Certificados.

4.5.2.2.- Respaldo manual

Se puede realizar un respaldo manual de la CA utilizando el Asistente para respaldo del Servidor de Certificados. Un respaldo manual incluye la base de datos y los archivos de registro de la CA. Este puede incluir el par de llaves de la CA, pero no incluye los valores de la configuración del registro. Es recomendable utilizar un respaldo manual únicamente cuando el respaldo automático de sistema no este disponible.

Para respaldar el Servidor de Certificados utilizando un respaldo manual, se debe respaldar el Servidor de Certificados e IIS. Cuando se respalda IIS se esta respaldando la metabase también. La metabase de IIS incluye extensiones que son creadas mediante las páginas de Registro Web las mismas que son instaladas con el Servidor de Certificados.

4.5.3.- Recuperación de servicios de certificados

Para la recuperación de una CA, se deben restaurar los Servicios de Certificados. El método usado para la restauración del Servidor de Certificados depende de lo que se este restaurando. Si se está respaldando el hardware que la CA usa se debe restaurar los Servicios de Certificados desde el respaldo automático del sistema. Si se esta respaldando los Servicios de Certificados únicamente en la CA se debe restaurar los servicios de certificados desde Servicios de Certificados y desde el respaldo de la metabase de IIS.

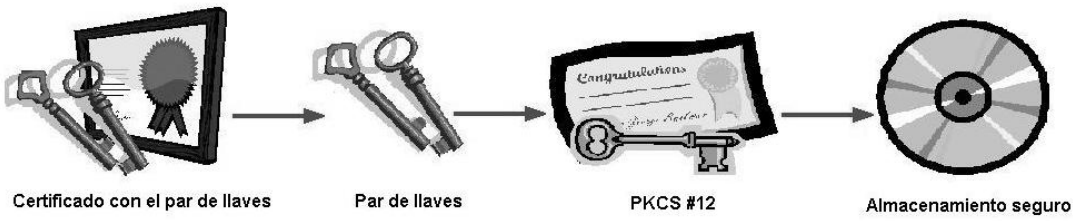

Figura 4.2: Esquema de almacenamiento de llaves

El método también difiere dependiendo de si la CA fue respaldada utilizando el Respaldo Automático de Sistema o si se utilizó el asistente de respaldos de la CA y el asistente de respaldos de IIS. Si se utiliza el Respaldo Automático de sistema este será el único método de restauración de la CA.

4.6.- Configuración del almacenamiento de llaves y su recuperación

4.6.1- Introducción

Si se pierde un par de llaves publica y privada (usualmente nos referimos a ellas como par de llaves) y los certificados relaciones debido a un fallo del sistema o a cualquier otra razón, esto puede consumir tiempo y gastos en reemplazar las llaves y los datos que las llaves protegen. Como una parte del plan de administración de certificados es necesario crear una estrategia para la recuperación de los datos y las llaves.

Usando el almacenamiento y recuperación de llaves, se puede almacenar y recuperar la porción privada de un par de llaves, si un usuario pierde su clave privada o un administrador debe asumir el rol de un usuario por acceso o recuperación de información.

La recuperación de la llave privada no recupera ninguna información adicional. En lugar de eso esta recuperación habilita al usuario para acceder información cifrada restaurando la llave perdida o dañada del perfil del usuario

4.6.2- Recuperación de datos y recuperación de llaves

- **Recuperación de datos**. Permite a los agentes de recuperación de datos acceder a datos cifrados sin acceder al material de la llave privada del usuario que originalmente cifró la información.
- **Recuperación de llaves**. Permite a los Agentes recuperadores de llaves (KRA) recobrar el certificado original, la llave privada y la llave pública que son usadas para cifrar la información desde la base de datos de la CA.

4.6.2.1- Recuperación de datos

Se escoge la recuperación de los datos cuando:

- No existe PKI.
- No es necesario para los usuarios administrar certificados o llaves privadas.
- Las políticas de seguridad no permiten la recuperación del material de la llave privada.

4.6.2.2- Limitaciones de la recuperación de datos

Las limitaciones de la recuperación de datos son:

- Los usuarios no pueden recuperar su propia información. La recuperación de la información es un proceso administrativo.
- La recuperación de datos es un proceso manual y ocurre archivo por archivo básicamente.
- Los usuarios deben inscribirse para nuevos certificados debido a que la recuperación de datos no recupera las llaves de los usuarios.
- Puede ser necesario para los administradores revocar certificados EFS emitidos previamente si la clave privada está comprometida.

NOTA: Estas limitaciones son inherentes a la tecnología y serán revisadas en nuevas versiones del sistema operativo.

4.6.2.3- Recuperación de llaves

Se escoge la recuperación de llaves cuando:

- Cuando la organización quiere limitar la inscripción de certificados.
- Se requiere minimizar la revocación de certificados existentes.
- Se requiere recuperar la información cifrada en aplicaciones que non sean EFS.
- Se quiere importar el certificado y el par de llaves en varios computadores.

4.6.2.4- Limitaciones de la recuperación de llaves

Las limitaciones de la recuperación de llaves son:

- La recuperación de llaves de usuario es un proceso manual que involucra administración de certificados, KRA y usuarios.
- La recuperación de llaves permite a los KRA acceder a las llaves privadas de usuarios.

NOTA: Estas limitaciones son inherentes a la tecnología y serán revisadas en nuevas versiones del sistema operativo.

4.6.3- Almacenamiento de llaves y recuperación de llaves

Se utiliza el almacenamiento y la recuperación de la información, para recuperar una llave guardada o pedida. Este proceso es implementado en dos fases (almacenamiento de llaves y recuperación de llaves) y es también conocido como *custodia de llaves*.

Los usuarios pueden perder una llave privada debido a lo siguiente:

- **Eliminación del perfil de un usuario**. Un programa proveedor de servicios de criptografía (PSC) cifra y almacena la llave utilizando un API de protección de datos. La llave privada cifrada es almacenada en el sistema de archivo local y registrado en la carpeta del perfil del usuario. La eliminación del perfil resulta en la perdida de la llave privada.
- **Reinstalación del sistema operativo**. Cuando se instala el sistema operativo no se puede acceder a los perfiles previos, incluido el material de llave cifrada que se encuentra almacenado en la carpeta del perfil del usuario.
- **Daño de disco**. Si el disco está dañado algunos usuarios no podrían ingresar a su perfil, el acceso a la llave privada se pierde también.
- **Robo del computador**. Cuando la computadora de un usuario es robada, el acceso al material de la llave privada se pierde también.

4.6.4.1- Almacenamiento de llaves

Se utiliza el almacenamiento de llaves cuando las políticas de seguridad requieren protección automática de las llaves privadas. El almacenamiento de llaves guarda la llave privada del usuario en la base de datos de la CA entonces la llave privada puede ser recuperada si la llave privada esta perdida o dañada.

Cuando un administrador habilita al almacenamiento de llaves en una plantilla de certificados, los usuarios proveen su llave privada a la autoridad de certificación (CA) en un CMC (Protocolo de administración de certificados) protocolo de solicitud. CMC usa CMS (Sintaxis de Criptografía de Mensajes), una sintaxis basada en un formato de solicitud RFC. La CA almacena la llave privada en su base de datos.

4.6.3.2- Recuperación de llaves

Se utiliza la recuperación de llaves después de que el proceso de almacenamiento de llaves ha guardado el sujeto de la llave privada en la base de datos de la CA. Durante el proceso de recuperación de la llave, el administrador de certificados recupera la información cifrada que contiene el certificado y la llave privada desde la base de datos. Los KRA descifran la llave privada desde los archivos cifrados y regresan el certificado y la lave privada al usuario.

4.6.3.3- Formatos de solicitud y exportación de llaves

Una PKI usa varios formatos de archivos para importar y exportar certificados, cadenas de certificados y llaves privadas. Es necesario escoger el formato correcto de exportación, el cual depende básicamente de las necesidades del negocio para importar y exportar el certificado.

Tabla 4.2: Formatos y su propósito

Formato para exportar	Propósito
PKCS #7 (*.cer, *.crt)	Para exportar el certificado sin la llave privada
PKCS #12 (*.pfx, *.p12)	Para descargar cadenas de certificados desde una CA
Formato de solicitud	**Propósito**
PKCS #10 (*.req)	Para cargar la solicitud de un certificado en una CA fuera de línea
CMC (*.req)	Para cargar solicitudes de certificados firmados Para permitir atributos adicionales en la solicitud de un certificado

4.6.3.4- Formatos de exportación

Cuando un usuario exporta un certificado usando la Consola de Certificados, la Consola de la Autoridad Certificadota, Cetutil.exe, o Internet Explorer existen los siguientes formatos disponibles:

- *PKCS #7, Sintaxis de Mensaje Criptográfico Estándar*. Describe una sintaxis general para información criptográfica como firmas y sobres digitales. Se usa el formato de archivo PKCS #7 para los siguientes propósitos:
    - Para exportar certificados sin la llave privada.
    - Para descargar cadenas de certificados desde la CA.
- *PKCS #12, Sintaxis de Intercambio de Información Personal Estándar*. Especifica un formato transportable para almacenar o transportar la llave privada de un usuario y los certificados. Se escoge este formato de archivo cuando se quiere exportar un certificado y su llave privada asociada. Debido a que la llave privada es incluida en la exportación, el formato PKCS #12 es protegido con una contraseña.

4.6.3.5- Formatos de solicitud

El formato de solicitud define que información es incluida en la solicitud del certificado. Cuando una computadora, usuario o servicio solicita un certificado desde una CA sobre una plataforma Windows Server 2003, los siguientes formatos de solicitud están disponibles:

- *PKCS #10, Solicitud de Certificado Estándar.* Describe la sintaxis de una solicitud para la certificación de una llave pública, un nombre, y un conjunto de atributos. Cuando un usuario solicita un certificado desde una CA grabando la solicitud en un archivo, el formato PKCS #10 almacena la información de la solicitud y la llave pública o el par de llaves. El solicitante del certificado que genera la solicitud del archivo en formato PKCS #10 a una CA fuera de línea para completar el requerimiento.
- *CMC, Protocolo de Administración de Certificados utilizando CMS*. Provee un sobre para una solicitud en formato PKCS #10. El formato también permite la inclusión de más atributos, como una subordinación calificada restricciones y extensiones o de la firma de una solicitud de certificados.

4.6.4- Proceso de recuperación de llaves

Se puede utilizar el proceso de recuperación de llaves para recuperar una llave privada almacenada en la base de datos de la CA. El proceso involucra al Administrador de Certificados y los roles del KRA. El proceso de recuperación de llaves comienza cuando la llave de un usuario esta perdida o dañada.

El proceso de recuperación de llaves consiste en los siguientes pasos:

a) El proceso de recuperación comienza después que el usuario o la computadora no pueden ingresar mas al material de la llave privada.
b) El usuario, o el Administrador de certificados para la CA que emite el certificado determina el número de serie del certificado. El número de serie únicamente identifica un certificado emitido.

c) Un Administrador de certificados extrae la llave privada cifrada y el certificado de la base de datos de la CA. El formato para exportar la llave privada es un archivo de tipo PKCS #7, el mismo que es cifrado usando la clave pública o el certificado KRA. El administrador de certificados puede usar ya sea la Herramienta para recuperación de llaves (krt.exe), así como **certutil – getkey** para extraer el archivo PKCS #7 de la base de datos de la CA.

d) El Administrador de certificados transfiere el archivo PKCS #7 a una estación de trabajo segura para que se ejecute el KRA. Debido a que el PKCS #7 es cifrado solo una definición de KRA puede recuperar la llave privada y el certificado, no se requieren seguridades adicionales para la transferencia.

e) El KRA recupera la llave privada y el certificado desde un archivo PKCS #7 cifrado en una estación de trabajo segura, también conocida como la estación de trabajo de recuperación. Esta extracción es realizada utilizando **certutil – recoverykey** o la Herramienta de Recuperación de Llaves. La llave privada y el certificado están almacenados en una archivo PKCS #12 y están protegidas con una contraseña de tipo KRA.

f) El KRA proporciona el archivo PKCS #12 al usuario, quien provee la contraseña KRA asignada e importa el certificado y la llave privada en el almacenamiento de certificados usando el asistente de importación de certificados.

4.6.4.1- Exportación y almacenamiento manual una llave privada

Es posible realizar un almacenamiento manual para cualquier certificado que esta basado en plantillas o en el cual un administrador de certificados ha habilitado la opción "Permitir que la llave privada sea exportada**"**. Los usuarios pueden exportar sus llaves

privadas a un archivo PKCS #12 usando la Consola de Certificados, o hacia un formato de Exportación de Llave de Outlook. Ambos métodos permiten que el certificado y la llave privada sean almacenados en un archivo protegido por contraseña que se puede utilizar para recuperar la llave privada.

Para exportar manualmente un certificado y su llave privada asociada se debe:

a) **Escoger el método de exportación del archivo.** El método que use depende de la plantilla de certificados en la que esta basado el certificado que poseemos. Si el certificado contiene una política para una aplicación de Correo Seguro o un Objeto identificador para el uso de una Llave Extendida (OID), se puede utilizar Outlook o la Consola de Certificados. Si el certificado no contiene Correo Seguro OID, se debe utilizar la Consola de Certificados.
b) **Escoger el formato de exportación del archivo.** Esta decisión está basada en la herramienta que se utilizó para almacenar la llave privada. Si se utiliza la consola de certificados se puede exportar el archivo hacia un formato PKCS #12. Si se usa Outlook, se puede exportar el archivo hacia un Archivo de Seguridad de Exchange[20].

Cuando se exporta un certificado y su llave privada, las siguientes opciones están disponibles:

- **Incluir todos los certificados en la ubicación de certificación si es posible.** Esta opción incluye la cadena completa de certificación del certificado exportado. Esto

[20] Se puede exportar certificados en formato X.509v1 únicamente hacia el Archivo de Seguridad de Outlook. Para certificados en formato X.590v3 se puede usar Archivos de Seguridad de Outlook o un archivo en formato PKCS #12.

permite al momento de importar la opción de incluir todos los certificados en la cadena de certificados que se encuentran sobre la Entidad Raíz.

- **Habilitar niveles altos de protección**. Esta opción requiere una contraseña para acceder a la llave privada que se encuentra almacenada en una archivo PKCS #12. Utilizando esta contraseña los Administradores de la CA pueden importar la llave privada de la base de datos de la CA.
- **Borrar la llave privada si la exportación es exitosa**. Esta opción elimina la llave privada que esta asociada que esta asociada con el certificado desde el almacenamiento de certificados. Se debe usar esta opción cuando se exporta un certificado y la llave privada, entonces la llave privada es removida del perfil del usuario.
- **Almacenar la llave exportada en una ubicación segura.** Después de que el certificado y la llave privada hayan sido correctamente exportados es necesario almacenar el archivo exportado en una lugar físico seguro. Copiar el archivo exportado a un CD-ROM y almacenar el CR-ROM en una locación segura.

4.6.4.2- Recuperación de la llave privada

Si se ha forzado la separación de roles para la organización, el proceso de recuperar una llave privada se divide entre los roles de administración en la CA. El Administrador de certificados y el KRA deben trabajar conjuntamente para la recuperación de la llave privada.

4.6.5- Tareas del administrador de certificados

Para extraer la llave privada cifrada desde la base de datos de la CA, el Administrador de certificados debe realizar los siguientes pasos:

a) **Identificar el certificado en la base de datos de la CA**. Para identificar el certificado a ser recuperado, el Administrador de certificados debe conocer lo siguiente:

   - El número de serie del certificado
   - El nombre común (NC) del usuario que está solicitando el certificado.
   - El Nombre del Usuario Principal (NUP) del usuario almacenado en el sujeto del certificado o un nombre de sujeto alterno.
   - El valor hash de la llave pública del certificado.

b) **Determinar el KRA para la llave privada almacenada.** Después únicamente se identifica el certificado, el Administrador de certificados debe determinar uno o más KRA para que puedan recuperar la llave privada de la base de datos de la CA.

c) **Extraje el archivo binario PKCS #7.** Para extraer la llave privada almacenada desde la base de datos de la CA, el administrador de certificados puede usar la Herramienta de Recuperación de Llaves o con el comando **certutil – getkey <número de serie> <nombre de archivo>.** La herramienta o el comando extraen la llave privada almacenada para el certificado que coincida con el número de serie en el archivo PKCS #7. El archivo binario de salida es formateado como una estructura cifrada PKCS #7 que contiene la llave privada

cifrada con la llave pública del KRA, el KRA certifica toda la cadena de certificados.

4.6.6.- Tareas del Agente Recuperador de llaves

Cuando la llave privada almacenada es extraída a un archivo binario PKCS #7, el identificador KRA debe recuperar la llave privada. El KRA tiene la llave privada que puede descifrar la llave privada almacenada y la llave privada que fue cifrada con la llave pública del KRA. En otras palabras, únicamente el KRA que contiene la llave privada que esta asociada con la llave publica que fue usada para cifrar la llave privada almacenada puede recuperarla. Para recuperar la llave privada almacenada:

a) Recuperar la llave privada almacenada del archivo binario cifrado PKCS #7. El KRA puede usar la Herramienta para Recuperación de Llaves o el comando **certutil** para recuperar la llave privada. Este proceso utiliza la llave privada del KRA para recuperar la llave privada cifrada y almacenarla junto con la cadena de certificados en un archivo en formato PKCS #12 llamado **user.pfx**. El archivo PKCS #12 está protegido por una contraseña que se provee durante el proceso del comando.

b) Se entrega personalmente al usuario el archivo PKCS #12 o se lo coloca en una locación compartida de red que es accesible únicamente por dicho usuario. No se debe poner el archivo PCKS #12 en una carpeta de acceso público o enviarla en un mensaje de correo. Se informa al usuario acerca de la contraseña requerida para la importación del certificado así como también de la cadena de certificados contenida.

4.6.7- Tareas del usuario

Después de recibir el archivo PKCS #12 desde el KRA, el usuario debe importar la llave privada y la cadena de certificados asociado a su certificado personal. Se realiza doble clic sobre el archivo PKCS #12 y corre el Asistente para la Importación de Certificados. Cuando se procede a través del asistente el usuario debe ingresar la contraseña adecuada para proteger el archivo PKCS #12.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1- Conclusiones

Del análisis expuesto previamente se concluyen los siguientes aspectos:

- La infraestructura para la emisión de certificados implementada en Microsoft 2003 Server es extremadamente flexible, ya que puede adaptarse a las necesidades cambiantes de una empresa, permitiendo integración con las tecnologías actuales y futuras asegurando la escalabilidad de la plataforma.
- Los costos de propiedad se ven reducidos dramáticamente debido a que existe una alta integración con aplicaciones ya desarrolladas y compatibilidad con hardware existente.
- La firma Digital es una solución viable para la eliminación de documentos que requieran autenticación, integridad y no repudio de lo actuado. Esta tecnología vuelve obsoleto el almacenamiento físico de documentos muchos de los cuales son sensibles a pérdidas o alteraciones.
- Los certificados digitales permiten a dos personas o servicios mantener una relación de seguridad soportada en una tercera parte de confianza mutua denominada Autoridad Certificadora, por la motivo la autoridad debe poseer toda la infraestructura y procedimientos que garanticen esta confianza.
- El presente trabajo investigativo garantiza al CTT ESPE CECAI una guía para una implementación confiable de la tecnología par la emisión de certificados a nivel de

servidor siempre y cuando sea complementada por una infraestructura tecnológica dedicada exclusivamente a este fin.

- La ley de Comercio Electrónico del Ecuador es obsoleta y no se ha hecho una revisión profunda acorde con los avances tecnológicos y nuevas formas de comercio electrónico. Citamos como ejemplo la incompatibilidad con el estándar X.509 versión 1 que define los requerimientos mínimos para considerar valido un certificado.
- En la sección "Disposiciones Legales" articulo primero de la LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS DEL ECUADOR, el término revalidación de certificado tiene validez solamente jurídica mas no técnica debido a que el certificado depende de entidades emisoras de mayor jerarquía, las mismas que no se encuentran en el país.

5.2- Recomendaciones

- Informar a los usuarios la existencia de políticas de certificación las mismas que serán accesibles públicamente a través de la declaración del emisor que se encuentra en el certificado.
- Establecer todas las seguridades físicas y lógicas previa a la implantación de la autoridad de certificación. La exposición de las llaves privadas, certificados digitales y toda información que custodia la entidad de certificación, tiene por consecuencia severas sanciones estipuladas en la ley de comercio electrónico, que pueden ir desde multas hasta la instancia de reclusión mayor.
- La Autoridad Emisora de Certificados Digitales debe poseer total independencia de operación, es decir en sus equipos (UPS, servidores, firewalls), medios de respaldo, y administración del servicio, por lo tanto recomendamos separación de la infraestructura de certificación del cualquier departamento de sistemas.

BIBLIOGRAFIA

- Cross, David B (Abril 2002). Best Practices for Implementing a Windows .NET PKI. Microsoft Corporation.
- Carlisle Adams, Steve Lloyd (Noviembre 6, 2002). Understanding PKI: Concepts, Standards, and Deployment Considerations. Second Edition. Addison Wesley
- Manuel José Lucena López (Marzo 2003). Criptografía y Seguridad en Computadores. Tercera Edición
- Jorge Ramió Aguirre (Marzo 2004). Libro electrónico de seguridad informática y criptografía. Cuarta edición. Universidad politécnica de Madrid – España
- Kapil Raina (2003). PKI Security Solution for Enterprise. Wiley Publishing.
- Diffie y Hellman (1976). New Directions in Cryptography
- Using Certificate Services 2003

  http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_CS_UsingIntro.asp

- Aladdin eToken Enterprise product description

  http://www.ealaddin.com/etoken/default.asp?cf=tl

- TechNet Microsoft (Fuente Principal)

  www.microsoft.com/technet/

- Cryptography FAQ Index

  http://www.faqs.org/faqs/cryptography-faq/

- The OpenSSL Project

  http://www.openssl.org

  http://www.modssl.org/

- SSLeay Certificate Cookbook

  http://linux.nbs.at/SSLLeavy_cookbook/ssl_cook.htmlOpenSSL

- Ley de Comercio Electrónico (legislación Ecuatoriana)

  http://www.corpece.org.ec/documentos/ley/ley_ce.htm