ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

Certificados digitales para autoridades militares de la Fuerza Terrestre

Previa a la obtención del Título de:

INGENIERO EN SISTEMAS E INFORMÁTICA

POR: Sinthia Elizabeth Guaigua Guanopatin

CAPT. Juan Francisco Varela Núñez

SANGOLQUÍ, SEPTIEMBRE DEL 2007

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por la Srta. Sinthia Elizabeth Guaigua Guanopatin y el Capt. de Com. Varela Nuñez Juan Francisco como requerimiento parcial a la obtención del título de INGENIEROS DE SISTEMAS E INFORMÁTICA.

7 de Septiembre de 2007.

TCRN. DE E.M. ING. Ortega Luis
DIRECTOR DE TESIS

DEDICATORIA

A Dios por bendecirme y guiarme.

A mis padres David y Sara por ser unos padres excepcionales que siempre estuvieron presentes en los momentos difíciles y alegres de mi vida.

A mis hermanos Darwin y Pedro que son un soporte y alegría en mi vida.

Sinthia

DEDICATORIA

Esta Tesis la dedico Dios, quien ha bendecido y guiado mi camino, a mis queridos padres y hermanos, que siempre me dieron su apoyo incondicional, a la mujer que amo Janeth mi esposa, que siempre ha estado junto a mi lado y me ha brindado todo su amor y sobre todo paciencia, a mis tres grandes tesoros, mis hijas, todos me han ayudado a culminar mi carrera con éxito, ha todos ustedes muchas gracias.

Juan

AGRADECIMIENTOS

Agradezco a DIOS por darme la oportunidad de vivir y fuerzas para alcanzar este objetivo tan importante en mi vida.

A mis padres, David y Sara por ser unos padres ejemplares, por darme siempre su apoyo, cariño, confianza, paciencia y comprensión en cada instante de mi vida y sobre todo en el transcurso de mi carrera.

A mis hermanos Darwin y Pedrito, por su compresión y ayuda incondicional.

Sinthia

AGRADECIMIENTOS

A mi Dios que siempre con sus bendiciones ha estado junto a mi lado.

A mis Padres Angel Gabriel y Magdalena, a mis hermanos Rocío, Angel Gabriel, Luis, Roberto, que siempre están junto a mi lado en las buenas y en las malas, que con su sabiduría y buenos consejos me han enrumbado por el camino del bien, a todos ustedes gracias por ayudarme a lograr un objetivo más en mi vida.

Al amor de mi vida Janeth, por darme su apoyo incondicional en todo momento, gracias por todo tu esfuerzo sobre todo por ser madre y esposa a la vez.

A mis hijas, Annaely, Janeth, Jhoanna, que son la luz de mi camino, gracias por darme todo su amor, cariño y ternura.

A mi compañera de trabajo y amiga Sinthia, gracias por todo el esfuerzo y tesón puesto en la realización de este trabajo.

Juan

INDICE DE CONTENIDO

LISTADO DE FIGURAS

CAPÍTULO 1: INTRODUCCIÓN

1.1 TEMA:

CERTIFICADOS DIGITALES PARA AUTORIDADES MILITARES DE LA FUERZA TERRESTRE

1.1.1 Planteamiento del problema:

Internet es una red global y básicamente insegura, la cual no cumple con la suficiente protección que debe darse a los datos que por ella circulan, estando propensos a amenazas de seguridad relacionadas con la *confidencialidad* e *integridad* de los datos, provocando dudas sobre la validez de los datos que se transfieren o almacenan. Asimismo es realmente sencillo hacerse pasar en la red por quien realmente no se es, con los consiguientes riesgos de perdida de fiabilidad de la información para quien la recibe. .

Debido ha este tipo de vulnerabilidades y al número de transacciones importantes que manejan las Fuerzas Armadas del Ecuador, se han visto en la necesidad de utilizar tecnologías que permitan incorporar seguridades en los datos que van ha ser enviados a través del Internet.

Como primer paso las FF.AA, se encuentra cambiando de un sistema antiguo que no ofrecía las seguridades informáticas necesarias, a un nuevo sistema de información de la Fuerza Terrestre denominado SIFTE, el cual se encuentra ya en funcionamiento. SIFTE proveerá de mayores seguridades informáticas y permitirá la incorporación de nuevas tecnologías que contribuirán a la seguridad en el envío y recepción de datos confiables a través de la red, no solo militar sino también civil.

Como siguiente paso la Fuerza Terrestre a través de la DICOMSI necesita incorporar una tecnología que permita dar seguridad a los datos y permita la autenticidad de documentos firmados, razón por la cual requiere el uso de certificados digitales y la implementación de la firma digital como medida de seguridad para el tráfico en las redes de correo electrónico.

1.1.2 Presentación:

La elaboración de la presente tesis es de suma importancia para la Fuerza Terrestre, razón por la cual se seguirán metodologías que permitan obtener resultados con calidad y que estén de acuerdo con las expectativas de la Fuerza Terrestre.

Para el desarrollo de la presente tesis en primer lugar vamos a realizar un estudio minucioso de un certificado digital, su estructura básica, los elementos inmersos dentro de ellos, tales como autoridades certificadoras, criptografía y estándares.

Como siguiente paso se realizará el estudio de las firmas digitales y los elementos que se toman en cuenta para realizar su implementación.

Con la información recolectada, empezaremos ha realizar la implementación de la firma digital que se efectuará en un inicio dentro de la Dirección de Comunicaciones de la Fuerza Terrestre, para lo cual se va ha seguir una metodología en la que aplicaremos un conjunto de fases con el fin de gestionar adecuadamente el proyecto.

La metodología utilizará las siguientes fases:

- Análisis de la situación actual y de requisitos
- Diseño

- Implementación
- Pruebas

1.1.3 Justificación

Las FF.AA requiere la incorporación de tecnologías que permitan dar seguridad a los datos que viajan a través del Internet y el manejo de documentos firmados, como solución a esta petición se ha establecido:

- El uso de los certificados digitales permitirán proteger la información que se envía, tanto por el correo militar como por el correo electrónico evitando que terceros puedan leerlos o modificarlos durante su envío, la información que se maneja en el ámbito militar es secreta y no puede ser obtenida por ninguna persona que no este autorizada para hacerlo, teniendo en cuenta que cualquier información alterada o robada incurrirá en problemas legales.
- La implementación de la firma digital, permite aumentar el grado de seguridad en los documentos enviados y recibidos por las autoridades Militares a nivel nacional, a través del correo militar y electrónico.

  La firma digital tiente la misma validez y responsabilidad de una firma manuscrita, cumple con los requerimientos de una firma manuscrita en cuanto a la autenticación (permite identificar tanto al usuario que ha emitido el mensaje como al receptor); integridad del documento (asegura que el mensaje no ha sido alterado) y no repudio en virtud de que nadie excepto el emisor puede haberlo firmado y, en consecuencia, nadie podrá negar su existencia y validez legal.

1.2 OBJETIVOS:

1.2.1 Objetivo General

Realizar el análisis de los certificados digitales y análisis, diseño e implementación de firmas digitales como medida de seguridad para la autenticación de documentos firmados por las diferentes Autoridades Militares, para el tráfico en las redes de correo electrónico.

1.2.2 Objetivos Específicos

a.- Efectuar un análisis de la estructura de un certificado digital.

b.- Realizar un análisis actual del manejo de documentos firmados enviados a través del correo militar y correo electrónico.

c.- Elaborar el diseño de una estrategia para la implementación de la firma digital.

d.- Ejecutar la implementación de firmas digitales como medida de seguridad para el tráfico en las redes de correo militar y electrónico.

e.- Efectuar las respectivas pruebas, para verificar el adecuado funcionamiento del intercambio de información a través del correo militar y electrónico entre las Autoridades Militares, y esta se realice en forma segura.

1.3 ALCANCE

El proyecto de plan de tesis con el tema **"**Certificado digital para autoridades militares de la Fuerza Terrestre" tiene como alcance:

- Se realizará el análisis de certificados digitales y firma digital.
- Se utilizarán certificados digitales emitidos por una empresa que tenga la suficiente autoridad y reconocimiento a nivel de las FF.AA, en este caso será la Dirección de Comunicaciones y Sistemas, la cual actuará como Autoridad Certificadora, esta dispone de la infraestructura necesaria para realizar dicha acción.
- Se utilizarán certificados que permitan aplicar o implementar firmas digitales los cuales aumentarán el grado de seguridad en los documentos enviados y recibidos por las autoridades Militares a nivel nacional, a través del correo militar y electrónico.
- Se dará a conocer los reglamentos de la ley de Comercio Electrónico en el Ecuador a los futuros usuarios de la Firma Digital.
- Debido a la gran cantidad de usuarios que van ha usar los certificados digitales y firma digital, en un inicio se va ha realizar un prototipo en una red local.

CAPÍTULO 2: MARCO TEORICO

2.1 CRIPTOLOGÍA

2.1.1 Definición

La ***criptología*** es una rama de las matemáticas que estudia los principios, métodos y medios del cifrado[1] y descifrado[1] de la información, así como el diseño de sistemas que realicen dichas funciones, e inversamente la obtención de la información protegida.

La ***criptología*** comprende dos ramas principales: la Criptografía y el Criptoanálisis.

La criptografía se encarga de transformar la información de tal forma que sólo las partes involucradas en la comunicación entiendan el contenido, logrando este objetivo mediante la utilización de criptosistemas[1]. Por otro lado, ***el criptoanálisis*** abarca las diferentes metodologías y técnicas que permiten recuperar la información que ha sido previamente tratada por un procedimiento criptográfico[1], sin conocer las claves de acceso. Con respecto a las técnicas del criptoanálisis, destacamos:

- *Fuerza bruta*: se trata de encontrar la clave probando con todas las posibilidades posibles.
- *Análisis de frecuencia*: se pueden analizar estadísticas de las frecuencias de los caracteres o de bloques de caracteres para romper los criptosistemas.

[1] Ver glosario de términos

- *Diferencial*: se parte de pares de mensajes con diferencias mínimas (normalmente un bit) y se analizan las variaciones entre los correspondientes cifrados.
- *Algoritmos matemáticos*: se trata de diseñar algoritmos eficientes computacionalmente para averiguar la clave.

2.2 CRIPTOGRAFÍA

2.2.1 ¿Qué es la Criptografía?

Según el Diccionario de la Real Academia, la palabra ***Criptografía*** viene del griego **Kryptos**, que significa oculto y **gráphein**, escritura, y su definición es: " Arte de escribir con clave secreta o de un modo enigmático".

Según el libro electrónico de Seguridad Informática y Criptografía [2] la ***Criptografía*** es la "Rama inicial de las Matemáticas, y actualmente en la Informática y Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar, y por tanto proteger un mensaje o archivo por medio de un algoritmo, usando una o mas claves."

En conclusión podemos indicar que la ***criptografía*** es una ciencia que permite asegurar la confidencialidad de la información intercambiada mediante la utilización de criptosistemas los cuales permiten cifrar y descifrar la información utilizando claves que solamente ellos conocen, de esta manera la información es totalmente inentendible para terceras personas que pudieran hacer un uso fraudulento de tales datos.

[2] **Datos de :** Libro Electrónico de Seguridad Informática y Criptografía Versión 4.1; Sexta edición de 1 de Marzo de 2006; Autor: Jorge Ramió Aguirre

2.2.2 Objetivo de la criptografía

Proporcionar comunicaciones seguras y secretas sobre canales inseguros, utilizando mecanismos de cierta complejidad con el fin de proporcionar no solamente protección, sino también garantizar que haya confidencialidad.

2.2.3 Cifrado y descifrado

Cifrado es una transformación del texto original (llamado también texto inicial o texto claro) que lo convierte en el llamado texto cifrado o criptograma.

Descifrado a la transformación que permite recuperar el texto original a partir del texto cifrado.

En términos más comprensibles podemos indicar que ***cifrar*** es la acción de aplicar técnicas o algoritmos criptográficos para poder "esconder" el mensaje, luego de esto, manda el mensaje por una línea de comunicación que se supone insegura y después sólo el receptor autorizado puede leer el mensaje escondido, la acción para poder leer el mensaje la llamamos ***descifrar.***

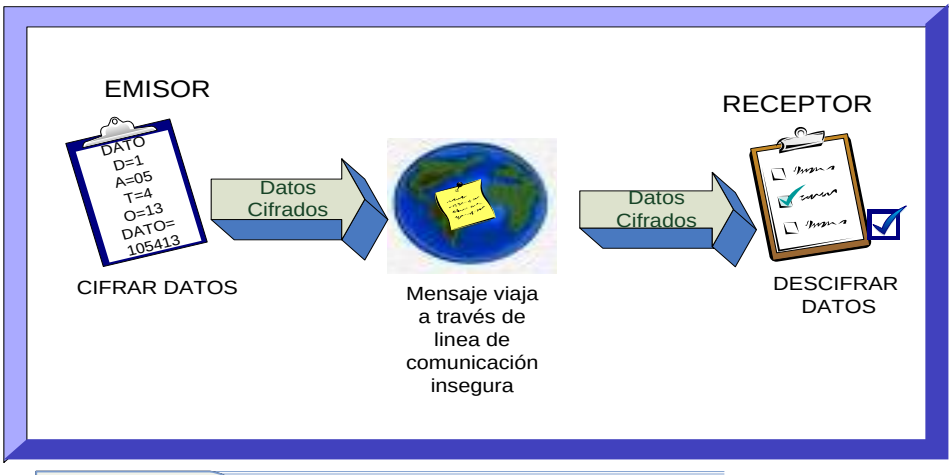


IMAGEN Nº 01 Envío y recepción de un mensaje cifrado

El proceso criptográfico tiene los siguientes elementos básicos:

- La información inicial, llamada texto plano.
- *El algoritmo criptográfico*. es un método matemático que se emplea para cifrar y descifrar un mensaje. Generalmente funciona empleando una o más claves (números o cadenas de caracteres) como parámetros del algoritmo, de modo que sean necesarias para recuperar el mensaje a partir del mensaje cifrado.
- *Claves de cifrado*. Son usadas por el algoritmo de cifrado para determinar como cifrar y descifrar datos, son similares a las contraseñas para acceder a una PC.
- *Longitud de clave*. Las claves largas son mas difíciles de adivinar que las claves cortas porque hay mas caracteres que probar en un ataque.
- *La información final* (el mensaje cifrado), llamado texto cifrado.

El proceso consta de tomar el texto plano, aplicarle el algoritmo y la salida es el texto cifrado.

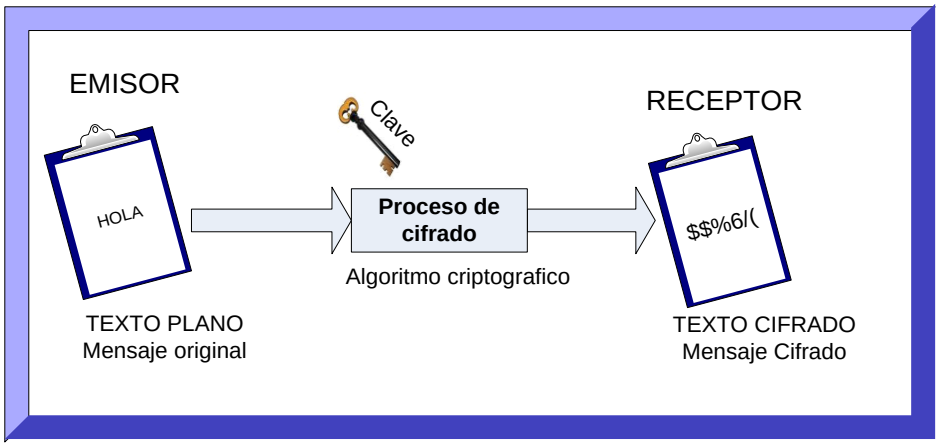


IMAGEN Nº 02 Cifrado de datos

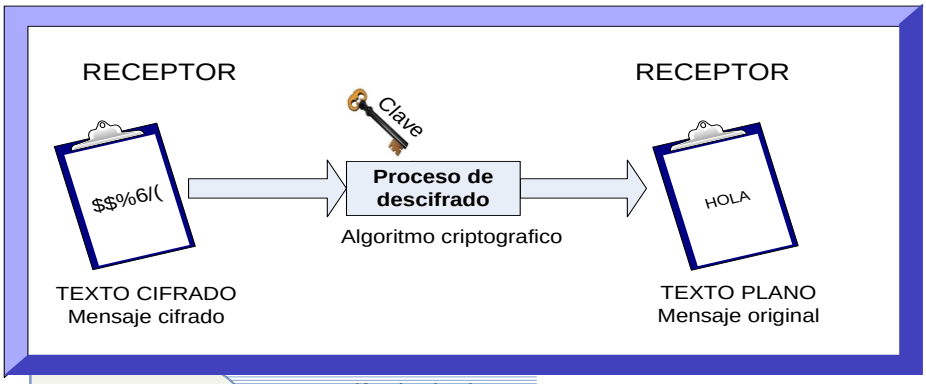


IMAGEN Nº03 Descifrado de datos

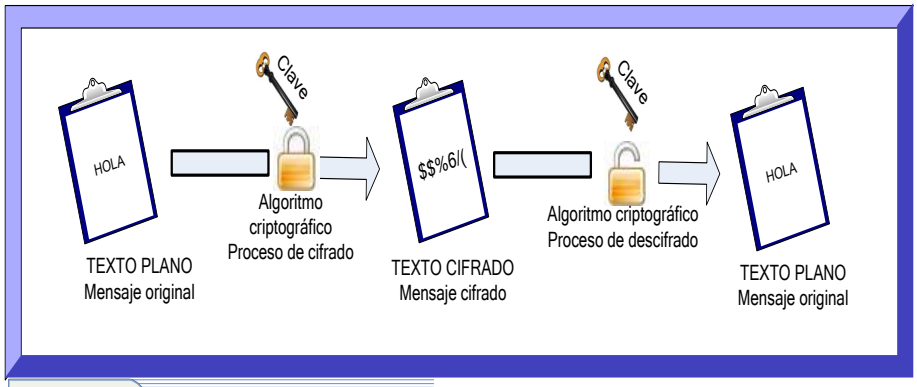


IMAGEN Nº04 Cifrado y descifrado

Descripción del proceso de Cifrado y Descifrado:

1. El emisor y el receptor acuerdan el método y algoritmo de cifrado a utilizar.
2. EL emisor cifra su mensaje utilizando el método de cifrado y envía al receptor por algún medio de comunicación.
3. El mensaje viaja a través de un medio de comunicación que generalmente es inseguro.
4. El receptor descifra su mensaje utilizando el método o algoritmo de descifrado.

Ejemplo:

1. El mensaje que el emisor desea enviar al receptor es el siguiente " HOLA "
2. El emisor y el receptor acuerdan el algoritmo a utilizar, en este ejemplo el valor de cada letra del alfabeto va ha ser 3 puestos más delante de la letra que se indica. Ej. Si es la letra **a** se colocará la letra **d**
3. Utiliza el algoritmo ya predefinido **H** = K; **O** = R; **L**= O; **A**= D; Obtiene el siguiente resultado: KROD
4. El emisor envía KROD por el medio inseguro de comunicación.
5. El receptor recibe el mensaje y lo descifra realizando el proceso inverso para obtener el mensaje en este ejemplo para descifrar el valor de cada letra del alfabeto va ha ser 3 puestos más atrás de la letra que se indica. Ej. Si es la letra **d** se colocará la letra **a**
   Utiliza el algoritmo ya predefinido **K** = H; **R** = O; **O**= L; **D**= A; Obtiene el siguiente resultado: HOLA

2.3 CRIPTOSISTEMA

Un **criptosistema**, o **sistema criptográfico**, son los fundamentos y procedimientos de operación algorítmica que participan en el cifrado y descifrado de un mensaje.

Todo sistema criptográfico consta de cinco componentes: M, C, K, E y D.

1. **M** representa el conjunto de todos los mensajes sin cifrar (texto plano) que pueden ser enviados.

2. **C** Representa el conjunto de todos los posibles mensajes cifrados, o criptogramas.
3. **K** representa el conjunto de claves que se pueden emplear en el Criptosistema.
4. **E** es el conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de **M** para obtener un elemento de **C**. Existe una transformación diferente $\mathbf{E_k}$ para cada valor posible de la clave K.
5. **D** es el conjunto de transformaciones de descifrado, análogo a **E**.

Todo criptosistema cumple la condición Dk (Ek (m))=m es decir, que si se tiene un mensaje m, se cifra empleando la clave K y luego se descifra empleando la misma clave, se obtiene el mensaje original m." [3]

2.3.1 Tipos de Criptosistemas

A lo largo de la historia, se han utilizado cientos de criptosistemas diferentes, pero a grandes rasgos pueden dividirse en tres tipos:

- *Criptosistemas de clave privada*.- usan la misma clave para cifrar y descifrar el mensaje. La clave secreta[4] es compartida con el emisor y el receptor del mensaje. Este tipo también se conoce como criptografía simétrica.

[3] Universidad Nacional de Comahue (UNCOMA), Criptografía pdf.

[4] Ver glosario de términos

- *Criptosistemas de clave pública*.- usan una clave pública para cifrar el mensaje y una clave privada para descifrarlo o viceversa. La clave privada debe mantenerse en secreto y la clave pública debe ser conocida por todas las restantes entidades que van a comunicarse con ella. Los sistemas de clave pública se conocen también como criptografía asimétrica.
- *Criptosistemas híbridos público/privados*.- Son una combinación de los criptosistemas simétricos y asimétricos.

2.3.1.1 Criptosistema simétrico o clave privada

Los ***cripstosistemas simétricos*** o llamados también de clave secreta, privada, o clásicos, se caracterizan por que en ellos se usa la misma clave para cifrar y para descifrar.

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.

IMAGEN Nº05 Llave simétrica

2.3.1.1.1 Clasificación

Existe una clasificación de este tipo de criptografía en tres familias, la cual se basa en el número de símbolos cifrados a la vez:

- ***La criptografía simétrica de bloques***, la cual toma el texto en claro y lo divide en bloques de igual longitud y cifra cada bloque independientemente. Suelen emplearse bloques de 64 bits.

Descripción del Funcionamiento:

Divide el mensaje en claro en bloques de n bits cada uno, la característica principal de este tipo de cifradores consiste en que cada bloque se cifra de igual forma, independientemente del lugar que ocupe en la cadena, de manera que todos los bits del bloque se cifran conjuntamente, participando en operaciones que tratan de oscurecer las posibles relaciones que tuviesen en el mensaje original.

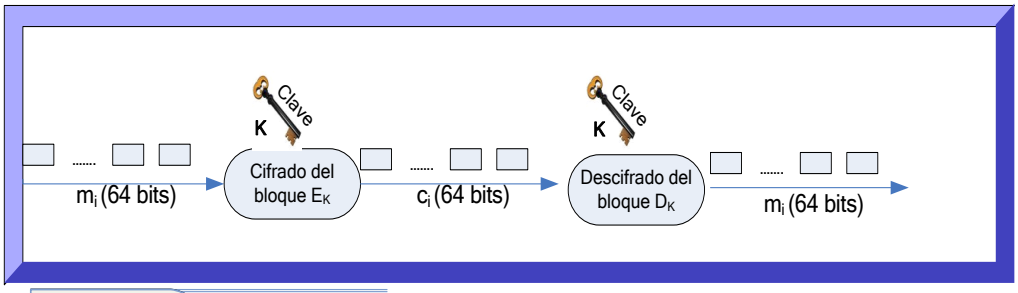


IMAGEN Nº06 Cifrado en bloque

En la imagen anterior los m1, m2, m3,…. mn bloques en que se ha dividido el mensaje se van pasando, uno detrás de otro, como entrada del cifrador y los c1, c2,…….. cn resultantes se concatenan

uno detrás de otro, y en el mismo orden, para constituir el mensaje cifrado final, c.

La criptografía simétrica de flujo, en donde el texto en claro se cifra símbolo tras símbolo, cifrándose cada uno con clave diferente. La característica principal del cifrado en flujo consiste en considerar el mensaje en claro como un flujo continuo de bits(o de caracteres) y generar a la salida el correspondiente flujo de bits resultante de la transformación producida en el proceso de cifrado.

Descripción del Funcionamiento

Se cifra bit a bit mediante una operación de suma modulo 2 (XOR), que puede conseguirse mediante un dispositivo electrónico o una simple operación computacional.

Si se realiza la operación XOR entre el mensaje en claro y la secuencia cifrante que depende de la clave secreta k, se obtiene le mensaje cifrado:

$c = m \oplus s$

Si en el receptor se usa esa misma secuencia cifrante para realizar la operación XOR con el mensaje cifrado, c, se obtiene como resultado el mensaje en claro.

$m = c \oplus s$

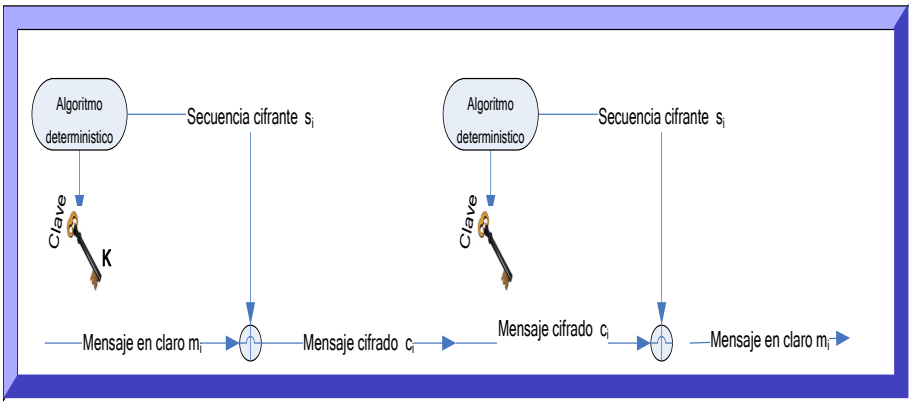


IMAGEN Nº 07 Cifrado en flujo

La sencillez de las operaciones de cifrado y descifrado hace que con este tipo de sistema puedan conseguirse velocidades muy elevadas.

- ***La criptografía simétrica de resumen*** (funciones hash).

  Ver sección 2.1.5

2.3.1.1.2 Descripción del proceso de comunicación

Proceso para realizar una comunicación utilizando este tipo de criptosistema:

1. Emisor y receptor se ponen de acuerdo en usar este sistema de cifrado.

2. Emisor y receptor se ponen de acuerdo en la clave que van a usar.

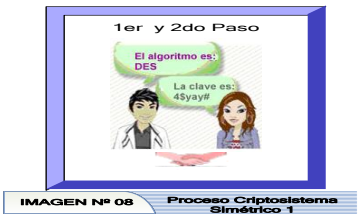


IMAGEN Nº 08 Proceso Criptosistema Simétrico 1

3. Emisor cifra el mensaje con la clave elegida y se lo envía al receptor. El proceso de obtención del mensaje cifrado *c* es:

$$c= E_K(m)$$

Donde *k* es la clave secreta, E_k representa la operación de cifrado con esa clave y m es el mensaje en claro.

4. Receptor recibe el mensaje enviado por el remitente y lo descifra con la clave elegida. El proceso de recuperación del mensaje original, se realiza mediante la operación de descifrado D_k, en el que se utiliza la misma clave secreta *k*.

$$m=D_K(c)$$

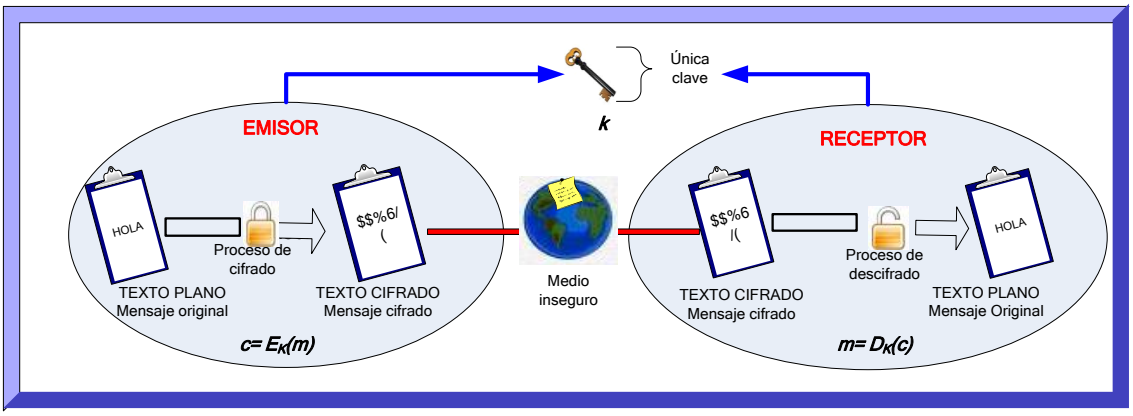


IMAGEN Nº09 Proceso Criptosistema Simétrica 2

Los pasos 1 y 2 se realizan sólo una vez, cuando se desea tener una forma de comunicarse con un usuario particular, luego cuando se quiere enviar un mensaje se aplican los pasos 3 y 4.

La seguridad del sistema depende del secreto de la clave, y son, generalmente, más fáciles de criptoanalizar que los de clave pública porque requieren menos operaciones matemáticas en relación con el tiempo el

cifrado de clave privada, es más rápido que el de clave pública (de 100 a 1000 veces).

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.

Como resumen se puede señalar:

- Debido a la velocidad de ejecución, los criptosistemas simétricos son indispensables para proporcionar servicios de confidencialidad en las aplicaciones telemáticas[7] de alta velocidad.
- Debido a su principio de funcionamiento, el número de claves necesarias para proporcionar confidencialidad en un entorno, en el que participen un número considerable de entidades comunicantes (emisores y receptores), es tan elevado que hace prácticamente inaplicable el uso exclusivo de criptosistemas simétricos en estos escenarios.
- La mayor vulnerabilidad de estos criptosistemas es la clave secreta que se maneja entre el emisor y el receptor, para garantizar la seguridad es necesario la renovación periódica de las claves.

Todos los sistemas criptográficos clásicos se pueden considerar ***simétricos***, y los principales algoritmos simétricos actuales son DES, TDES, IDEA, RC5, AES y algoritmos de resumen (funciones Hash).

A continuación se hará un pequeño resumen de cada uno de los algoritmos simétricos anteriormente mencionados.

- **DES.-** (Estándar de Cifrado de datos) cifra bloques de 64 bits con una clave de 56 bits. Se convirtió en estándar durante casi treinta años. Hoy es vulnerable por su pequeña longitud de clave de 56 bits y ha dejado de ser estándar mundial.

  Utilizando fuerza bruta se puede obtener la clave del sistema en un tiempo relativamente corto, por lo que lo hace inseguro para propósitos de alta seguridad

  Funcionamiento

  Proceso de cifrado con DES.

  El texto original que se va ha cifrar, se divide en bloque de 64 bits cada uno.

  La clave K de cifrado es de 64 bits, es decir, ocho octetos, de los cuales ocho bits son para control de paridad, por lo que el tamaño real de la clave a efectos criptográficos es de 56 bits.

  El procesamiento del mensaje se realiza en 3 fases:

  - Primero, los 64 bits del texto en claro se transforman por medio de una permutación inicial (IP) que reordena los bits para producir la entrada permutada.
  - A esto le sigue una fase que consta de 16 iteraciones de la misma función.

La salida de la última iteración (la 16) consta de 64 bits que son función del texto en claro y la clave. Se intercambia los 32 bits de la parte izquierda con los 32 bits de la derecha para producir la salida previa.

- Finalmente, la salida previa se permuta con IP-1, que es la inversa de la función de permutación inicial, para producir los 64 bits del texto cifrado.

El procesamiento de la clave es como sigue:

- Inicialmente la clave se transforma por una función de permutación.
- Después, para cada una de las 16 iteraciones, se produce una subclave (Ki) por medio de un desplazamiento circular y una permutación.
- La función de permutación es la misma para cada iteración, pero se produce una subclave diferente debido al desplazamiento repetido de los bits de la clave.

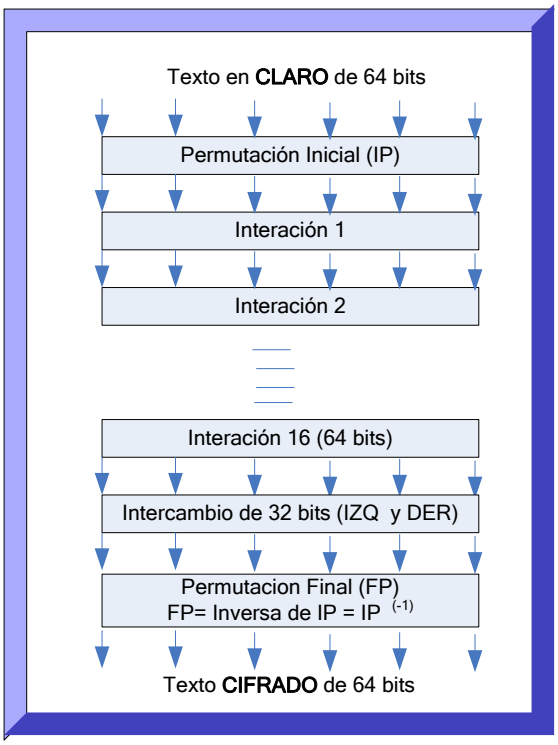


IMAGEN Nº10 Algoritmo DES

En cuanto al proceso de descifrado con DES:

- Es esencialmente el mismo que el utilizado en el proceso de cifrado.
- La regla es como sigue: usar el texto cifrado como entrada al algoritmo DES, pero usando la clave en orden inverso. Esto es, utilizar K16 en la primera iteración, K15 en la segunda iteración y así hasta que K1 se utilice en la iteración número 16 y última.

La preocupación más seria hoy en día es el tamaño de la clave.

Con una longitud de 56 bits, existen 256 claves posibles, lo que es aproximadamente 7,6 x 1016 claves.

- **TDES.-** Es el sucesor de DES, que aplica tres veces el mismo algoritmo (DES) para fortalecer la longitud de la clave.

  Este sistema usa entonces una clave de 128 bits, aunque se ha podido mostrar que los ataques actualmente pueden romper a TDES mediante la utilización de fuerza bruta.

- **IDEA.-** (Algoritmo Internacional de Cifrado de Datos), trabaja con bloques de texto de 64 bits y una clave de 128 bits. Este algoritmo esta libre de restricciones y permisos nacionales, y es de libre distribución por Internet. Hasta la actualidad no ha sido roto nunca, debido a la longitud de su clave. Es usado principalmente para el correo electrónico PGP.

- **RC5.-** Fue inventado por Rivest (del RSA), proviene del RC4, y es propiedad de RSA Data Segurity Inc. ***RC5*** es un cifrador de bloque el cual permite definir la longitud de la clave, el tamaño del bloque de datos y el número de rondas de cifrado. La empresa Netscape utiliza este cifrador para su sistema de seguridad SSL.

  La versión RC4 con clave de 40 bits ya fue rota en un tiempo de 8 días, esto ha hecho dudar de su seguridad.

  Su uso es restringido, solo se permite exportar la versión con clave de 56 bits.

- **AES.-** (Estándar de Cifrado Avanzado) es un algoritmo simétrico con bloques de 128 bits y con un tamaño de clave variable: 128,192 y 256 bits (estándar) o bien múltiplo de 4 bytes.

En abril de 2005, D.J. Bernstein anunció un ataque temporizado de caché que solía romper un servidor a medida que usaba el cifrado ***AES*** para OpenSSL. Este servidor fue diseñado para dar la mayor cantidad de información acerca del tiempo como fuera posible, y el ataque requería cerca de 200 millones de ficheros de texto plano. Se dice que el ataque no es práctico en implementaciones del mundo real.

2.3.1.2 Algoritmos Hash (algoritmos de resumen de mensajes)

Es un algoritmo que crea una representación digital en la forma de un valor ***hash*** o resultado ***hash*** de una longitud estándar, el cual representa un resumen del documento. Este resultado es usualmente mucho más pequeño que el documento, pero sin embargo sustancialmente único.

Cualquier cambio en el mensaje invariablemente producirá un resultado ***hash*** diferente aun cuando se use la misma función ***hash***. En el caso de una función ***hash*** segura, a veces llamada una función ***hash*** de una sola dirección, es infalsificable computacionalmente para derivar el mensaje original desde su valor ***hash***. Se considera una función de una sola dirección, ya que es posible producir un número a partir de una entrada, pero es imposible deducir la entrada a partir del número arrojado por la función ***hash***.

Estos métodos son muy variados, pueden llegar a tomar en cuenta diversos parámetros tales como el nombre de un archivo, su longitud, hora de creación, datos que contenga, etc. aplicándole diversas transformaciones y operaciones matemáticas.

2.3.1.2.1 Funciones:

- Transforma un mensaje de longitud arbitrariamente grande a un número fijo de bits de longitud fija.

IMAGEN Nº 11 Función Hash

- Permiten *resolver* el problema de la integridad de los mensajes, así como la autenticidad de mensajes y de su origen.
- Una función ***hash*** es también ampliamente usada para la firma digital, ya que los documentos a firmar son en general demasiado grandes, la función ***hash*** les asocia una cadena de longitud 160 bits que los hace más manejables para el propósito de firma digital.

2.3.1.2.2 Descripción del Proceso:

Un mensaje de longitud arbitraria lo transforma de forma "única" a un mensaje de longitud constante.

6. Primero se toma el mensaje entrante de longitud variable.
7. Se lo divide en partes iguales por Ej. 160 bits.

8. Se combinan de alguna forma parte por parte hasta obtener un solo mensaje de longitud fija como muestra la figura siguiente:

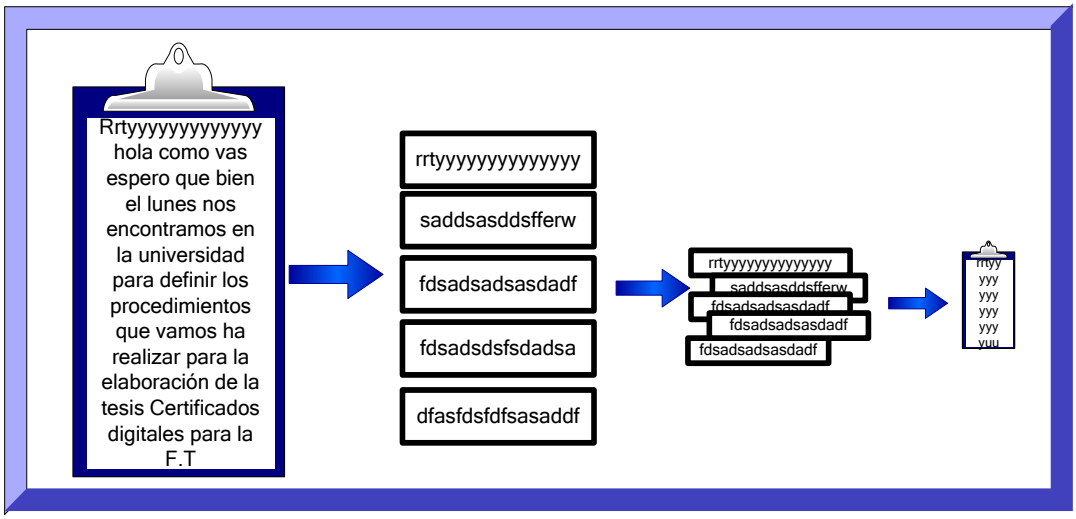


IMAGEN Nº12 Proceso de Función Hash

Las funciones hash (o primitivas hash) pueden operar como:

- **MDC** (**M**odification **D**etection **C**odes)

  Los **MDC** sirven para resolver el problema de la integridad de la información, al mensaje se le aplica un **MDC** (una función hash) y se manda junto con el propio mensaje, al recibirlo el receptor aplica la función hash al mensaje y comprueba que sea igual al hash que se envió antes.

  Es decir, se aplica un hash al mensaje **M** y se envía con el mensaje (**M**, *h* (**M**)), cuando se recibe se le aplica una vez más el hash (ya que **M** fue enviado) obteniendo *h*' (**M**), si *h* (**M**)=*h*' (**M**), entonces se acepta que el mensaje se a transmitido sin alteración.

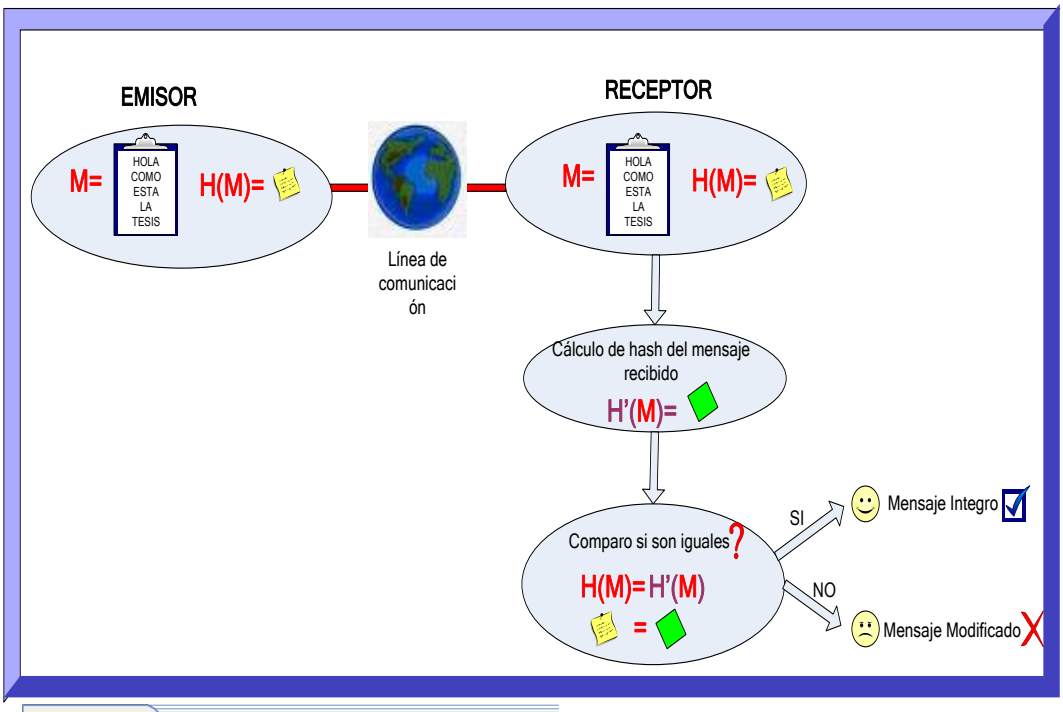


IMAGEN Nº 13 o MDC (ModificationDetection Codes)

- **MAC** (**M**assage **A**uthentication **C**odes)

  Los **MAC** sirven para autenticar el origen de los mensaje así como también su integridad, para hacer esto se combina el mensaje **M** con una clave privada **K** y se les aplica un hash *h* (**M, K**). Se envía esto y al llegar a su destino si se comprueba la integridad de la clave privada K, entonces se demuestra que el único origen del mensaje es el que tiene la parte propietaria de la otra clave K.

  De forma simple se muestra en la siguiente figura el funcionamiento de un **MAC**.

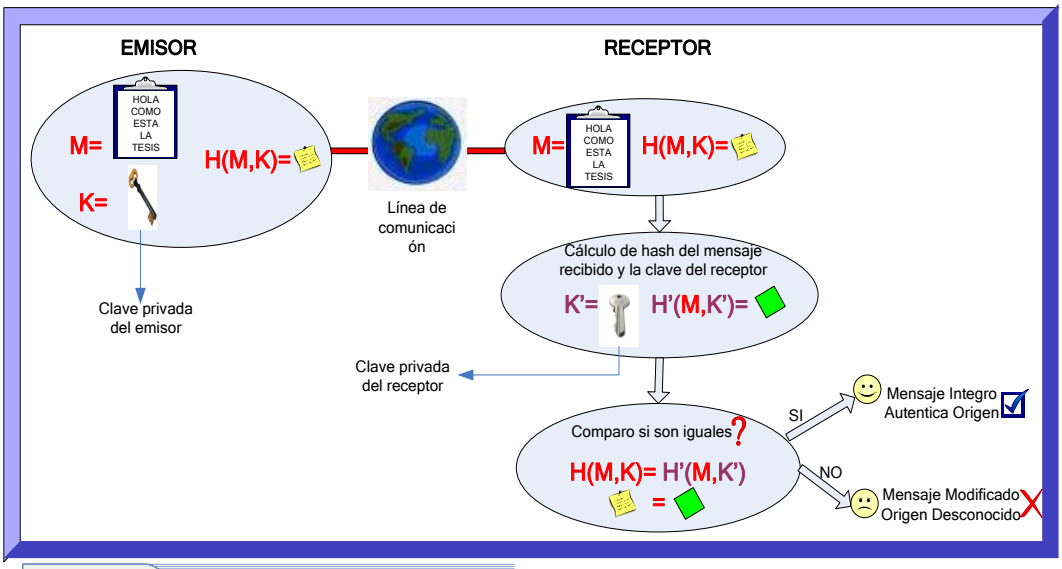


IMAGEN Nº 14 MAC (Massage Authentication Codes)

2.3.1.2.3 Propiedades:

Estos algoritmos deben tener tres propiedades para ser criptográficamente seguros:

1. No debe ser posible averiguar el mensaje de entrada basándose sólo en su resumen, es decir, el algoritmo es una función irreversible de una sola dirección.
2. Dado un resumen debe ser imposible encontrar un mensaje que lo genere.
3. Debe ser computacionalmente imposible encontrar dos mensajes que generen el mismo resumen.

2.3.1.2.4 Tipos de Algoritmos Hash:

Existen muchos algoritmos para la creación de funciones de resúmenes entre los más comunes son:

- **MD5.** En criptografía, ***MD5*** (acrónimo de **M**essage-**D**igest Algorithm **5**, Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits ampliamente usado. El código ***MD5*** es la quinta de una serie de funciones de dispersión diseñadas por Ron Rivest (el del algoritmo RSA) en el año 1992. Las anteriores versiones MD2, MD4 son más lentas. Opera alterando los bits de una manera tan complicada que cada bit de salida es afectada por cada bit de entrada. Durante el año 2004 fueron divulgados ciertos defectos de seguridad, lo que hizo que se cambie de este sistema a otro más seguro.
- **SHA.** La familia SHA (**S**ecure **H**ash **A**lgorithm, Algoritmo de Hash Seguro) es un sistema de funciones hash criptográficas relacionadas de la Agencia de Seguridad Nacional de los Estados Unidos y publicadas por el National Institute of Standards and Technology (NIST). El primer miembro de la familia fue publicado en 1993 es oficialmente llamado SHA. Sin embargo, hoy día, no oficialmente se le llama SHA-0 para evitar confusiones con sus sucesores. Dos años más tarde el primer sucesor de SHA fue publicado con el nombre de SHA-1. Existen cuatro variantes más que se han publicado desde entonces cuyas diferencias se basan en un diseño algo modificado y rangos de salida incrementados: SHA-224, SHA-256, SHA-384, y SHA-512 (todos ellos son referidos como SHA-2).

2.3.1.3 Criptosistema asimétrico o clave pública

Ideado por los matemáticos Whitfield Diffie y Martín Hellman (DH) con el informático Ralph Merkle en 1976. La ***criptografía asimétrica*** es por definición aquella que utiliza dos claves diferentes para cada usuario, una para cifrar que se le llama clave pública y otra para descifrar que es la clave privada.

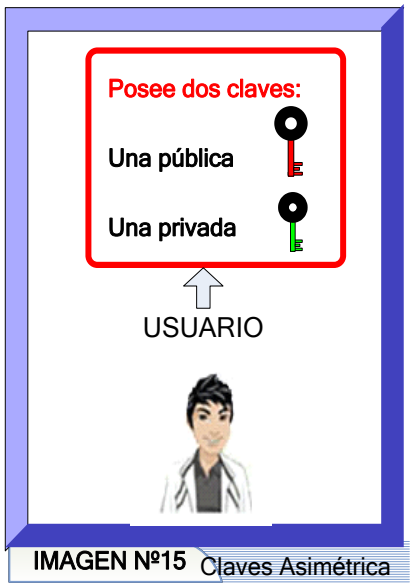


IMAGEN Nº15 Claves Asimétrica

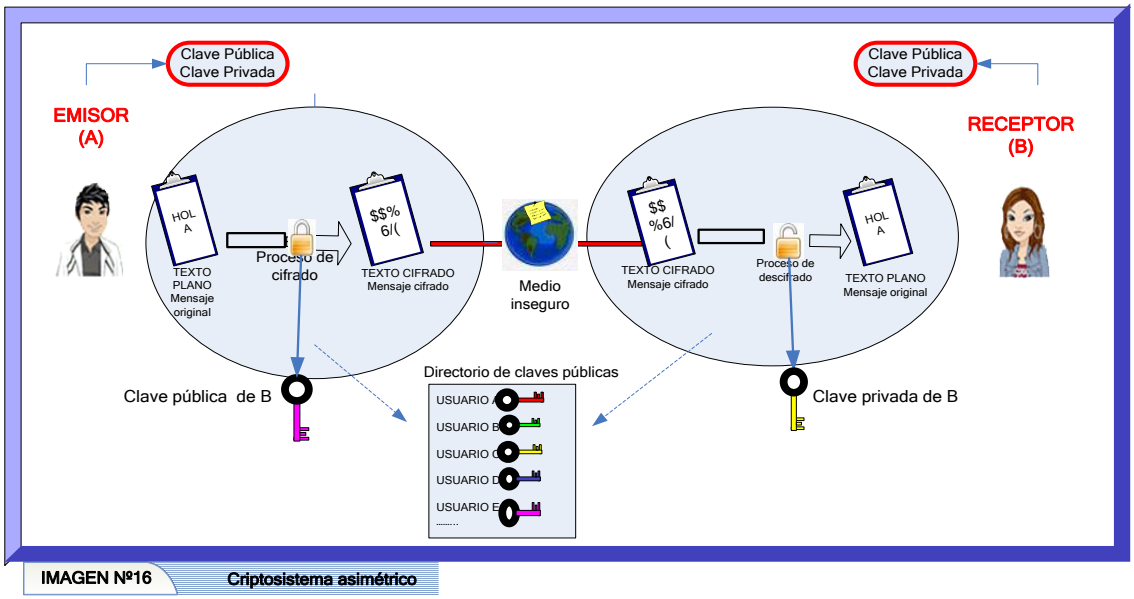


IMAGEN Nº16 Criptosistema asimétrico

La clave privada debe conservarse en lugar seguro, ya que solamente puede tener acceso a ella el propietario de la clave. En cambio, la clave pública se puede distribuir, y debe comunicarse a las personas con las que se quiera intercambiar correo seguro.

La clave privada y pública están relacionadas matemáticamente, pero esta relación debe ser suficientemente compleja para que el criptoanalista no la pueda encontrar.

Proceso de Comunicación

1. Emisor y receptor se ponen de acuerdo en usar este sistema.
2. Emisor y receptor obtienen sus propias claves privadas e intercambian sus claves públicas.
3. Emisor cifra el mensaje con la clave pública del receptor y lo envía.
4. Receptor recibe el mensaje enviado por el emisor y lo descifra con la clave privada (nadie más puede descifrar ya que sólo el receptor posee y conoce la clave privada).

Observación: los pasos 1 y 2 se realizan sólo una vez, cuando se desea tener una forma de comunicarme con un usuario en particular, luego cuando se quiere enviar un mensaje este sólo se aplican los pasos 3 y 4. Además puede haber una variante en éstos pasos, ya que el emisor puede cifrar el mensaje con su clave privada, y cualquiera que conozca la clave pública puede descifrarlo, generalmente se usa para mensajes no muy confidenciales y para tener la certeza de la identidad del emisor.

Un algoritmo de clave pública debe cumplir:

- Conocido el criptograma no se puede descifrar el texto ni adivinar la clave.
- Conocido el texto y el criptograma es más caro (en tiempo y/o dinero) descifrar la clave que el valor de la información.
- Conocida la clave pública y el texto no se puede generar un criptograma cifrado con clave privada.

2.3.1.3.1 Servicios del criptosistema Asimétrico

La Criptografía asimétrica es muy usada, sus principales servicios son la confidencialidad, integridad y autenticación del origen de los datos, además el uso del mecanismo de firma digital.

Para cada servicio se cifra de manera diferente:

- **Confidencialidad.-** El emisor cifra el texto con la clave pública del receptor y el receptor lo descifra con su clave privada. Así cualquier persona puede enviar un mensaje cifrado, pero solo el receptor, que tiene la clave privada, y el emisor que lo ha creado, puede descifrar el contenido.

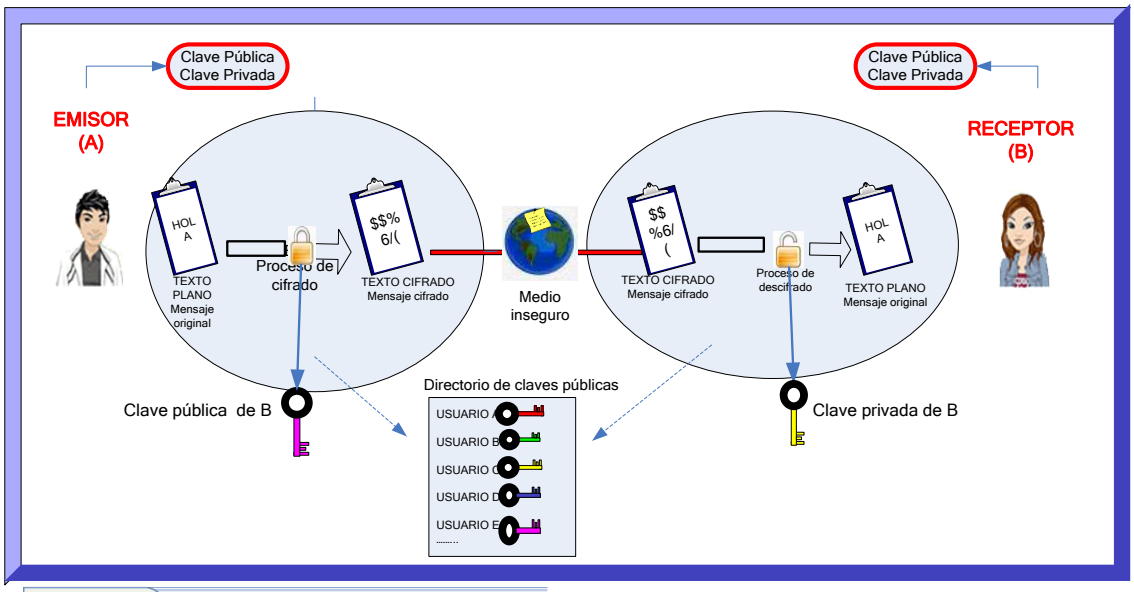


IMAGEN Nº17 Confidencialidad en Criptografía asimetrica

- **Autenticación**.- Se cifra este o un resumen de este mediante la clave privada y cualquier persona puede comprobar su procedencia utilizando la clave pública del emisor. El mensaje es auténtico porque solo el emisor verdadero puede cifrar con su clave privada.

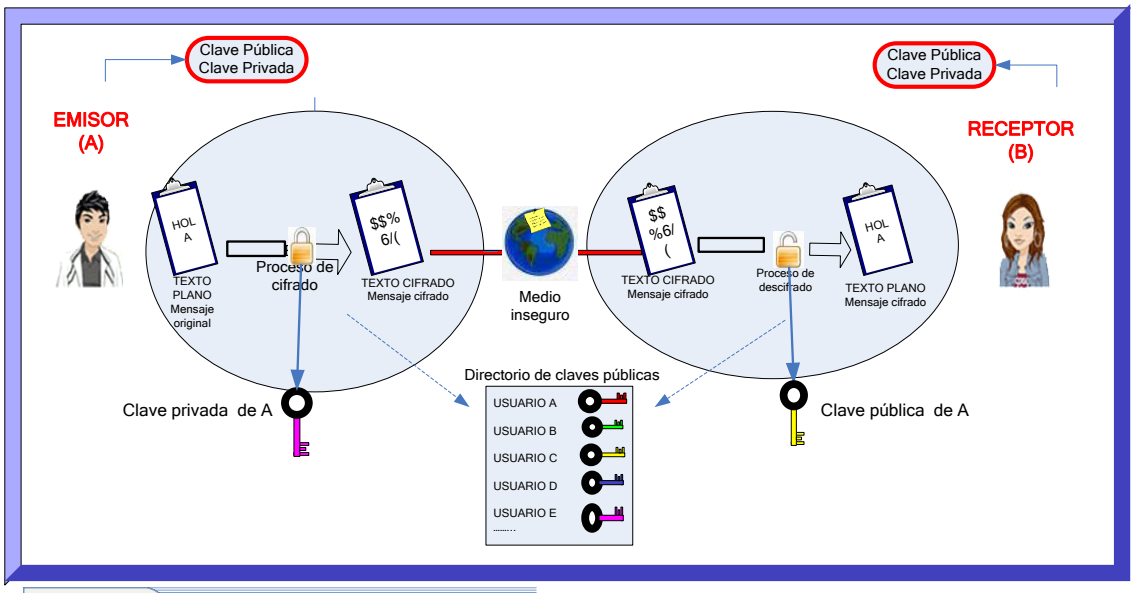


IMAGEN Nº18 Autenticación en criptografía asimétrica

- **Firma Digital.-** Igual que la autenticación pero siempre se cifra el resumen del mensaje, cuyo criptograma es la firma del emisor. Así el emisor no puede negar la procedencia ya que se ha cifrado con su clave privada. Por otro lado, el receptor no puede modificar el contenido porque el resumen sería diferente y se observaría que no coincide con el descifrado de la firma. Pero el receptor sí puede comprobar que el resumen coincide con la firma descifrada para ver si es auténtico y goza de **integridad**.

  Aclarando, el receptor B puede tener confianza sobre la autoría de A en el cifrado de los datos de origen, pero no en que haya sido A quien los ha enviado a través de un medio de transferencia de datos, este es otro servicio el de **no repudio de envió**, que exige otro escenario de comunicaciones y la presencia de terceras partes de confianza (Autoridad Certificadora AC).

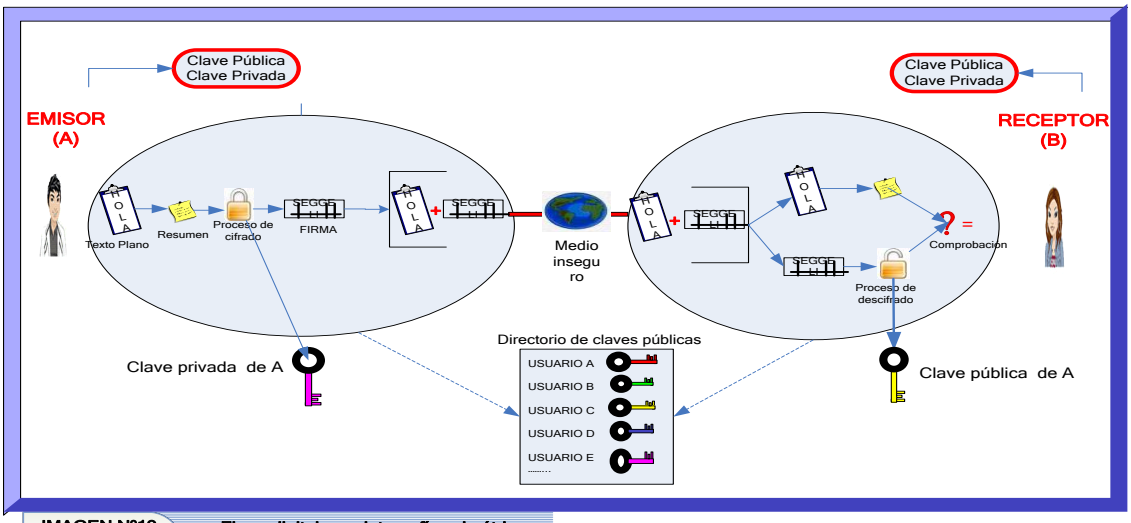


IMAGEN Nº19 Firma digital en criptografía asimétrica

En la figura anterior se puede notar que se envía a través del medio de comunicación, el mensaje sin cifrar acompañado de la firma, para evitar esto generalmente se combinan con el servicio de autenticación.

2.3.1.3.2 Ventajas y Desventajas

Ventajas:

- La principal ventaja de los sistemas de clave pública frente a los simétricos es que la clave pública y el algoritmo de cifrado son o pueden ser de dominio público y que no es necesario poner en peligro la clave privada en tránsito por los medios inseguros, ya que ésta se encuentra siempre oculta y en poder únicamente de su propietario.
- El que solamente la clave pública tenga que darse a conocer permite una adecuada gestión de claves en entornos distribuidos donde se requiere la interconexión de sistemas abiertos.
- Las facilidades que estos sistemas ofrecen para el diseño de mecanismos de autenticación, permitiendo emular sobre las redes, mediante el cifrado con la clave privada del emisor, los esquemas de firmas de documentos que se presentan en las comunicaciones convencionales mediante papel.

Desventajas:

- Dificultan la implementación del sistema, debido a que son mucho más lentos y costosos que los simétricos. En la práctica los métodos

asimétricos se emplean únicamente para cifrar la clave de sesión [5] (simétrica) de cada mensaje.

2.3.1.3.3 Clasificación:

Los principales algoritmos asimétricos actuales son Deffie-Hellman, RSA, DSA.

- **Deffie-Hellman**.- Es un criptograma que permite desarrollar e intercambiar una clave privada compartida y usada a través de un canal de comunicaciones público. Es ampliamente utilizado en sistemas de Internet que requieran confidencialidad (VPNs, SSL, etc.…).

Funcionamiento

1. El usuario A elige una clave pública **KP_A** (KP_A =7) y el usuario B elige una clave pública **KP_B** (KP_B =5).
2. El usuario A elige una clave privada **KS_A** (KS_A=9) y el usuario B elige una clave privada **KS_B** (KS_A =11).
3. A partir de las claves públicas el usuario A calcula **Atx= (KPB ^ KS_A) % KP_A** (5^9 % 7 = 6) y se lo envía a B, mientras que B calcula **Btx= (KPB ^ KS_B) % KP_A** (5^11 % 7 = 3) y se lo envía al usuario A.
4. Finalmente los usuarios A y B pueden calcular una clave conocida por ambos.

[5] Ver glosario de términos y sección 2.1.9

Aclave= (Btx^ KP_A) % KP_A (3^9 % 7 = 6)

Bclave= (Atx^ KS_B) % KP_A (6^11 % 7 = 6)

Donde CA = CB = C.

- **RSA.-** Es el algoritmo mas ampliamente conocido para realizar criptografía de clave pública. Su nombre se debe a sus inventores, Ronald **R**ivest, Adi **S**hamir y Leonard **A**dhelman. Es utilizado tanto para cifrado como para autenticación, usa dos tipos de claves una pública y una privada. En la actualidad RSA emplea claves de 1024 bits (1024 bits, equivale a un número de 308 dígitos), consideradas lo bastante largas como para resistir ataques de fuerza bruta (se han roto claves de hasta 512 bits, aunque se necesitaron más de 5 meses y casi 300 ordenadores trabajando juntos para hacerlo).

  Su seguridad se basa en la dificultad de factorizar números primos de gran tamaño. En principio se puede deducir la clave secreta conocida la clave pública, pero solamente por medio de la factorización de números de gran longitud (centenares de cifras).

  Una gran ventaja del **R.S.A.** es que permite asegurar las cualidades de No Repudio, Autenticidad e Integridad de los criptosistemas cuando se lo utiliza para firmar mensajes, razón por la cual le convierte en un sistema muy completo y uno de los más seguros que existen.

  Los servicios de autenticación y firma digital solo se pueden implementar con estos sistemas**.** Para confidencialidad se puede

utilizar también clave simétrica (DES, IDEA, RC4, etc.) Siendo estos mucho más rápidos que el **RSA.** En la actualidad se utilizan sistemas mixtos, simétricos para confidencialidad y asimétricos para distribución de claves simétricas, autenticación y firma digital. [6].

En líneas generales **RSA** se considera que es entre 100 y 10000 veces mas lento que el DES. **RSA** debe utilizarse solamente para cifrar piezas de información de reducido tamaño, siendo necesario recurrir a mecanismos de firma digital que no se basen en cifrar todo el mensaje completo con la clave privada, así como al uso combinado de criptografía simétrica y de clave pública cuando se trate de proveer los tres servicios básicos (autenticación, integridad y confidencialidad).

- **DSA.-** Es un algoritmo de firmas digitales desarrollado por la NSA. Es realizado específicamente para firmas digitales.

  Utiliza más parámetros que el RSA y así se consigue un grado mayor de seguridad.

2.3.1.4 Criptosistemas híbridos público/privados

Es un criptosistema que combina las propiedades de los criptosistemas asimétricos y criptosistemas simétricos, aprovechando las ventajas de cada uno de ellos. También son llamados sistemas criptográficos mixtos.

Se suele utilizar las técnicas del sistema asimétrico, cifra y envía la clave simétrica. Las técnicas del sistema simétrico son utilizadas para cifrar el mensaje con la clave simétrica y posteriormente el envió masivo de datos.

[6] Datos de: Introducción a la Criptografía Autor: Universidad Politécnica de Mataro

El software mas conocido que utiliza el criptosistema híbrido es el sistema PGP.

2.3.1.4.1 PGP

El sistema ***PGP*** (Pretty Good Privacity - Intimidad Bastante Buena) fue diseñado por Philip Zimmermann en 1991 para proporcionar una forma segura de intercambio de correo electrónico.

PGP se implementa tanto para el cifrado del correo y ficheros como para la firma digital de documentos.

Para el cifrado del documento usa un algoritmo simétrico, para el intercambio de clave lo realiza mediante el sistema asimétrico que generalmente es ***RSA***.

Para la firma digital suele utilizar la función hash MD5.

Es un sistema ampliamente configurable lo que permite al usuario elegir entre diferentes sistemas asimétricos, funciones hash y longitudes de clave.

Normalmente el sistema PGP viene implementado mediante alguna aplicación específica, que se instala en el computador del usuario. Esta aplicación se integra perfectamente con los programas de correo más comunes, permitiendo al usuario el uso directo del sistema PGP, con tan sólo pulsar los botones que aparecerán en la barra de menús de la aplicación de correo.

Desventaja de PGP:

PGP sirve para grupos pequeños de usuarios donde siempre hay un enlace entre ellos, razón por lo cual no es útil para los millones de usuarios de Internet, no podrían certificarse todos entre si.

Para solucionar, se han creado las Autoridades de Certificación (CA), las cuales generan claves públicas y certificados para usuarios.

2.4 ADMINISTRACIÓN DE CLAVES

La administración de claves es un problema latente y muy serio en la criptografía, razón por lo cual es imprescindible llevar un control de las claves utilizadas, la dificultad que esto conlleva va ha depender más del número de equipos involucrados en un determinado dominio de seguridad que de los algoritmos o criptosistemas que sea necesario soportar en cada extremo de una comunicación (emisor, receptor) , para solucionar este problema se establece una serie de procedimientos y normas para su distribución, almacenamiento y selección, que variará notablemente en función del sistema de cifrado empleado, ya sea este simétrico o asimétrico.

2.4.1 Administración de claves en un sistema simétrico

En los sistemas de clave privada se gestiona mayor cantidad de claves razón por la cual surgen problemas en los procedimientos de distribución y en los de almacenamiento.

Cuando se trabaja con varias claves de pequeño tamaño es posible memorizarlas sin necesidad de recurrir a ningún sistema para su almacenamiento, pero cuando se deben utilizar diversas claves para cifrar información y acceder a diferentes sistemas, se hace imprescindible su almacenamiento.

Selección de clave

A la hora de elegir una clave, ya sea para cifrado de información, como de acceso a un sistema, debe evitarse la utilización de claves sencillas de descubrir y que puedan hacer inútil el sistema de cifrado más avanzado.

Es necesario llegar a un compromiso entre facilidad para recordar una clave y dificultad de que alguien la descubra. La utilización de algoritmos para obtener las claves soluciona el problema de la mala elección de estas por parte de los usuarios, aunque producirán claves difíciles de recordar. Existen diversos algoritmos de uso extendido para la generación de claves basados en operaciones como desplazamientos, rotaciones o permutaciones, y también es común la simple generación aleatoria.

Las claves deben tener un tiempo de vida limitado, al menos por dos razones:

- Criptoanálisis
- Si la clave por alguna razón puede ser comprometida o criptoanalizada, limitando el tiempo de vida, se limita el daño que puede ocurrir [7]

Almacenamiento:

- Hay varias soluciones a este problema. La más simple es almacenar todas las claves de un usuario o las comunes a un grupo de usuarios en un fichero cifrado. Para extraer cualquier clave no habría más que

[7] **Datos de :** Titulo.- Criptografía; Autor.- Universidad Nacional de Comahue (UNCOMA) (Chirino, María Andrea)

conocer la clave de cifrado del fichero o clave maestra que daría acceso a todas las demás.

- También se podría establecer una estructura jerárquica donde determinados usuarios puedan extraer sólo ciertas claves, existiendo también una clave maestra que daría acceso a todas las claves contenidas.

  El hecho de almacenar claves en ficheros centralizados conteniendo información tan sensible como la relacionada con las claves secretas de los usuarios representa un riesgo muy importante, ya que cualquier problema de robo o ataque con éxito a uno de estos sistemas tendría consecuencias desastrosas y de muy difícil restauración. Estos sistemas de recuperación de claves pueden tener utilidad en entornos empresariales reducidos, pero son, por su propia concepción, mas costoso, mas difíciles de utilizar y menos seguros que los sistemas convencionales basados en el uso combinado de criptografía simétrica y de clave pública.

Distribución de claves

- Depende del dominio, si la red tiene un número reducido de usuarios, en el que, además estos tengan alguna relación personal o corporativa que haga que tengan entre si cierto nivel de confianza, el intercambio de claves puede ser manualmente o a través de un medio magnético por Ej. Diskette.

- Pero si al contrario el número de usuarios es considerable, pertenecientes a organizaciones distintas y bastante separadas geográficamente, como es el caso de las entidades conectadas a redes de área extensa (Internet). Los problemas que ello conlleva son de tal magnitud que solo son posibles mediante la presencia de elementos centrales. Asimismo, se comprueba que la existencia de estos elementos representan una amenaza insalvable para la privacidad de los participantes. La única solución está en la eliminación de esta centralización esto es lo que se consigue con los criptosistemas de clave pública, tal como el algoritmo de Diffie-Hellman[8], el cual permitirá el intercambio de claves.

2.4.2 Administración de claves en un sistema asimétrico

Los sistemas de clave pública dependen de algunas claves que deber ser secretas, por lo que se debe contar con un sistema seguro y eficiente para la generación, registro, backup, recuperación, distribución, actualización , revocación y terminación. En general, la protección de las claves necesita ser realizada a través de todo su tiempo de vida.

Almacenamiento

Todas las claves secretas necesitan ser protegidas por propósitos de integridad y confidencialidad, razón por la cual deben ser almacenadas en un lugar físico seguro.

[8] Ver sección 2.1.6.2 Algoritmo Diffie-Hellman

En los sistemas de clave pública, el problema del almacenamiento está resuelto puesto que el usuario sólo debe mantener su clave privada en secreto y su clave pública se encuentra en una base de datos o directorio de claves públicas que alguien se encarga de mantener. Estos directorios, que contienen la identidad de los usuarios y sus claves, así como otros datos referentes a los usuarios y claves incluyen firmas digitales para su certificación.

Distribución de claves

En un dominio homogéneo con pocos usuarios por ejemplo una empresa en la que sus usuarios compartan las mismas restricciones y necesidades de comunicación se utiliza una ***Autoridad de Seguridad*** que dictará las normas de seguridad y en la que todos los usuarios confiarán. Esta ***autoridad de seguridad*** será la que genere las claves públicas y privadas, y defina la forma de distribución de las mismas. Los usuarios aceptarán las claves entregadas y confiarán plenamente en que ellos y solo ellos serán los únicos poseedores de sus claves privadas y por tanto los únicos responsables de lo que se haga con ella.

En un dominio mucho mas extenso como es el caso de Internet este tipo de distribución ya no funciona porque no se tiene un control de las claves que se va ha entregar y además surge un problema mucho mas complicado, tiene que ver con la revocación de claves, cuando un usuario considere, que por algún motivo su clave ha sido comprometida, bien porque tenga evidencias o simplemente sospechas de que alguien a copiado su clave. Para la ***autoridad de seguridad*** le resultará muy

complicado definir un procedimiento para informar al resto de los usuarios del valor de la nueva clave pública y la fecha de revocación de la antigua clave.

Una solución a este problema sería la utilización de un ***Servidor automático***, accesible a través de la red, que gobernase una base de datos que contuviese todas las claves públicas del dominio, la cuál estaría debidamente protegida para que nadie, excepto su gestor, pudiese modificarla. Pero a pesar de esta solución existe un problema, si el emisor desea obtener la clave pública del receptor (a quien desea enviar un mensaje confidencial), un intruso puede engañar al emisor y hacerse pasar por el servidor y entregarle su clave pública (intruso), en vez de la clave pública del receptor. A partir de ese instante los mensajes confidenciales que el emisor envié al receptor solo podrán ser leídos por el Intruso.

La clave pública solo hay que darla a conocer a los miembros del dominio de seguridad de que se trate, pero como su conocimiento no tiene nada de reservado, no importa que sea conocida por quienes no tengan nada que ver con este entorno. Lo que si hay que garantizar de algún modo es su **validez**.

Cuando un usuario recibe una clave pública, como puede estar seguro de la identidad del propietario de esa clave, puede que una persona se haga pasar por otra y envíe claves públicas a los receptores este problema es conocido como suplantación de personalidad.

Para solucionar este tipo de problema los sistemas asimétricos utilizan los certificados de claves públicas que son una estructura de datos que identifica el propietario de una clave pública particular.

El certificado es un bloque de datos firmado digitalmente que contiene una clave pública y el nombre del usuario de la clave. (Se hablará mas detalladamente de los certificados en la sección **2.3**).

2.5 CLAVES DE SESIÓN

Las ***claves de sesión*** son aquellas claves utilizadas durante una única sesión. El objetivo es no utilizar la misma clave para muchas transmisiones porque se puede estar expuesto a los siguientes problemas:

- Al utilizar un criptograma con la misma clave es más fácil romper un sistema.
- Si un criptoanalista descubre la clave, podrá descifrar todas las transmisiones sin que los implicados sean conscientes.

La mayoría de sistemas actuales utilizan técnica mixta de clave simétrica para confidencialidad y clave asimétrica para autenticación o firma y para distribuir las claves de sesión simétricas.

El proceso es el siguiente:

1. El ordenador emisor genera una clave de sesión aleatoria
2. Se cifra el mensaje con la clave de sesión.
3. Se envía el mensaje cifrado y la clave de sesión cifrada con la clave pública del receptor

4. El receptor descifra la clave de sesión y , con ella, descifra el mensaje

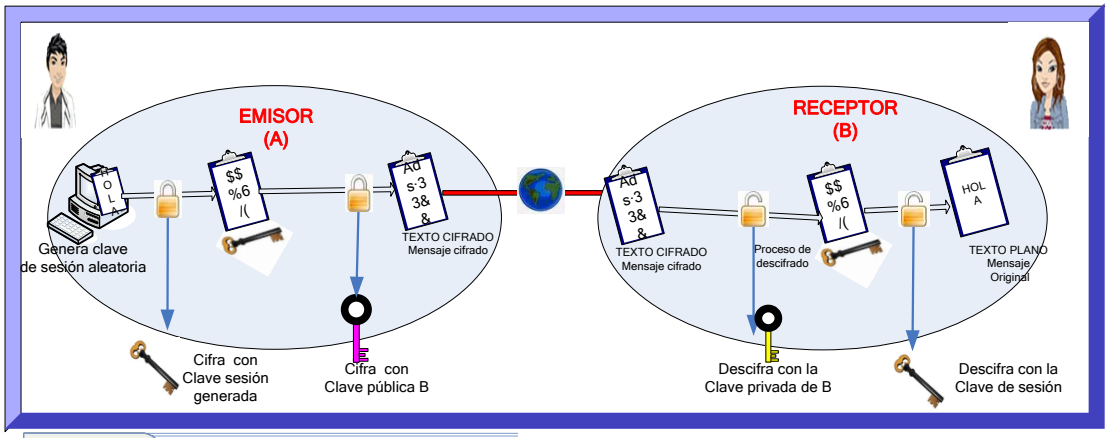


IMAGEN Nº 20 Confidencialidad con clave de sesión

2.5.1 Confidencialidad con usuarios anónimos

Si la comunicación se realiza entre dos usuarios que no tienen las claves públicas del otro, como en el caso de comunicación de usuario anónimo con una Web pública, se envía una clave pública en claro al comenzar la conexión ya que no hay peligro si la ven personas externas. Ejemplo de este sistema son los protocolos de Internet: SSL, SET, etc.

El proceso es el siguiente.

1. El cliente se conecta a un servidor de Internet seguro.
2. El servidor de Internet envía su clave pública al cliente.
3. El cliente cifra una clave de sesión aleatoria con la clave pública del servidor y la envía.
4. Todas las comunicaciones se realizan cifradas con la clave de sesión.

2.6 PROTOCOLOS DE SEGURIDAD

Un protocolo de seguridad es la parte visible de una aplicación, es el conjunto de programas y actividades programadas que cumplen con un objetivo específico mediante el uso de esquemas de seguridad criptográfica.

El ejemplo más común es **SSL** (**S**ecure **S**ockets **L**ayer),lo vemos integrado en un Browser por ejemplo Netscape el cual muestra un candado en la barra de herramientas cerrado y también la dirección de Internet cambia de http a https, otro ejemplo es ***PGP*** que es un protocolo libre ampliamente usado de intercambio de correo electrónico seguro, otro ejemplo es el conocido y muy publicitado ***SET*** que es un protocolo que permite dar seguridad en las transacciones por Internet usando tarjeta de crédito y proporciona seguridad en la conexión de IPsec Internet a un nivel más bajo.

Estos y cualquier protocolo de seguridad procura resolver algunos de los problemas de seguridad como la integridad, la confidencialidad, la autenticación y el no rechazo, mediante sus diferentes características

Las características de los protocolos se derivan de las múltiples posibilidades con que se puede romper un sistema, es decir, robar información, cambiar información, leer información no autorizada, y todo lo que se considere no autorizado por los usuarios de una comunicación por red.

Así por ejemplo sobre la seguridad por Internet se deben de considerar las siguientes tres partes: seguridad en el browser (Netscape o Explorer), la seguridad en el Web server (el servidor al cual nos conectamos) y la seguridad de la conexión.

2.6.1 SSL (Secure Sockets Layer)

El protocolo ***SSL*** es un sistema de seguridad desarrollado por Netscape en 1994 y utilizado actualmente por la mayoría de empresas que comercializan a través de Internet. SSL actúa en la capa de comunicación situada entre el protocolo de la capa de red (Ej. TCP/IP) y un protocolo de la capa de aplicación (Ej. HTTP), es como un túnel que protege a toda la información enviada y recibida.

2.6.2 Funciones

SSL proporciona mecanismos para establecer una comunicación segura entre un cliente y un servidor:

- Cifrado de datos: la información transferida, aunque caiga en manos de un atacante, será indescifrable, garantizando así la confidencialidad.
- Autenticación de servidores: el usuario puede asegurarse de la identidad del servidor al que se conecta y al que posiblemente envíe información personal confidencial.
- Integridad de mensajes: permite detectar modificaciones intencionadas o accidentales en la información mientras viaja por Internet.
- (Opcionalmente) Autenticación del cliente: permite al servidor conocer la identidad del usuario, con el fin de decidir si puede acceder a ciertas áreas protegidas.

SSL proporciona mecanismos para establecer una comunicación segura entre un cliente y un servidor mediante el uso tanto de la criptografía asimétrica como de la criptografía simétrica. SSL negocia en una primera

fase utilizando criptografía asimétrica (por ejemplo RSA), y cifra posteriormente la comunicación utilizando criptografía simétrica (RC4, RC5, IDEA...).

Este protocolo esta diseñado para soportar un rango de algoritmos de criptografía. Esto le permite a los servidores elegir que tipo de algoritmo va a utilizar y además toma ventaja de futuros nuevos algoritmos. Las opciones se negocian entre el cliente y el servidor al inicio de la sesión.

Con ***SSL*** se pueden usar diferentes algoritmos para las diferentes aplicaciones, por ejemplo usa DES, TDES, RC2, RC4, MD5, SHA-1 y RSA.

2.6.3 Procedimiento para establecer una comunicación con SSL

Cuando un navegador solicita una página a un servidor seguro, ambos intercambian una serie de mensajes para negociar las mejoras de seguridad. Este protocolo sigue las fases que se exponen a continuación:

- **La fase inicial**, utilizada para ponerse de acuerdo sobre el conjunto de algoritmos para garantizar la confidencialidad e integridad y para la autenticación mutua. El navegador le informa al servidor de los algoritmos que posee disponibles. Normalmente, se utilizarán los más fuertes que se puedan acordar entre las dos partes. En función de las posibilidades criptográficas del navegador, el servidor elegirá los algoritmos con una cierta longitud de claves.
- **La fase de autenticación**, en la que el servidor envía al navegador su certificado x.509v3 que contiene su clave pública y solicita a su vez al

cliente su certificado X.509v3 (solo si la aplicación exige la autenticación de cliente).

- **La fase de producción** de clave de sesión, en la que el cliente envía al servidor una clave maestra a partir de la cual se generará la clave de sesión para cifrar los datos intercambiados posteriormente mediante el algoritmo de cifrado simétrico acordado en la fase inicial. El navegador envía cifrada esta clave maestra usando la clave pública del servidor que extrajo de su certificado en la fase de autenticación. Más adelante, ambos generarán idénticas claves de sesión a partir de la clave maestra generada por el navegador.
- **La fase final**, en la que se verifica mutuamente la autenticidad de las partes implicadas y que el canal seguro ha sido correctamente establecido. Una vez finalizada, puede comenzar la sesión segura.

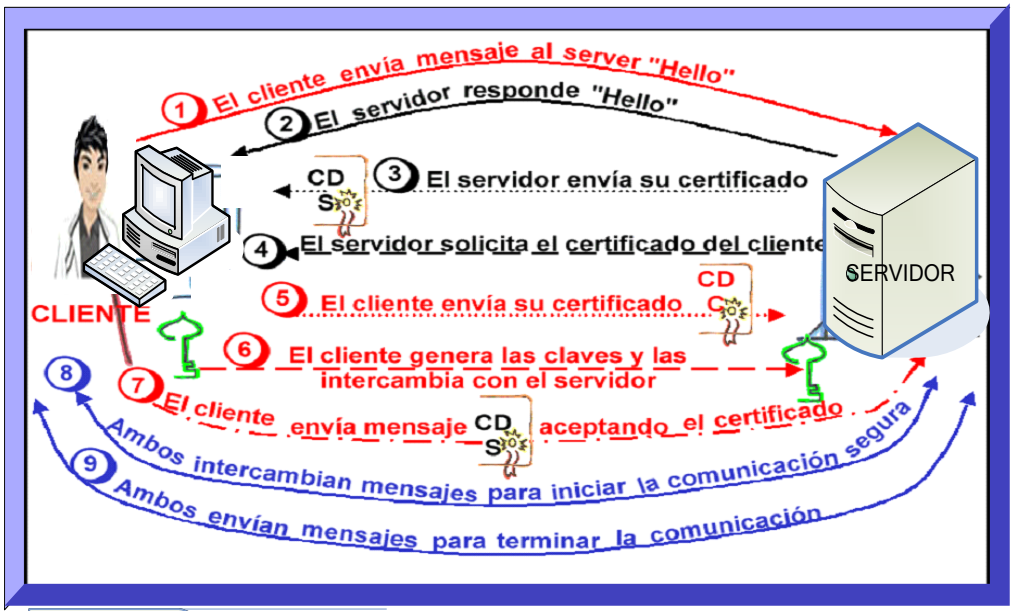


IMAGEN Nº 21 Protocolo SSL

De ahí en adelante, durante la sesión segura abierta, ***SSL*** proporciona un canal de comunicaciones seguro entre los servidores Web y los clientes (los navegadores) a través del cual se intercambiará cifrada la siguiente información:

- El URL del documento solicitado.
- Los contenidos del documento solicitado.
- Los contenidos de cualquier formulario enviado desde el navegador.
- Las "cookies" enviadas desde el navegador al servidor y viceversa.
- Los contenidos de las cabeceras HTTP.

2.7 HTTPS

Uno de los usos comunes de SSL es el de establecer una comunicación Web segura entre un browser y un Web Server. Es aquí donde se usa ***https*** que es básicamente http sobre ssl con un esquema de invocación por medio de url. Es importante hacer notar que el uso del protocolo ***https*** no impide en caso alguno que se pueda utilizar http, por lo que la mayoría de los browsers advierten cuando una página tiene elementos que no son seguros en entornos seguros, como también advierten cuando se invoca un protocolo distinto al de la pagina actual (http -> ***https*** o https -> http).

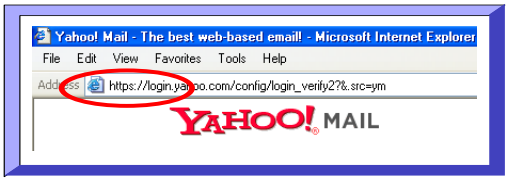


IMAGEN Nº 22 HTTPS

2.8 AUTORIDADES DE CERTIFICACIÓN

2.8.1 ¿Qué son los las autoridades certificadoras?

"***Autoridad Certificadora*** es un ente u organismo que, de acuerdo con unas políticas y algoritmos, certificará por ejemplo las claves públicas de usuarios o servidores".[9]

"Una Autoridad Certificadora es la responsable de emitir certificados de clave pública. Estos certificados se firman digitalmente con la llave privada del CA emisora." [10]

En conclusión una Autoridades de Certificación (CA) es una entidad u organismo fiable que tiene la capacidad de emitir y garantizar la validez de los certificados que emite firmándolos con su propia clave privada, asegurando de esta manera la integridad del vínculo existente entre una determinada clave y su propietario real.

Una CA tiene como obligación proporcionar a sus clientes una Declaración de Prácticas de Certificación (Certification Practice Statement o CPS) que indique claramente sus políticas y prácticas relativas a la seguridad y mantenimiento de los certificados, las responsabilidades de la CA respecto a los sistemas que emplean sus certificados y las obligaciones de los subscriptores respecto de la misma.

Una CA actúa como mediador en una red de confianza establecida entre todos los certificados que dependen de ella. La red de confianza, además, se

[9] Libro Electrónico de Seguridad Informática y Criptografía Versión 4.1 Autor: Dr. Jorge Ramió Aguirre. Universidad Politécnica de Madrid

[10] Libro: PKI - Concepts, Standards, Deployment and Considerations - 2nd Ed – lAutor: Addison Wesley – 2002

puede extender jerárquicamente con otras CA estableciendo vínculos y relaciones entre ellas, facilitando la comunicación entre certificados pertenecientes a distintas CA vinculados en una red común de confianza.

Las CAs locales son certificadas por otras de nivel superior hasta llegar a la principal que es de confianza en todo el mundo. Así se consigue que la confianza sea mundial, para la red de Internet, y que la gestión pueda ser local, facilitando el proceso de identificación personal y procesos judiciales.

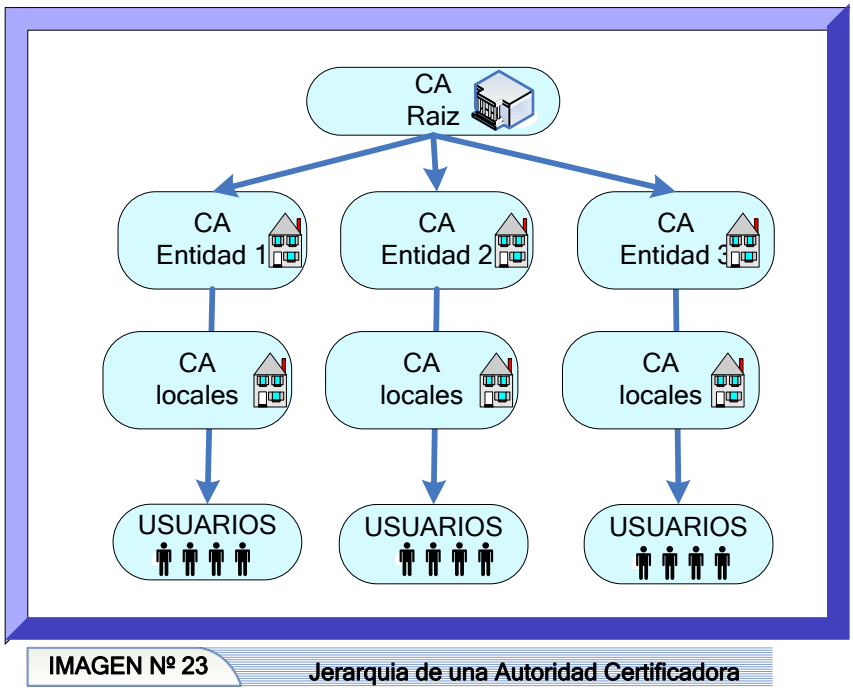


IMAGEN Nº 23 Jerarquia de una Autoridad Certificadora

En una estructura compleja (por número de certificados o ramificaciones de confianza entre distintas CA) es posible crear organismos intermedios entre la CA y los administradores, que se encarguen de tareas meramente de registro. Estos organismos se denominan Autoridades de Registro (RA) y su función es la de descargar a la CA de las funciones de gestión de certificados: expedición, revocación, etc.

2.8.2 Autoridades de registro (RA)

Las **autoridades de registro** (RA), son CA regionales, que actúan de intermediarios entre los usuarios y la CA principal.

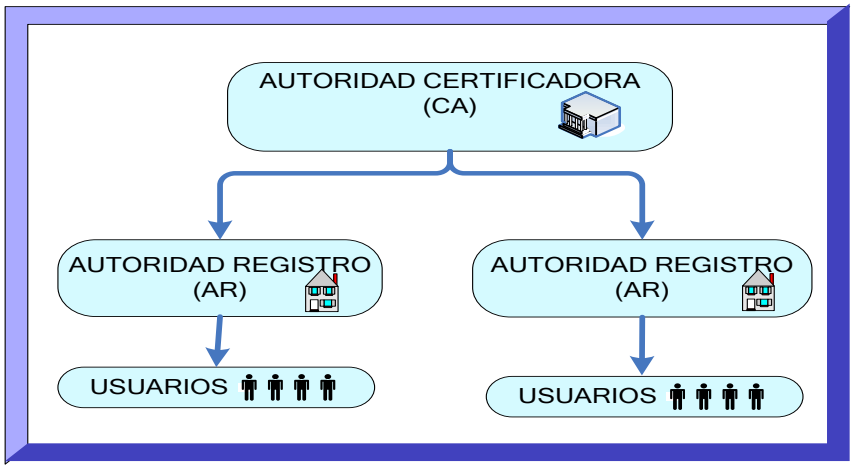


IMAGEN Nº 24 Autoridad Certificadora

Las principales funciones que realiza una autoridad de registro:

- Recibir las solicitudes de certificación
- Proceso de la autenticación de usuarios
- Generar las claves
- Respaldo de las claves
- Proceso de Recobrar las claves
- Reportar las revocaciones….[11]

2.9 CERTIFICADOS DIGITALES

Una de las debilidades de los criptosistemas de clave pública consiste en que si alguien se le engaña acerca del valor de la clave pública de otro usuario, la

[11] Criptografía para principiantes Autor: José de Jesús Ángel

seguridad del algoritmo se viene abajo. La solución a este problema consiste en garantizar la propiedad y validez de la clave pública mediante la generación de un certificado de la clave pública firmado digitalmente por una Autoridad de Certificación CA.

2.9.1 ¿Qué son los certificados digitales?

"Un ***certificado digital*** es un documento que contiene diversos datos, entre ellos el nombre de un usuario y su clave pública, y que es firmado por una Autoridad de Certificación (AC)."

"El ***certificado digital*** o electrónico es un fichero que contiene unos datos identificativos y una información técnica (clave pública), que garantiza que el certificado pertenece a la persona identificada por los datos. "

Como conclusión podemos decir que un *certificado digital "es un documento electrónico emitido por una entidad de certificación autorizada para una persona física o jurídica, con el fin de almacenar la información y las claves necesarias que faciliten su identificación ante terceros, ofreciendo los mecanismos necesarios para prevenir la suplantación de su identidad."*

2.9.2 Funciones

Los ***Certificados Digitales*** permiten efectuar comunicaciones electrónicas seguras, proporcionando y garantizando:

- **Autenticación** permite que la identidad del emisor y el receptor sean reconocidas y autorizadas así como la información que de ellos proviene. El certificado digital asocia los datos del usuario a una clave pública que permite a otros verificar que esa clave es válida.

- **Confidencialidad** de la información transmitida mediante el uso de algoritmos de cifrado con el propósito de que sólo el destinatario del documento pueda acceder a su contenido
- **No repudio o irrenunciabilidad**, permite probar la participación de las partes en una comunicación, existiendo dos posibilidades:
    - No repudio en origen: El emisor no puede negar que envío porque el destinatario tiene pruebas del envío.
    - No repudio en destino: El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción.
- **Integridad** de la información que se transfiere, garantizando que no se ha producido manipulación alguna en el mensaje original.

2.9.3 Funcionamiento De Los Certificados Digitales

2.9.3.1 Claves de Funcionamiento

Mediante un algoritmo cualquier persona puede obtener un par de números matemáticamente relacionados, denominados claves. Una clave es un número de gran tamaño, que se puede conceptualizar como un mensaje digital, como un archivo binario, o como una cadena de bits o bytes. Cada persona genera un par de claves:

- **Clave privada**

  La clave privada debe conservarse en lugar seguro, ya que solamente puede tener acceso a ella el propietario de la clave pública.

- **Clave pública**

La clave pública se puede distribuir, y debe comunicarse a las personas con las que se quiera intercambiar correo seguro.

La clave pública y privada tienen características únicas, su generación es siempre en parejas y están relacionadas de tal forma que todo lo que sea cifrado por una de ellas sólo podrá ser descifrado por la otra.

2.9.3.2Descripción del Funcionamiento

Un certificado digital es emitido por una Autoridad Certificadora (AC) la cual es la encargada de verificar que una clave pública pertenece a un determinado individuo o entidad. Entre los datos más importantes, contiene la identidad de la persona (nombre), el periodo de validez de dicho certificado, restricciones de uso, su clave pública y el nombre de la AC. Todos estos datos son previamente validados por la AC, asegurando de esta forma la veracidad de la información.

La persona que conozca la clave pública de la AC puede autenticar un Certificado Digital de la misma forma que se autentica cualquier otro documento firmado, como se ilustra en la siguiente figura.

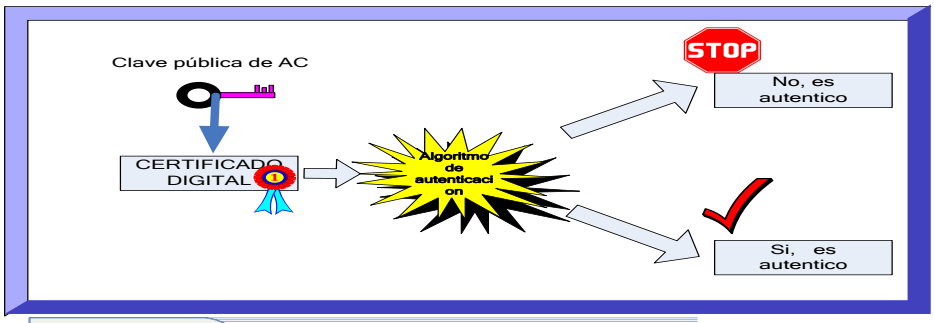


IMAGEN Nº25 Autenticidad del Certificado Digital

Si el Certificado es auténtico y confiamos en la AC, entonces, podemos confiar en que el sujeto identificado en el Certificado Digital posee la clave pública que se señala en dicho certificado. Los certificados ayudan a evitar que alguien utilice una clave falsa haciéndose pasar por otro.

2.9.4 Ciclo de vida de un certificado digital

2.9.4.1 Obtener un certificado digital

Para obtener un certificado digital, debemos en primer lugar saber quien o quienes intervienen en este proceso, los cuales analizamos a continuación:

1) Autoridad de Certificación (AC): es quién emite el certificado digital y quién interviene como tercero de confianza.

2) Autoridad de Registro (AR): persona o entidad delegada por la AC para la verificación de la identidad de los solicitantes y otras funciones dentro del proceso de expedición y manejo de certificados digitales.

3) Suscriptor: Es la persona para la cual se expide el certificado.

4) Solicitante: Persona física que solicita la expedición del certificado, puede ser distinta que el suscriptor ya que, por ejemplo, el solicitante puede ser la DICOMSI y el suscriptor el director de Comunicaciones de la Fuerza Terrestre.

5) Usuario: Persona que voluntariamente decide confiar en un certificado.

Después de haber analizado quienes intervienen en el proceso de certificación, tenemos que tomar en cuenta con que empresa vamos a

trabajar. Cada AC concede o niegan un certificado cuando alguien lo solicita, estas aplican su propio conjunto de requisitos a las solicitudes. Los requisitos pueden depender del propósito de los certificados. Es relativamente fácil obtener un certificado para firmar los mensajes de correo electrónico y puede ser difícil obtener uno para firmar software.

Se puede solicitar un certificado a muchas entidades de cobran una tasa por la concesión de certificados y cada una tiene sus propios métodos.

A nivel mundial existen muchas entidades certificadoras que proporcionan certificados personales con diferentes propósitos, entre ellos tenemos:

- GlobalSign
- Thawte
- Verisign, Inc.

De acuerdo a los navegadores con los que vayamos a trabajar, veremos que cada uno tiene registrados varias empresas certificadoras, que al momento de obtener un certificado, estos nos indican si es de confianza o no.

Para obtener estos certificados, muchos usuarios finales simplemente se registran con la CA o RA vía Internet usando un navegador Web, el usuario final puede revisar las políticas del certificado publicadas por parte de la CA, después de que todos los datos de registro están completos y existe una relación de confianza con la CA, el usuario final, puede ya solicitar un certificado digital.

2.9.4.2 Renovar un certificado digital

Cuando un certificado emitido por una CA, se encuentra caducado o por caducarse, puede ser renovado, para lo cual puede renovarlo con las mismas claves o con nuevas claves, de acuerdo con las necesidades de la empresa o el sujeto que va a utilizar dicho certificado.

2.9.4.3 Revocar un certificado digital

Un certificado de clave pública tiene un tiempo limitado de validez, indicado por el tiempo de comienzo y tiempo de expiración, los cuales son incluidos dentro de la parte firmada del certificado. La longitud de tiempo depende de la política utilizada.

Sin embargo bajo algunas circunstancias el certificado puede ser revocado antes de que llegue a su tiempo de expiración, tales circunstancias son:

- Cambio de nombre
- Cambio de relación entre sujeto y autoridad de certificación.
- Solicitud voluntaria del Suscriptor.
- Pérdida o daños en el soporte del certificado.
- Fallecimiento del suscriptor o de su representado, incapacidad sobrevenida, total o parcial, de cualquiera de ellos,
- Finalización de la representación o extinción de la entidad representada.
- Inexactitudes en los datos aportados por el suscriptor para la obtención del certificado,

- Que se detecte que las claves del suscriptor o de la AC han sido comprometidas

Quién toma la decisión de revocar es la CA y luego deberá informarlo. Una forma es mediante una publicación de una lista de revocación de certificados (CRL), pero cada cuánto y cómo es variante pues no hay un consenso y depende de la política.

2.9.4.4 Borrar un certificado digital

Si va a cambiar de equipo y lo va a entregar a otra persona, debe borrar sus certificados personales, también lo puede borrar si es que ya no confía en la persona u organización a quien se emitió el certificado, independientemente de la razón que tenga para borrar el certificado, debe tener una copia de seguridad por si lo necesita en el futuro.

2.9.5 Estados de los certificados

- **Activo**: Cuando la fecha en curso cae dentro del intervalo de vigencia de un certificado.
- **Suspendido:** Certificado anulado temporalmente, para ello, la Autoridad de Certificación pasa al estado de Suspendido. Con ello no se invalida de forma irreversible el certificado, sino que se le retira de circulación hasta que se le vuelva a dar el estado de Activo.
- **Revocado:** Cuando las condiciones que llevaron a la emisión de un certificado cambian antes de que éste expire, y son de importancia suficiente, la Autoridad de Certificación deberá anularlo; para ello, emite un

segundo certificado especial, denominado “de revocación”, por el cual, desde ese instante desautoriza al certificado previo y lo hace de un modo irreversible.

- **Caducado**: Este es el estado final de cualquier certificado y se produce cuando la fecha en curso es posterior a la fecha de caducidad indicada en el propio certificado. El estado de “certificado caducado” no le resta valor histórico ya que, mientras estuvo activo, las operaciones en las que participó eran perfectamente válidas.

2.9.5.1 Usos

Los certificados permiten realizar una gran cantidad de acciones a sus titulares, entre los cuales tenemos:

- **Identificación**: control de accesos a sitios Web o servicios en línea restringidos. Desarrollo de comunidades cerradas, intranets corporativas. Control de acceso físico de tarjetas inteligentes. Firma de software para su uso en Internet de manera que se puedan realizar acciones en el navegador del usuario que de otro modo le serían negadas.
- **Transacciones electrónicas**: como por ejemplo los movimientos en una cuenta corriente o las transacciones comerciales seguras.
- **Trámites fiscales**: como por ejemplo declaraciones juradas de impuestos, pago on-line de tributos.
- **Seguridad en servidores Web**: se trata de tener la certeza de que se está en el verdadero sitio y no en una copia, permitiendo realizar interacciones seguras.

- **Documentos electrónicos**: da la posibilidad de firmar contratos, órdenes de compra o cualquier otro documento de uso público o privado en forma digital con los mismos efectos que los celebrados por escrito y en soporte de papel. Así mismo, se puede asegurar la confidencialidad en procesos administrativos o consultas de información de importancia en servidores de la Administración.
- **Correo Seguro:** permite enviar correo electrónico cifrado y firmado de manera de proteger este canal identificando a quién emite, a quién recibe y además cifrando el contenido del mensaje.

2.9.5.2 Clases

De acuerdo a la empresa con la que se vaya a trabajar, estas tienen sus políticas de certificación establecidas por la Autoridad de Certificación, los certificados se pueden clasificar por los requisitos que se defina para la identificación del usuario que solicita el certificado. Así, el solicitante tendrá que presentarse físicamente con una credencial ante el administrador para firmar la petición, o bien, es el propio administrador quien autoriza directamente la emisión del certificado.

Las siguientes clases de certificados son definidos de acuerdo a una política de seguridad:

- **Clase 1.** No exige de mucha información para obtener el certificado, el usuario se identifica con su nombre y ofrece una dirección de correo donde se le envía el certificado y el procedimiento para obtenerlo.

- **Clase 2.** Es utilizado para transacciones que ya conllevan un mayor grado de responsabilidad. Para la obtención del certificado el usuario debe presentar información que verifique su identidad, pero no requiere su presencia.
- **Clase 3.** Son los usados para transacciones de alto riesgo como banca electrónica o compras por Internet de gran valor. Para su obtención es requisito la presencia física del solicitante junto con la documentación que acredite su identidad.

2.10 CLASIFICACION

- **Certificados SSL Para Cliente**

  Identifica a un cliente frente a un servidor.

- **Certificados S/MIME**

  Firmado y cifrado de correo electrónico.

- **Certificados para CAS**

  Identifica a una CA frente a otra CA o RA.

- **Certificados de servidor**

  Son certificados en software que identifican que una determinada página Web pertenece a una determinada empresa y que la información transmitida entre el usuario de la página y el servidor está cifrada, de forma que no pueda ser vista ni manipulada por terceros.

- **Certificados para WAP**

Los Certificados WAP permiten a las WEB comerciales existentes y de nueva creación la realización de transacciones seguras con los consumidores móviles. Los nuevos portales basados en transacciones móviles seguras expandirán el comercio electrónico entre los usuarios móviles y los WEB SITES dedicados al comercio.

Los servidores WAP necesitan proporcionar seguridad y confianza a los usuarios potenciales. Esta es la base para que se establezca una contraprestación que satisfaga a ambas partes. Los Certificados WAP permiten mantener conexiones seguras basadas en cifración y autenticación con dispositivos de telefonía móvil.

- **Certificados para firmar código**

  El Certificado para la firma de código, permitirá a un administrador, desarrollador o empresa de software firmar su software (ActiveX, Applets Java, Plug -ins, etc.) y macros, y distribuirlo de una forma segura entre las unidades (usuarios).

- **Certificados para IPSEC-VPN**

  Los Certificados para VPN son los elementos necesarios para que la empresa aproveche las cualidades y ventajas de la utilización de las VPNs de un modo plenamente seguro.

  Las VPNs surgen como consecuencia de la creciente demanda de seguridad en las comunicaciones ya sea entre Router-Router o Cliente-Servidor. La apertura de las redes corporativas a empleados remotos (con gran importancia en el caso del Teletrabajo), sucursales, business partners o clientes.

Todos o algunos de estos tipos de Certificados Digitales son proporcionados por las autoridades de certificación o, como señala la legislación sobre firma electrónica, los prestadores de servicios de certificación.

- **Certificado digital de persona física**

  Dirigido a una persona que tiene una vinculación laboral o comercial con una entidad con personalidad jurídica, como por ejemplo una empresa. Este certificado garantiza únicamente la pertenencia a dicha empresa, pero no la capacidad de obligarse en su nombre.

- **Certificado digital de representante**

  Dirigido a una persona representante de una entidad jurídica con capacidad para obligarse en su nombre.

- **Certificado digital de persona jurídica**

  Dirigido a una entidad con personalidad jurídica.

Un certificado de usuario puede ser instalado en el ordenador, una vez que se está en posesión del mismo. Comúnmente, tanto los navegadores como las aplicaciones que lo soporten, leerán el certificado cuando lo requieran, bien sea para realizar la autenticación del propietario en una aplicación, bien para firmar un documento.

2.11 ¿EN DÓNDE SE GUARDA EL CERTIFICADO DIGITAL?

El certificado estará protegido normalmente por un identificador que sólo conoce el propietario del mismo, pero existen dispositivos más seguros donde es posible

almacenar el certificado sin necesidad de instalarlo en el ordenador, ya que muchas personas pueden tener acceso fácilmente a los ordenadores, algunos de estos dispositivos son:

- **Tarjetas inteligentes (smartcards):** Son tarjetas similares a las de los bancos pero que llevan un chip integrado donde se almacena el certificado de forma segura (ISO 7816). Existen tarjetas que además incorporan un microprocesador con una memoria de hasta 4KB (ISO 7816/ISO 14443).

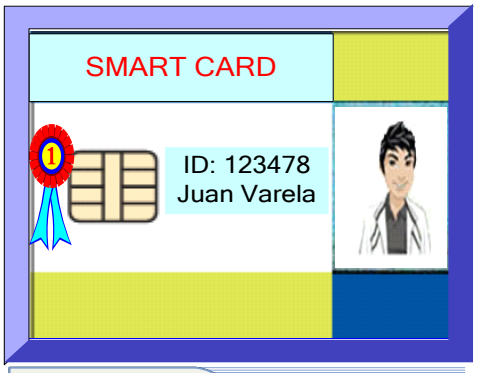


IMAGEN Nº26 Tarjeta Inteligente

- **Llaves (tokens):** Las llaves son dispositivos que almacenan de forma segura los certificados y pueden conectarse al ordenador por alguno de sus puertos, comúnmente el puerto USB. Algunas versiones protegen el acceso al certificado con un dispositivo biométrico como, por ejemplo, un lector de huellas digitales.

IMAGEN Nº27 Tokens

2.12 ESTANDAR X.509 Y ESTRUCTURA DE UN CERTIFICADO DIGITAL

Para el formato de los certificados digitales, existe un estándar internacional ampliamente reconocido; denominado “X.509”. Este estándar establece en detalle la estructura de información que contendrán los certificados, y su formato. El uso de un estándar permite que un certificado sea reconocido y compatible con distintas aplicaciones de software y en variados ambientes. Adicionalmente, tales formatos podrán modificarse o adecuarse a la luz de nuevos avances tecnológicos o nuevos estándares.

Existen tres versiones que señalamos a continuación:

La primera versión apareció en 1988 y fue publicada como el formato X.509v1, siendo la propuesta más antigua para una infraestructura de clave pública (PKI) a nivel mundial. Esto junto con su origen ISO/ITU han hecho de X.509 el PKI más ampliamente utilizado. Más tarde fue ampliada en 1993 por la versión 2 únicamente en dos campos, identificando de forma única el emisor y usuario del certificado. La versión 3 de X.509 amplia la funcionalidad del estándar X.509

El certificado digital almacena información sobre su validez, sobre la entidad (física o jurídica) propietaria del mismo, información sobre la entidad de certificación que reconoce el certificado, e información variable necesaria para el uso específico que podría tener y la clave pública asociada al certificado.

A continuación veremos como se encuentra estructurado el estándar X.509 v3:

Versión	Versión del protocolo
No. De serie	Número único asignado por la CA al certificado
Algoritmo	Algoritmo usado para firmar el certificado
Parámetros	
Autoridad de certificación	Nombre de la CA
Fecha inicio validez	Periodo de validez del certificado
Caducidad	
Nombre del usuario	Nombre del usuario
Algoritmos	Clave pública
Parámetros	
Clave pública del usuario	
Firma de la CA	Firma del certificado con la clave privada de la CA

IMAGEN Nº28 X.509 V3

2.13 LISTAS DE ANULACION DE UN CERTIFICADO DIGITAL (CRL)

Todos los certificados tienen dentro de sus elementos un periodo de validez que va de un mes a unos pocos años. Durante el tiempo que el certificado es válido la AC que lo generó mantiene información sobre el estado del certificado.

Las razones de anulación de un certificado son varias: la clave privada del sujeto se ha visto comprometida, la clave privada de la CA se ha visto comprometida o se ha producido un cambio en la afiliación del sujeto (por ejemplo cuando un empleado abandona una empresa).

Las ***listas de anulación de certificados*** *(*Certification Revocation Lists o ***CRL****)* son un mecanismo mediante el cual la CA publica y distribuye información acerca de los certificados anulados a las aplicaciones que los emplean. Una CRL es una estructura de datos firmada por la CA que contiene

su fecha y hora de publicación, el nombre de la entidad certificadora y los números de serie de los certificados anulados que aun no han expirado. Cuando una aplicación trabaja con certificados debe obtener la última CRL de la entidad que firma el certificado que está empleando y comprobar que su número de serie no está incluido en él.

La Autoridad de Certificación debe tener en todo momento registrado cuales son los estados en los que se encuentran sus certificados. En la literatura informática se habla de las "Listas de Certificados Revocados" o ***CRL's***, como unas listas "negras" en las que la entidad, publica a los cuatro vientos cuales son los certificados que ha anulado para, con ello, desentenderse de las responsabilidades que pudieran acarrear la utilización y/o aceptación por parte de alguna entidad de los mencionados certificados.

Según la importancia de las transacciones que realicen las entidades basándose en los certificados digitales que utilizan, algunas veces no será necesario que consulten si las credenciales presentadas están todavía vigentes en el momento de la transacción, pero habrá otros casos en los que este requisito sea absolutamente necesario, por lo que la entidad se pondrá en contacto con la Autoridad de Certificación y le consultara por el estado de vigencia (actividad) de ese certificado en concreto (número de referencia).

2.14 FIRMA DIGITAL

2.14.1 ¿Qué es una firma digital?

La seguridad es uno de los elementos clave en el desarrollo positivo de las redes de información mundial y particularmente en el comercio electrónico, ésta genera confianza, y hace que los usuarios al depositar sus datos en la red, estén seguros de que no serán alterados ni desviados a usuarios no autorizados.

Según Camerfina: "Es una firma que se puede aplicar sobre documentos electrónicos, consiguiendo los mismos efectos que una firma manuscrita.**"**[12]

En Argentina según sus leyes nos indica que la firma digital resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose esta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

En Uruguay sus leyes definen a la firma digital como el resultado de aplicar a un documento un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, de manera tal que dicha verificación permita, simultáneamente, identificar al firmante y detectar alteración del documento digital posterior a su firma.

[12] **CAMERFINA:** autoridad certificadora de España

En Perú se la define como firma digital a aquella que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública puedan derivar de ella la clave privada.

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

De todas las definiciones legales podemos concluir que la firma digital es: "Un conjunto de datos adjuntados o asociados a un mensaje y utilizados como medio para identificar al autor y garantizar la integridad de los documentos digitales. Entonces, es el resultado de obtener un patrón que se asocie en ambos sentidos a un individuo y su voluntad de firmar, utilizando determinados mecanismos, técnicas o dispositivos electrónicos que garanticen que después no pueda negar su autoría".

2.14.2 ¿Cuáles son sus finalidades?

- Cifrar el contenido de tus mensajes, incluyendo archivos adjuntos, y asegurarse así que el destinatario del mensaje será el único que podrá leerlo.

- Firmar digitalmente y probar la autenticidad de tus mensajes de E-mail, impidiendo así que roben tu identidad y envíen correspondencia enmascarando tu dirección.
- Asegurar que tus mensajes de E-mail, incluidos archivos adjuntos, lleguen a su destino sin ser modificados a través de su viaje por Internet.

2.14.3 ¿Cuáles son sus características?

- Característica de no repudio (el emisor no puede rechazar el envío del mensaje de E-mail).
- Característica de autenticación (confirmación de la identidad del emisor del mensaje).
- Característica de integridad de datos (el mensaje de E-mail, incluidos archivos adjuntos, llega a su destino con un aviso que le permite conocer al destinatario si fue modificado o no en su paso por Internet).

2.14.4 ¿Por qué se necesita una firma digital?

Una firma digital es el equivalente electrónico de una firma manuscrita y que cumpliendo los requerimientos de las leyes de cada País, tiene la misma validez y responsabilidad de una firma convencional.

Una firma digital le permite proteger los datos que se envían por correo electrónico evitando que terceros puedan leerlos o modificarlos durante su envío.

En la actualidad muchas empresas, instituciones de gobierno, etc. han optado por la utilización de firmas digitales para asegurar tanto sus comunicaciones

internas como externas, sin embargo usted como individuo puede también utilizarlas.

2.14.5 ¿Cómo se realiza o funciona una firma digital?

La firma digital se realiza o funciona utilizando complejos procedimientos matemáticos que relacionan al documento firmado con información propia del firmante, y permiten que terceras partes puedan reconocer la identidad del firmante y asegurarse que los contenidos no han sido modificados.

La firma digital utiliza los criptosistemas de clave pública, aunque más lentos que los simétricos, resultan adecuados para los servicios de autenticación, distribución de claves de sesión y firmas digitales, se utilizan los algoritmos de RSA, Diffie−Hellman, etc.

En general, el cifrado asimétrico se emplea para cifrar las claves de sesión utilizadas para cifrar el documento, de modo que puedan ser transmitidas sin peligro a través de la red junto con el documento cifrado, para que en recepción éste pueda ser descifrado. La clave de sesión se cifra con la clave pública del destinatario del mensaje, que aparecerá normalmente en una libreta de claves públicas. El cifrado asimétrico se emplea también para firmar documentos y autenticar entidades, como se describe a continuación. En principio, bastaría con cifrar un documento con la clave privada para obtener una firma digital segura, puesto que nadie excepto el poseedor de la clave privada puede hacerlo. Posteriormente, cualquier persona podría descifrarlo con su clave pública, demostrándose así la identidad del firmante.

2.14.6 ¿En que consiste una firma digital?

Consiste en el uso de sistemas de claves que permiten varias cosas a las partes que intervengan en la transacción o comunicación efectuada a través de Internet: por un lado, que la información, al viajar por la red, vaya cifrada, con la finalidad de que si alguien intercepta dicha comunicación durante su tránsito, no la pueda entender, por otro lado, si alguien, interceptando dicha comunicación, intenta modificarle, ello sería técnicamente detectable, a su vez nos permite tener la certeza de saber quien es la otra parte con la que nos contactamos, lo cuál nos dará la confianza mínima en el sentido de saber que la otra parte es quién dice ser, y no un farsante o un impostor que se este haciendo pasar por él, y para terminar posibilita que el destinatario del mensaje no pueda negar haberlo recibido.

2.14.7 ¿Cómo se utiliza la firma digital?

Supongamos que el emisor desea enviar un mensaje firmado al receptor. Primero crea un mensaje comprimido utilizando una función numérica (hashing) sobre el mensaje. Sí cualquier parte de este mensaje es modificado, la función numérica devuelve un resultado distinto. Después, el emisor cifra el mensaje numérico con su clave privada. Dicho mensaje cifrado es la firma digital del mensaje. El emisor envía tanto el mensaje como la firma digital. Cuando el receptor los recibe, descifra la firma utilizando la clave pública del emisor y descodifica el mensaje. Para verificar la integridad del mensaje, el receptor utiliza la misma función numérica utilizada por el emisor y compara el resultado con el que le envió aquella. Si son idénticos, el receptor se habrá asegurado de que el

mensaje proviene verdaderamente del emisor y que no ha sido modificado desde que fuera firmado. Si el mensaje numérico es diferente, el mensaje fue originado por alguien distinto del emisor o fue modificado desde que fue firmado. Observe que utilizar una firma digital no cifra el texto del mensaje. En caso que el emisor quiera asegurar la privacidad de éste, debe cifrarlo utilizando la clave pública del receptor. De esta forma, sólo el receptor puede leer el mensaje al descifrarlo utilizando su clave privada.

No es factible encontrar un mensaje que posea una determinada numeración, o encontrar dos mensajes que posean una numeración idéntica. Si estos supuestos fueran posibles, un intruso podría adjuntar un mensaje falso junto con la firma del emisor. Las funciones numéricas específicas de hashing han sido diseñadas para tener la certeza de que no es posible encontrar dos mensajes iguales. Uno o más Certificados Digitales pueden acompañar a una firma digital. En caso que un Certificado Digital se encuentre vigente, el receptor (o una tercer parte) puede verificar la autenticidad de la clave pública.

2.14.8 ¿Cómo se comprueba la validez de la firma digital?

Para comprobar su validez debemos primeramente aplicar la función 'hash' al contenido del documento recibido. Esta operación es la misma que realizó el emisor a la hora de firmar el documento. Supondremos que el resultado de dicha operación es H.

A continuación el receptor, descifra la firma electrónica utilizando la clave pública del emisor. Supongamos que el resultado de la operación es F.

Se procederá, a continuación, a comparar H y F. Si coinciden quiere decir que quien envió el mensaje era el verdadero emisor, puesto que sólo el verdadero emisor posee la clave privada, que ha utilizado para codificar la función 'hash' del documento (H) la cual, recordemos, es la firma electrónica del documento.

Para clarificar más el tema, supongamos que alguien intenta hacerse pasar por otra persona a la hora de enviar un documento. Entonces el suplantador podrá generar la función 'hash' del documento (ésta no cambia), la podrá codificar utilizando su clave privada, generando la firma del documento. En el momento en que el receptor haga la comparación entre H y F no coincidirá, puesto que si bien el receptor ha generado correctamente H (el resultado de la función 'hash' no varía, puesto que el contenido del documento no cambia), en el momento en que proceda a descodificar la firma electrónica, éste utilizará la clave pública del emisor, y no la del suplantador, con lo cual el resultado no será H.

2.14.9 ¿Cómo se comprueba la integridad de un documento?

El procedimiento es el mismo que el anterior. Si tenemos en cuenta la propiedad que tiene la función 'hash': "dos documentos distintos tienen funciones 'hash' distintas", entonces si alguien después de la firma del documento hubiera modificado el contenido del documento, la función 'hash' sería distinta (al ser distinto el documento), y por lo tanto el resultado de aplicar la función 'hash', por parte del receptor, ya no seria H, sino H', con lo cual en el proceso de comparación entre H' y F se generaría un error.

2.14.10 ¿Cómo se garantiza el no-repudio?

Aquí ya no debemos hacer comprobaciones adicionales. Si el receptor tiene un documento firmado electrónicamente en el cual puede garantizar la identidad de quien lo ha escrito, así como que nadie ha modificado su contenido con posterioridad a su firma, entonces el emisor nunca podrá decir que no lo ha hecho él, ni que el contenido del documento no era el suyo. En consecuencia, se garantiza el no-repudio.

2.14.11 ¿Cómo se verifican las llaves generadas?

Lo mas importante dentro del proceso de la firma digital, es la "Autoridad certificadora", cuya función es la de establecer la unión entre el firmante y las llaves utilizadas para crear la firma digital. Por ello, la autoridad certificadora revisa los documentos que identifican al firmante, como licencia, pasaporte, o cualquier documento que ratifique su persona y posteriormente certifica que la persona que esta utilizando la llave sea realmente la persona que dice ser. Cualquiera que desee verificar una firma digital debe de confiar en la autoridad de certificación en lugar de personalmente revisar los documentos de identificación del firmante.

2.14.12 Aplicaciones:

- Correo seguro
- Desmaterialización de documentos
- Transacciones comerciales electrónicas
- Invitación electrónica
- Notificaciones judiciales electrónicas

- Dinero electrónico
- Créditos de seguridad social
- Sellado de tiempo
- Voto electrónico
- Contratos comerciales electrónicos
- Factura _ electrónica
- Mensajes con autenticidad asegurada
- Decretos ejecutivos (gobierno)
- Contratación pública

2.14.13 ¿Cómo se usan los certificados con el objeto de verificar una firma digital?

Los certificados se usan para generar confianza en la legitimidad de una clave pública. Estos son documentos digitales que protegen a las claves públicas del fraude, de la falsa representación o de la alteración. Con la autenticación de las firmas se puede adjuntar uno o más certificados con cada mensaje firmado.

El receptor del mensaje verificará que el certificado usado tenga la clave pública de la Autoridad Certificadora, posteriormente, asegurada su confianza en la clave pública del remitente, verificará la firma del mensaje.

Cuanto mayor sea la confianza que tenga el receptor de que la clave pública es realmente del emisor, menor es la necesidad de adjuntar y verificar estos certificados.

2.15 PKI (INFRAESTRUCTURA DE CLAVE PÚBLICA)

PKI son sistemas mixtos hardware/software, basados en el certificado X.509 versión 3, y CLR's versión 2, que permiten dotar a máquinas y usuarios de Certificados Digitales de Identidad, la administración de éstos, y dotar de la confianza que se necesita para los procesos de identificación y autenticación, así como la administración de las claves públicas y privadas de los usuarios. El manejo de certificados digitales en combinación con las claves públicas y privadas, permite la identificación precisa de los participantes mediante la validación de su identidad, y el acceso a la información requerida sólo al personal autorizado (control de acceso), asegurando la confidencialidad e integridad de los datos gracias a las técnicas criptográficas o de cifrado de datos.

2.15.1 Objetivo:

El objetivo de cualquier ***PKI*** es proporcionar a cada usuario de las claves necesarias para:

1. Identificarse, frente a los servidores que lo soliciten y bajo el pleno control del titular;
2. Firmar Digitalmente pedidos, órdenes de pago, correo electrónico, entre otras cosas;
3. Para disponer de Correo Electrónico Seguro haciendo que los demás puedan enviar mensajes que sólo el destinatario genuino puede abrir y leer; y para

4. Establecer canales de comunicación realmente privados entre usuarios sin la supervisión de ningún otro agente que pudiese aprovecharse de lo que a través de ese canal se comunica. [13]

2.15.2 Componentes de un PKI

Una PKI consta de:

- Política de seguridad.
- Autoridad de Certificación
- Autoridad de Registro
- Sistema de Distribución de Certificados.
- Aplicaciones aptas para PKI.

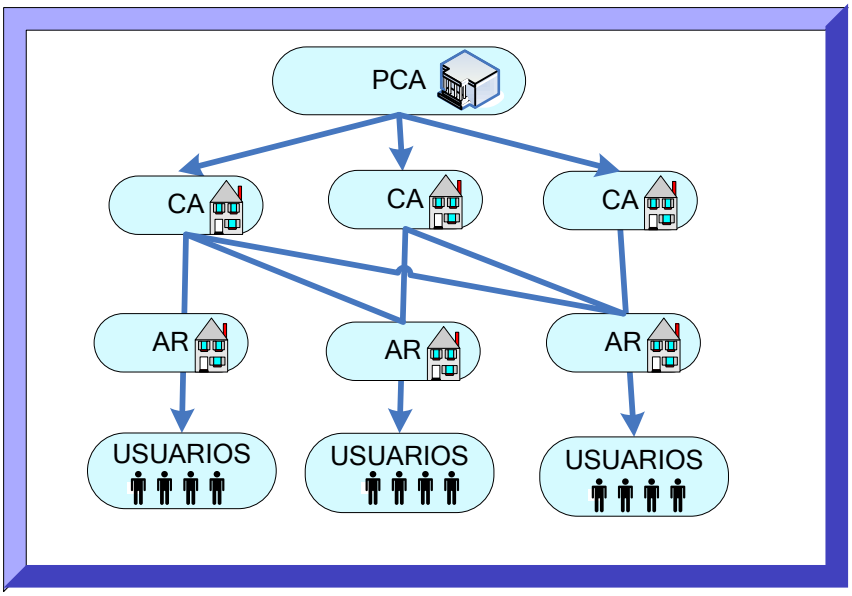


IMAGEN Nº29 Componentes de PKI

PCA

Es el nodo raíz, y es el nodo que define las políticas de certificación, para todo el modelo, sin embargo esto no significa que no existan sub-políticas

[13] Roberto Gonzáles Cruz Universidad UNACOMA

propias de una AC en particular. En este caso si existieran varias AC's, una podría tener alcance internacional y las demás nacionales, de las cuales podrían subdividirse por tipo de organización (ejemplo Universidad, sector público, sector privado, banca, y otros). A este nivel, solo existirá una sola política de certificación (la cual podría ser una simple o compuestas por varias sub-políticas, que estarán aplicados en un ámbito nacional), siguiendo con los lineamientos de sencillez y confiabilidad por parte del usuario.

Una política de seguridad establece y define la dirección de máximo nivel de una organización sobre seguridad de información, así como los procesos y principios para el uso de la criptografía. Por lo general, incluye declaraciones sobre cómo gestionará la empresa las claves y la información critica, y establecerá el nivel de control requerido para afrontar los niveles de riesgo.

CA - Autoridad Certificadora

Una ***CA*** es la base de confianza y uno de los pilares fundamentales de un PKI. Su función principal es el de garantizar los datos de cualquier certificado emitido por la PKI.

Una ***CA*** a su vez es avalada por otra ***CA*** que tiene reconocido prestigio y confianza internacionalmente. (Ej.Verisign, la cual se auto afirma su certificado).

Cada certificado emitido por una ***CA*** debe estar firmado por una ***CA*** de mayor grado en el esquema jerárquico de autoridades certificadoras,

formándose así una cadena de certificados, en los que unas ***CA*** se avalan a otras hasta llegar a la ***CA*** superior, que se avala a sí misma.

Esta jerarquía de firmas y la cadena con ella formada están contempladas en el estándar X.509 v3, que indica la forma correcta de realizar estas cadenas de certificaciones.

RA-Autoridades de Registro

Una **RA**, proporciona la interfaz entre el usuario y el CA, registra y autentifica la identidad de los usuarios finales o entidades.

Se debe recalcar que las RA's no realizan ninguna función de certificación., solo es el medio por el cual se puede entregar la solicitud de un certificado a la CA.

Las Autoridades de Registro estarán asociadas a las distintas CA's que definen la jerarquía de un árbol (PCA, CA's normales).

Las ***RA's*** pueden abrir varias oficinas regionales dispersas por todo el país, llegando hasta los usuarios en los sitios más remotos, mientras que la *CA* se limitaría así a certificar a todos los usuarios aceptados por las RA's dependientes de ella. Gracias a esta descentralización se agiliza el proceso de certificación y se aumenta la eficacia en la gestión de solicitudes.

Una PKI incluirá una o varias Autoridades de Registro para certificar la identidad de los usuarios; una o varias Autoridades de Certificación que emitan los certificados de clave pública; un repositorio de certificados, accesible vía Web u otro medio, donde se almacenen los certificados; las

listas de revocación de certificados (CRL), donde se listan los certificados suspendidos o revocados; y, por supuesto, los propios certificados.

USUARIOS

El ***usuario*** por su parte es el encargado de realizar las siguientes actividades:

- Solicitar el certificado
- Solicitar la revocación del certificado
- Solicitar la renovación del certificado….

Una vez que un ***usuario*** tiene un certificado digital este puede usarlo para poder navegar por la red con nombre y apellido en forma de bits, esto permite entrar al mundo del comercio electrónico. "El usuario dueño de un certificado digital tiene la potencialidad de poder autentificarse con cualquier otra entidad usuaria, también puede intercambiar información de forma confidencial y estar seguro de que esta es integra, así estar seguro que contactos vía el certificado digital no serán rechazados." [14]

2.15.3 Proceso de interacción entre la AC, AR Y Usuarios

- La generación del certificado se hace primero por una solicitud de un usuario, el usuario genera sus claves pública y privada y manda junto con los requerimientos de la solicitud su clave pública para que esta sea certificada por la AC

[14] Roberto Gonzáles Cruz PKI y Software Libre

- Una vez que la AR (es la AC regional) verifica la autenticidad del usuario, la AC vía la AR firma el certificado digital y es mandado al usuario
- El status del usuario puede estar en: activo, inactivo o revocado. Si es activo el usuario puede hacer uso del certificado digital durante todo su periodo válido
- Cuando termina el período de activación del certificado el usuario puede solicitar su renovación.

2.15.4 Funciones de un PKI

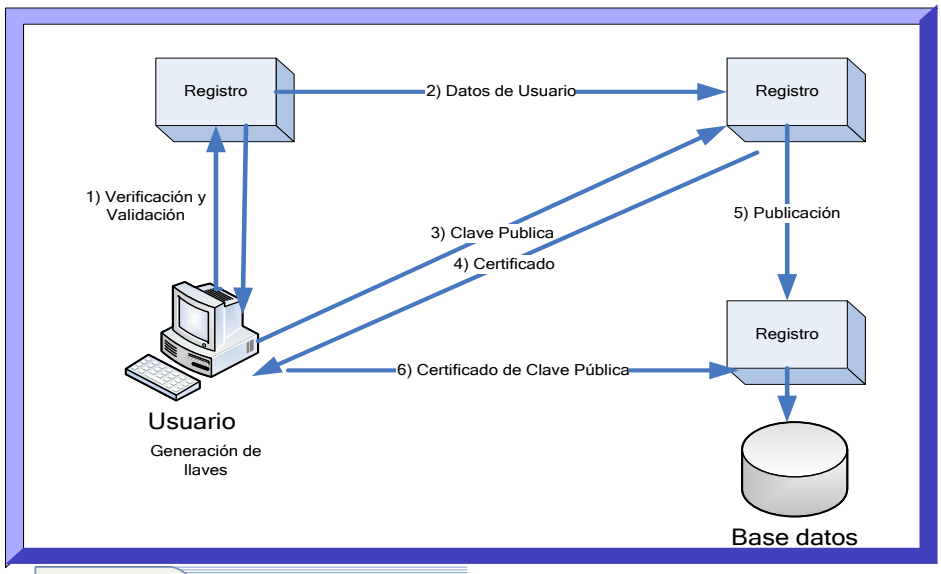


IMAGEN Nº30 Funciones de PKI (3)

- **Atención de solicitud de certificados**

  Las Autoridades de Registro verifican, registran y archivan los elementos característicos de cada usuario (fotografía, firma manuscrita, huellas dactilares, timbre de voz, fondo de ojo, fechas de nacimiento, etc.), para

la emisión de sus certificados de identidad, diferente será la confianza que éstos puedan ofrecer.

Una Autoridad de Registro puede requerir sólo el Carné de Identidad y comprobar que la fotografía y la apariencia del solicitante coinciden, en el caso de personas, en el caso de equipos electrónicos, servidores, computadores, podría ser además algunas características del equipo (ej. Nº de Serie).

- **Generación y registro de claves**

  Los usuarios sea cual sea siempre van ha poseer dos claves una pública y una privada, estas pueden ser generadas por el usuario, o también por medio de un algoritmo que permita la generación de claves o a través de un portal o pagina Web.

  Una vez, completado la solicitud y generadas las claves, la entidad final debe "registrar" su clave pública ante la Autoridad de Certificación a través de una Autoridad de Registro aceptada dentro del escenario. Para la inscripción sólo tiene que enviar su clave pública y, el documento digital de solicitud firmado con dicha clave, con respecto a la clave privada debe mantenerse bien asegurada.

- **Emisión de certificado**

  Satisfechas las condiciones marcadas por la Autoridad de Registro envía todos los documentos a la Autoridad de Certificación, la cual podrá generar el certificado correspondiente y devolver al solicitante un certificado digital que atestigua la validez de su clave pública para actuar dentro del sistema.

El certificado que se utiliza en el modelo, es el certificado X.509 en su versión 3. Esto es conveniente de utilizar por la definición de extensiones que tiene y poder incluir información relativa a la política de certificación, al uso del certificado y a la identificación del camino de certificación.

La Autoridad de Certificación debe tener en todo momento registrado cuales son los estados en los que se encuentran sus certificados (activo, suspendido, revocado y caducado). Antes de utilizar un certificado digital se verifica si no esta revocado en la "Listas de Certificados Revocados" o CRL's lugar donde se encuentran todos los certificados que se encuentran anulados.

- **Almacenamiento en la CA de llaves**

  Las claves privadas de la CA, éstas se generan y almacenan permanentemente en unidades hardware de alta seguridad (recomendable), sometidas a sofisticadas medidas de seguridad física y dentro de entornos a prueba de intrusión electrónica, que es lo recomendado y aconsejable. A dichas unidades se las denomina "Unidades de Firmado de Certificados", CSU. Estas unidades son, por su naturaleza, irrepetibles, y están diseñadas para que, ante la sospecha de cualquier intento de intromisión, las claves y demás informaciones relacionadas con ellas se destruyan antes de que puedan ser alcanzadas desde el exterior.

  Los administradores de la Autoridad de Certificación no tienen acceso a la clave privada, sino a un equipo hardware que firma los documentos que éstos le entreguen.

- **Servicios de directorio**

  Cada entidad puede almacenar sus certificados en su correspondiente directorio cuyo acceso es seguro. Si la entidad es una CA, además de sus certificados, en su directorio puede almacenar las CRLs asociadas. Cuando una entidad necesita obtener un certificado de otra entidad o una CRL, una vez identificado el nombre de la otra entidad, puede localizar la información buscada en la entrada del directorio de la otra entidad y la puede extraer, ya que estos atributos se configuran con permiso de lectura para todo el mundo

- **Políticas de certificación**

  Algunas Políticas de Seguridad Propias de cada CA son:

  - Procedimientos para el registro de usuarios. Se deben definir los mecanismos para la identificación y aceptación de usuarios finales.
  - Procedimientos para la gestión de claves. Se deben definir aspectos relacionados con la generación, distribución y validez de las claves. También se deben especificar los mecanismos de distribución permitidos, el tamaño de las claves y su período de validez.
  - Registro y auditoria. Se deben definir los mecanismos necesarios para registrar y auditar los eventos y la información que resulte necesaria para garantizar la protección de una CA y los usuarios que dependen de ella

- **Servicios de Certificación**

Uno de los mecanismos más utilizados en entornos de seguridad, y que más ligado se encuentra a los modelos de certificación basados en la utilización de claves asimétricas, es la firma digital. El proceso de verificación de una firma digital implica la utilización de la correspondiente clave pública que es validada por un certificado digital.

En general se puede decir, que cualquier proceso de verificación o validación de mecanismos de seguridad basados en técnicas criptográficas asimétricas, implica la validación del certificado de la correspondiente clave pública, proceso a que a su vez lleva implícita la validación de una cadena de certificados que garantice el establecimiento de la confianza entre dos entidades.

El proceso de validación o certificación se puede realizar de la siguiente manera

- Obtención del certificado a validar o certificar
- Determinación de la posibilidad de establecer la confianza entre las entidades implicadas.
- En caso de poder establecer la confianza, identificación de los certificados necesarios en el proceso.
- Obtención de los certificados identificados.

Como todos los usuarios operaran bajo la misma política siempre se puede establecer la confianza entre ellos. El nodo común en el árbol será

siempre la CA que los certifica a todos, y el certificado en el que finaliza el proceso de validaciones el certificado autofirmado por la propia CA.

- **Servicios de Revocación de Certificados**

  Los certificados que no han vencido su período de validez pueden ser revocados por la Autoridad que los emitió. La principal causa de la revocación es que se haya detectado un compromiso de la clave secreta asociada, aunque pueden existir otros motivos, como pueden ser el cese de la actividad para que el certificado haya sido emitido, que el propietario del certificado cambie de papel dentro del grupo o cambie de afiliación, o simplemente, que la CA emisora decida revocarlo. En cualquier caso la decisión de revocar un certificado debe ser tomada por la CA emisora, pero se permite a cada usuario que pueda solicitar la revocación de su propio certificado. En el caso de que la solicitud de revocación de un certificado provenga de una entidad que no es la propietaria, es responsabilidad de la CA comprobar los motivos por los que se solicita la revocación.

  Al igual que la renovación de un certificado de una CA implica la revocación de todos certificados que dependen del mismo, la revocación del certificado de una CA produce el mismo efecto, con la diferencia de que si el certificado revocado no es sustituido por uno nuevo.

- **Escenarios de Aplicación**

  Los escenarios de aplicación del modelo puede ser varias: (Comunicaciones entre servidores, Correo electrónico, Intercambio Electrónico de Datos, Redes Privadas Virtuales (VPN)).

CAPITULO 3: ANÁLISIS DE LA SITUACIÓN ACTUAL Y RECOPILACIÓN DE REQUERIMIENTOS

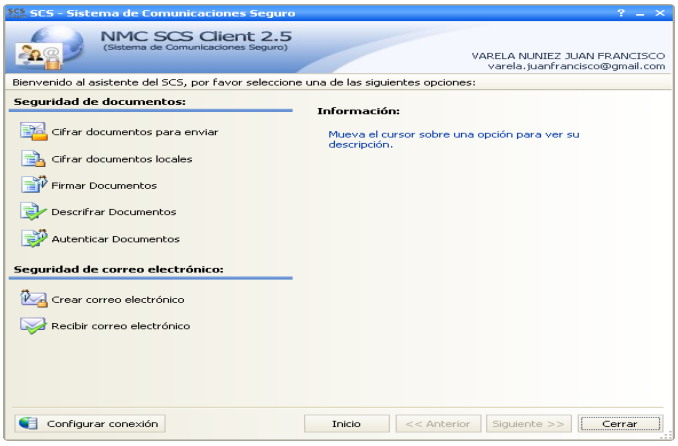
3.1. ANÁLISIS DE LA SITUACIÓN ACTUAL

Con respecto a la seguridad el año anterior (2006) las Fuerzas Armadas del Ecuador, realizó la adquisición e implementación de un software llamado NMC SCS Client 2.5 (Sistema de Comunicaciones Seguras), al momento este software proporciona licencia para 500 usuarios con un costo de alrededor de los 2000 dólares americanos anuales, siendo esto un gran obstáculo ya que la cantidad de usuarios que necesitarían utilizar este software es de 25000, por ende el costo aumentaría considerablemente.

Para la administración de este software se tiene un servidor el cuál se encarga de la inscripción de usuarios con una clave privada que solo el usuario conoce y posee.

El sistema NMC SCS Client 2.5 proporciona:

- Seguridad de documentos
- Seguridad de Correo Electrónico



Características del Servidor:

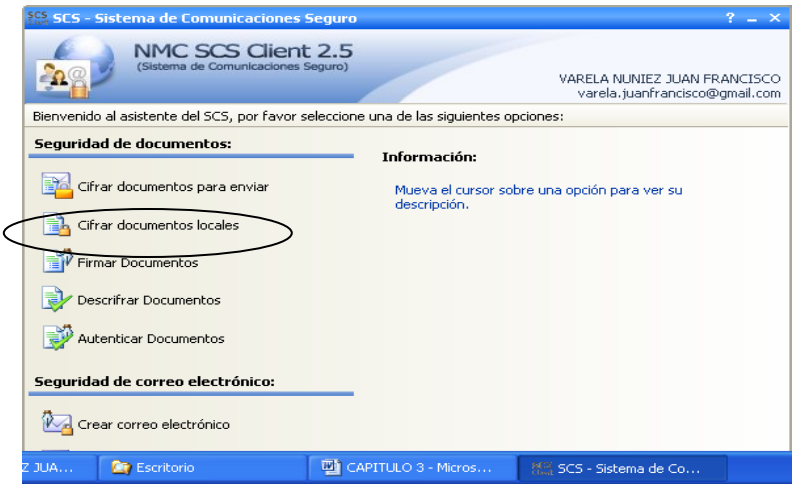
- Procesador: 3.6 GHZ
- Sistema operativo: Windows 2000 Server
- Capacidad en RAM de: 1 GB
- 3 discos duros de : 15 GB c/u

3.2. FUNCIONAMIENTO DEL SCS:

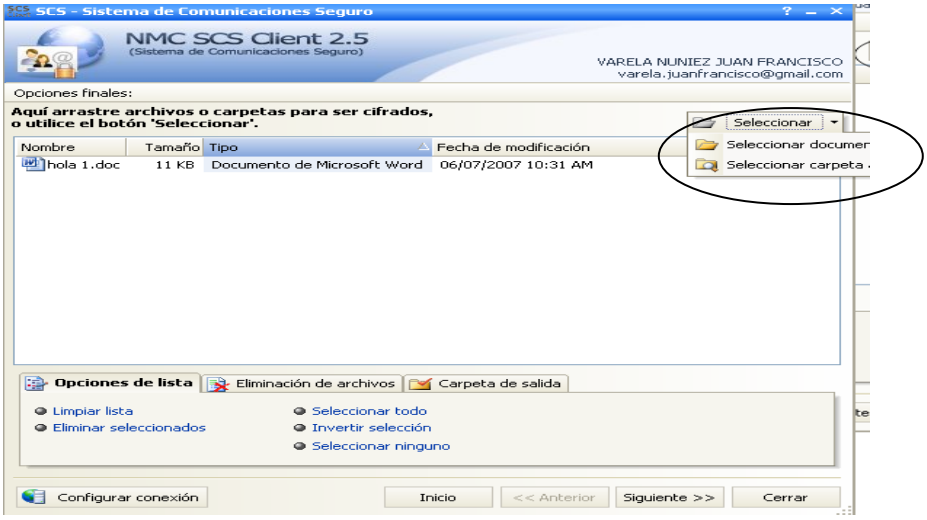
El sistema en si permite cifrar cualquier documento para protegerlo de amenazas de terceras personas.

1. Si el emisor quiere mantener en secreto la información que posee, entonces realiza los siguientes pasos :
   - El emisor ingresa al sistema.

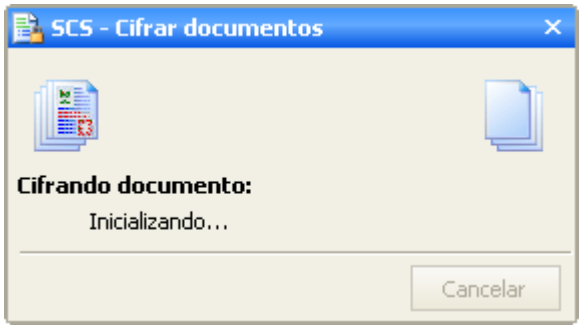
   - Escoge la opción cifrar documentos locales



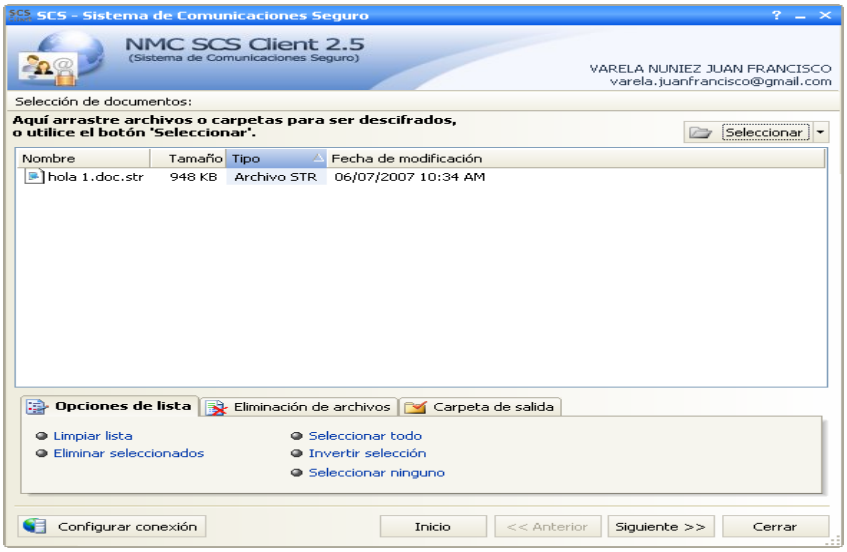
- El emisor elige la información que va ha cifrar, dando clic en seleccionar

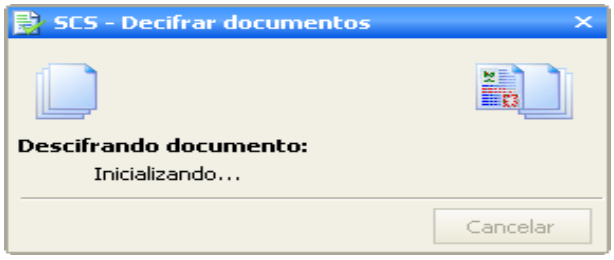


- El emisor cifra la información dando clic en siguiente, y lo guarda en un lugar seguro (flash, disco duro, CD)



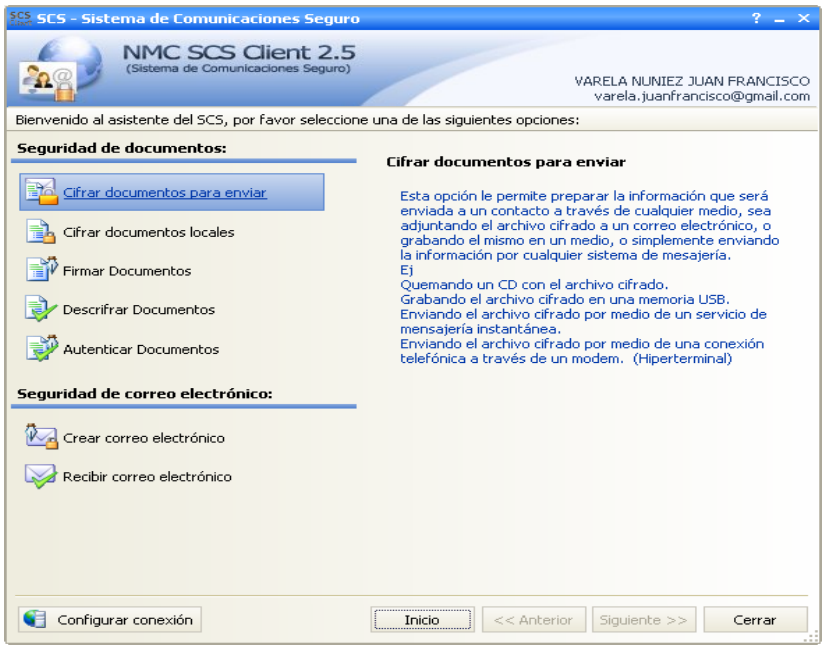
- Cuando el usuario necesite utilizar dicha información, la descifra, utilizando el software. Elige el documento que va ha descifrar y da clic en siguiente.



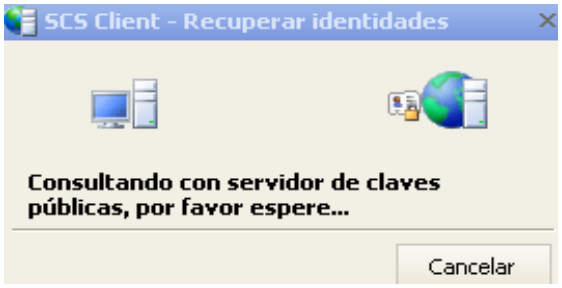


2. Si el emisor desea enviar información a través de un correo al receptor, o simplemente quiere enviar información por algún medio como por ejemplo flash, CD, etc., realiza los siguientes pasos:

- El emisor ingresa al sistema
- Elige la siguiente opción



- El emisor elige al receptor que va ha enviar la información, y el servidor lo busca.



- Cifra el mensaje
- Si es por medio de correo copia el mensaje cifrado y lo envía por cualquier correo electrónico por Ej. gmail, hotmail, yahoo etc.
- El receptor recibe el mensaje y copia este texto cifrado
- El receptor ingresa al sistema con su password
- El receptor pega el texto copiado para descifrar y listo.

3.2.1. Desventajas de SCS:

- Número de usuarios limite 500 usuarios, siendo un requerimiento de 25000 usuarios.
- Costo elevado del software
- Este software se autentica a si mismo no utiliza una autoridad certificadora de reconocimiento mundial que permita garantizar la veracidad del servidor y de su aplicación.
- El proceso de cifrado y descifrado de información en el envío y recepción de correo electrónico es muy largo, debido a que la información a enviar se tiene que copiar, pegar en el software SCS, cifrar, copiar, y por ultimo pegar en el correo que se va ha utilizar. Este mismo procedimiento tiene que realizar el receptor.

3.3. CONCLUSIONES DE LA SITUACIÓN ACTUAL

- SCS no posee ninguna autoridad certificadora de reconocimiento, razón por lo cual no se lo puede utilizar en una red externa e insegura como es el Internet.
- Cabe recalcar que en el campo informático existen varios software que cumplen las mismas y mejores características que este software, entre ellos tenemos el PGP que es software libre y se lo puede obtener fácilmente a través del Internet. Posteriormente se realizará un estudio de PGP.

- Aparte del software SCS, el correo electrónico de las Fuerzas Armadas no cuenta con ningún otro tipo de seguridad para el envío y recepción de mensajes.

3.4. IDENTIFICACIÓN DE REQUISITOS

- La Fuerza terrestre necesita garantizar la confidencialidad, integridad, autenticidad y no repudio de la información enviada a través del correo electrónico.
- El correo electrónico se utiliza dentro de la red local y externa.
- La Fuerza Terrestre necesita, tener la seguridad de que el usuario envía información a través de la red, con su firma digital, este no podrá negar por ninguna razón su autoría, y de igual forma si lo ha recibido no puede negar que lo ha recibido apoyado en la Ley de Comercio Electrónico (ver anexo).
- El número de usuarios aproximado es de 25000 usuarios entre, oficiales, voluntarios y empleados civiles.
- Cada usuario debe poseer su firma digital para el envío de correo electrónico a través de la red.

3.5. ANÁLISIS DE REQUISITOS

De acuerdo a la identificación de los requisitos señalados en el inciso anterior vemos que es necesario la implementación de certificados digitales y por ende firmas digitales, para cada uno de los miembros de la Fuerza Terrestre, con el fin

de garantizar la confidencialidad, autenticidad, integridad y no repudio de la información enviada a través del correo electrónico.

3.6. MODELADO (PROTOTIPO)

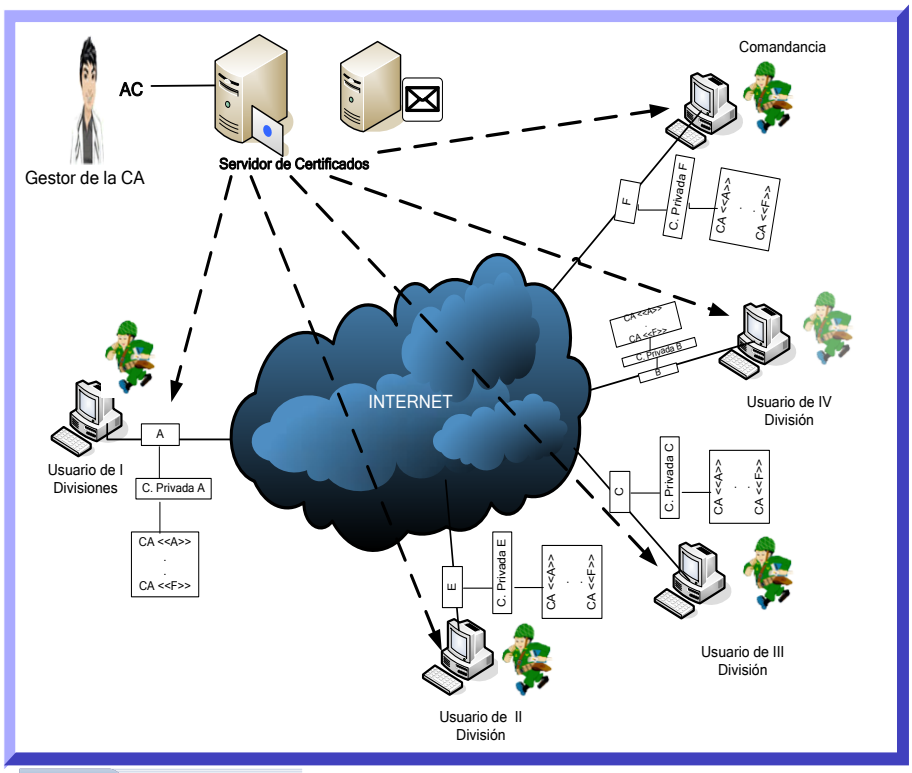


IMAGEN Nº31 Modelado de Requisitos

3.6.1. Especificación de requisitos

- Certificados digitales
- Firmas digitales

3.7. DISEÑO DEL PROYECTO

3.7.1. Diseño arquitectónico

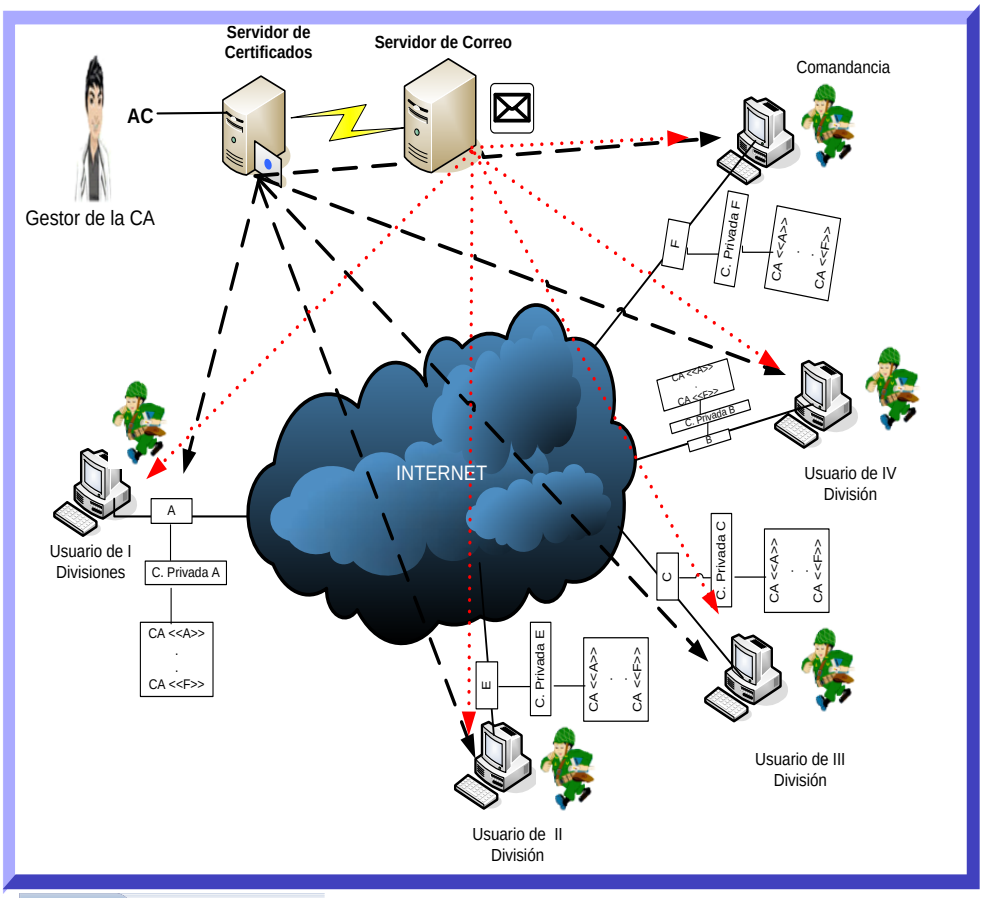


IMAGEN Nº 32 Diseño Arquitectónico

3.7.2. Análisis y modelado de tareas

Autoridad Certificadora

- Emitir, revocar, renovar y eliminar un certificado para el servidor de certificados.
- Garantizar la autenticidad del servidor de certificados y de los usuarios que administran este servidor.

Servidor de Certificados

- Registrar a los usuarios.

- Emitir, revocar, renovar, eliminar certificados a los usuarios
- Distribuir certificados a los usuarios.
- Generar claves públicas y privadas.

Usuarios

- Solicitar un certificado al servidor
- Realizar aplicaciones de correo electrónico, aplicando cifrado y firma digital.
- Custodiar su clave secreta.

3.7.3. Requerimientos técnicos

Servidor:

- Procesador: 3.6 GHZ
- Sistema operativo: Centos 1.4
- Capacidad en RAM de: 1 GB
- Capacidad de Disco duro : 120 G

Usuarios:

- Procesador: Pentium IV
- Sistema operativo: Windows XP, Linux
- Capacidad en RAM de: 256 MB
- Capacidad de Disco duro : 40 GB

CAPITULO 4: IMPLEMENTACIÓN

4.1 INSTALACION DE CENTOS

En la instalación se escogerá los paquetes que serán utilizados:

- Sendmail
- Apache
- DNS (bind)
- SSL openssl
- Dovecot

4.2 CONFIGURACION DE RED

4.2.1 Servidor

Hostname: servidor

Dirección IP servidor: 192.168.1.1

Mascara: 255.255.255.0

Gateway: 192.168.1.254

Servidor DNS preferido: 192.168.1.1

a) Ingresar al fichero /etc/hosts

Digitar la dirección de nuestro servidor y del dominio

192.168.1.1 servidor.dicomsi.com servidor

Donde:

- 192.168.1.1 = dirección IP del servidor
- servidor = nombre del host
- dicomsi.com = dominio

b) Ingresar al fichero /etc/sysconfig/network:

Digitar el nombre del host y del dominio

NETWORKING=yes
HOSTNAME=servidor.dicomsi.com

Donde:

- servidor = nombre del host
- dicomsi.com = dominio

c) Ingresar al fichero /etc/sysconfig/network-scripts/ifcfg-eth0

Digitar los parámetros de red:

DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.1
NETMASK=255.255.255.0
GATEWAY=192.168.1.254

d) Reiniciar el servicio y depurar la configuración

Digitar el siguiente comando: service network restart

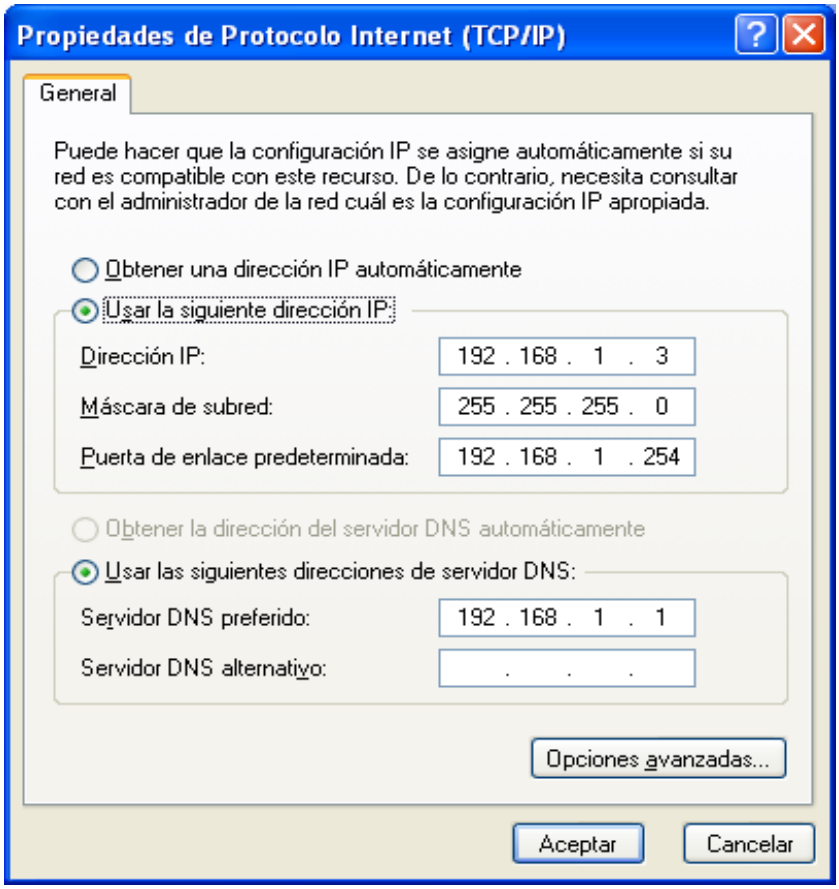
e) Incorporar el servicio de red al inicio del arranque del sistema

Digitar el comando: chkconfig network on

4.2.2 Clientes

Dirección IP servidor: 192.168.1.2
Mascara: 255.255.255.0
Gateway: 192.168.1.254
Servidor DNS preferido: 192.168.1.1

Dirección IP servidor: 192.168.1.3
Mascara: 255.255.255.0
Gateway: 192.168.1.254
Servidor DNS preferido: 192.168.1.1



4.3 CONFIGURAR DNS

a) Editar el fichero /etc/resolv.conf

NOTA.- digitar la IP del servidor del servidor DNS (resolución de nombres de dominio).

```
nameserver 192.168.1.1
```

Donde:

- 192.168.1.1: dirección IP del servidor

b) Editar el fichero /var/named/chroot/etc/named.conf

Digitar las zonas de resolución (directa e inversa), el nombre del dominio y las direcciones IP.

NOTA: Digitar al final del documento

```
include "/etc/rndc.key";
# CONFIGURACION PARA MI DOMINIO
zone "dicomsi.com." IN {
        type master;
        file "dicomsi.com.zone";
        allow-update { none; };
};
zone "1.168.192.in-addr.arpa" IN {
        type master;
        file "1.168.192.in-addr.arpa.zone";
        allow-update { none; };
};
```

c) Editar y crear el fichero

etc/named/chroot/var/named/dicomsi.com.zone

NOTA: crear el archivo dicomsi.com.zone y editar. Zona de reenvío del dominio.

```
$TTL    86400
@               IN    SOA  dns.dicomsi.com.  administrador.dicomsi.com. (
```

```
                        200707137      ; serial formato: yyyymmddn
                        28800          ; refresh
                        7200           ; retry
                        604800         ; expiry
                        86400          ; minimum
                        )
@                       IN      NS      dns
@                       IN      MX      10    mail
@                       IN      A       192.168.1.1
dicomsi.com.            IN      A       192.168.1.1
dns                     IN      CNAME   dicomsi.com.
www                     IN      CNAME   dicomsi.com.
mail                    IN      A       192.168.1.1
```

d) Editar y crear el fichero /var/named/chroot/var/named/1.162.198.in-addr.arpa.zone

Digitar la Zona de resolución inversa del dominio

```
$TTL    86400
@               IN      SOA   dns.dicomsi.com.
administrador.dicomsi.com.(
                        200707136      ; serial formato: yyyymmddn
                        28800          ; refresh
                        7200           ; retry
                        604800         ; expiry
                        86400          ; minimum
                        )
@               IN      NS      dns.dicomsi.com.
1    IN             PTR    dicomsi.com.
3    IN             PTR    www.dicomsi.com.
```

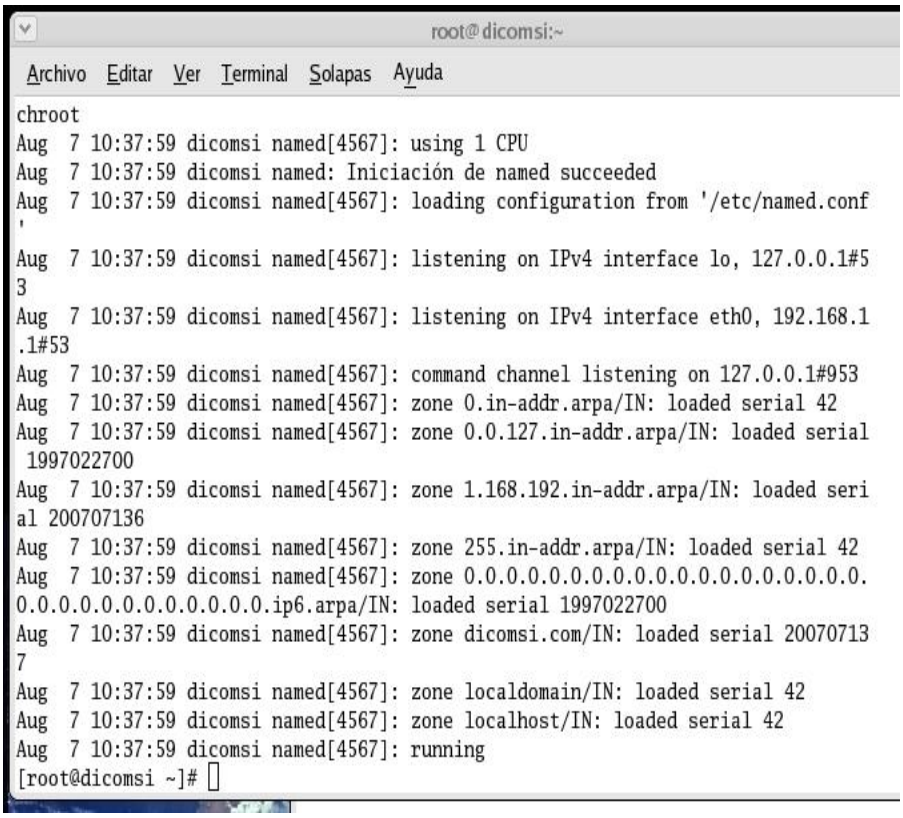
e) Reiniciar el servicio y depurar la configuración.

Digitar el siguiente comando: service named restart

f) Comprobar el funcionamiento del dominio.

Digitar el siguiente comando:

tail -80 /var/log/messages |grep named



g) Incorporar el servicio de nombres de dominio al inicio del arranque del sistema

Digitar el comando: chkconfig named on

4.4 CONFIGURAR SERVIDOR SENDMAIL

a) Crear cuentas de usuario

Digitar los siguientes comandos

useradd -s /sbin/nologin sinthia
passwd sinely

useradd -s /sbin/nologin varela
passwd amvl00
Donde:

- Sinthia = nombre de usuario

- Sinely = contraseña de usuario Sinthia
- Juan = nombre de usuario
- amvl00 = contraseña de usuario Juan

b) Editar el fichero vi /etc/mail/local-host-names

Digitar los dominios a administrar:

```
dicomsi.com
mail.dicomsi.com
```

c) Editar el fichero vi /etc/mail/relay-domains

Digitar los dominios permitidos para poder enviar correo

```
dicomsi.com
mail.dicomsi.com
```

d) Editar el fichero vi /etc/mail/access

Digitar la lista de control de acceso, permiten incluir solo las IPs locales del servidor, dominios.

```
localhost.localdomain    RELAY
localhost                RELAY
dicomsi.com              RELAY
```

e) Editar el fichero /etc/dovecot.conf

Establecer los protocolos para acceder hacia el correo y habilitar los servicios de imap y/o pop3

```
# imap imaps pop3 pop3s
protocols = imap pop3
```

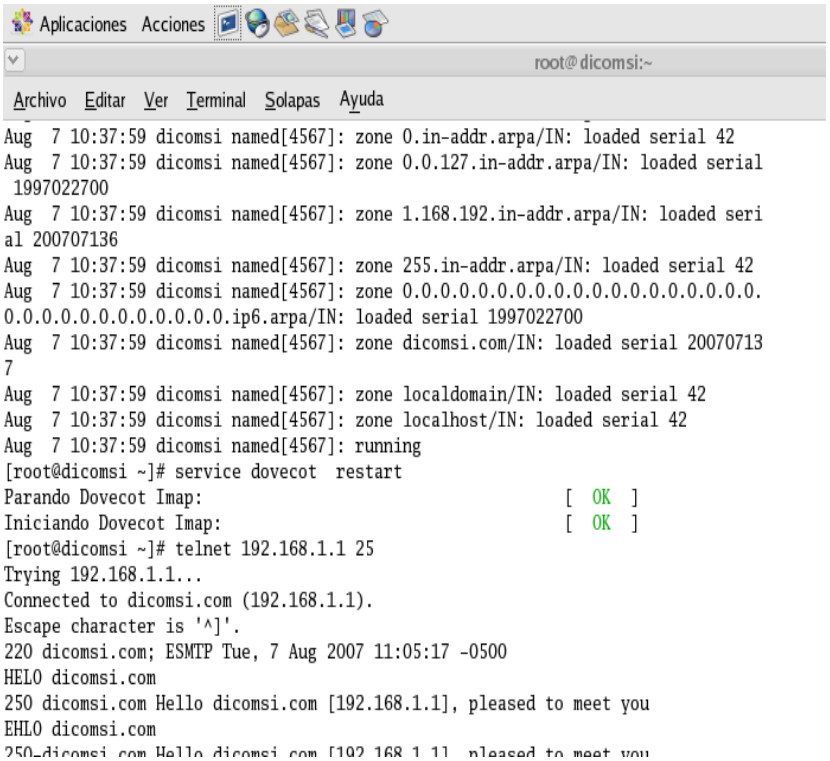
f) Reiniciamos el servicio de Sendmail

Digitar el siguiente comando: service sendmail restart

g) Verificar el servicio sendmail

Digitar los siguientes comandos:

$ telnet 192.168.1.1 25
HELO dicomsi.com
EHLO dicomsi.com



h) Incorporar el servicio de sendmail al inicio del arranque del sistema

Digitar el comando: chkconfig sendmail on

4.5 SENDMAIL CON SSL

NOTA: Se debe crear primero la Autoridad Certificadora descrito en el literal **7).**

a) Ingresar al directorio /ssl

Digitar el siguiente comando: cd /ssl

b) Crear fichero de parámetro DSA.

NOTA: Sendmail requiere una llave creada con algoritmo DSA de 1024 octetos. Para tal fin, se crea primero un fichero de parámetros DSA.

Digitar el siguiente comando:

openssl dsaparam 1024 -out dsa1024.pem

DONDE

- dsaparam 1024 = especifica algoritmo de cifrado dsa de 1024 bits
- -out dsa1024.pem = archivo de salida con extensión .pem

c) Crear la llave privada utilizando el archivo .pem. Generar en el mismo paso el requerimiento de certificado.

Digitar el siguiente comando:

openssl req –new –newkey dsa:dsa1024.pem -keyout sendmail.key.pem -out sendmail.csr .pem -days 360 –nodes

d) Llenar los datos que solicitan que ingrese.

NOTA: El nombre del país solo se digita dos letras

Código de dos letras para el país: **Ec**
Estado o provincial: **Pichincha**
Ciudad: **Quito**
Nombre de la empresa o razón social**: Fuerza Terrestre**
Unidad o sección: **Dicomsi**
Nombre del anfitrión.: **dicomsi.com**
Dirección de correo: **administrador@dicomsi.com**

e) Crear el certificado, firmado por nuestra autoridad certificadora.

Digitar el siguiente comando:

openssl ca -policy policy_anything -out sendmail.cert.pem - infiles sendmail.csr.pem

DONDE:

- ca = indica que se firmará con la CA
- -policy policy_anything = verifica si los datos dados en el archivo sendmail.csr.pem, están completos.

Digitar la contraseña de la CA y se crea el certificado firmado por la CA.

f) Dar permiso de lectura solo al usuario root para los ficheros de claves y certificados.

Digitar el siguiente comando:

chmod 400 /ssl/sendmail.*

g) Verificar el contenido del certificado.

Digitar el siguiente comando:

openssl x509 -noout -text -in /ssl/sendmail.cert.pem

h) Editar el fichero /etc/mail/sendmail.mc.

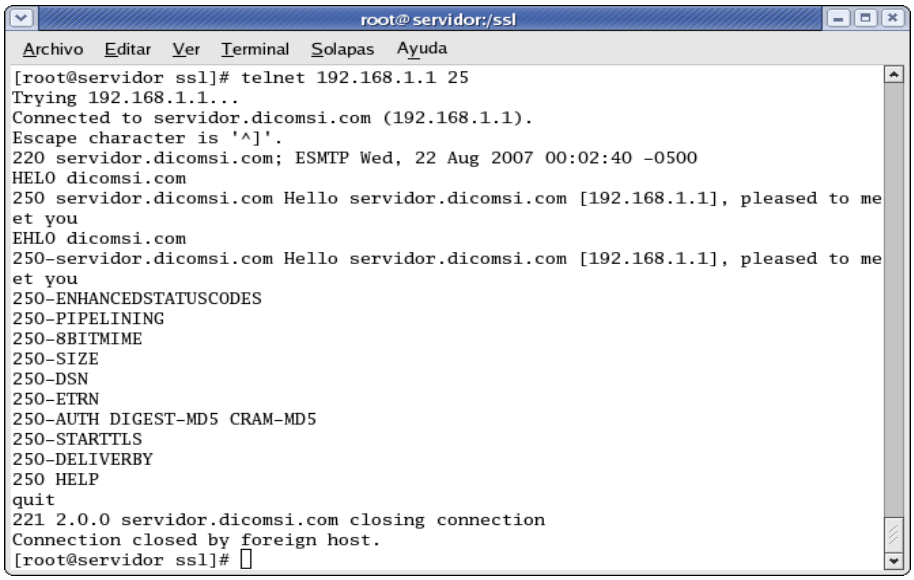
NOTA: Se configura la ubicación del directorio donde se encuentra el certificado y su clave privada, para que sendmail pueda encontrarlos.

```
define(`confCACERT_PATH',`/ssl')
define(`confCACERT',`/ssl/cacert.pem')
define(`confSERVER_CERT',`/ssl/sendmail.cert.pem')
define(`confSERVER_KEY',`/ssl/sendmail.key.pem')
DAEMON_OPTIONS(`Port=smtps, Name=TLSMTA, M=s')dnl
```

i) Reiniciar y depurar Sendmail.

Digitar el siguiente comando: service sendmail restart

j) Verificar el funcionamiento realizando telnet mediante el puerto 25.Digitar el siguiente comando: telnet 192.168.1.1 25



4.6 CONFIGURAR DOVECOT CON SSL

NOTA: Se debe crear primero la Autoridad Certificadora descrito en el literal **7).**

a) Ingresar al directorio /ssl

Digitar el siguiente comando: cd /ssl

b) Crear la llave privada y generar en el mismo paso el requerimiento para el certificado.

NOTA: Dovecot es más simple, pero requiere utilizar una clave con algoritmo RSA de 1024 octetos, con estructura X.509.

Digitar el siguiente comando:

```
openssl req -new -newkey rsa:1024 -nodes \
-keyout dovecot.key.pem -out dovecot.csr.pem
```

DONDE:

- rsa:1024= indica el algoritmo de cifrado de la clave (rsa)

- –nodes = indica “no” pedir una clave simétrica al generar la llave privada.

c) Llenar los datos que solicitan que ingrese.

NOTA: El nombre del país solo se digita dos letras.

Código de dos letras para el país : **Ec**
Estado o provincial: **Pichincha**
Ciudad: **Quito**
Nombre de la empresa o razón social**: Fuerza Terrestre**
Unidad o sección: **Dicomsi**
Nombre del anfitrión.: **dicomsi.com**
Dirección de correo. **administrador@dicomsi.com**

d) Crear el certificado, firmado por nuestra autoridad certificadora.

Digitar el siguiente comando:

openssl ca -policy policy_anything -out dovecot.cert.pem - infiles dovecot.csr.pem

DONDE:

- ca = indica que se firmará con la autoridad certificadora.
- -policy policy_anything = verifica si los datos dados en el archivo dovecot.csr.pem, están completos.

Digitar la contraseña de la CA y se genera el certificado firmado por la CA.

e) Dar permiso de lectura solo al usuario root para los ficheros de claves y certificados.

Digitar el siguiente comando: chmod 400 /ssl/ dovecot..*

f) Editar el fichero /etc/dovecot.conf.

NOTA: En este fichero se activan todos los servicios (imap, imaps, pop3 y pop3s), y se indican la clave y certificado recién creados.

```
protocols = imap imaps pop3 pop3s
#ssl_disable = no
ssl_cert_file = /ssl/dovecot1.cert.pem
ssl_key_file = /ssl/dovecot.key.pem
```

g) Reiniciar y depurar dovecot

Digitar el siguiente comando: service dovecot restart

4.7 AUTORIDAD CERTIFICADORA (CA)

a) Crear las carpetas ssl y dicomsiCA.

Digitar los siguientes comandos:

```
# mkdir –p /ssl
# mkdir –p /ssl/dicomsiCA
```

b) Editar el fichero vi /usr/share/ssl/openssl.cnf

Para indicar la ubicación de la CA, digitar lo siguiente:

```
[ CA_default ]
dir= /ssl/dicomsiCA
```

c) Editar el fichero vi /usr/share/ssl/openssl.cnf

Nota: para indicar que la AC va ha ser utilizada para manejo de correo seguro

Digitar las siguientes líneas en la parte inferior de `[CA_default ]`

```
Basic constraints (critica) CA=FALSE
Extended key usage:  emailProtection.
```

DONDE:

- extendedKeyUsage= emailProtection: indica el manejo de correo seguro.

d) Ingresar al directorio /ssl

Digitar el siguiente comando: `cd /ssl`

e) Generar las llaves privada y el certificado de la Entidad Certificadora (CA).

NOTA: El certificado es autofirmado por la misma CA. Esta es una forma abreviada de crear una clave privada y generar al mismo tiempo el certificado.

Digitar el siguiente comando:

```
# openssl req –new –x509 –keyout cakey.pem –out
cacert.pem –days 360 –sha1
```

DONDE:

- cakey.pem = llave privada
- cacert.pem = certificado de la CA
- days 360 = tiene validez de un año (el tiempo puede variar).
- sha1 = algoritmo hash
- –keyout cakey.pem = genera la llave privada.

NOTA: Se debe observar que las extensiones de los archivos deben ser **.pem**.

f) Digitar el passphrase (contraseña) que protege la clave privada de la CA. La idea es que nadie más pueda abrir la llave privada.

g) Llenar los datos que solicitan que ingrese.

NOTA: El nombre del país solo se digita dos letras

Código de dos letras para el país : **Ec**
Estado o provincial: **Pichincha**
Ciudad: **Quito**
Nombre de la empresa o razón social**: Fuerza Terrestre**
Unidad o sección: **Dicomsi**
Nombre del anfitrión.: **dicomsi.com**

Dirección de correo. **administrador@dicomsi.com**

h) Generar un directorio para firmar requerimientos de llaves públicas, ya que el servidor dicomsi.com es una entidad Certificadora o CA.

Digitar los siguientes comandos

```
# mkdir –p /ssl/dicomsiCA/private
# mkdir –p /ssl/dicomsiCA/newcerts
```

DONDE:

- Carpeta private = directorio de llaves privadas
- Carpeta newcerts = directorio de llaves públicas

i) Copiar la llave privada cakey.pem al directorio de llaves privadas.

Digitar el siguiente comando:

```
# cp cakey.pem /ssl/dicomsiCA/private
```

j) Copiar la llave pública cacert.pem al directorio de llaves públicas.

Digitar el siguiente comando: # cp cacert.pem /ssl/dicomsiCA

k) Generar el archivo index.txt que contendrá una lista de los certificados públicos generados

NOTA: este archivo es la base datos de los certificados existentes.

Digitar el siguiente comando: # touch /ssl/dicomsiCA/index.txt

l) Generar el archivo de nombre “serial”

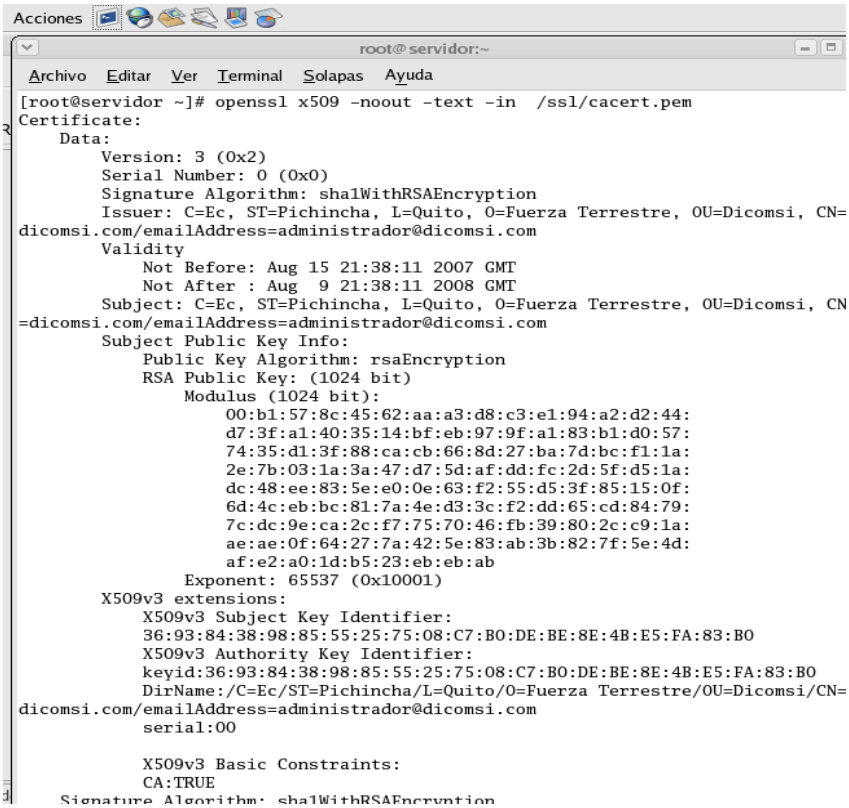
NOTA: este archivo contendrá el consecutivo de certificados públicos generados, este debe iniciar en uno:

```
# echo 01 > /ssl/dicomsiCA/serial
```

NOTA: Listo ya se ha completado las operaciones para que dicomsiCA sea una autoridad certificadora.

m) Verificar el certificado creado.

Digitar el siguiente comando: openssl x509 –noout –text –in /ssl/cacert.pem



4.8 GENERAR CERTIFICADOS PARA LOS CLIENTES

a) Generar la clave privada del cliente:

Digite el siguiente comando:

openssl genrsa -out sinthia-key.pem -des3 1024

DONDE:

- genrsa = genera la clave privada.
- -des3 1024 = algoritmo de cifrado triple des (-des3) de 1024 y se almacena en el fichero (-out) sinthia-key.pem.

b) Digitar la contraseña que protege a la clave privada.

NOTA: la contraseña de sinthia-key.pem será sinthia

c) Generar un requerimiento de clave publica.

Digitar el siguiente comando:

openssl req -new -key sinthia-key.pem -out sinthia-csr.pem -config /usr/share/ssl/openssl.cnf -sha1 -outform PEM

DONDE:

- -key sinthia-key.pem = llave privada del cliente
- -out sinthia-csr.pem = requerimiento de clave publica, archivo de salida.
- outform PEM = extensión de los archivos de salida
- sha1 = algoritmo hash
- -config /usr/share/ssl/openssl.cnf = ubicación del archivo de configuración de openssl.

d) Llenar los datos que solicitan que ingrese.

NOTA: El nombre del país solo se digita dos letras

Código de dos letras para el país : **Ec**
Estado o provincial: **Pichincha**
Ciudad: **Quito**
Nombre de la empresa o razón social**: Fuerza Terrestre**
Unidad o sección: **Dicomsi**
Nombre del anfitrión.: **sinthia**
Dirección de correo. **sinthia@dicomsi.com**

e) Verificar el requerimiento se digita:

#openssl req -in sinthia-csr.pem -verify -text -noout

```
[root@servidor ssl]# opensssl req -in sinthia-csr.pem -verify -text -noout
bash: opensssl: command not found
[root@servidor ssl]# openssl req -in sinthia-csr.pem -verify -text -noout
verify OK
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=Ec, ST=Pichincha, L=Quito, O=Fuerza Terrestre, OU=Dicomsi, CN=sinthia/emailAddress=sinthia@dicomsi.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:bf:5f:7c:87:42:90:61:b8:35:8f:f2:52:0b:e3:
                    28:86:ad:5c:9c:09:50:da:96:64:ac:d7:b0:6e:38:
                    f0:12:10:93:e1:e6:c0:f4:92:60:7a:ac:48:25:47:
                    88:9a:9c:b2:ef:35:14:75:a7:0d:8e:aa:59:03:d2:
                    06:10:0d:d7:ef:7d:41:0e:32:c0:b2:c3:cd:41:07:
                    b6:60:54:65:68:8f:86:0c:c1:cb:75:15:06:c1:02:
                    c3:a2:1b:a9:d3:16:7d:10:94:d2:fa:22:d9:4b:eb:
                    5c:a4:38:1c:be:7e:f3:b2:d4:89:fa:af:71:3c:3c:
                    43:7b:ee:71:4a:39:d5:d4:21
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha1WithRSAEncryption
        a2:40:be:cc:6b:e7:87:f5:fa:9c:57:4a:a4:35:68:84:e4:19:
        21:bb:aa:7a:09:6d:d0:92:46:f6:a9:67:7f:f3:0d:81:da:8d:
        91:81:be:6d:7e:a8:a1:ff:7b:e0:4a:08:86:39:0d:c2:7f:3b:
        05:aa:56:1b:64:cd:4f:38:31:96:cf:9c:eb:8c:e5:02:0f:6d:
        1a:2a:17:61:9c:34:e8:8c:7b:23:32:1a:d9:26:0d:88:10:b8:
        fe:db:f8:37:28:eb:a3:64:33:c7:93:59:5e:55:8b:65:5f:8d:
        e8:30:a2:5c:e4:82:f1:7f:b1:63:68:98:a0:4f:15:f8:79:32:
        d0:4e
```

f) Editar el archivo openssl.cnf

Digitar lo siguiente al final del fichero.

[proteccion_de_correo]
basicConstraints =critical,CA:FALSE
nsCertType = client, email
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage=emailProtection

DONDE:

- nsCertType=client, email : indica que el certificado será usado por un cliente de correo y no por un servidor web
- keyUsage =nonRepudiation,digitalSignature,keyEncipherment indica que el certificado será utilizado para firmar y cifrar documentos.
- extendedKeyUsage= emailProtection: nos indica el manejo de correo seguro

g) Generar el certificado de clave publica del cliente.

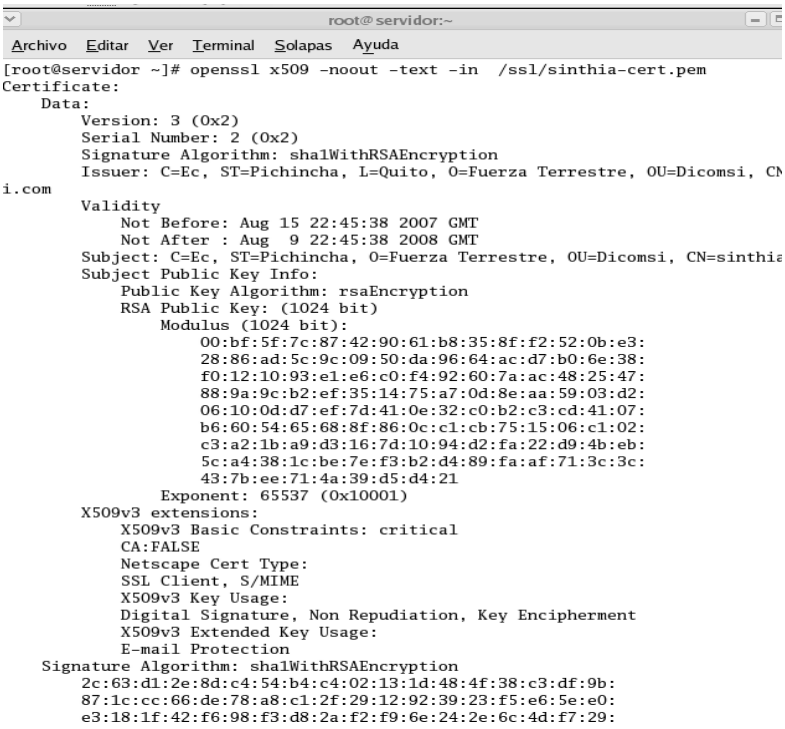
openssl ca -verbose -policy policy_match -out sinthia-cert.pem -days 60 -config /usr/share/ssl/openssl.cnf -in sinthia-csr.pem -extensions proteccion_de_correo -passin pass:amvl00

DONDE:

- extensions proteccion_de_correo = manda ha llamar al código que digitamos en el fichero openssl.cnf
- -passin pass:amvl00 = es obligatorio cuando el tamaño de la clave es muy pequeño y amvl00 es la clave de la CA.
- - config /usr/share/ssl/openssl.cnf = ubicación del archivo de configuración de openssl.

h) Verificar el contenido del certificado:

openssl x509 –noout –text –in /ssl/sinthia-cert.pem



i) Verificar el certificado cliente con el certificado de la CA.

Digitar el siguiente comando:

openssl verify -verbose -CAfile cacert.pem sinthia-cert.pem

Y openssl responde: verify OK

```
[root@servidor ssl]# openssl verify -verbose -CAf
ile cacert.pem sinthia-cert.pem
sinthia-cert.pem: OK
[root@servidor ssl]#
```

j) Exportar la clave con el formato PKCS#12

NOTA: Los ficheros PKCS#12 se pueden exportar desde diversas aplicaciones, como por ejemplo Microsoft IIS. Con frecuencia están asociados a la extensión .pfx.

Digitamos el siguiente comando:

openssl pkcs12 -export -out sinthia-cert.pfx -in sinthia-cert.pem

-name "Sinthia Certificado" -inkey /ssl/sinthia.key.pem

DONDE:

- -in sinthia-cert.pem = certificado en formato .pem
- -name "Sinthia Certificado" = nombre como se mostrará el certificado.
- -inkey /ssl/sinthia.key.pem = ubicación de la clave secreta del certificado.
- -out sinthia-cert.pfx = nombre del fichero en formato .pfx (pkcs12).

k) Digitar la contraseña que protege a la clave privada

4.9 REVOCAR CERTIFICADOS

Lo primero que debemos hacer es crear una lista de revocación, en la cual se reflejaran todos aquellos certificados que han sido revocados y por lo tanto son inválidos y no utilizables por los clientes.

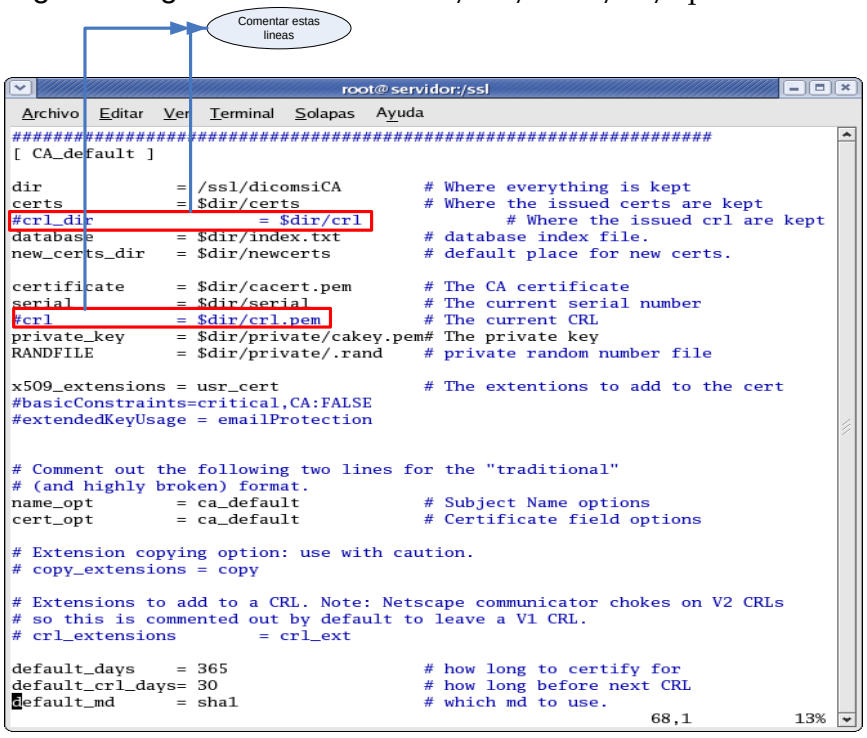
El fichero ubicado en el directorio /ssl/dicomsiCA/index.txt tiene todas las entradas de certificados revocados (base de datos de certificados).

También tenemos que tener bien configurado el archivo openssl.cnf para que coja las rutas adecuadamente.

a) Comentar las siguientes líneas en el fichero

/usr/share/ssl/openssl.cnf

Digitar el siguiente comando: vi /usr/share/ssl/openssl.cnf



b) Ingresar al directorio /ssl

Digitar el siguiente comando: cd /ssl

c) Crear la lista de revocación o CRL, con extensión **.crl**.

Digitar el siguiente comando:

openssl ca -gencrl -out listarev.crl

Digitar la contraseña de la autoridad certificadora.

d) Crear la lista de revocación o CRL, con extensión **.pem**.

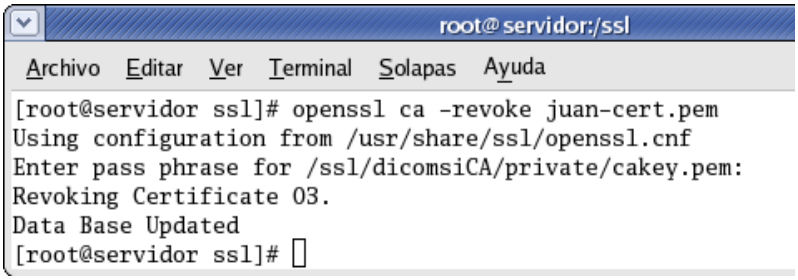
Digitar el siguiente comando: openssl ca -gencrl -out listarev.pem

Digitar la contraseña de la autoridad certificadora.

NOTA: listo ya se ha creado la lista de revocación de certificados CRL.

e) Revocar un certificado cliente creado.

Digitar el siguiente comando: openssl ca –revoke juan-cert.pem

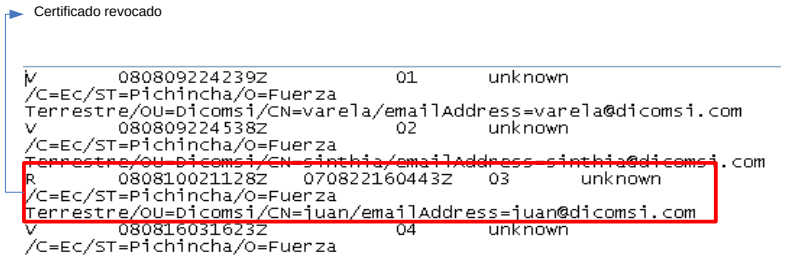


f) Actualizar la lista de revocación.

Digitar los siguientes comandos.

-openssl ca -gencrl -out listarev.crl
-openssl ca -gencrl -out listarev.pem

NOTA: revisar el archivo index.txt, el certificado del usuario Juan ya se ha revocado



4.10 CONFIGURAR CERTIFICADOS PARA EL SERVIDOR WEB

a) Ingresar al directorio /ssl

Digitar el siguiente comando: cd /ssl

b) Generar la clave privada del servidor y el requerimiento

Digitar el siguiente comando:

openssl req -new -newkey rsa:1024 -nodes -keyout server.key.pem -out server.csr.pem

DONDE:

- server.csr.pem = es la llave de solicitud de requerimiento de llave pública X.509.
- –nodes = indica “no” pedir una clave simétrica al generar la llave privada.

c) Crear el archivo config1.txt, donde se define las características de un certificado.

Digitar el siguiente comando: vi config1.txt

Digitar las siguientes líneas dentro del fichero:

basicConstraints=critical,CA:FALSE

extendedKeyUsage=serverAuth

DONDE:

- basicConstraints = critical,CA:FALSE : para que cumpla con el X509v3 y con la RFC3280
- extendedKeyUsage=serverAuth: el certificado es para un servidor Web.

d) Crear el certificado para el servidor Web firmado con la clave privada de nuestro CA.

Digitar el siguiente comando:

openssl ca -verbose -out server.cert.pem -days 360 -config

/usr/share/ssl/openssl.cnf -in server.csr.pem -extfile config1.txt

DONDE:

- ca: indica que va ha ser firmado por nuestra autoridad certificadora.
- -days 360: tiempo de validez del certificado.
- -extfile config1.txt = la configuración registrada en el archivo config1.txt .
- -in server.csr.pem = petición de certificado.
- -out server.cert.pem = genera el certificado en el fichero server.cert.pem
- -sha1 = lgoritmo de cifrado SHA1

Una vez lanzado el comando nos pedirá el password de la CA que lo emite y listo el fichero se generará.

e) Crear una carpeta en el directorio /var/www/

```
mkdir -p /var/www/dicomsi.com/
```

f) Editar y crear el siguiente fichero /etc/httpd/conf.d/dicomsi.conf

NOTA: se configura un sitio de red virtual.

Digitamos las siguientes líneas:

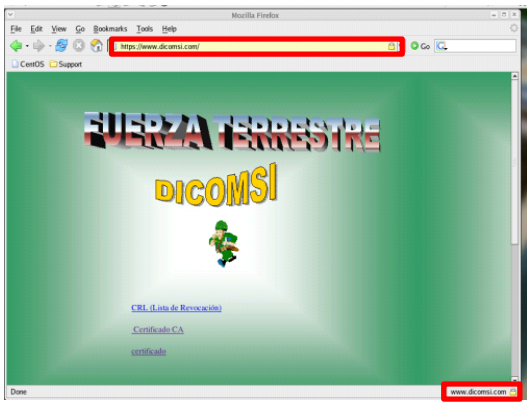
```
### dicomsi.com ###
NameVirtualHost 192.168.1.1:80
    <VirtualHost 192.168.1.1:80>
        ServerAdmin administrador@dicomsi.com
        DocumentRoot /var/www/dicomsi.com/html
        ServerName www.dicomsi.com
        ServerAlias dicomsi.com
        Redirect 301 / https://www.dicomsi.com/
        CustomLog /var/www/dicomsi.com/logs/access_log combined
        Errorlog /var/www/dicomsi.com/logs/error_log
    </VirtualHost>

NameVirtualHost 192.168.1.1:443
    <VirtualHost 192.168.1.1:443>
        ServerAdmin administrador@dicomsi.com
        DocumentRoot /var/www/dicomsi.com/html
        ServerName www.dicomsi.com
        ScriptAlias /cgi-bin/ /var/www/dicomsi.com/cgi-bin/
        SSLEngine on
        SSLCertificatefile /ssl/server.cert.pem
        SSLCertificateKeyfile /ssl/server.key.pem
        SetEnvIf User-Agent ".*MSIE.*" nokeepalive ssl-unclean-
shutdown
        CustomLog /var/www/dicomsi.com/logs/ssl_request_log \
            "%t %h %x %x \"%r\" %b"
        CustomLog /var/www/dicomsi.com/logs/ssl_access_log
combined
        Errorlog /var/www/dicomsi.com/logs/error_log
    </VirtualHost>
```

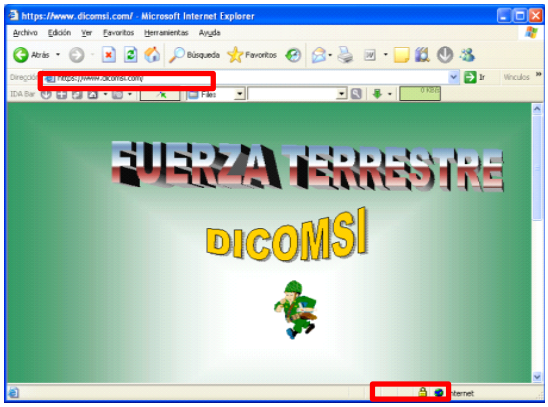
g) Reiniciar y depurar el servicio httpd

Digitar el siguiente comando: service httpd restart

h) Ingresar a un navegador Web y probar el correcto funcionamiento.

Mozilla **Internet Explorer**





4.11 CONFIGURACÓN DEL SERVIDOR LDAP (LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL)

LDAP es un protocolo para consulta y modificación de servicios de directorio que se desempeñan sobre TCP/IP. LDAP utiliza el modelo X.500 para su estructura, es decir, se estructura árbol de entradas, cada una de las cuales consiste de un conjunto de atributos con nombre y que a su vez almacenan valores.

Este servicio posibilita la búsqueda de información sobre personas que forman parte de un dominio.

a. Crear un directorio específico para este directorio y se configurará con permisos de acceso exclusivamente al usuario y grupo ldap.

Digitar los siguientes comandos:

mkdir /var/lib/ldap/addressbook

```
chmod 700 /var/lib/ldap/addressbook
chown ldap.ldap /var/lib/ldap/addressbook
```

b. Crear una clave de acceso que se asignará en LDAP para el usuario administrador del directorio.

Digitar el siguiente comando: slappasswd

NOTA: el resultado es {SSHA}PahRehYeZemjaQ3+GuwjHy6yp0xOqd2K

Este texto cifrado se debe copiar porque será utilizado en el siguiente paso.

c. Editar el fichero ubicado en /etc/openldap/slapd.conf

NOTA: se define el nuevo directorio que en adelante se utilizará como libreta de direcciones. Digitar las siguientes líneas al final del fichero.

```
database       bdb
suffix         "dc=dicomsi,dc=com"
rootdn         "cn=Administrador,dc=dicomsi,dc=com"
rootpw         {SSHA}PahRehYeZemjaQ3+GuwjHy6yp0xOqd2K
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd and slap tools.
# Mode 700 recommended.
directory      /var/lib/ldap/addressbook
# Indices to maintain for this database
index objectClass                       eq,pres
index ou,cn,mail,surname,givenname      eq,pres,sub
index uidNumber,gidNumber,loginShell    eq,pres
index uid,memberUid                     eq,pres,sub
index nisMapName,nisMapEntry            eq,pres,sub
```

d. Iniciar el servicio de LDAP y añadir éste al resto de los servicios que arrancan junto con el sistema.

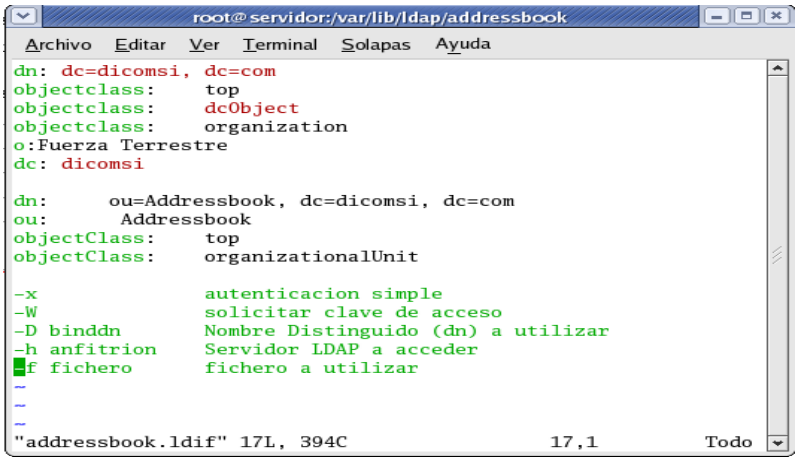
Digitar los siguientes comandos:

```
service ldap start
```

chkconfig ldap on

e. Ingresar al directorio var/lib/ldap/addressbook y crear el fichero addressbook.ldif.

Digitar las siguientes lineas dentro del fichero.



f. Insertar la información generada en el directorio

ldapadd -x -W -D 'cn=Administrador, dc=su-dominio, dc=com' -h 192.168.1.1 -f addressbook.ldif

NOTA: realizado este se podrá comenzar a poblar el directorio con datos de usuarios nuevos.

g. Cambiar la extensión de un certificado .pem a un certificado con la extencion .der

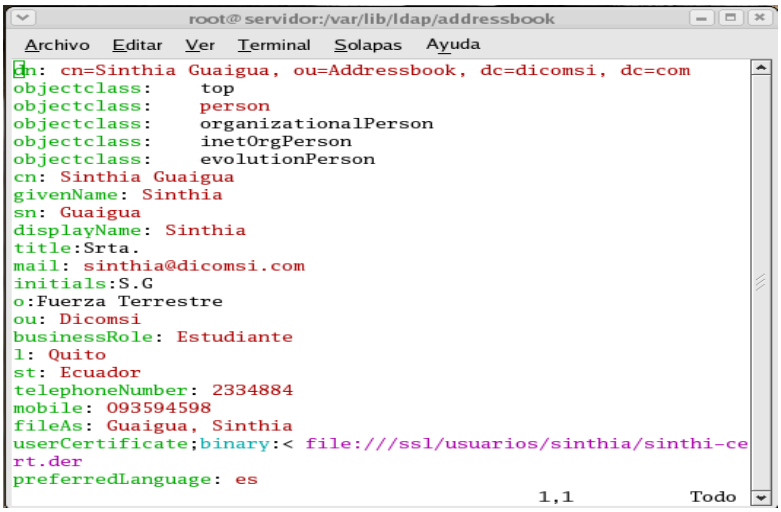
NOTA: se realiza este cambio porque los datos de un certificado deben estar en binario caso contrario no reconoce LDAP.

Digitar el siguiente comando:

openssl x509 -inform pem -outform der < sinthia-cert.pem > sinthia-cert.der

h. Crear el fichero sinthia.ldif dentro del directorio var/lib/ldap/addressbook

Digitar las siguientes líneas.



i. Insertar la información generada en el directorio

Digitar el siguiente comando.

ldapadd -x -W -D 'cn=Administrador, dc=su-dominio, dc=com' -h 192.168.1.1 -f sinthia.ldif

j. Para modificar un usuario se debe modificar el archivo .ldif , luego se digitara el siguiente comando.

ldapmodify -x -W -D 'cn=Administrador, dc=dicomsi, dc=com' -h 192.168.1.1 -f sinthia.ldif

CAPITULO 5: PRUEBAS

5.1 CREAR CUENTAS EN OUTLOOK EXPRESS.

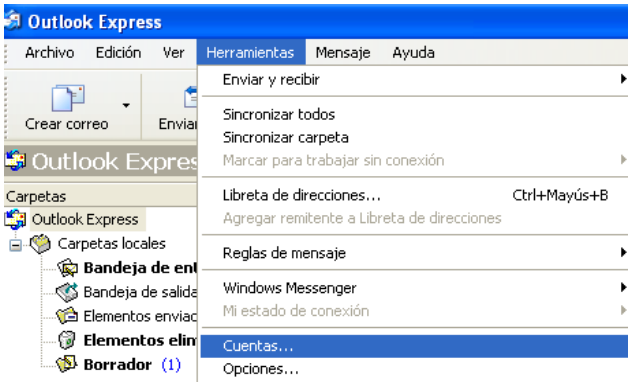
a) Ingresar a Outlook Express

Inicio → Todos los programas → Outlook Express

b) Crear una cuenta

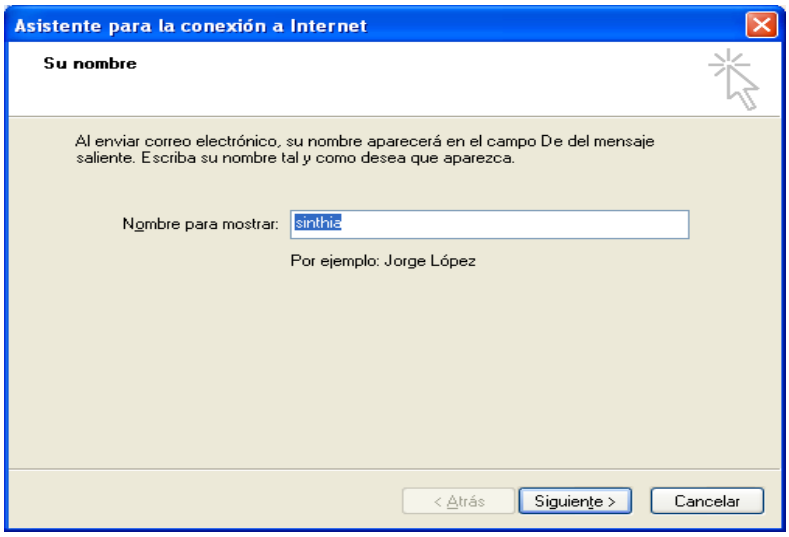
i. Ingresar a cuentas de Internet.

Herramientas → Cuentas

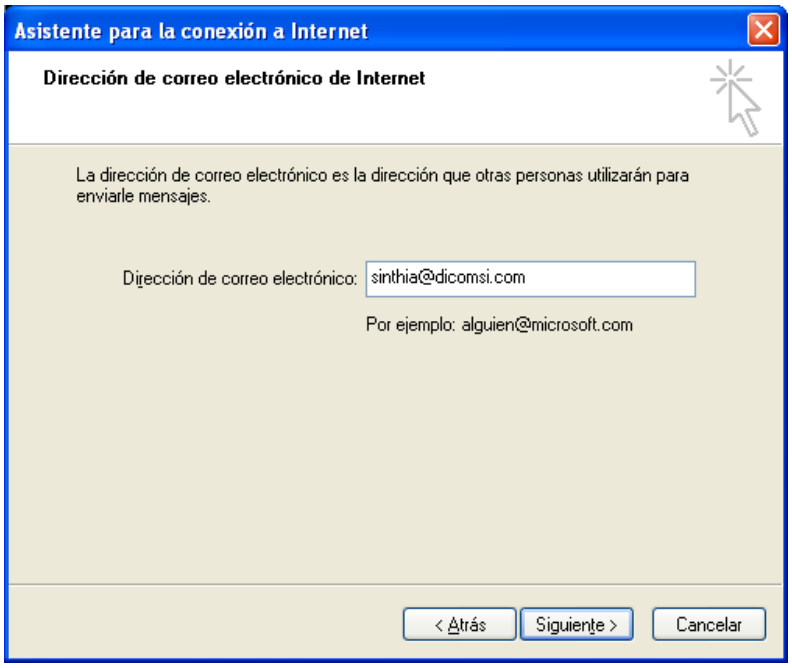


c) Elegir la pestaña Todo → Agregar → Correo

i. Digitar el nombre para la cuenta.



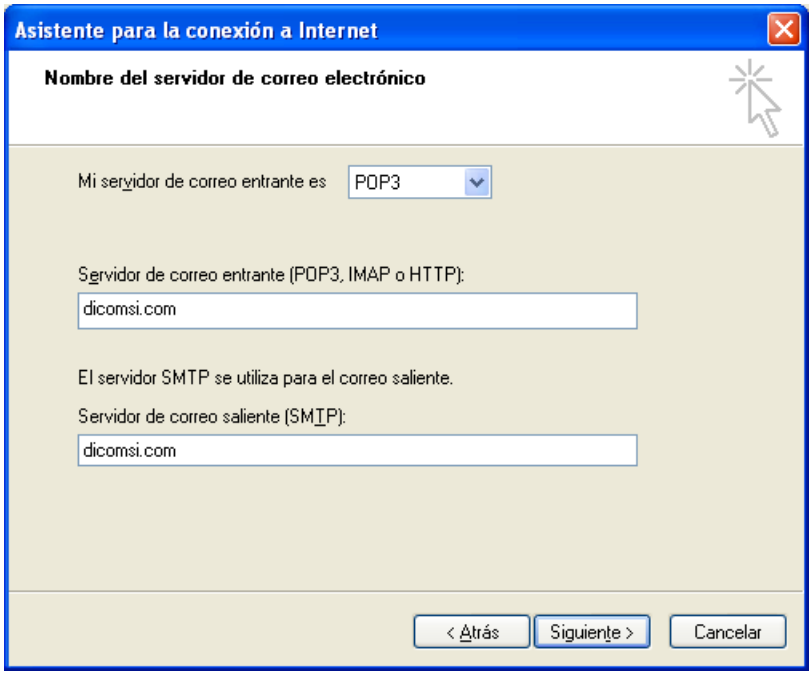
ii. Digitar el correo electrónico del cliente.



iii. Digitar el servidor de correo entrante y saliente

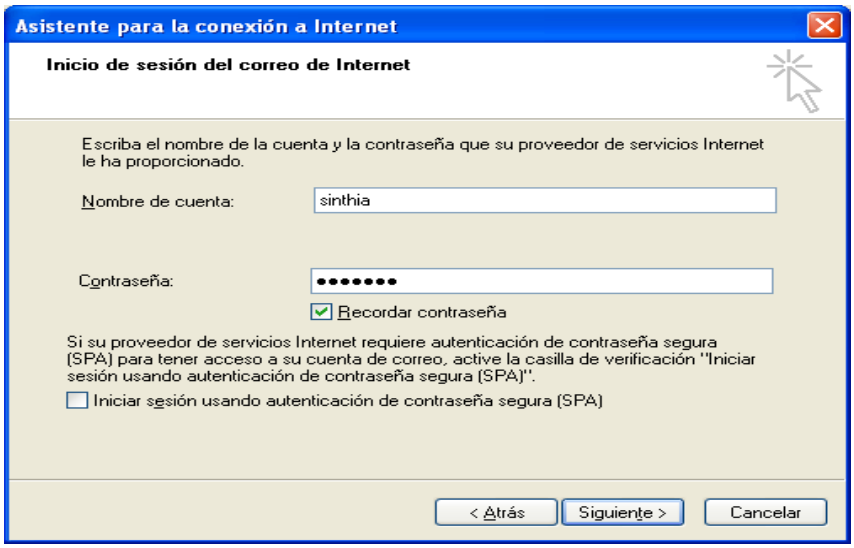
NOTA: el servidor de dominio tiene resuelto la dirección del servidor de correo, en este caso es 192.168.1.1 -> dicomsi.com

Si no se tiene un servidor de dominio se colocará la dirección IP del servidor de correo.



iv. Digitar el nombre de usuario y contraseña.

El usuario debe haber sido registrado, por el administrador de correo y asignado una contraseña.



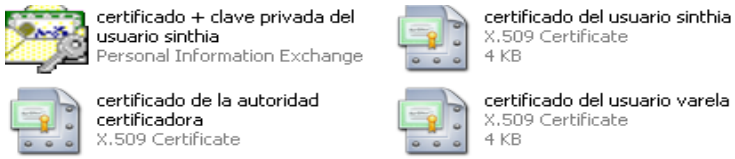
v. Dar clic en finalizar.

5.2 CONFIGURACIÓN PREVIA DE CERTIFICADOS DEL EMISOR Y RECEPTOR.

DATOS PREVIOS:

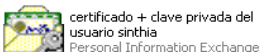
- Emisor = usuario Sinthia
- Receptor = usuario Varela

a) El administrador de certificados digitales debe proporcionar los siguientes archivos, al usuario Sinthia.



DONDE:

- Fichero “certificado + clave privada del usuario sinthia = fichero que solo el usuario Sinthia puede tener y cuidar de su seguridad porque contiene la clave privada.
- Fichero “certificado del usuario sinthia” = fichero solo contiene el certificado con la clave publica, el usuario Sinthia debe entregar a las personas a las que va enviar mensajes firmados.
- Fichero “certificado de la autoridad certificadora” = se debe instalar en los certificados raíz de confianza.
- Fichero “certificado del usuario varela” = fichero solo contiene el certificado con la clave publica, el usuario Varela debe entregar a las personas a las que va enviar mensajes firmados.

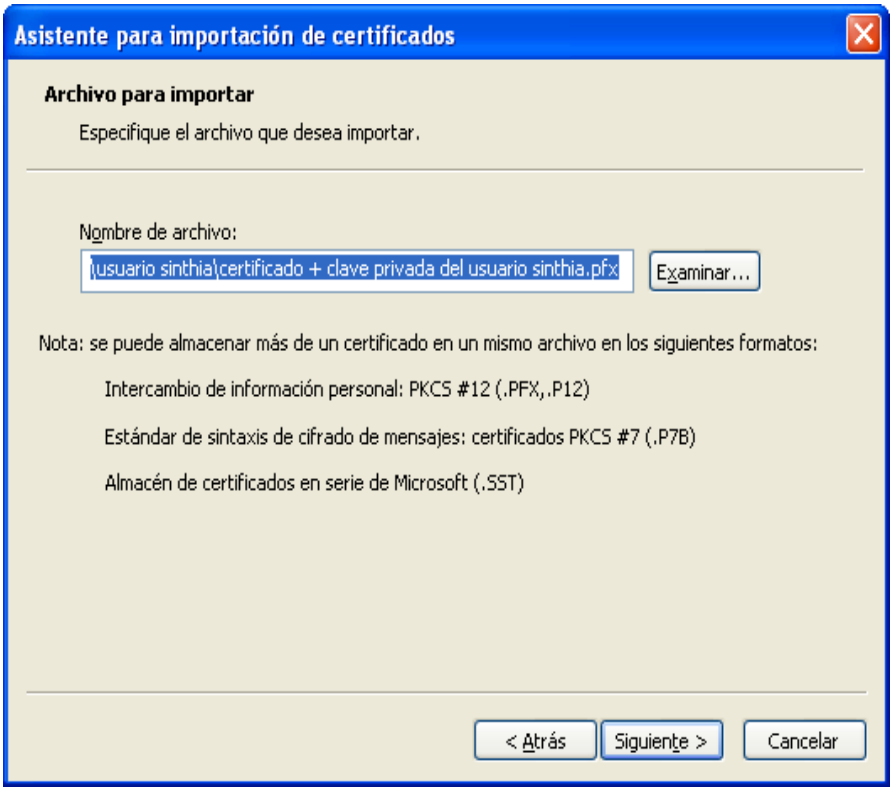
b) Dar doble clic sobre el fichero 

. Se activa el asistente para importación de certificados digitales.

NOTA: este es un certificado con extensión PKSC#12, se instala el certificado en el almacén personal de certificados, porque contiene la clave secreta.

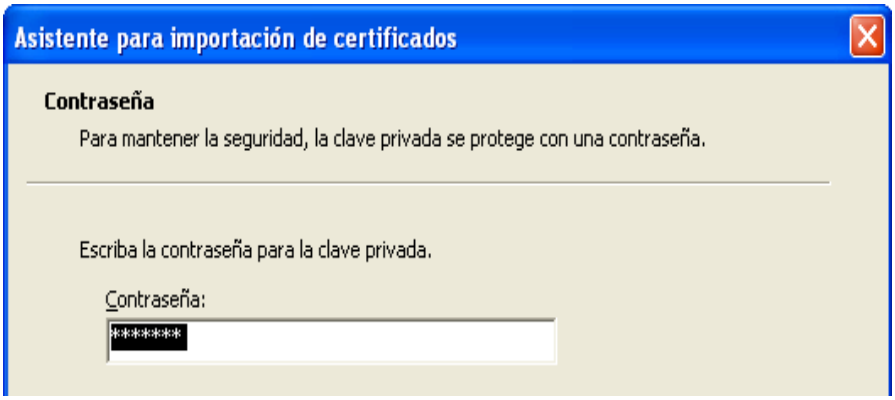
c) Dar clic en siguiente, la ubicación del certificado es por default.

Dar clic en siguiente.



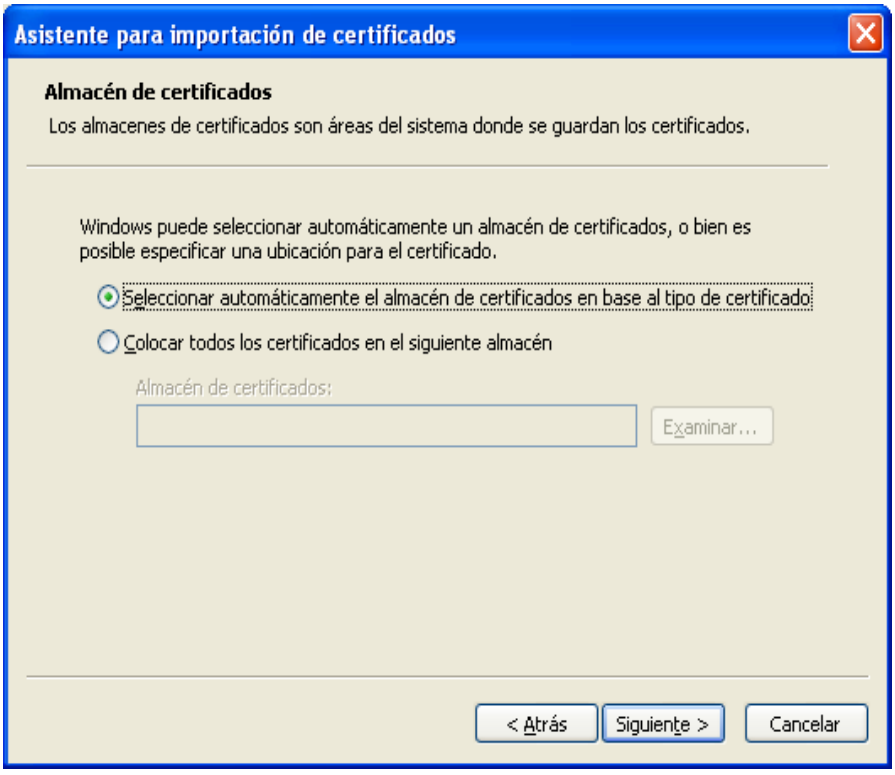
d) Digitar el passphrase (contraseña) que protege a la clave secreta.

Dar clic en siguiente.



e) Dar clic en siguiente y para terminar en finalizar.

NOTA: este es un certificado que contiene la clave privada por esta razón se importará por default en el almacén de certificados personales.

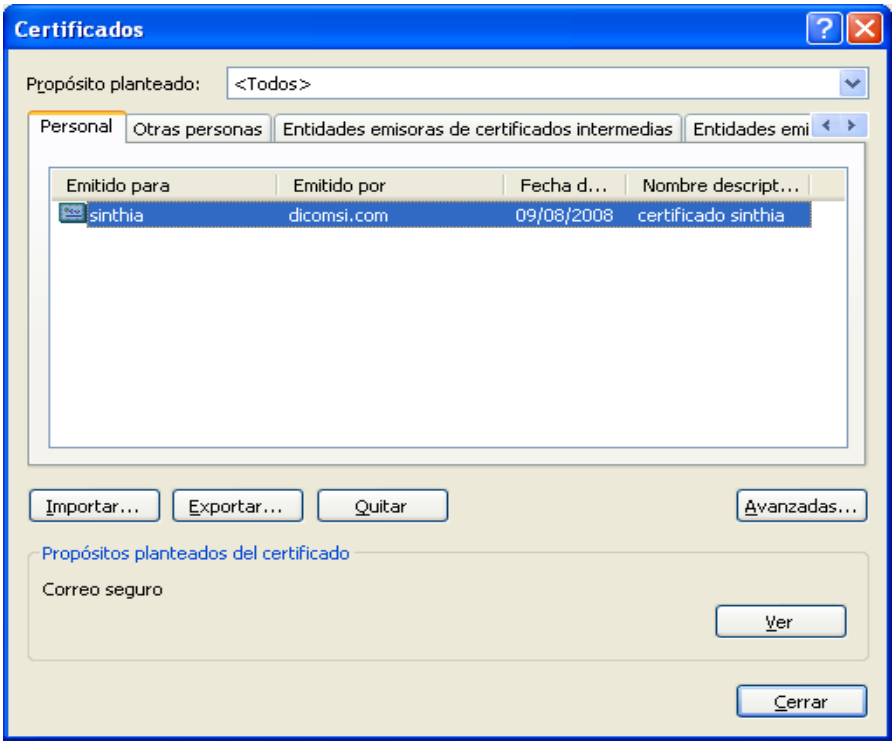


f) Dar clic en finalizar y luego aceptar.

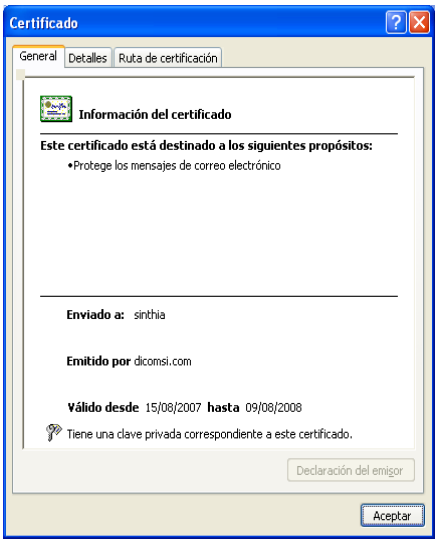
NOTA: si la importación es satisfactoria, y la contraseña es correcta el asistente para importación de certificados, dará como respuesta lo siguiente:

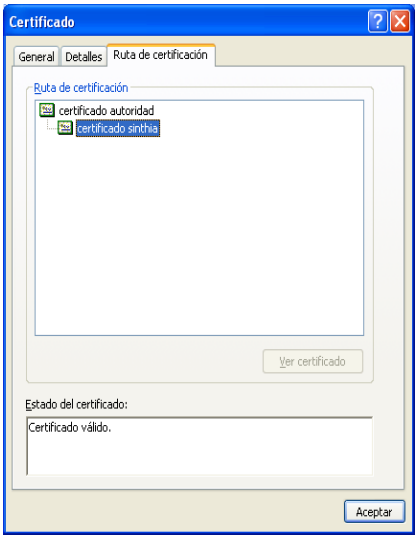
g) Verificar el certificado recién importado.

Ingresar a Outlook Express → Herramientas → Opciones → Seguridad Id digitales → personal



h) Ver las propiedades del certificado dando clic en la opción ver.





i) Importar el certificado del receptor "Varela"

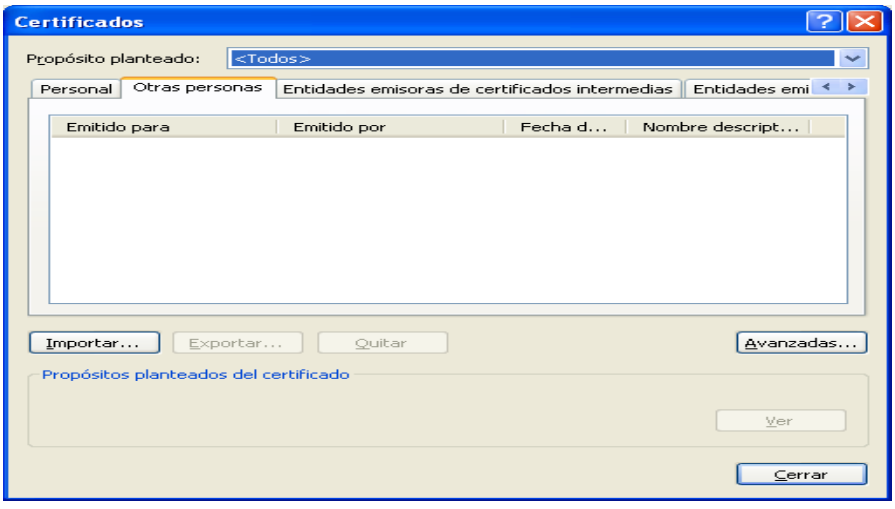
Ingresar a Outlook Express → Herramientas → Opciones → Seguridad Id digitales → Otras personas → Importar

NOTA: Los almacenes de certificados digitales están organizados según el tipo de certificados, entre los más importantes tenemos.

a. Personal.- certificado y clave privada incluida.

b. Otras personas.- solo certificados sin clave privada.

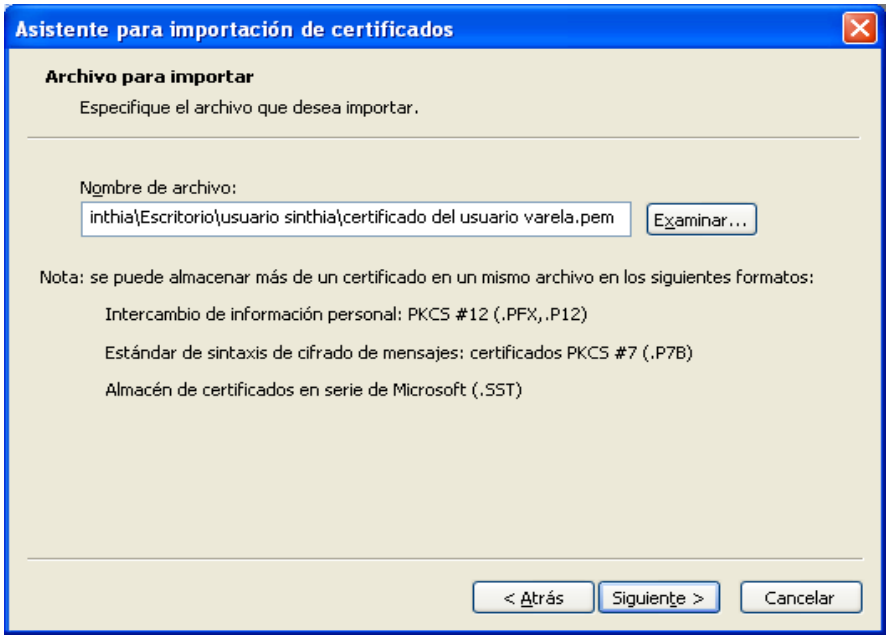
c. Entidades emisoras raíz de confianza.- certificados de CA.



j) Se activa el asistente para importación de certificados.

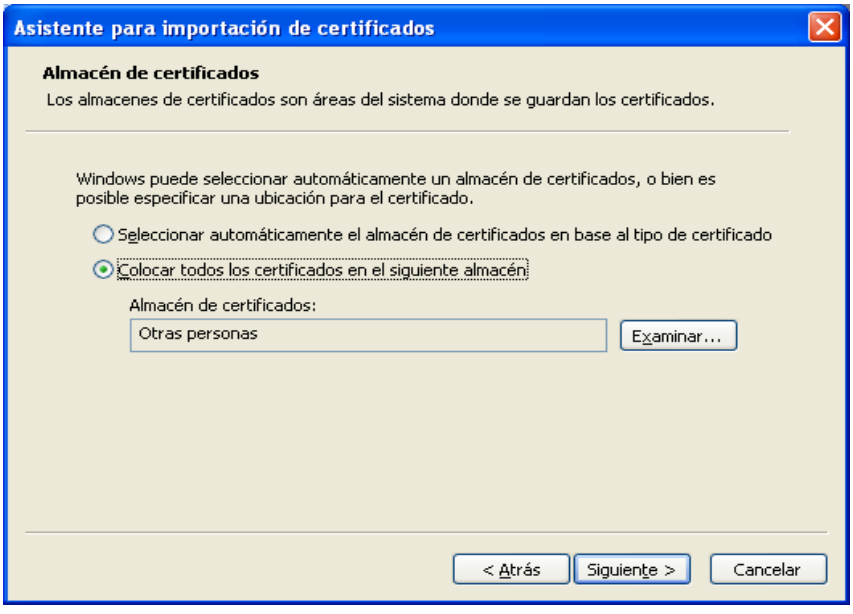
Dar clic en siguiente → siguiente.

Seleccionar el archivo que contiene al certificado de "**Varela".**

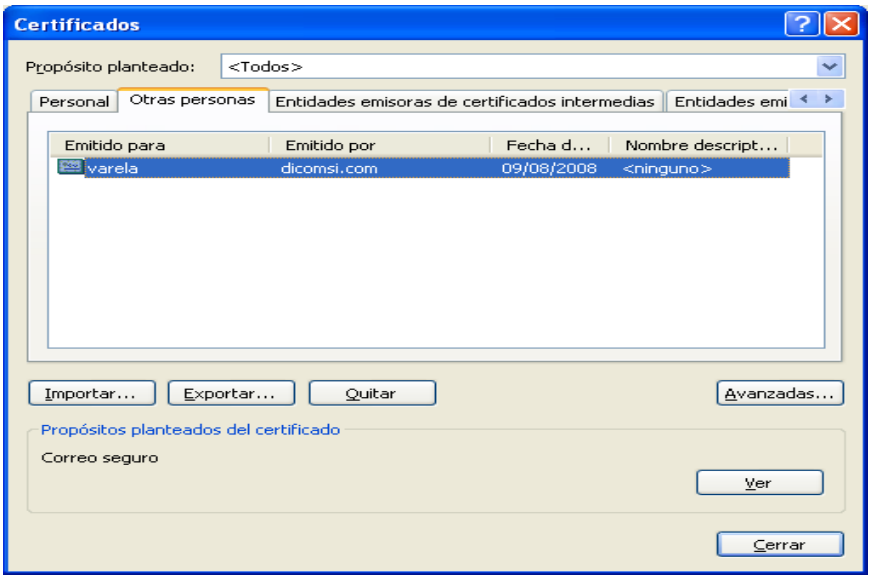


k) Dar clic en siguiente.

NOTA: por default se selecciona en el almacén **"otras personas".**



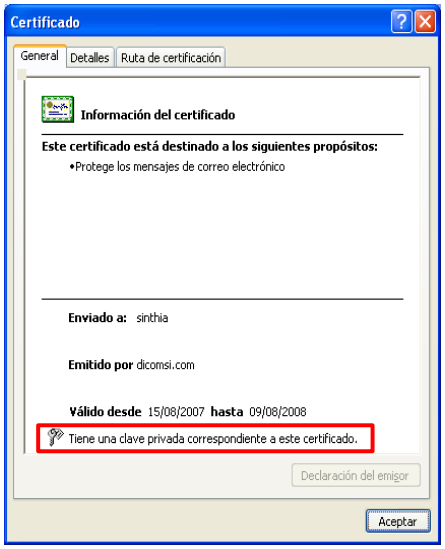
l) Para terminar la importación, dar clic en finalizar.



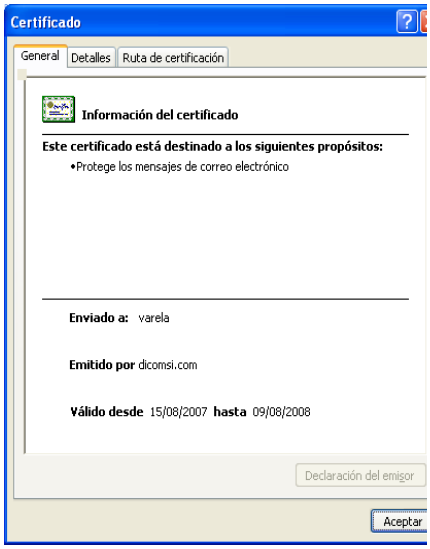
m) Dar clic en Ver.

Se observa que este certificado no contiene una clave privada, como es el caso del certificado del usuario **Sinthia.**

Certificado SINTHIA

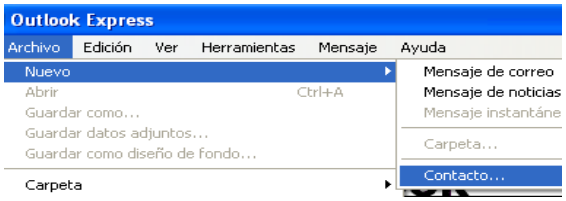


Certificado VARELA



n) Crear Contactos asociados a un identificador digital

Ingresar a Outlook Express → Archivo → Nuevo → Contacto

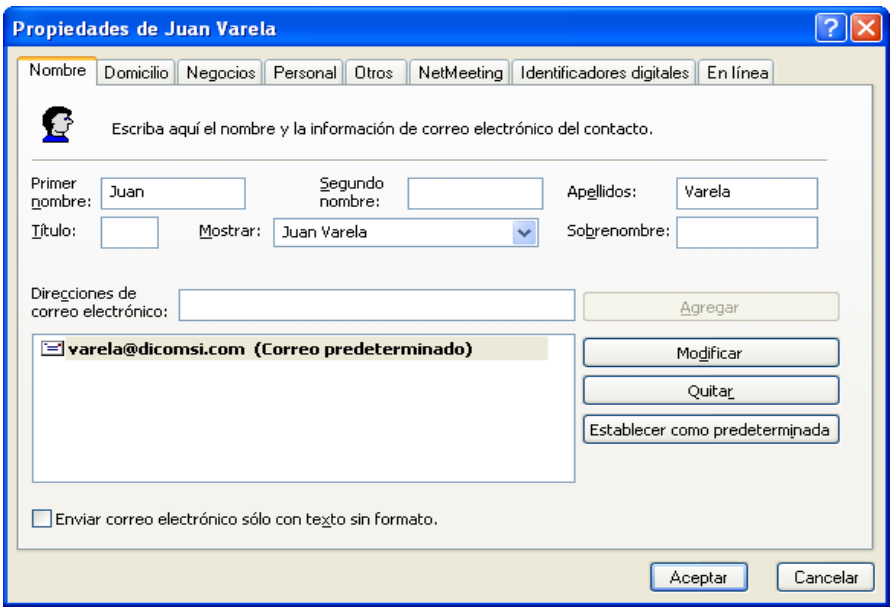


NOTA: un identificador digital es el certificado digital, este va asociado a un correo electrónico. Por esta razón se debe tener cuidado al momento de crear el certificado, se debe colocar la dirección mail correcta.

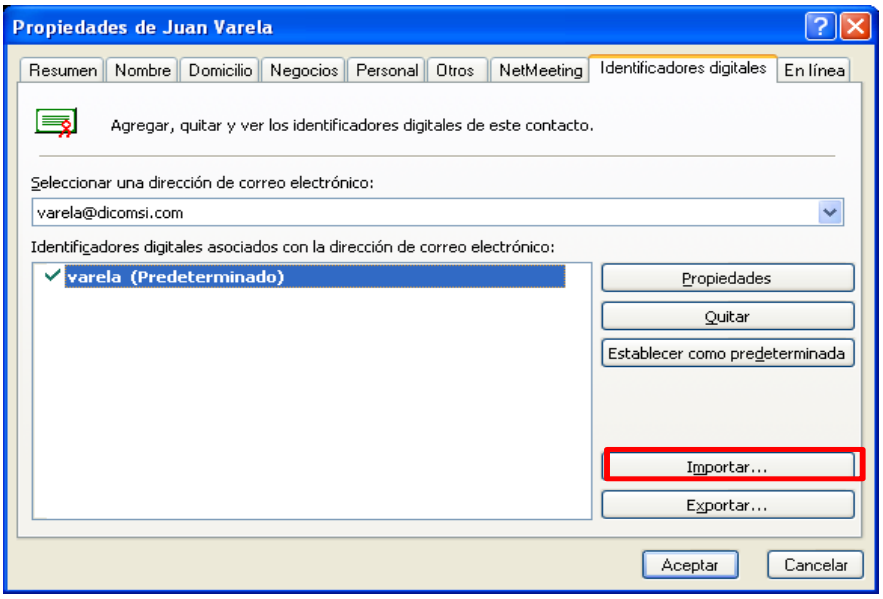
Para poder comenzar a enviar mensajes firmados digitalmente, se debe obtener un identificador digital. Si envía mensajes cifrados, la Libreta de direcciones debe contener un identificador digital para cada destinatario.

o) Ingresar los datos del usuario

Digitar el correo del usuario y dar clic en agregar.



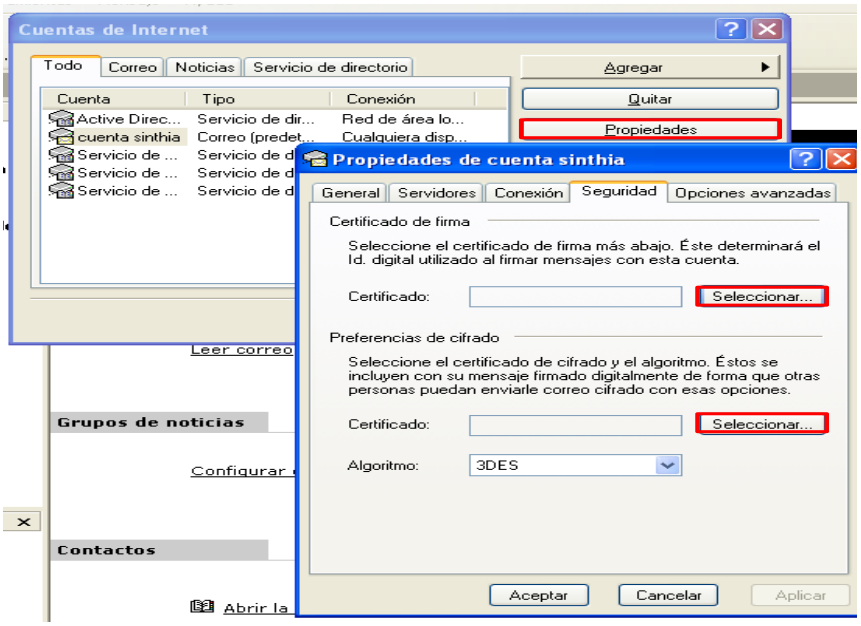
p) Seleccionar la pestaña Identificadores digitales → Importar → Seleccionar el certificado



q) Asignar un certificado a la cuenta del emisor (Sinthia)

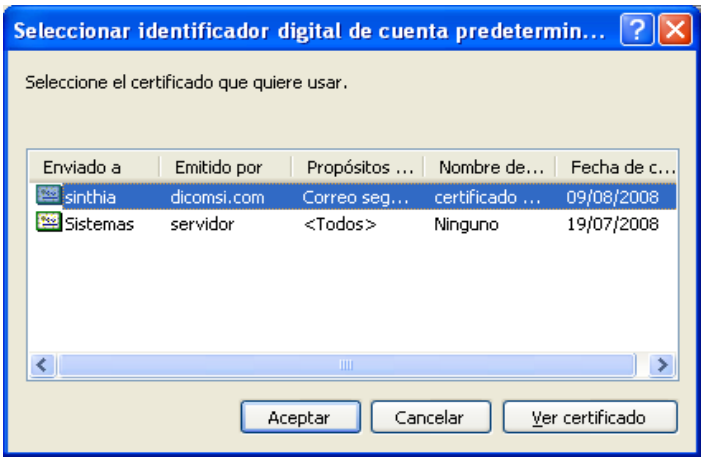
Ingresar a Outlook Express → Herramientas → Cuentas → Cuenta Sinthia → Propiedades → Seguridad

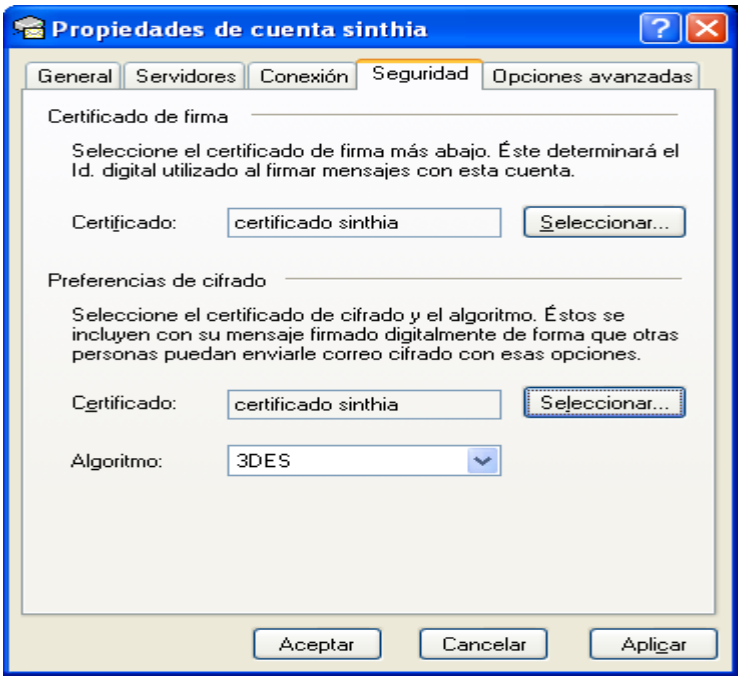
NOTA: La Cuenta del emisor ya fue creada en el literal **b).**



r) Dar clic en Seleccionar.

NOTA: escoger el certificado tanto para firma y cifrado.





s) Para terminar

Dar clic en Aplicar → Aceptar

5.3 ENVIAR UN MENSAJE FIRMADO.

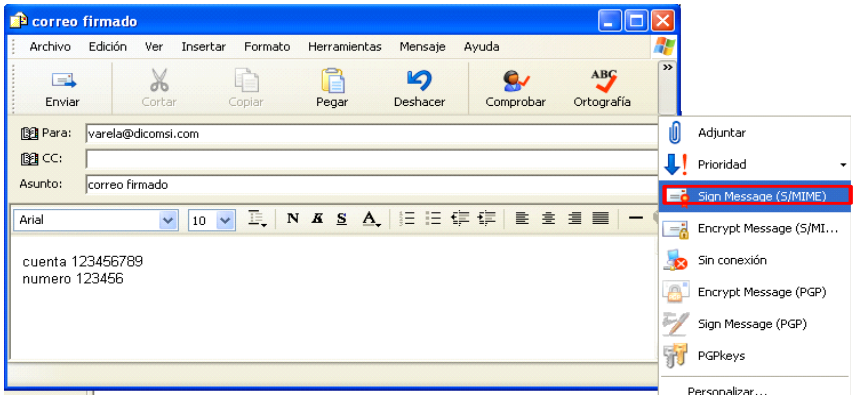
NOTA: Emisor → sinthia@dicomsi.com

Receptor → varela@dicomsi.com

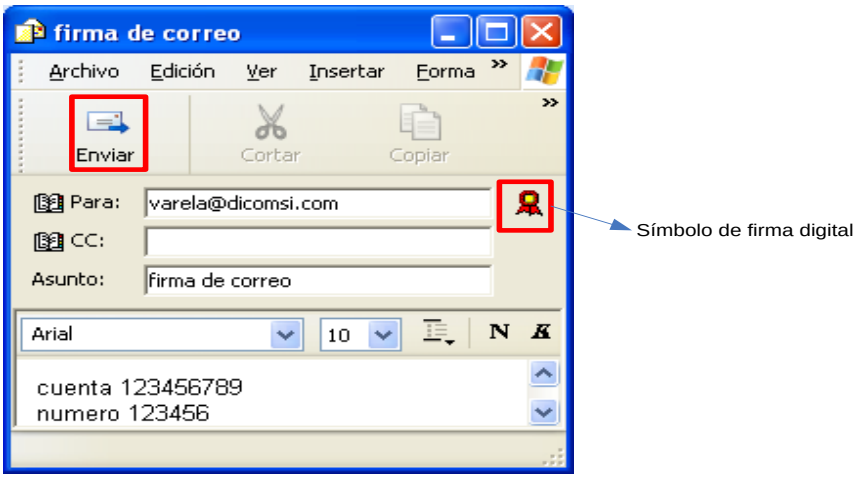
EMISOR

a) Ingresar a Outlook Express → Archivo → Nuevo → Mensaje de correo.

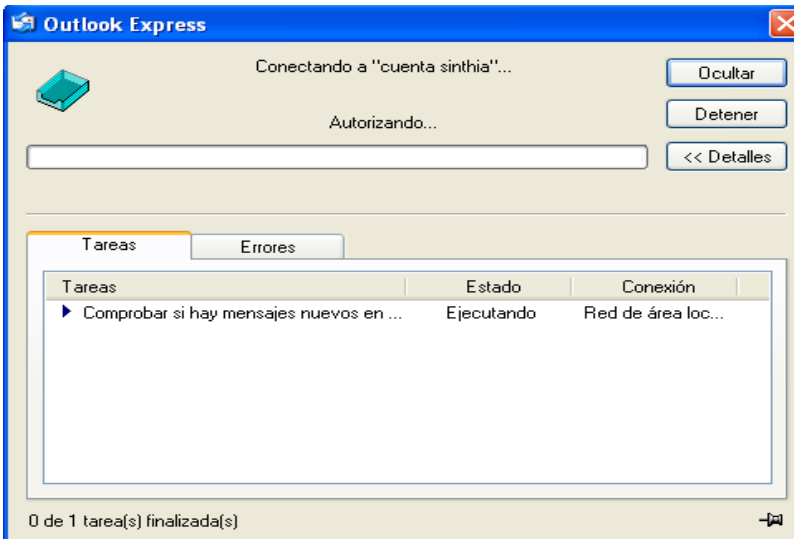
b) Seleccionar firmar mensaje (S/MIME).



c) Seleccionar **Enviar**

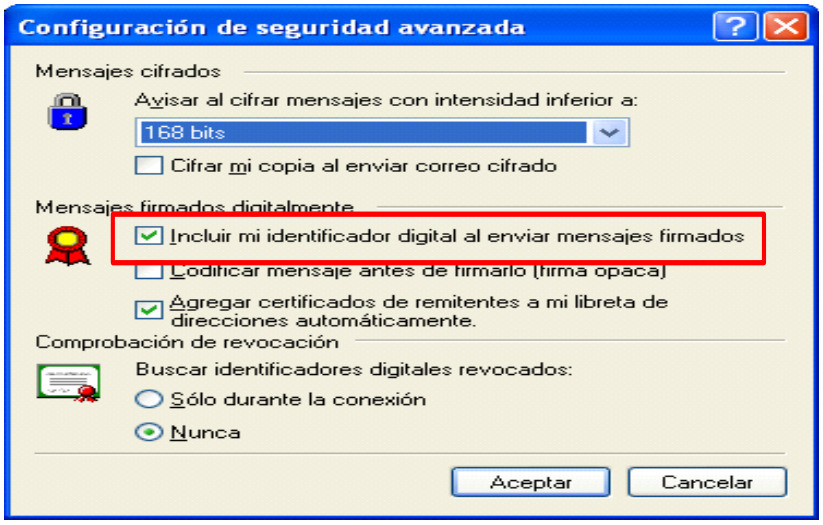


d) Seleccionar Enviar y Recibir

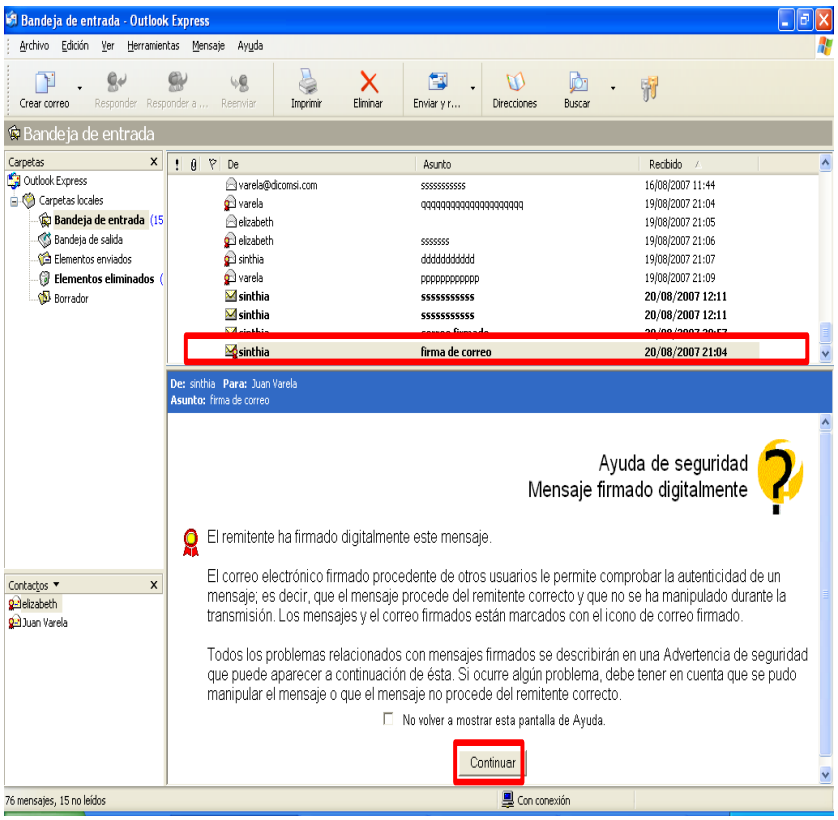


e) Ir a Archivo → Herramientas → Opciones → Seguridad

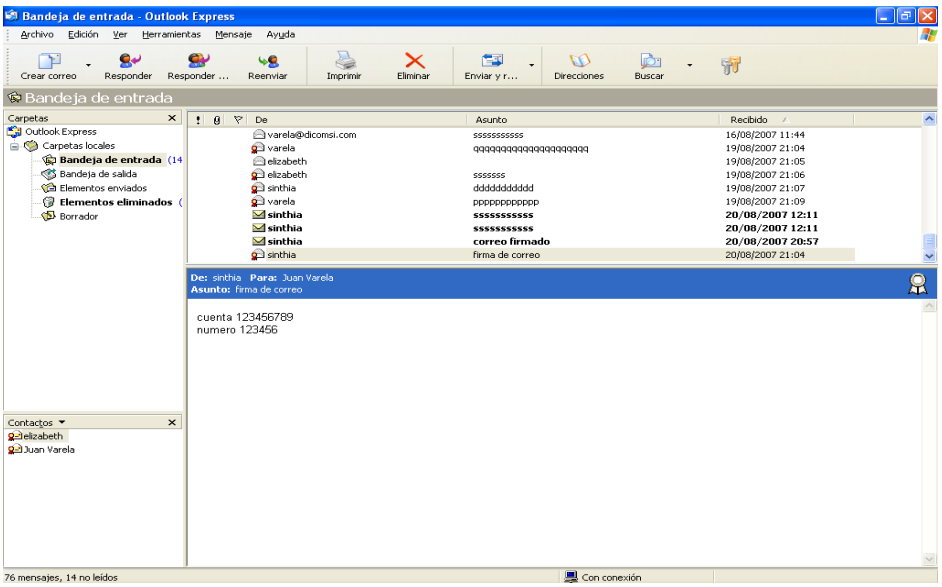
NOTA: en esta sección permite importar y exportar certificados digitales y configurar opciones avanzadas de seguridad de mensajes. La opción "Incluir mi identificador digital al enviar mensajes firmados ", proporciona el certificado digital de la persona que está enviando el mensaje firmado.



f) El usuario Varela crea una cuenta de usuario (como en la sección 10. b). Realizar la configuración realizada en el literal anterior e)**.** Revisar su mensaje y proceder a abrirlo.



g) Dar clic en continuar y listo el mensaje ya se puede leer.



5.4 CIFRAR UN MENSAJE.

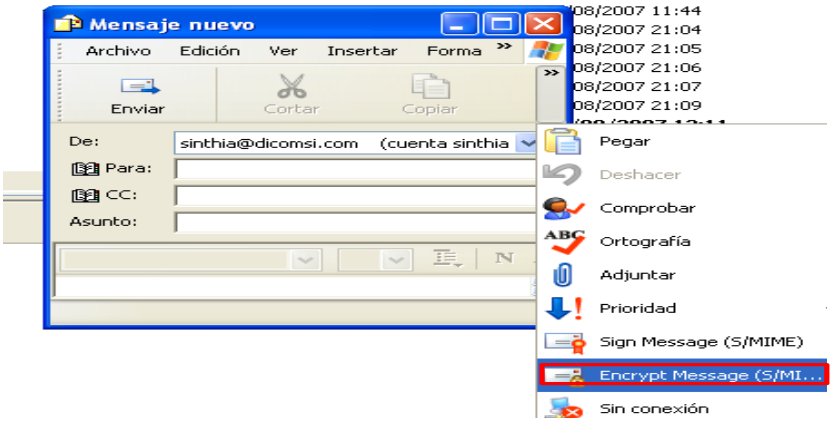
NOTA: el proceso es similar a firmar un mensaje, pero la diferencia esta en que al cifrar se tiene que utilizar la clave publica del receptor y se descifra con la clave privada del receptor.

EMISOR

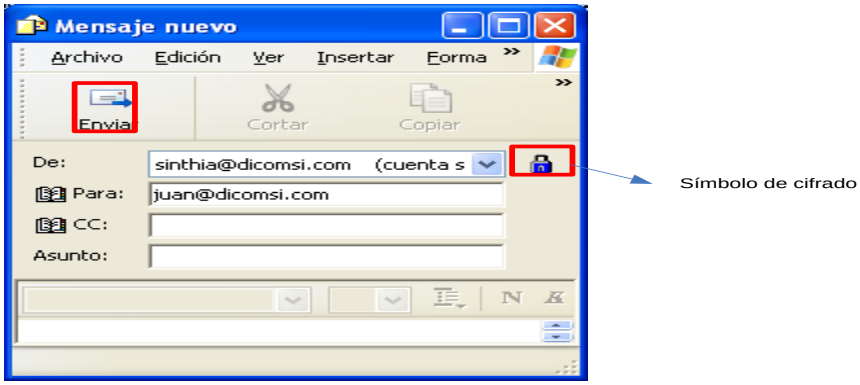
a) El emisor debe tener e importar el identificador digital del receptor para que pueda enviar el mensaje cifrado.

b) Ingresar a Outlook Express → Archivo → Nuevo → Mensaje de correo

c) Seleccionar cifrar mensaje (S/MIME).



d) Seleccionar **Enviar**

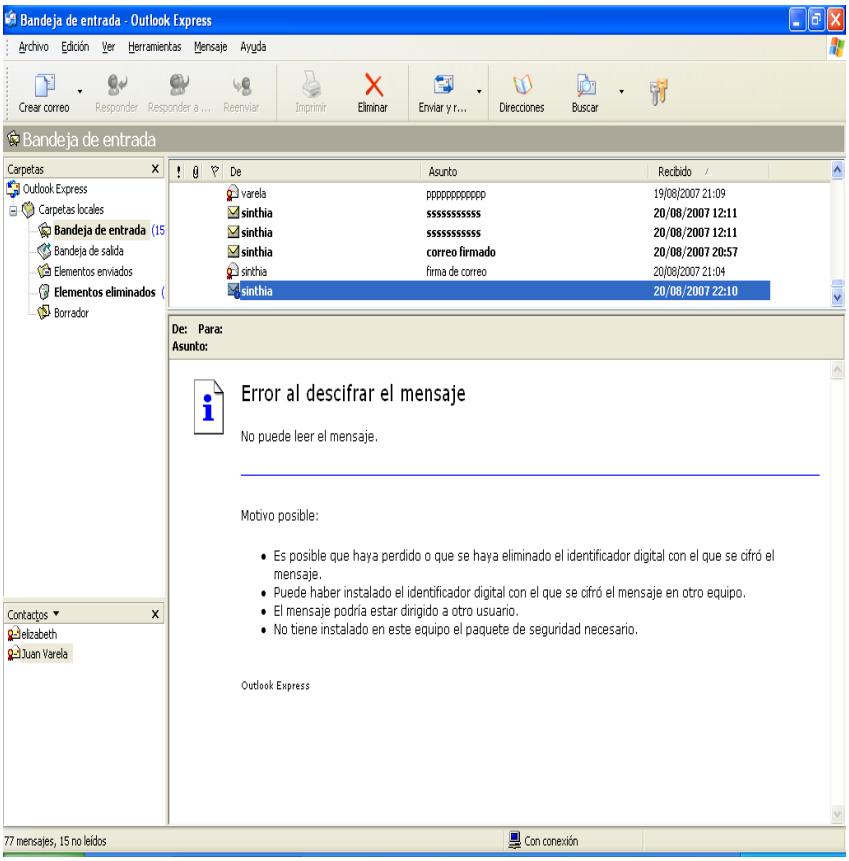


e) Seleccionar Enviar y Recibir

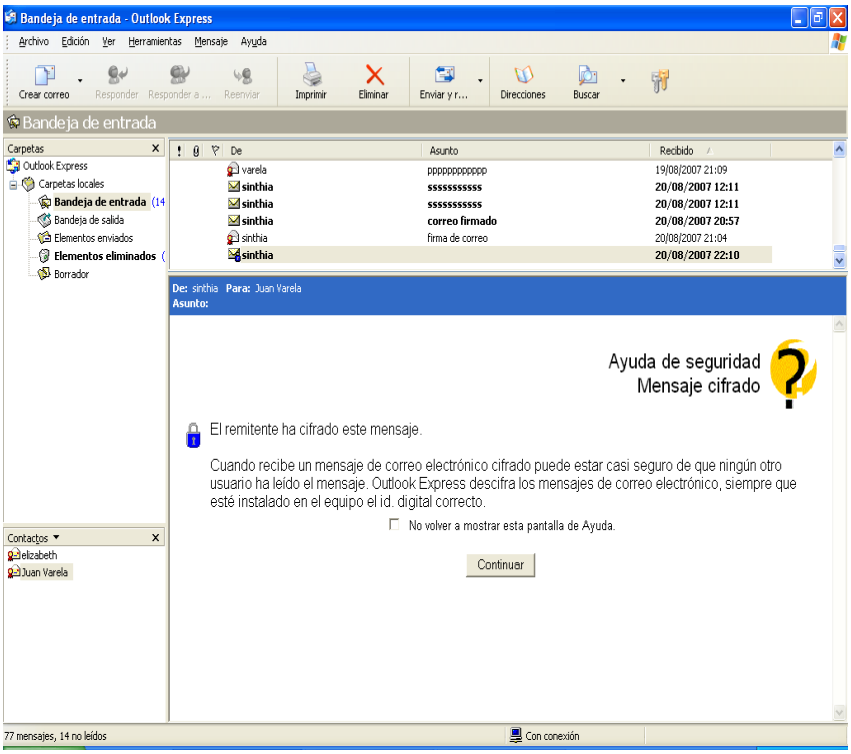
RECEPTOR

f) El usuario Varela crea una cuenta de usuario (como en la sección 10. b). Importa su certificado con la clave privada incorporada y asigna a su cuenta.

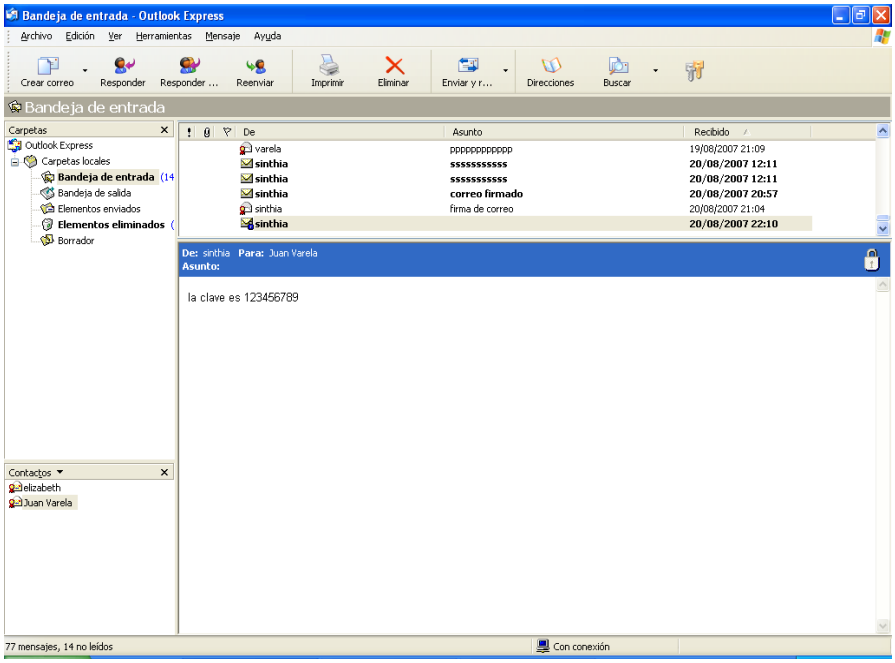
g) Si el receptor no importar su certificado con la clave privada dará un error como el siguiente:



h) Una vez realizado el literal **f)** revisar el mensaje y proceder a abrirlo.



i) Dar clic en continuar y listo el mensaje ya se puede leer.



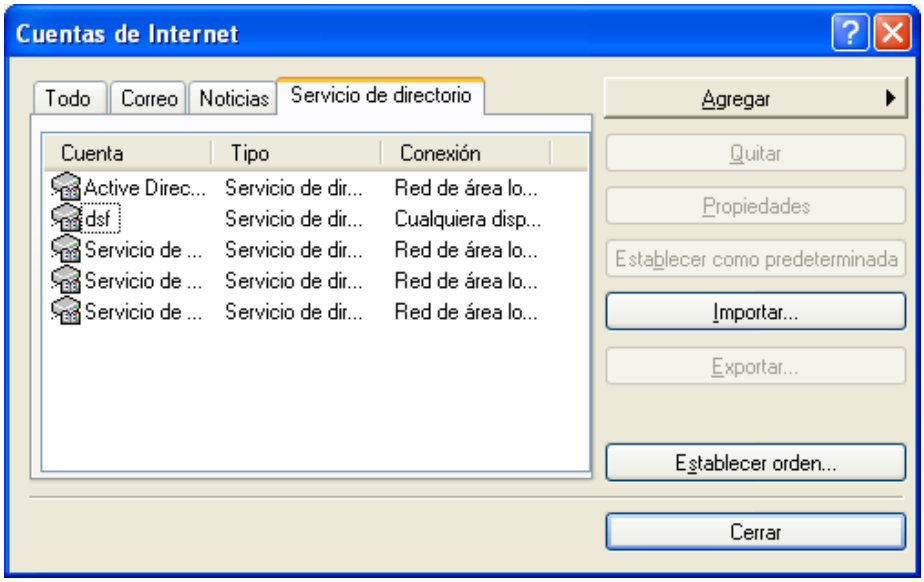
5.5 ENVIAR UN MENSAJE FIRMADO Y CIFRADO.

NOTA: se realiza los mismos anteriormente ya descritos.

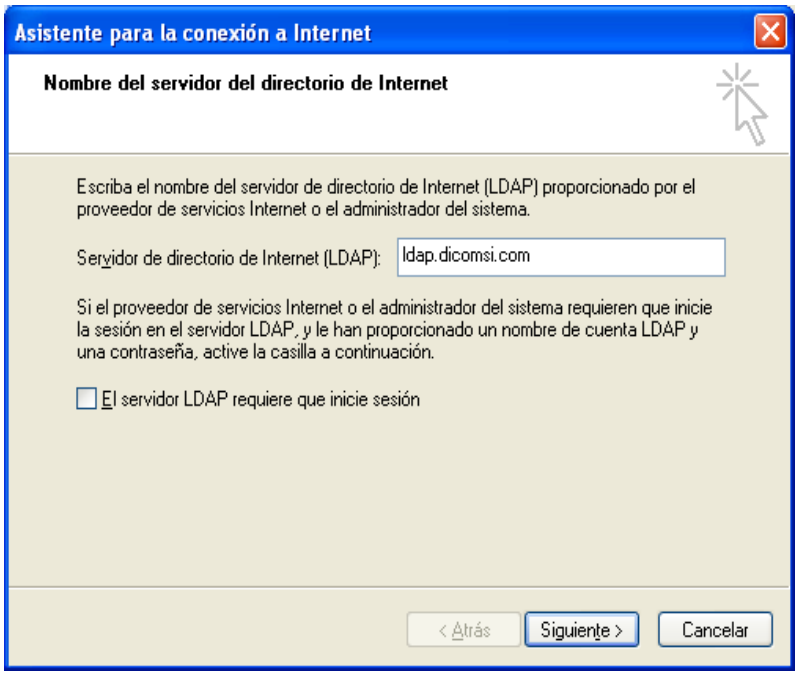
5.6 CONFIGURAR EL CLIENTE LDAP EN OUTLOOK EXPRESS

a. Pulsar sobre el botón "Direcciones" que se encuentra en la barra de menús → "Herramientas" →"Cuentas".

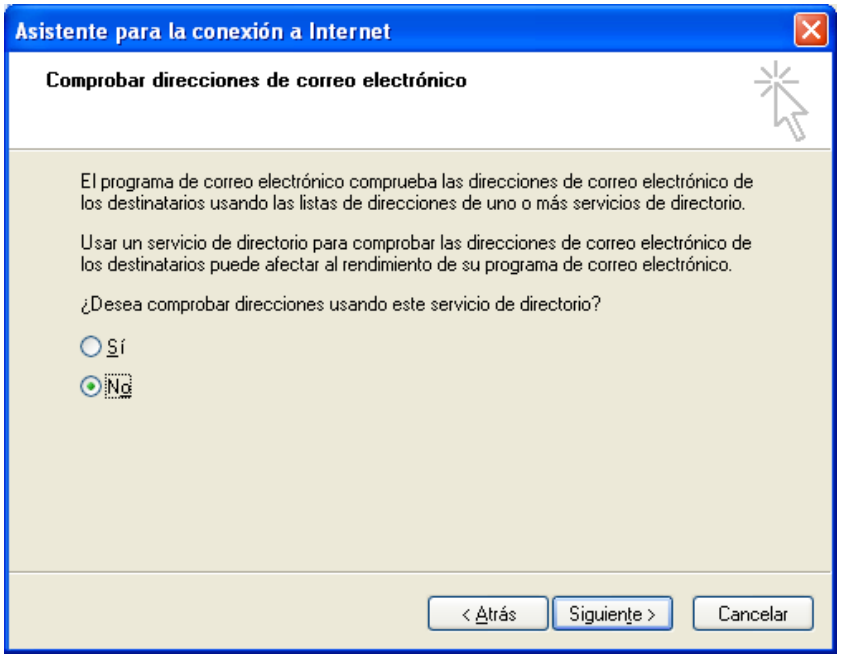
b. Pulsar "Agregar".



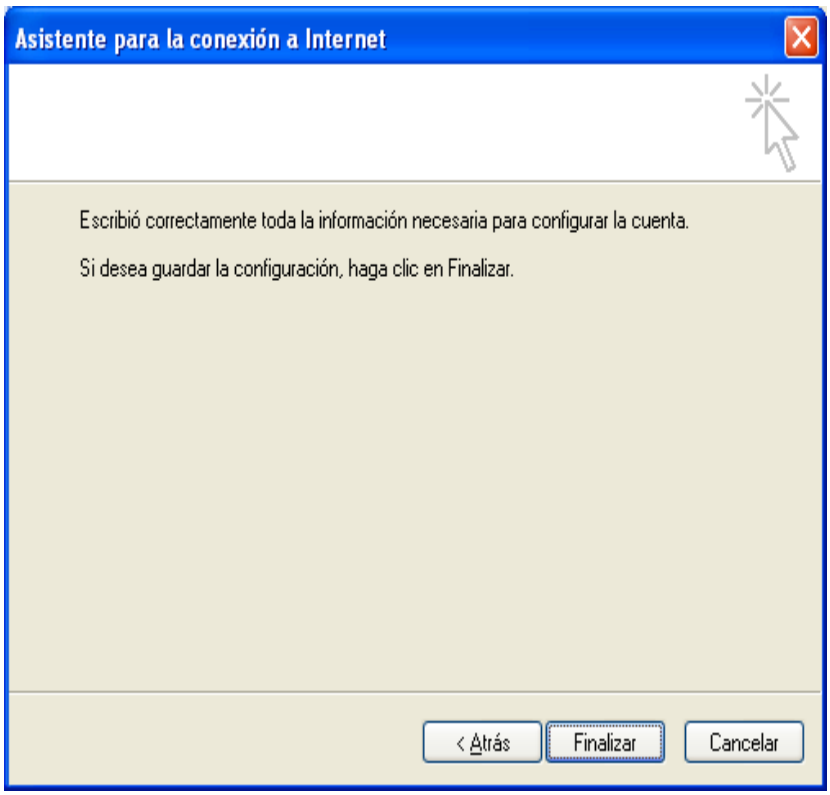
c. Escribir ldap.dicomsi.com en el recuadro de la ventana que le aparecerá:



d. Marcar NO para evitar un retardo a la hora de mandar mensajes. Una vez seleccionada una opción, pulsar el botón 'Siguiente'.

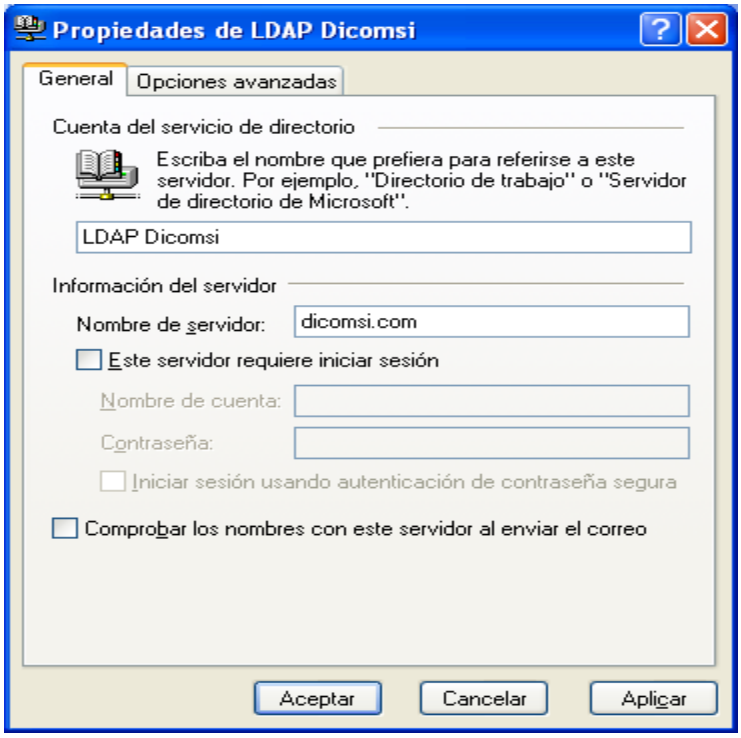


e. Pulsar el botón 'Finalizar'.



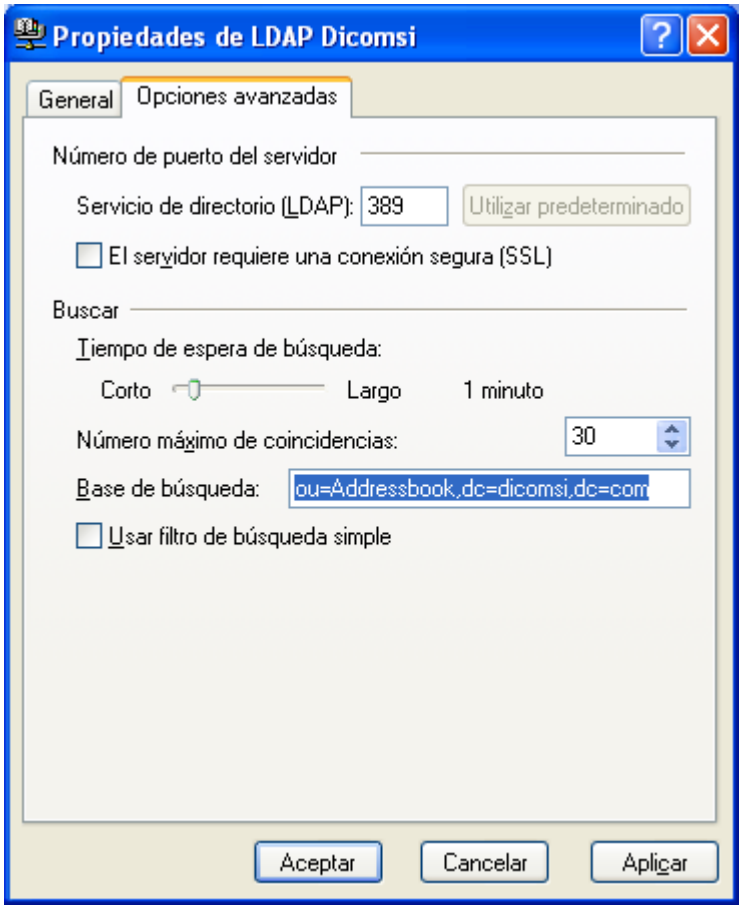
f. Configurar las opciones que definen el acceso al servidor. Para ello seleccionar la cuenta ldap.dicomsi.com recién creada y dar clic sobre el botón 'Propiedades'.

g. Modificar el nombre de la cuenta, escribir 'LDAP de la Dicomsi'.



h. Seleccionar la pestaña 'Avanzada' u 'Opciones Avanzadas', en la que observamos los campos que vamos a modificar.

i. Empezaremos escribiendo en el recuadro 'Base de búsqueda:' lo siguiente: ou=Addressbook,dc=dicomsi,dc=com



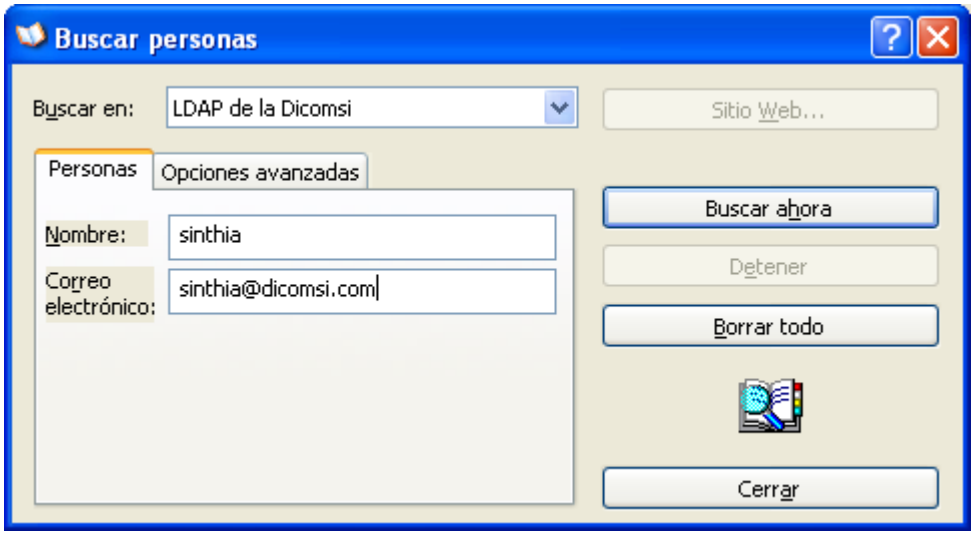
j. Pulsar sobre el botón 'Aplicar' y después sobre el botón ‘Aceptar’.

k. Para poder buscar personas debemos estar en la ventana de 'Libreta de direcciones' para lo cual, podemos llegar pulsando sobre el botón 'Direcciones'.

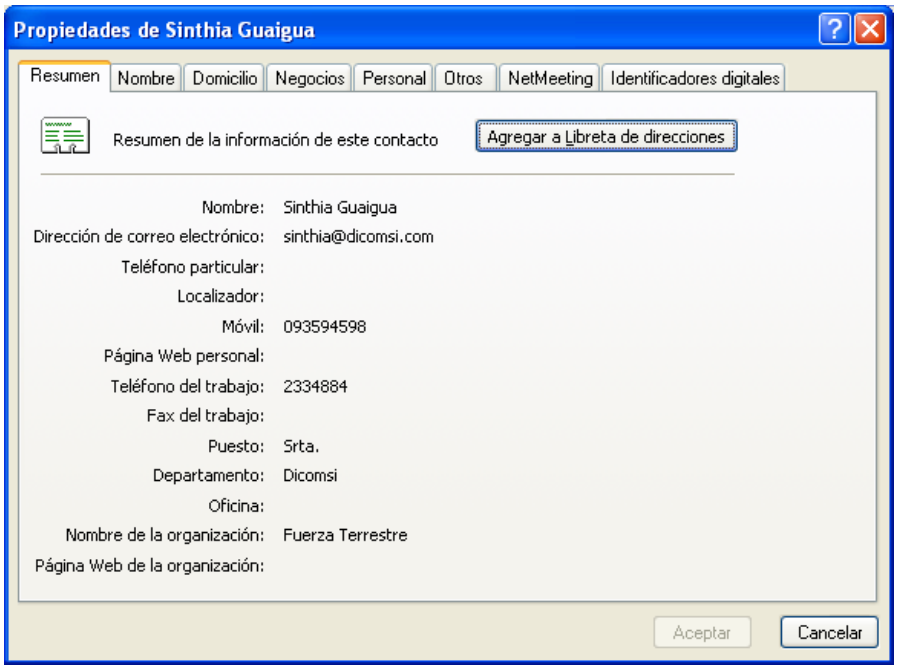
l. Pulsar el botón 'Buscar Personas’.

m. Seleccionar para la entrada 'Buscar en ' el servicio que hemos configurado en pasos anteriores, es decir 'LDAP de la Dicomsi'.

n. En este punto deberemos rellenar los campos



o. Listo se puede acceder a los datos del usuario y lo más importante a su certificado.



CAPÍTULO 6: CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES:

- Luego del análisis realizado sobre la información trasmitida por correo electrónico en la Fuerza Terrestre, se ha llegado a la conclusión que la información carece de confiabilidad porque no cumplen con las normas de seguridad necesarias, razón por la cual se requiere garantizar la información a través de comunicaciones electrónicas seguras, proporcionando medios de autenticidad, confidencialidad, no-repudio e integridad sobre la información transmitida, implementando certificados digitales.

- Para evitar las inconsistencias entre las distintas aplicaciones de software, por la implementación de certificados digitales se debe manejar un estándar internacional ampliamente reconocido denominado “X.509 v3” que establece en detalle la estructura de información que contendrán los certificados, y su formato.

- Los mensajes de correo necesitan de un protocolo de transmisión seguro que permita implementar mecanismos de seguridad, por esto hemos utilizado el protocolo S/MIME el cual nos permite realizar operaciones de firma digital y cifrado, dando un grado de seguridad elevado para la transmisión de datos a través de la red.

- Debido a que no existe una Autoridad Certificadora a nivel nacional, hemos creado una Autoridad Certificadora local la cual permitirá generar certificados digitales para las diferentes autoridades militares, esta va ha estar representada por la DICOMSI que es el Departamento encargado del manejo de todos los sistemas informáticos, que se encuentran en funcionamiento dentro del Ejercito Ecuatoriano.

6.2 RECOMENDACIONES:

- Para mayor seguridad y confiabilidad de los datos, es indispensable utilizar un sistema operativo Linux que permita el manejo de certificados digitales. Además se debe recalcar que los directorios que contengan los certificados digitales deben tener permisos de lectura y escritura solo para el administrador.

- El administrador de la certificados digitales debe ser una persona con conocimiento, experiencia y lo mas importante debe de ser de suma confianza, porque va ha emitir y revocar, certificados digitales a los usuarios, junto con sus respectivas claves.

- La autoridad certificadora creada en esta tesis, debe ser certificada a su vez por una autoridad certificadora reconocida.

  Pero para obtener este tipo de certificado se debe pedir la autorización del consejo nacional de telecomunicaciones, y cumplir ciertos requisitos expuestos en la Ley de comercio electrónico del Ecuador.

- La tecnología de certificados digitales ya viene incorporada en aplicaciones de correo electrónico usadas en Internet, como son Microsoft Outlook2000, Mozilla, los cuales permiten enviar e-mails firmados digitalmente, y transmitir e-mails cifrados. Para ello basta con tener previamente instalado un “certificado digital” .

- PGP, es un software gratuito que permite cifrar mensajes e implementar firmas digitales, que por sus características puede reemplazar fácilmente al software que actualmente se encuentra en funcionamiento dentro de la Fuerza Terrestre que es el SCS (sistema de correo seguro). PGP posee una red de confianza realizada por el mismo usuario. De esta forma cada usuario puede validar por si mismo las claves tanto privadas como públicas generadas con este software.

REFERENCIAS BIBLIOGRAFICAS

Libros:

[1] RAMIÓ, Jorge. Libro Electrónico de Seguridad Informática y Criptografía Versión 4.1. Sexta edición, 2006

[2] WESLEY, Addison. PKI - Concepts, Standards, Deployment and Considerations. Segunda edición, 2002.

[3] McGraw-Hill. RSA Security's Official Guide to Cryptography. Segunda edición, 2002.

[4] STALLINGS, William. Cryptography and Network Security Principles and Practices. Cuarta edición, 2005.

Internet:

[5] Documentación y foros.
www.kriptopolis.com

[6] Certificación Digital.
www.camerfirma.com

[7] Documentación y foros.
www.rediris.com

[8] Firma digital, 1999
http://www.criptored.upm.es/guiateoria/gt_m148e.htm

[9] Documentación
http://www. thawte.com

[10] Criptografía
http://www.criptored.upm.es/guiateoria/gt_m148k.htm

[11] Seguridad en Redes. Comunicaciones Encriptadas

http://www.criptored.upm.es/guiateoria/gt_m148m.htm

[12] Manipulación de certificados

http://www.dns.bdat.net/documentos/certificados_digitales/x249.html - 45k -

[13] Certificado Digitales con OpenSSL I

http://www.bulma.net/body.phtml?nIdNoticia=2280 - 48k

[14] Implementación de Servidores Implementación de Servidores

www.ine.gob.mx/csi/download/sistema_linux.pdf

ANEXOS

ANEXO A: GLOSARIO DE TÉRMINOS

A

Algoritmo (criptográfico) reglas matemáticas (lógicas) usadas en el proceso de cifrado y descifrado.

Algoritmo de Hash.- Son algoritmos que permiten verificar que un mensaje no ha sido modificado (integridad). Dado un mensaje de tamaño arbitrario, producen una salida de tamaño fijo.

Autenticación.- Es el proceso de verificar la identidad de una entidad (emisor o receptor).

C

CA (Autoridad Certificadora).- Es una entidad u organismo fiable que tiene la capacidad de emitir y garantizar la validez y la unicidad de los certificados que emite

firmándolos con su propia clave privada, asegurando de esta manera la integridad del vínculo existente entre una determinada clave y su propietario real.

Certificado (Certificado Digital).- Es un documento que contiene diversos datos, entre ellos el nombre de un usuario y su clave pública, y que es firmado por una Autoridad de Certificación (AC)."

Cifrar.- Operación de transformación de un mensaje en claro en un mensaje cifrado.

Criptografía asimétrica. - Es un criptosistema que utiliza dos tipos diferentes de claves una para cifrar y la otra para descifrar (clave publica, clave privada).

Criptografía Simétrico.- Es un criptosistema que usa la misma clave para cifrar y descifrar.

Clave privada (secreta).- La clave privada debe ser solo conocida por el creador.

Clave publica.- Es conocida públicamente, es usada en conjunto con una correspondiente clave privada.

Clave de sesión.- Es una clave de cifrado temporal, usada entre dos claves principales (publica, privada).

Criptoanálisis.- Arte y ciencia de romper mensajes cifrados, descubriendo la clave, el mensaje en claro o ambos.

Criptografía.- Arte y ciencia de conservar los mensajes seguros (ocultos), durante la transmisión a través de un canal inseguro entre dos entes (emisor, receptor).

Criptología.- Rama de la ciencia que comprende a la Criptografía y al Criptoanálisis.

Criptosistema.- Un criptosistema utiliza un algoritmo criptográfico para cifrar y descifrar los mensajes. Se trata, por tanto, de un sistema que implementa un algoritmo.

CRL.- (Lista de Revocación de Certificados).- Son un mecanismo mediante el cual la CA publica y distribuye información a cerca de los certificados anulados a las aplicaciones que los emplean.

Confidencialidad.- Solo los usuarios autorizados pueden acceder a la información.

D

Descifrar.- Operación de transformación de un mensaje cifrado en un mensaje en claro.

F

Firma Digital.- Es un mecanismo criptográfico que identifica a una persona o cosa, cifra con la clave privada del firmante una muestra reducida, un resumen o hash de tamaño fijo e independiente del tamaño del mensaje a firmar, verificando así la integridad de los datos y la identidad de la persona que envía los datos.

Firma electrónica: es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

Firma electrónica avanzada: es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

Firma electrónica reconocida: es la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

Integridad.- Garantiza que los datos no han sido modificados, por una persona no autorizada) durante el proceso de transmisión de datos.

M

Mensaje.- Cualquier información, ya sea un archivo o una cadena de caracteres.

P

Permutación.- Es un reordenamiento de una colección de objetos. Diferentes ordenamientos.

PGP/MIME.-Es un estándar que provee privacidad y autenticación de corro a través del Internet.

PKCS. - Public Key Cryptography Standards. Conjunto de estándares de-facto sobre implementación de algoritmos de claves públicas.

PKI (Infraestructura de Clave Pública).- Conjunto de hardware, software, personas, políticas, y procedimientos necesarios para dotar a máquinas y usuarios de Certificados Digitales de Identidad, la administración de éstos, y dotar de la confianza que se necesita para los procesos de identificación y autenticación, así

como la administración de las claves públicas y privadas de los usuarios. **Repudiar.-** Se denomina así al hecho que el presunto autor desconozca el origen de un mensaje.

S

Servicio de seguridad.- Es un proceso que permite dar seguridad a los datos procesados y la información transferida de una organización.

SSL.- Es un sistema de seguridad desarrollado por Netscape, proporciona mecanismos para establecer una comunicación segura entre un cliente y un servidor.

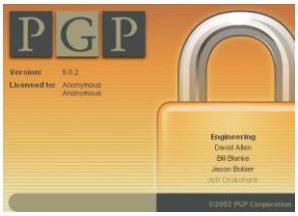
T

Telemática.- Integración de las comunicaciones con el cálculo automático o proceso de datos, produciendo nuevas aplicaciones o servicios para el tratamiento y distribución de la informática entre usuarios alejados.

Texto Cifrado.- Mensaje o documento cifrado

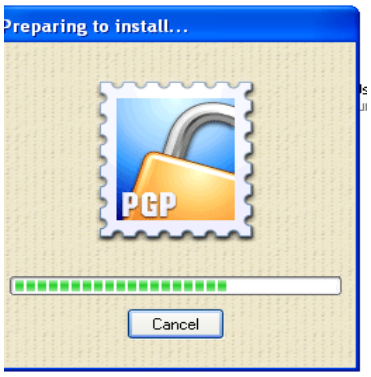
Texto en Claro.- Mensaje o documento original que va a ser objeto de cifrado.

ANEXO B: MANUAL DE PGP (PRETTY GOOD PRIVACY) VERSIÓN 8.2

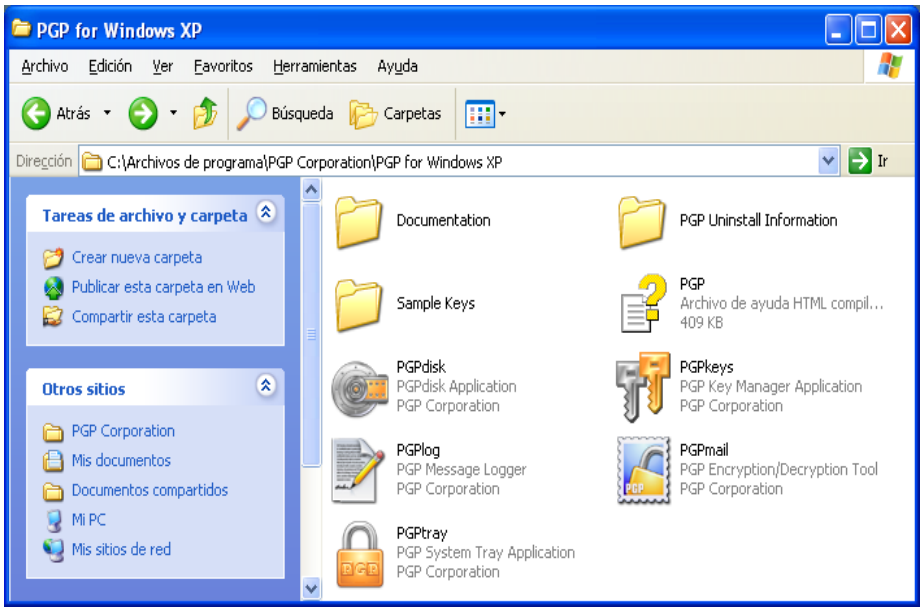


1. Instalación

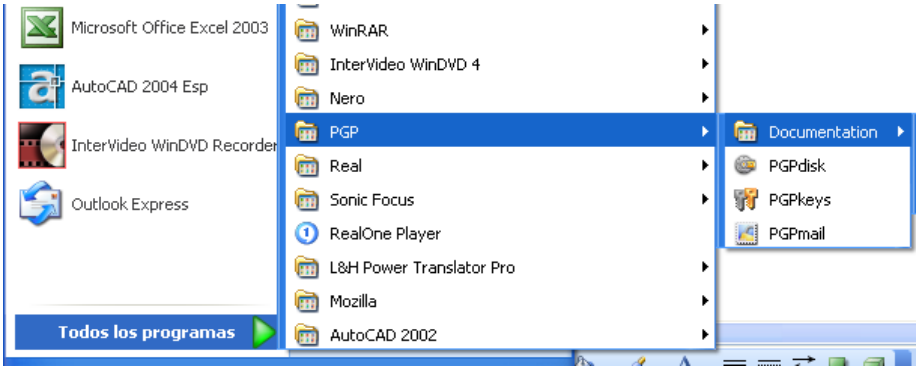
- Ejecutar el archivo Pgp8.exe



- El paquete se instala en la carpeta:

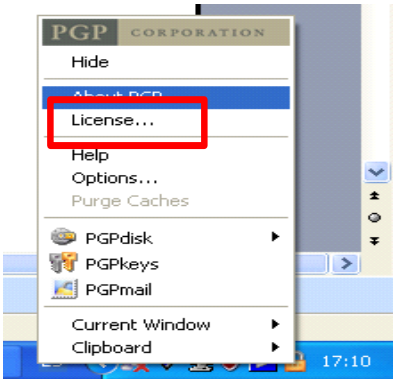


- Se puede acceder a PGP a través del menú inicio o a través de la barra de estado



- Activar la licencia

    i. Dar clic derecho sobre el candado de la barra de estado y seleccionar licencia



ii. Llenar las cajas de texto con los siguientes datos:

- **Name**: Anonymous
- **Organization:** Anonymous
- **License Number:** CUFH4-MQVQW-QEK6F-95QB0-ALPAF-AEA

iii. Dar clic en el botón manual y copiar y pegar el siguiente texto.

-----BEGIN PGP LICENSE AUTHORIZATION-----

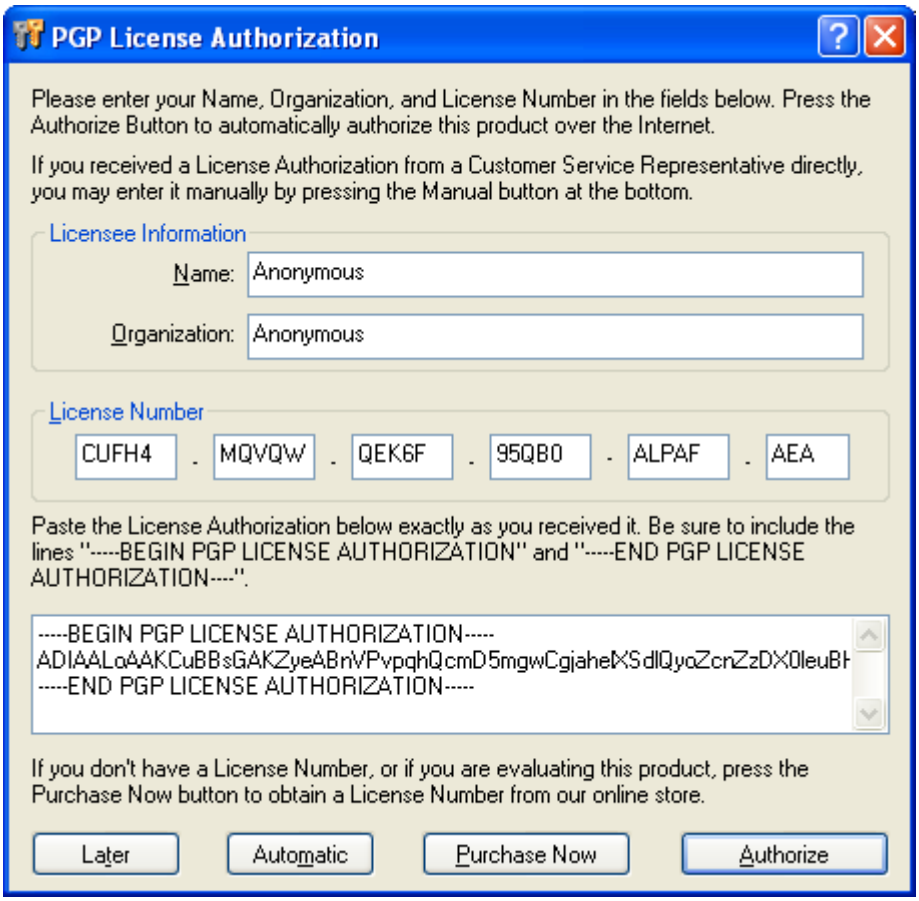
ADIAALoAAKCuBBsGAKZyeABnVPvpqhQcmD5mgwCgja

helXSdlQyoZcnZzDX0leuBHAA=

-----END PGP LICENSE AUTHORIZATION-----

iv. Dar clic en el botón "Authorize"

v. Completado el cuadro quedara de la siguiente manera.



NOTA: Con la activación de la licencia se pueden utilizar todas las opciones de PGP caso contrario negará el acceso a algunas de ellas.

2. FUNCIONAMIENTO

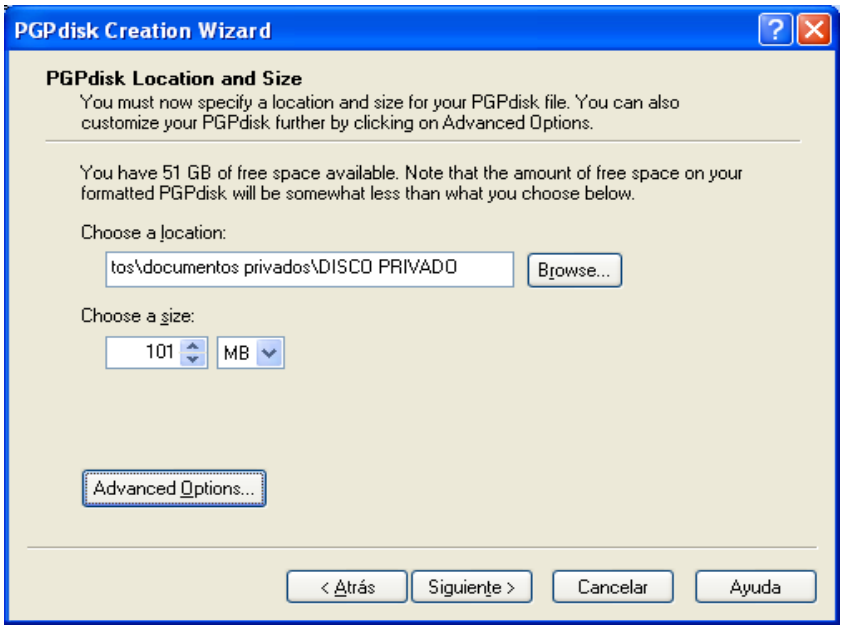
i. OPCIÓN PGPdisk

A diferencia de las anteriores versiones, la versión 8.02 viene con un software denominado PGPdisk, el cual permite montar una sección del disco como si se tratase de una unidad más en su PC. De esta forma toda la información que allí se almacene estará protegida por una clave.

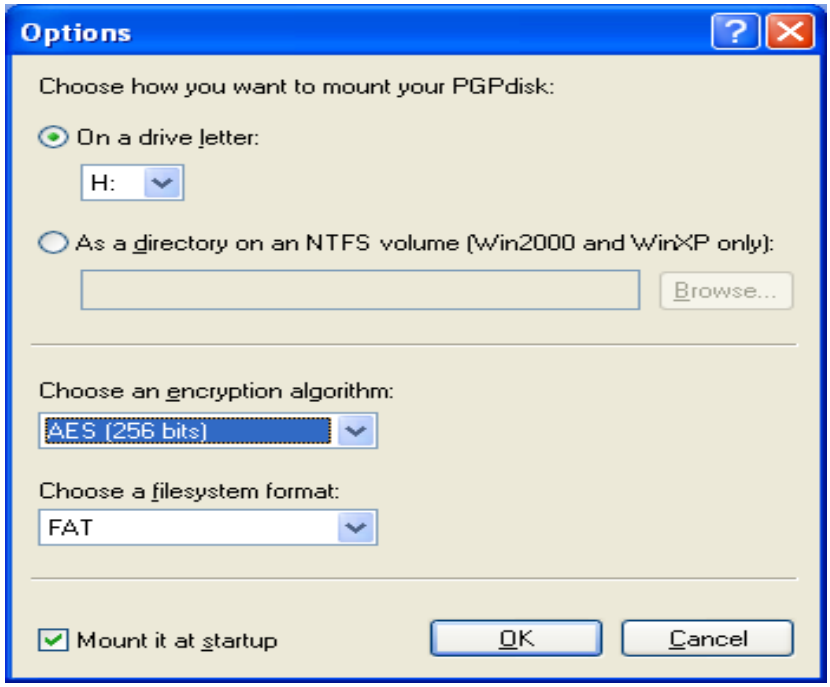
a) Crear un Nuevo volumen

- ✓ PGP → PGPdisk → New Disk

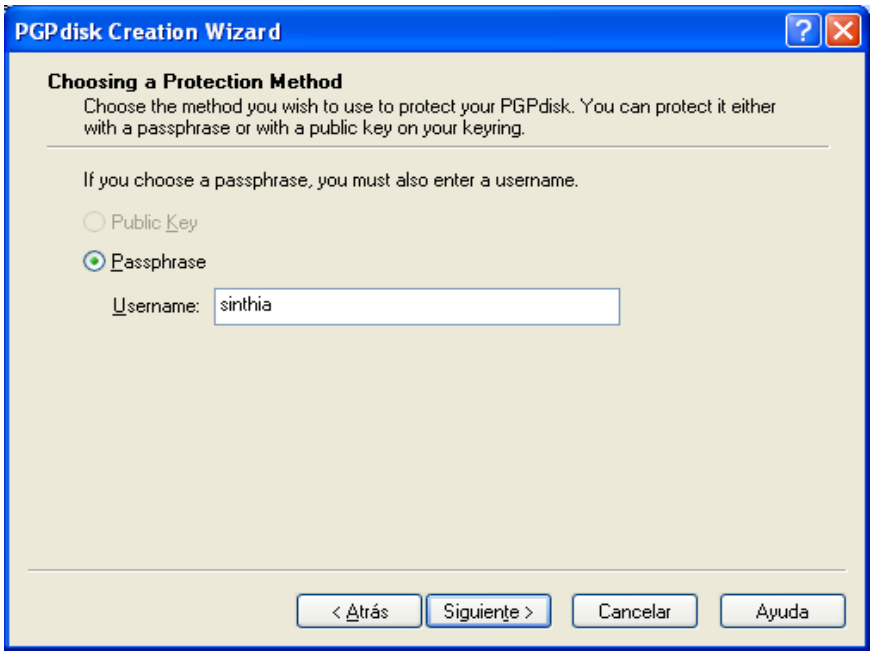
- ✓ Escogemos el lugar donde va ha estar el archivo pgd de nuestro disco, digitamos el tamaño (el tamaño es según al espacio libre de nuestro disco duro), escribimos el nombre del disco.



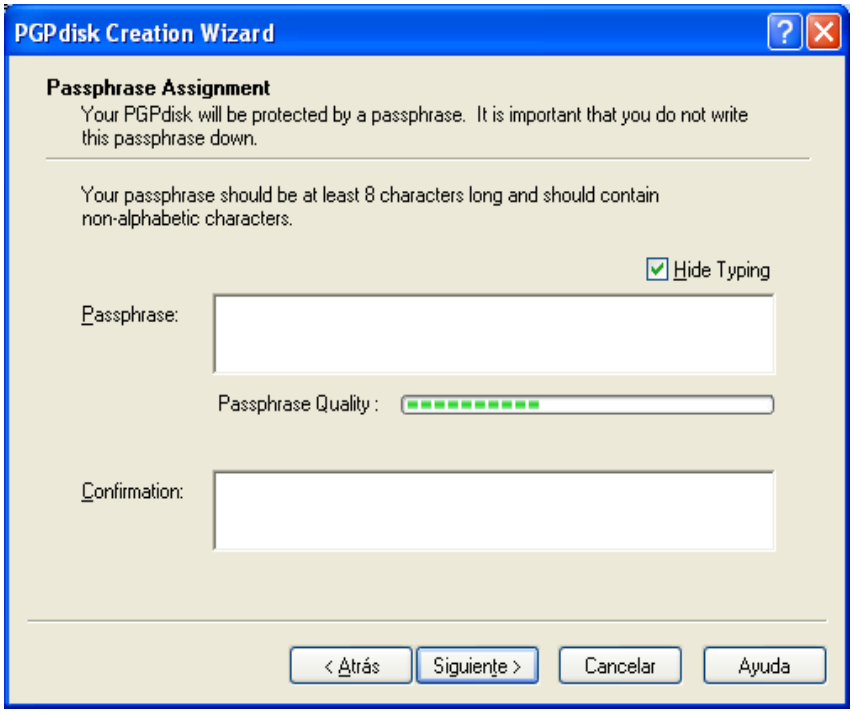
✓ Seleccionamos opciones para escoger el nombre de la unidad, el tipo de algoritmo de encriptación, y el formato de archivos. Damos clic en OK.

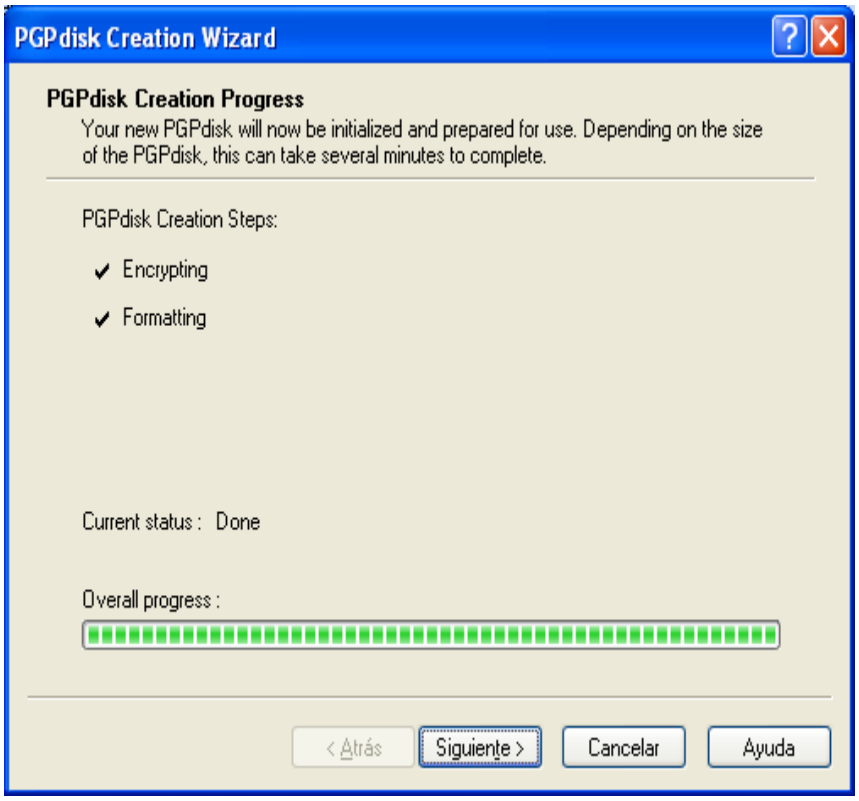


✓ Damos clic en siguiente y digitamos el username (nombre que el usuario escoja)

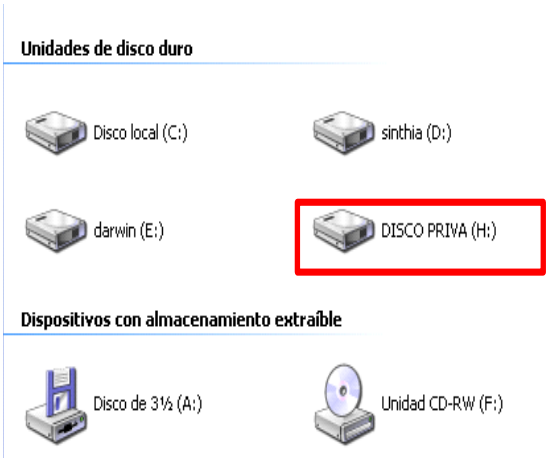


- ✓ Clic en siguiente y digitaremos la frase con la que se cifrará, luego clic en siguiente y comenzará la operación, por ultimo damos clic en finalizar.



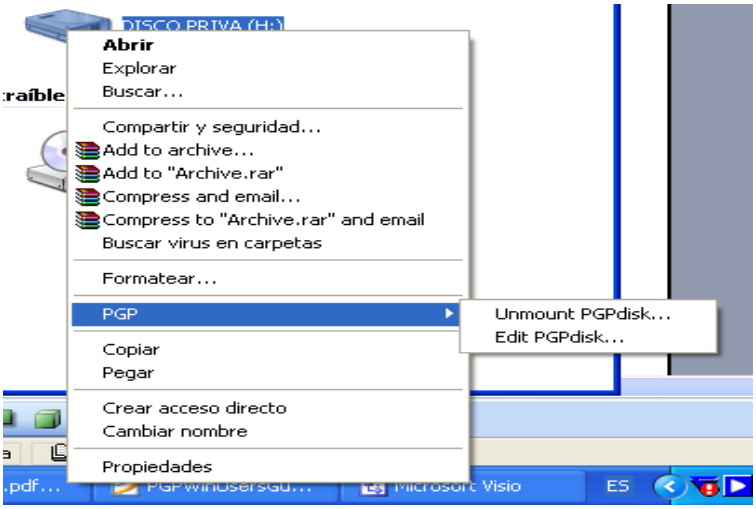


✓ Revisamos el archivo .pgd en la dirección seleccionada y verificamos el disco ingresando en Mi PC



b) Desmontar un disco

- ✓ Para desmontar damos clic derecho en la unidad y elegimos PGP→Unmount PGPdisk y listo.



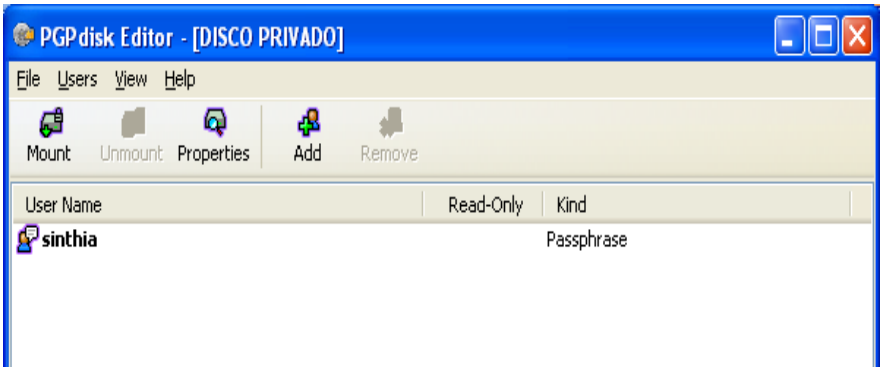
c) Montar un disco

- ✓ Damos clic derecho sobre el archivo –pgd y elegimos PGP→ mount PGPdisk, inmediatamente nos pedirá la passphrase.

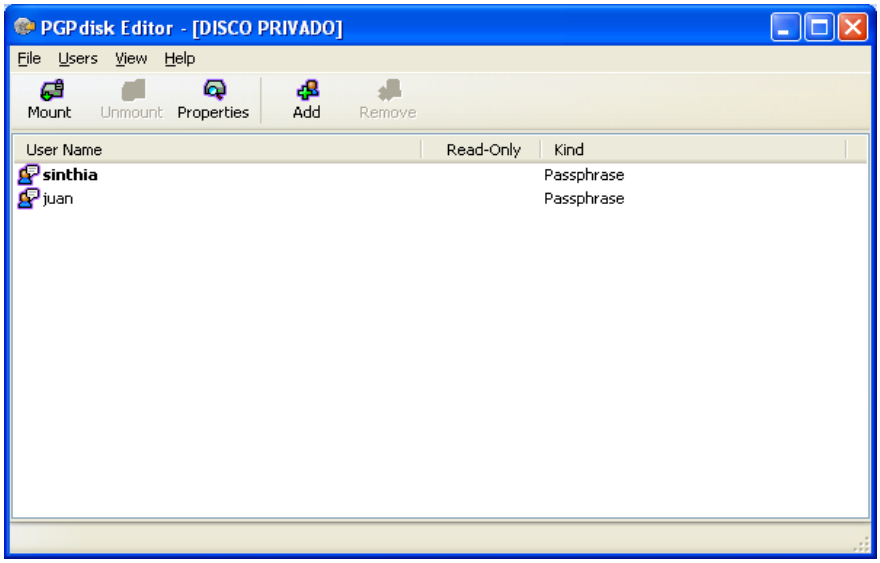
- ✓ Listo la unidad ya esta disponible en MI PC

d) Editar o modificar opciones del disco creado

- ✓ Damos clic derecho sobre el archivo –pgd y elegimos PGP→ Edit PGPdisk.



- ✓ Para añadir nuevos usuarios que puedan acceder a nuestro disco vamos ha Users→Add y escribimos nuestra passphrase y creamos nuestro nuevo usuario con su passphrase respectiva.

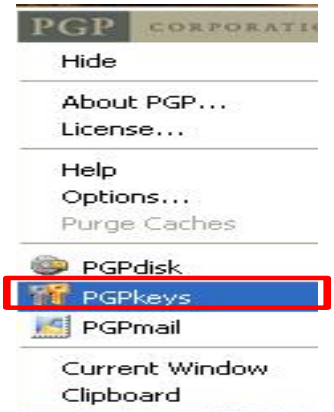


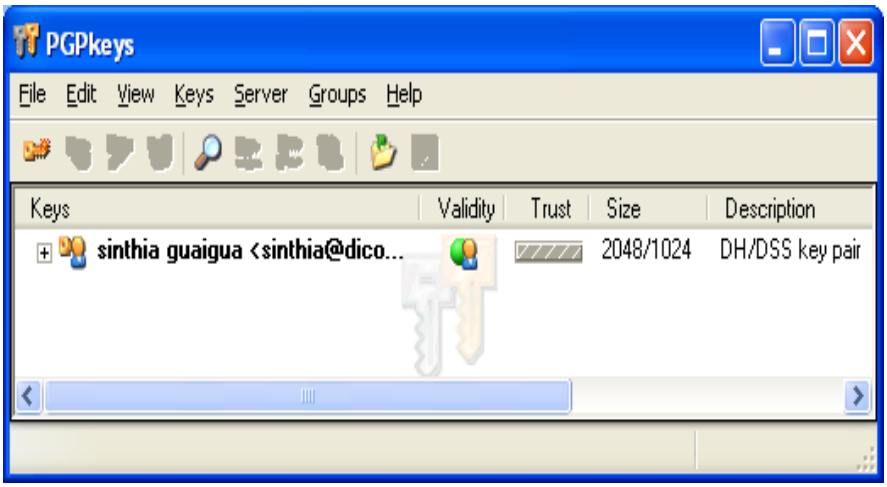
- ✓ Para cambiar las propiedades de encriptación o del lugar de almacenamiento damos clic en el icono Properties.

ii. OPCIÓN PGPkeys

Esta opción permite crear el par de claves conformadas por una clave privada a la que sólo usted tiene acceso y una clave pública que usted puede copiar y distribuir libremente a cualquiera con quien intercambie información.

La clave privada se utiliza para firmar los mensajes de correo electrónico y los archivos adjuntos que usted envía a otros y para descifrar los mensajes y archivos que ellos le envían a usted. A la inversa, usted utiliza las claves públicas de otros para enviarles correo electrónico cifrado y para verificar las firmas digitales de ellos.





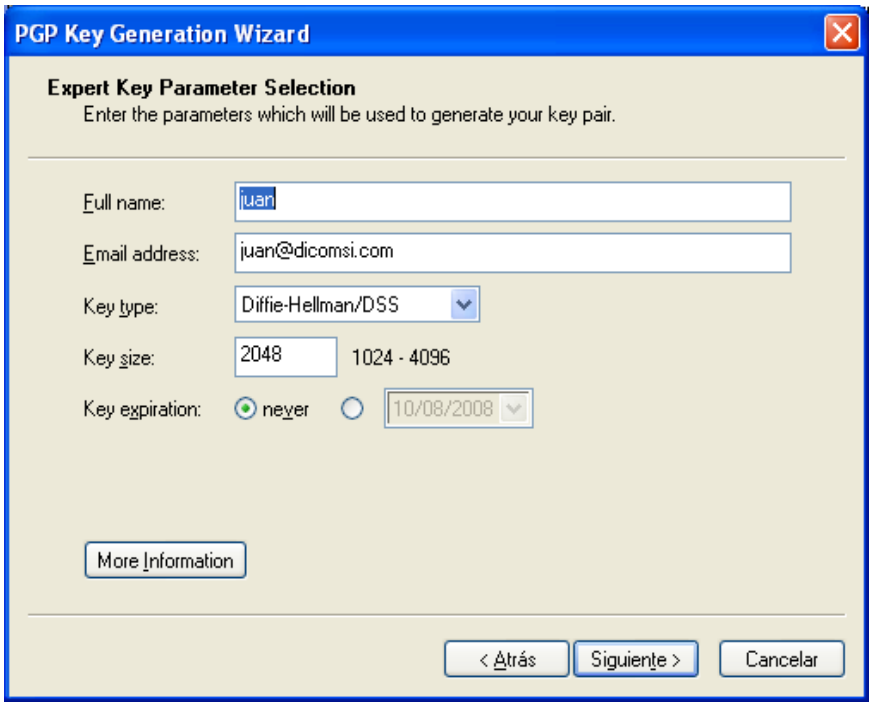
a) Crear nueva clave

- Escoger keys→ NewKey→ siguiente
- Dar clic en expert para poder escoger el algoritmo de cifrado y el tiempo de caducidad de la claves.

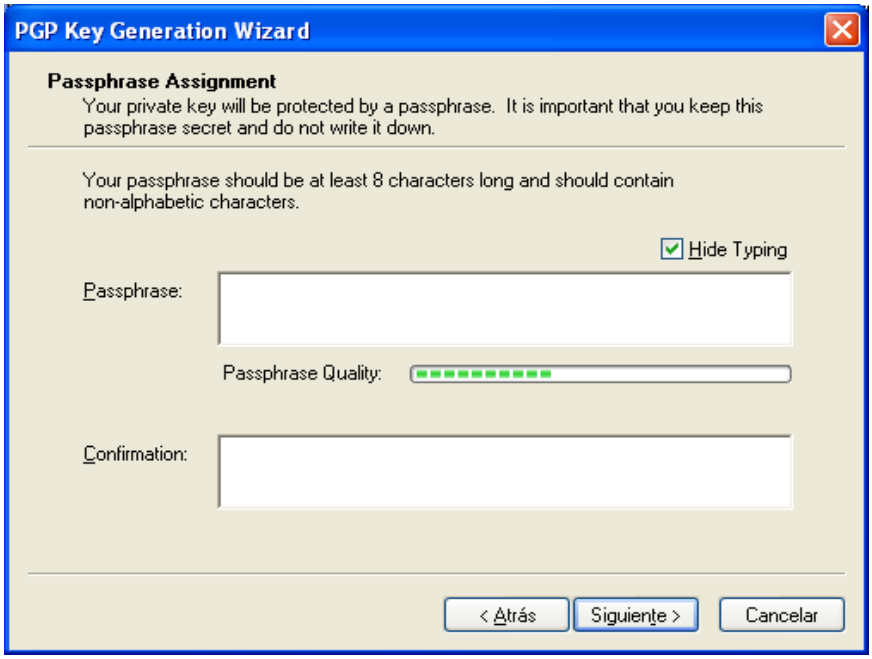
- Ingresar el nombre y la dirección de correo electrónico.

  No es estrictamente necesario que introduzca su nombre o su dirección de correo electrónico verdaderos. Sin embargo, utilizar su nombre verdadero facilita a otros el identificarle como el propietario de su clave.

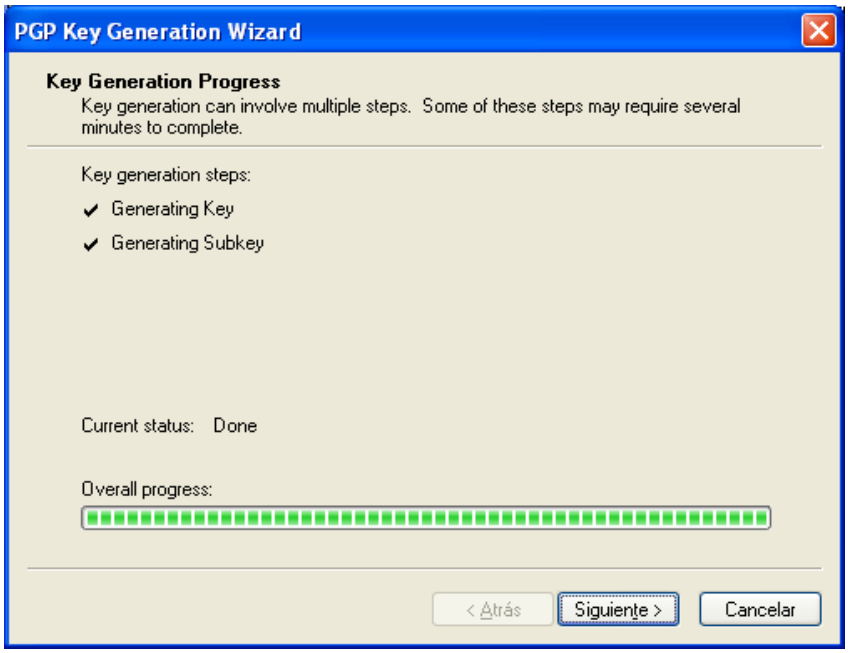
  Si se escoge Diffie-Hellman/DSS el tamaño de la clave esta entre 1024 a 4096 bits. Si es RSA de 1024 a 2048 bits. La fortaleza de una clave de firmar Diffie-Hellman/DSS de 1024 bits es aproximadamente equivalente a la de una clave RSA de 2048 bits.



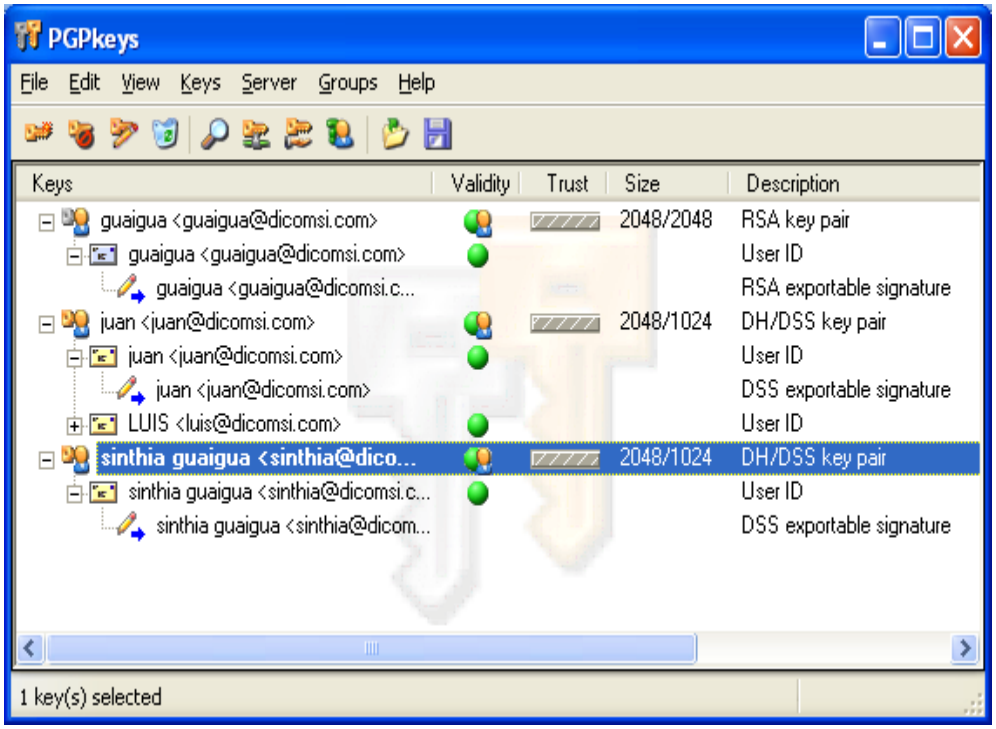
- El Asistente de Generación de Claves de PGP le pide que introduzca una contraseña (Passprhase). Esta contraseña se utiliza para mantener el acceso exclusivo a su clave privada.



- Haga clic en Siguiente para comenzar con el proceso de generación de claves, luego siguiente y por último finalizar.



- Aparecerá un par de claves representando sus nuevas claves creadas en la ventana de PGPkeys.



Algunos iconos utilizados con su respectivo significado:

ICONO	SIGNIFICADO
	Clave amarilla y un usuario representa a un par de claves Diffie-Hellman/DSS
	Clave gris y un usuario representa a un par de claves RSA
	Llave amarrilla representa una clave publica Diffie-Hellman/DSS
	Llave gris representa una clave publica RSA
	Una clave gris con una tarjeta representa una clave RSA en una smart card
	Una llave con un circulo rojo cruzado representa que la llave fue revocada
	Una llave con un reloj representa una clave ya expirada
	Un lápiz o una pluma indican la firma de los usuarios de PGP que han certificado la autenticidad de la clave
	Una firma cruzada con una línea roja indica una firma revocada.
	Un lápiz opaco indica una firma incorrecta o no válida.
	Una firma con una flecha azul próxima a ella indica que es exportable.
	Indica un certificado X509 correcto
	Indica un certificado X509 tiempo expirado

	Indica un certificado X509 revocado o no valido
	Un círculo vacío indica que la clave no es válida.
	Un círculo relleno indica que la clave es válida (verde) o que tiene una ADK (rojo).
	Una barra vacía indica una clave no válida o un usuario no fiable.
	Una barra medio llena indica una clave marginalmente válida o un usuario marginalmente fiable.
	Una barra completa indica una clave completamente válida o un usuario completamente fiable.

b) Guardar una copia de claves.

Es importante guardar copias de seguridad de las clave en cualquier lugar que desee.

- Cuando se cierra la aplicación PGPkeys nos permite guardar las claves en un lugar predeterminado por nosotros, pero este paso es opcional.

iii. PUBLICAR LAS CLAVES PUBLICAS

Después de crear sus claves, usted tiene que hacerlas accesibles a otros para que le puedan enviar correo electrónico cifrado y verificar su firma digital.

Tiene tres alternativas para distribuir su clave pública:

- Hacer su clave pública disponible a través de un servidor de claves públicas.
- Incluir su clave pública en un mensaje de correo electrónico.
- Exportar su clave pública o copiarla en un archivo de texto.

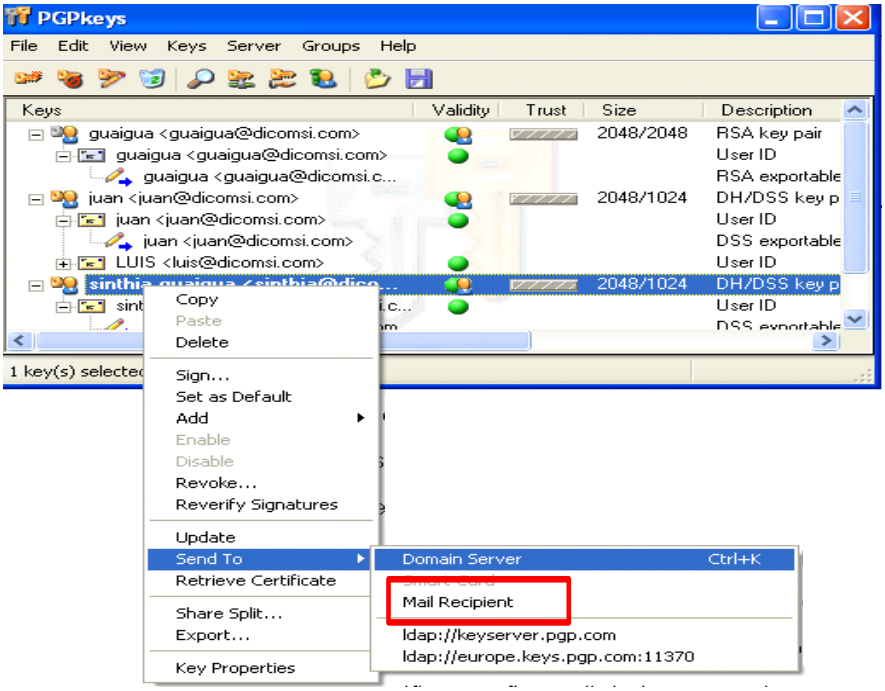
a) Para enviar su clave pública a un servidor de claves públicas

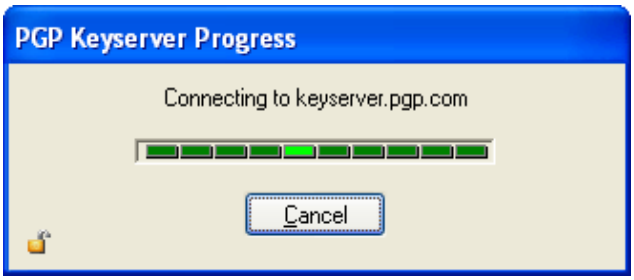
✓ Conéctese a Internet.

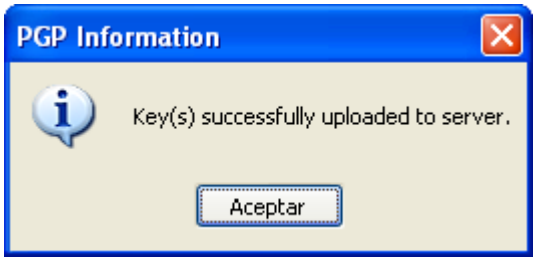
✓ Abra la ventana PGPkeys.

✓ Seleccione el icono que representa la clave pública que usted quiere mandar al servidor de claves.

✓ Escoja por Dominio en el submenú Enviar a Servidor del menú Claves.

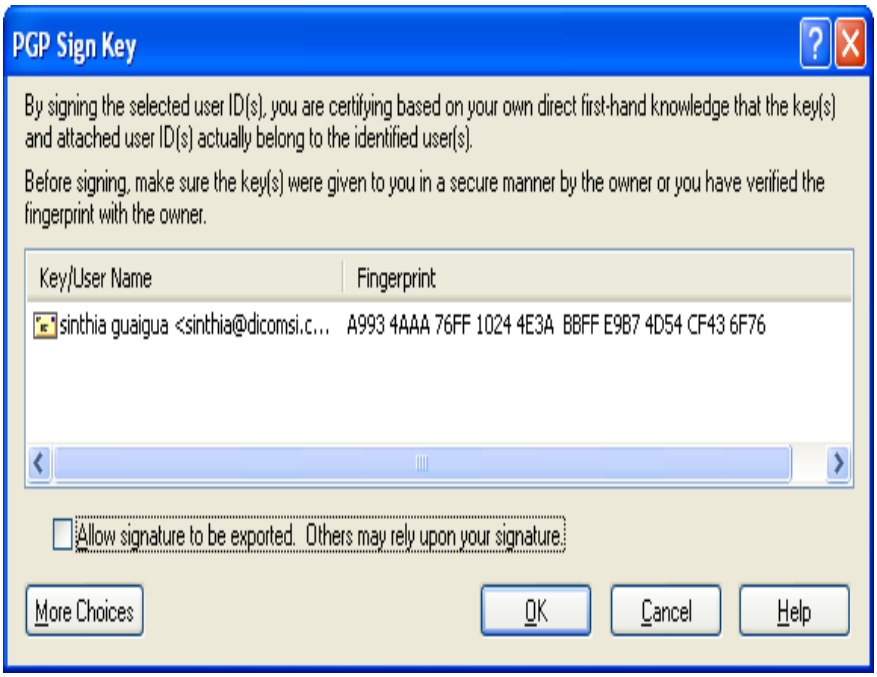




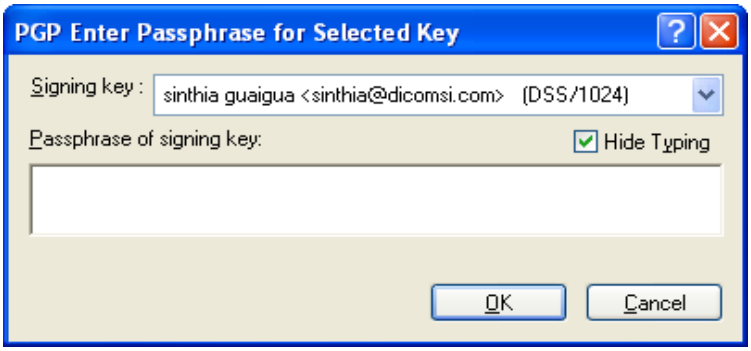


b) **Incluir su clave pública en un mensaje de correo** electrónico

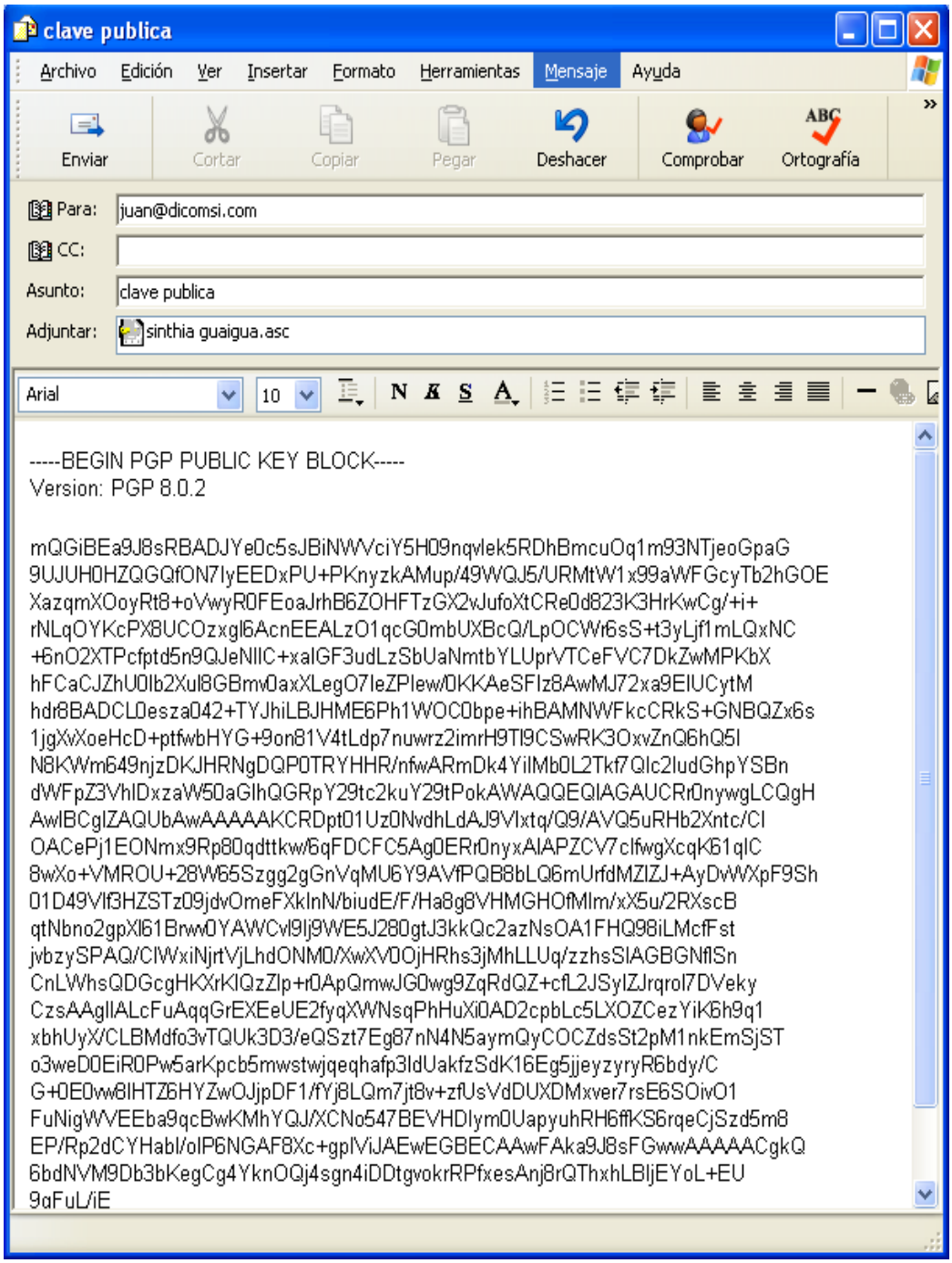
- ✓ Abra la ventana PGPkeys.
- ✓ Cuando envíe a alguien su clave pública, asegúrese de firmar el correo electrónico. De ese modo, el destinatario puede verificar su firma y estar seguro de que nadie ha alterado la información por el camino.
- ✓ Seleccione su par de claves, clic derecho y escoger firmar (sign)



- ✓ Escriba el passprhase de su clave privada y luego clic en OK



- ✓ Seleccione su par de claves y después escoja copiar en el menú Edición.
- ✓ Abra el editor que usted utiliza para componer sus mensajes de correo electrónico, coloque el cursor en el área deseada, y después escoja Pegar.

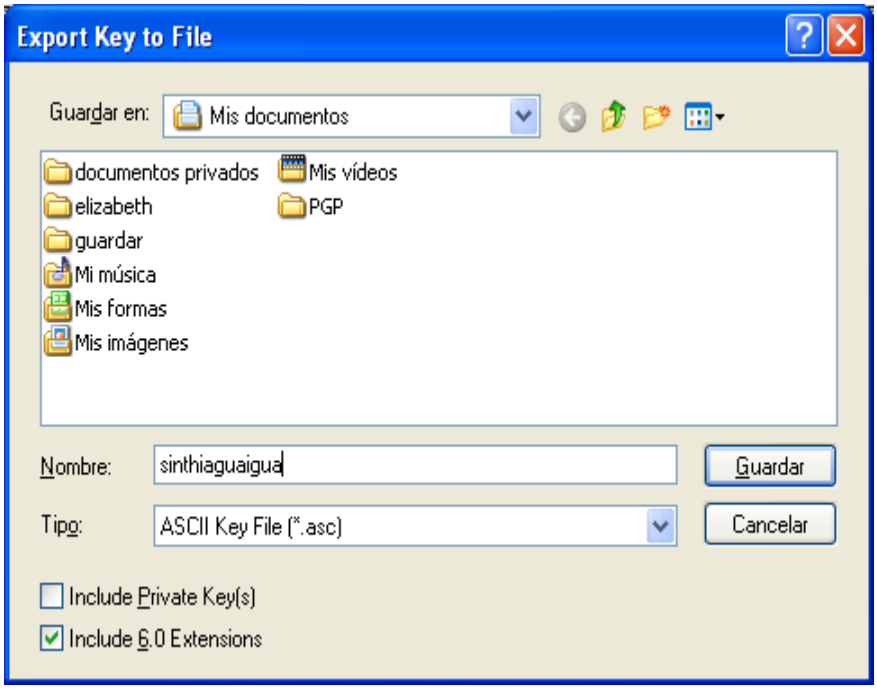


- ✓ Envíe el correo

c) Exportar su clave pública a un archivo

- ✓ Seleccione el icono que representa su par de claves en la ventana PGPkeys, después escoja Exportar en el menú

Claves e introduzca el nombre y posición del archivo donde quiere que se guarde la clave.



✓ Listo revisar el archivo

iv. OBTENER LAS CLAVES PÚBLICAS DE OTROS

Al igual que usted tiene que distribuir su clave pública a aquellos que quieren enviarle correo cifrado o verificar su firma digital, usted tiene que obtener las claves públicas de otros para poder enviarles correo cifrado o verificar las firmas digitales de ellos. Tiene tres alternativas para obtener la clave pública de alguien**.**

- Conseguir la clave en un servidor de claves públicas.

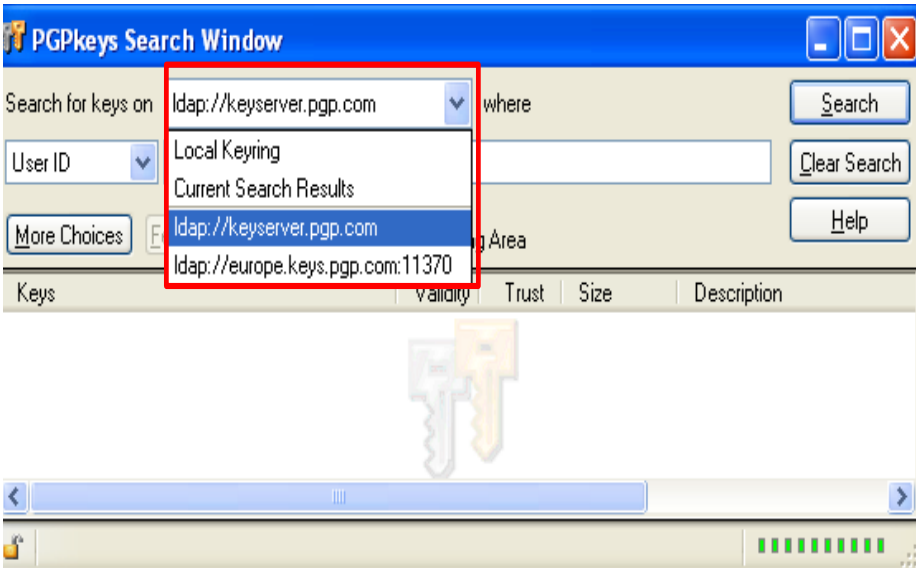
- Añadir la clave pública directamente desde un mensaje de correo electrónico.
- Importar la clave pública desde un archivo.

a) Conseguir la clave en un servidor de claves públicas

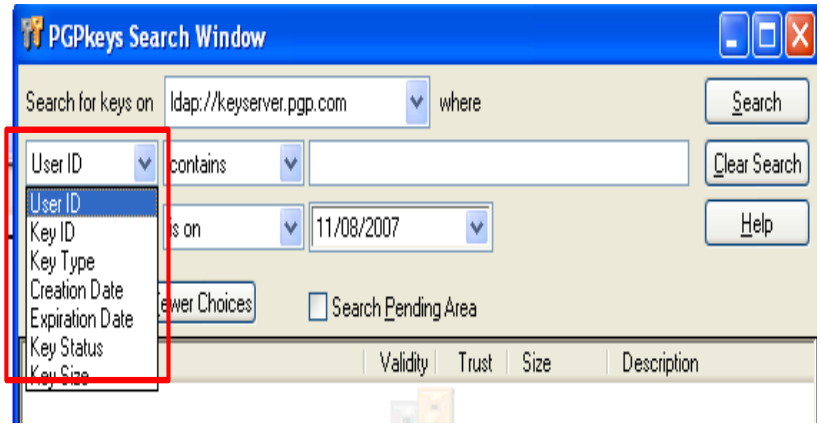
✓ Conectarse al Internet

✓ Abra la aplicación PGPkeys y escoja Buscar en Servidor en el menú Claves.

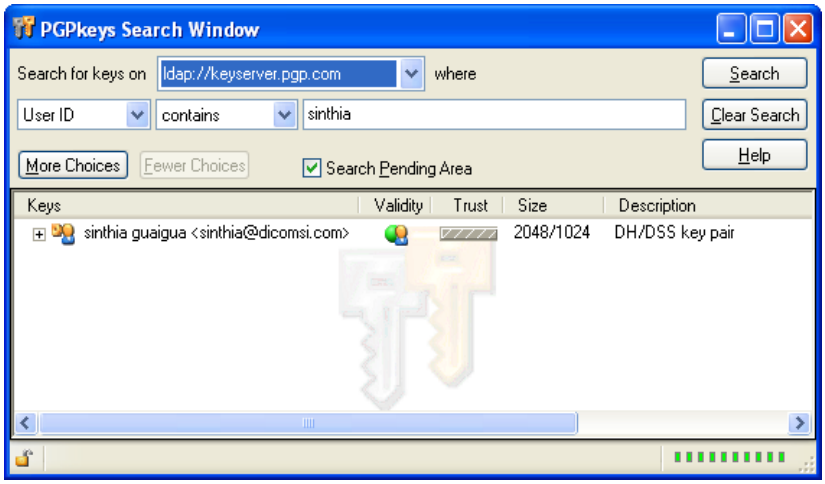
✓ Seleccione la localización del servidor en el que quiere buscar en el menú Buscar Claves.



✓ Introduzca criterios de búsqueda para localizar la clave pública del usuario. Para limitar su búsqueda, haga clic en Más Opciones para especificar criterios adicionales.

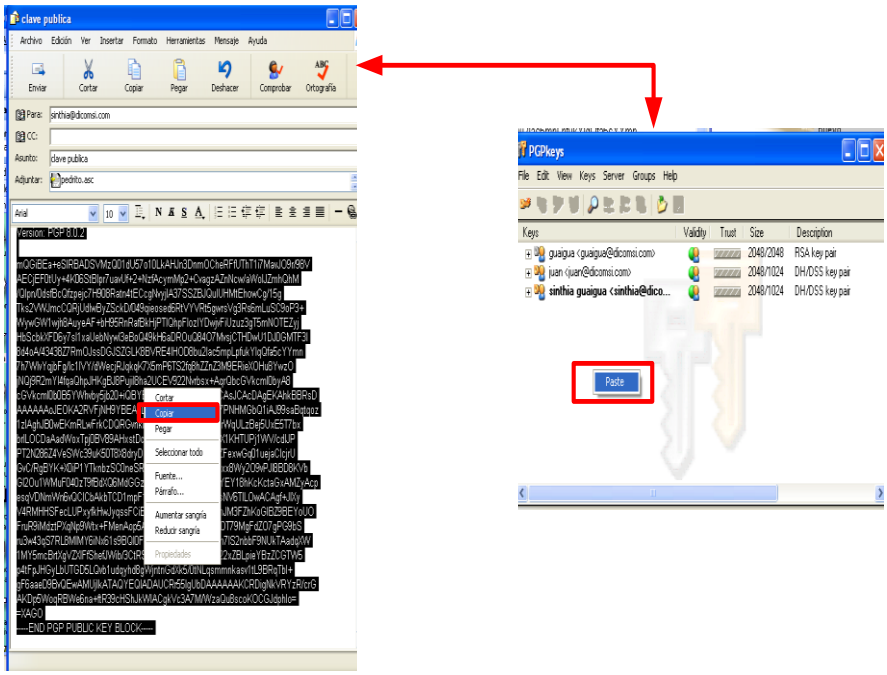


✓ Si se encuentra la clave pública del usuario especificado, se le pregunta si quiere añadirla a su archivo de claves públicas. Cuando usted añade una clave pública a su archivo de claves, la clave se muestra en la ventana PGPkeys, donde puede examinarla para asegurarse de que es válida.



b) Añadir la clave pública directamente desde un mensaje de correo electrónico

De la aplicación de correo se puede añadir la clave pública al archivo de claves copiando el bloque de texto que representa la clave pública y pegándolo en la ventana PGPkeys.



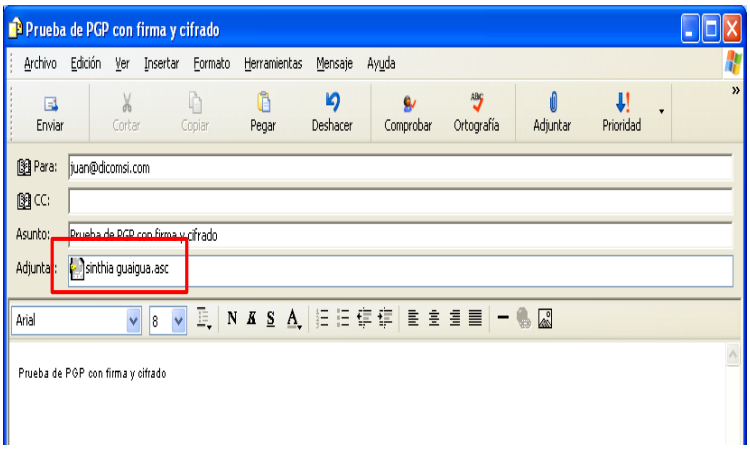
c) Importar la clave pública desde un archivo

Escoja Importar en el menú Claves y después introduzca el nombre del archivo donde se encuentra la clave pública.

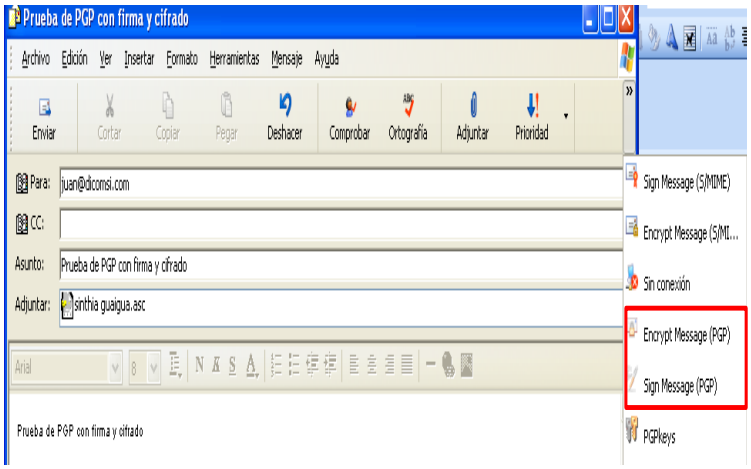
Arrastre el archivo que contiene la clave pública sobre la ventana PGPkeys.

v. CIFRAR Y FIRMAR MEDIANTE APLICACIONES DE CORREO ELECTRÓNICO SOPORTADAS POR PGP

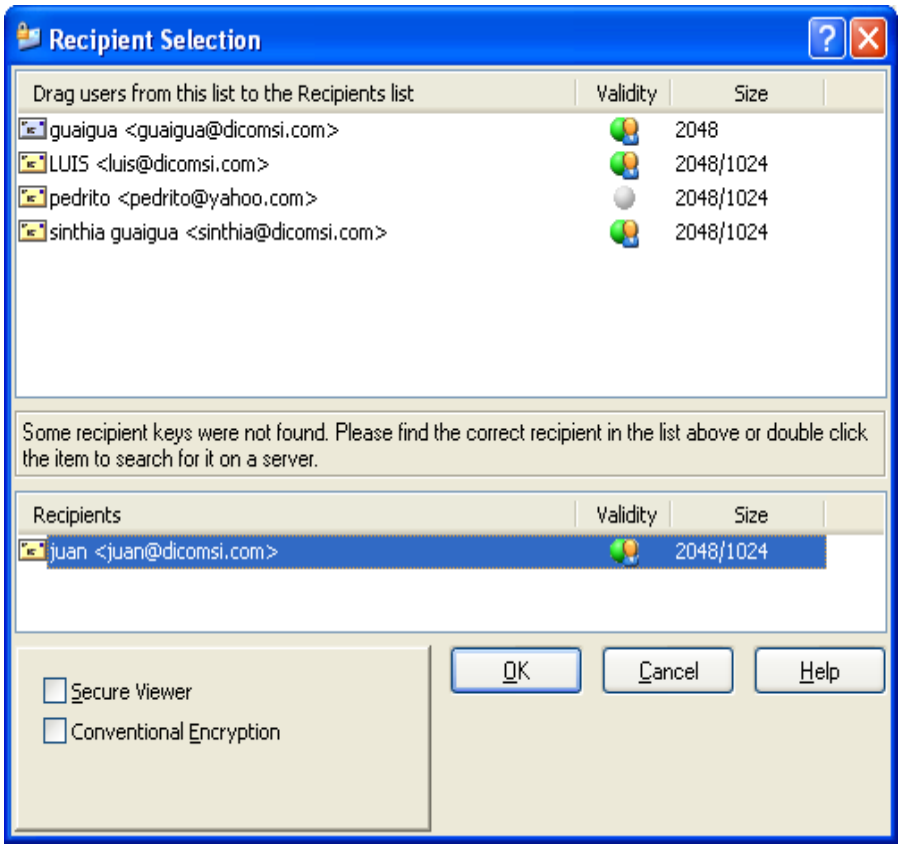
a) Adjuntamos nuestra clave pública al mensaje para que nuestro receptor pueda descifrar el mensaje firmado.



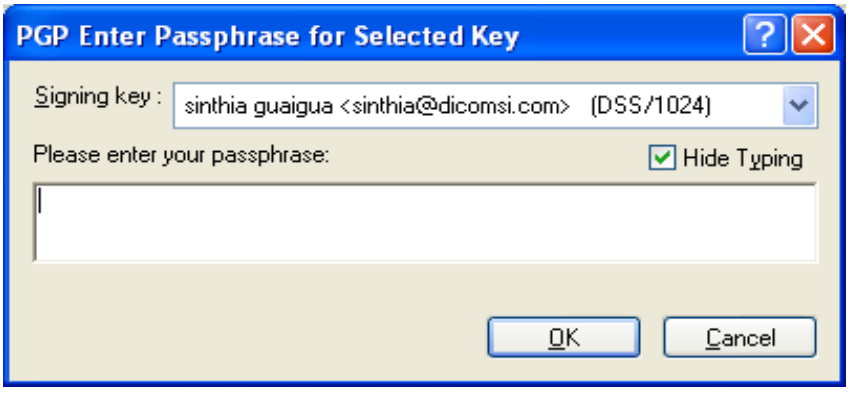
b) Escogemos la opción firmar y cifrar con PGP



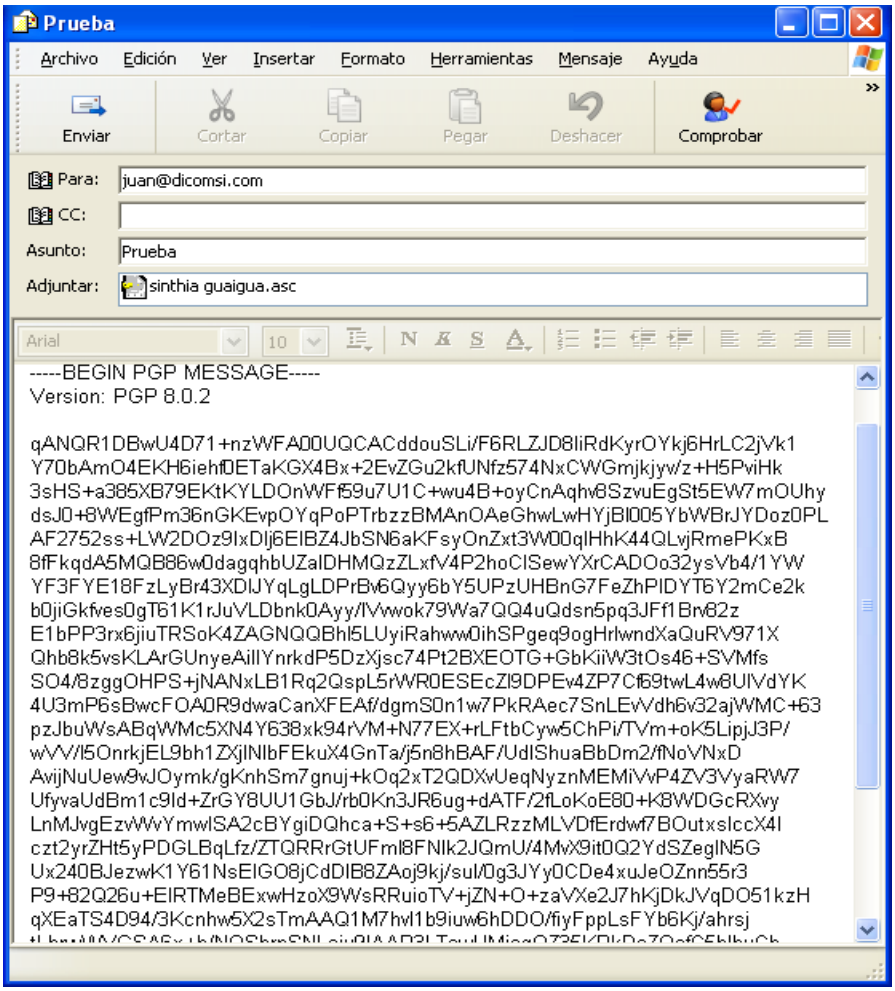
c) Con la opción cifrar, debemos escoger certificado de nuestros receptores. En el ejemplo vamos a enviar cifrado el mensaje a JUAN por lo tanto escogemos el certificado de JUAN.



d) Con la opción firmar nos pedirá el pasphrase de nuestra clave privada.

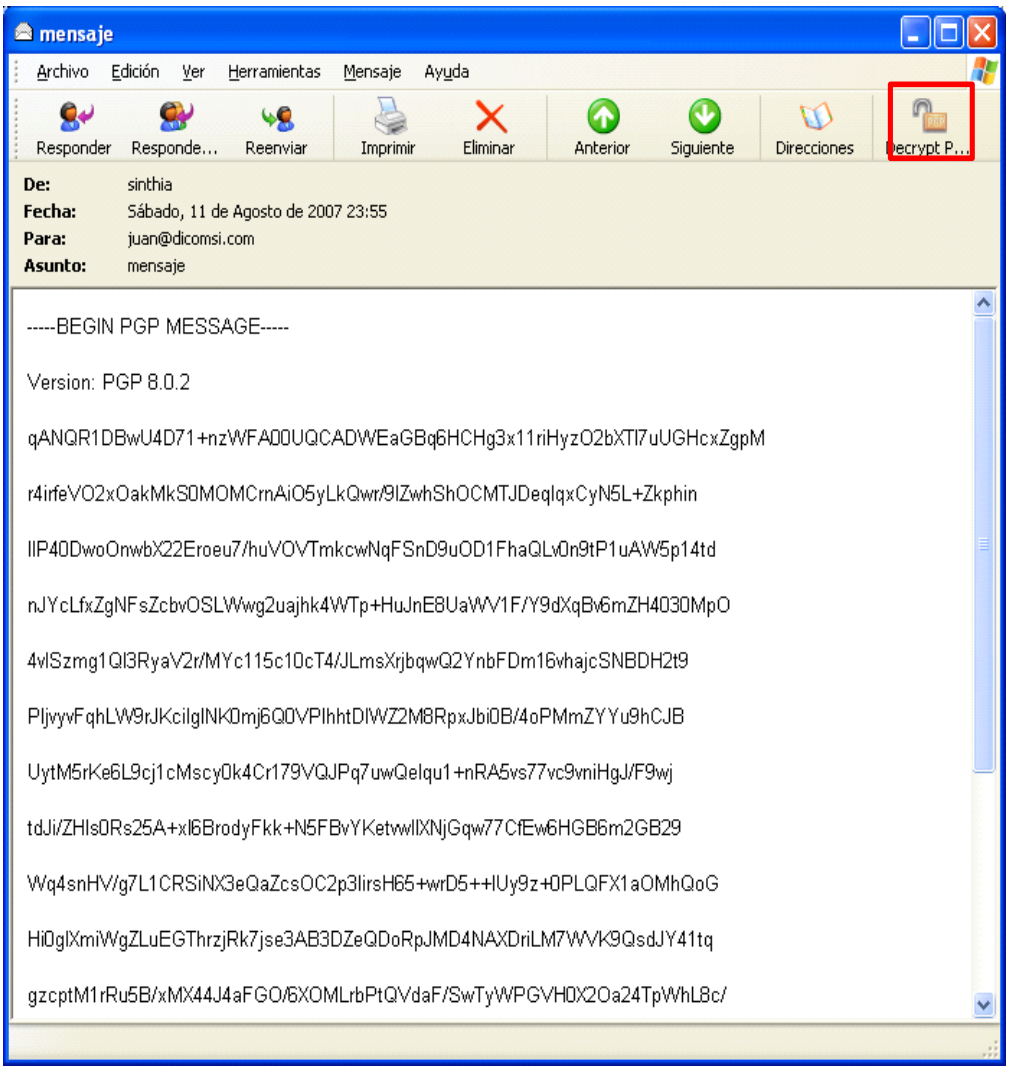


e) El mensaje se ha cifrado y firmado. Para finalizar pulsamos enviar.



vi. DESCIFRAR Y VERIFICAR DESDE APLICACIONES DE CORREO ELECTRÓNICO SOPORTADAS POR PGP

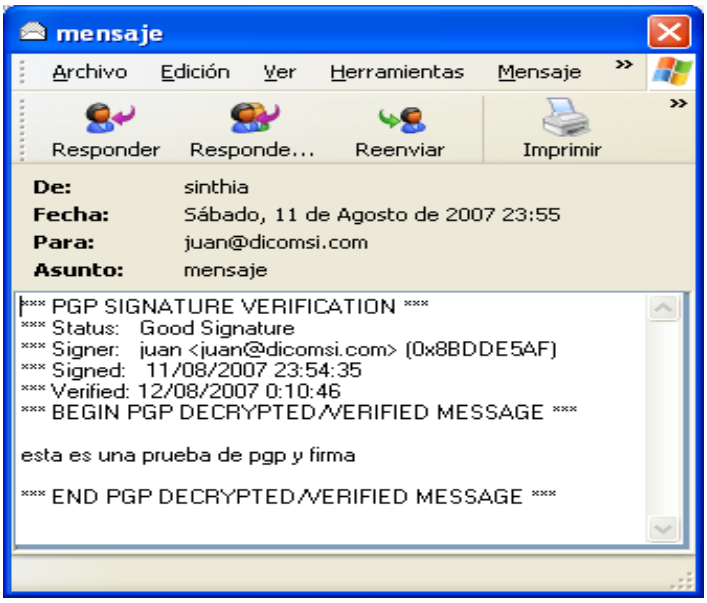
a) Abra su mensaje de correo electrónico. Verá un bloque de texto cifrado totalmente incomprensible en el cuerpo de su mensaje de correo electrónico.



b) Para descifrar y verificar el contenido de este mensaje de correo electrónico, haga clic sobre el botón Decript PGP.

c) Escribir el passphrase de nuestra clave secreta para descifrar el mensaje.

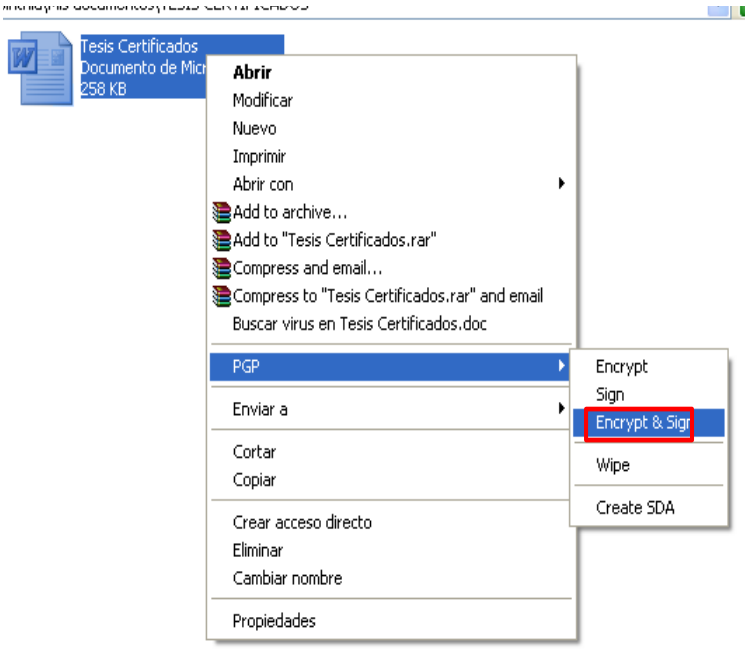
d) Listo el mensaje ya esta descifrado y se ha verificado la validez de la firma.



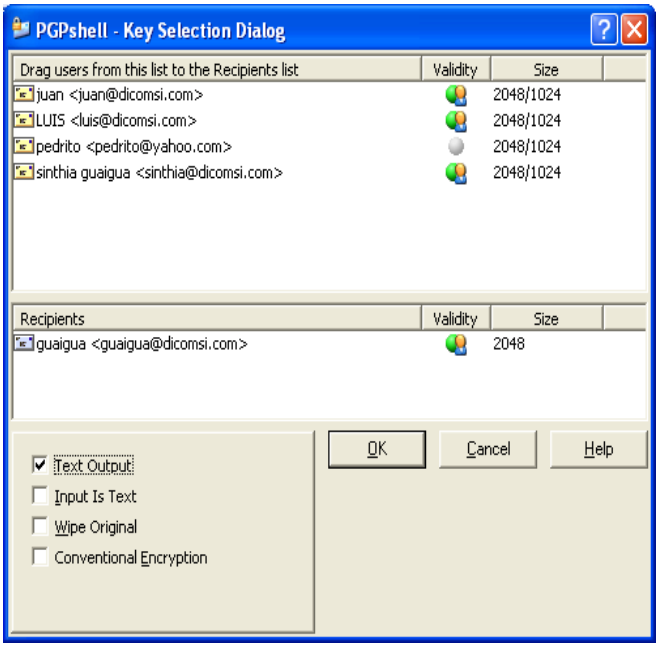
vii. ALMACENAMIENTO SEGURO DE ARCHIVOS

a) Cifrar y firmar archivos

- ✓ Seleccione el archivo o archivos que quiera cifrar, firmar, o cifrar y firmar, dar clic derecho.
- ✓ Escoja la opción deseada desde el PGPmenu. En este ejemplo seleccionaremos cifrar y firmar el archivo “Tesis Certificados”



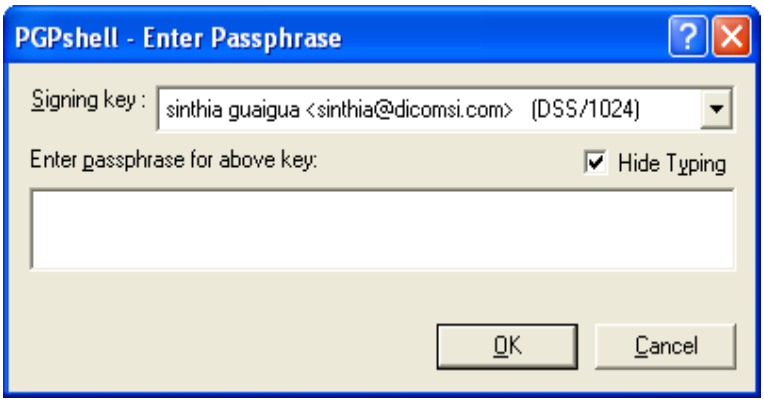
✓ Aparecerá la caja de diálogo de Selección de Claves de PGP en la que puede seleccionar las claves públicas de los destinatarios del archivo que está cifrando o firmando y luego dar clic en OK.



Dispone de las siguientes opciones de cifrado:

- Text Output (Salida a Texto).- Cuando envíe archivos adjuntos con alguna aplicación de correo electrónico, es posible que necesite seleccionar la opción Salida a Texto a fin de guardar el archivo como texto ASCII. Esto es necesario a veces cuando se envían archivos binarios utilizando aplicaciones de correo electrónico antiguas. Al seleccionar esta opción se aumenta el tamaño del archivo alrededor de un 30%.
- Convencional Encryption (Cifrado Convencional) Seleccione esta opción para utilizar una contraseña común en lugar de criptografía por clave pública. El archivo se cifrará utilizando una clave que cifra mediante una contraseña escogida por usted.
- Wipe Original (Destruir Original).- Seleccione esta opción para sobreescribir el documento que está cifrando o firmando, de forma que la información delicada no pueda ser leída por nadie que tenga acceso a su disco duro.

✓ Si ha firmado los archivos, se le pedirá que proporcione su contraseña.



- ✓ Si mira en la carpeta donde se encontraba el archivo original, encontrará un archivo con el mismo nombre seguido de un sufijo que indica el tipo de cifrado representado con uno de estos tres iconos:

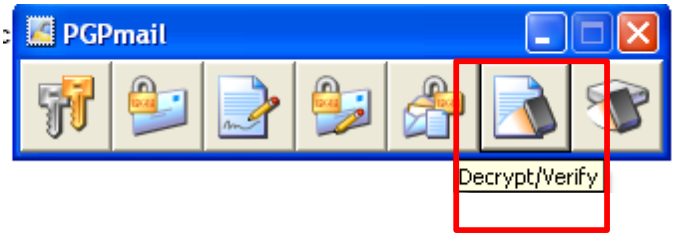
b) Cifrar y firmar utilizando la opción PGPmail

- ✓ Seleccione el archivo a ser cifrado y firmado y arrástrelo a la opción que desee (firmar, cifrar, firmar y cifrar).

- ✓ Siga los pasos ya realizados en la parte anterior.

c) Descifrar y verificar archivos

- ✓ Seleccione el archivo arrástrelo hacia la opción Descifrar/Verificar.



- ✓ Para descifrar debemos escribir el passphrase de la clave privada del receptor, en este ejemplo la clave de "guaigua".

- ✓ Indicamos el lugar donde guardar el archivo
- ✓ Listo el archivo ya se ha descifrado y se ha verificado la valides de la clave del emisor.


PGPlog
Name
Signer
Key ID
Validity
Signed
Tesis Certificados...
juan <juan@dicomsi.com>
0x8BDDE5AF
12/08/2007 22:02:25

ANEXO C: LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS DEL ECUADOR, Y SU REGLAMENTO.

República del Ecuador.

LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS DEL ECUADOR, Y SU REGLAMENTO.

Publicación hecha por:
NMC Research Cía. Ltda.
http://www.nmcresearch.com

Ley No. 67. R.O. Suplemento 557 de 17 de abril del 2002.

El H. CONGRESO NACIONAL

Considerando:

Que el uso de sistemas de información y de redes electrónicas, incluida la internet, ha adquirido importancia para el desarrollo del comercio y la producción, permitiendo la realización y concreción de múltiples negocios de trascendental importancia, tanto para el sector público como para el sector privado;

Que es necesario impulsar el acceso de la población a los servicios electrónicos que se generan por y a través de diferentes medios electrónicos;

Que se debe generalizar la utilización de servicios de redes de información e internet, de modo que éstos se conviertan en un medio para el desarrollo del comercio, la educación y la cultura;

Que a través del servicio de redes electrónicas, incluida la internet, se establecen relaciones económicas y de comercio, y se realizan actos y contratos de carácter civil y mercantil que es necesario normarlos, regularlos y controlarlos, mediante la expedición de una ley especializada sobre la materia;

Que es indispensable que el Estado Ecuatoriano cuente con herramientas jurídicas que le permitan el uso de los servicios electrónicos, incluido el comercio electrónico y acceder con mayor facilidad a la cada vez más compleja red de los negocios internacionales; y,

En ejercicio de sus atribuciones, expide la siguiente:

LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS

TÍTULO PRELIMINAR

Art. 1.- Objeto de la ley.- Esta ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

CAPÍTULO I

PRINCIPIOS GENERALES

Art. 2.- Reconocimiento jurídico de los mensajes de datos.- Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta ley y su reglamento.

Art. 3.- Incorporación por remisión.- Se reconoce validez jurídica a la información no contenida directamente en un mensaje de datos, siempre que figure en el mismo, en forma de remisión o de anexo accesible mediante un enlace electrónico directo y su contenido sea conocido y aceptado expresamente por las partes.

Art. 4.- Propiedad intelectual.- Los mensajes de datos estarán sometidos a las leyes, reglamentos y acuerdos internacionales relativos a la propiedad intelectual.

Art. 5.- Confidencialidad y reserva.- Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta ley y demás normas que rigen la materia.

Art. 6.- Información escrita.- Cuando la ley requiera u obligue que la información conste por escrito, este requisito quedará cumplido con un mensaje de datos, siempre que la información que este contenga sea accesible para su posterior consulta.

Art. 7.- Información original.- Cuando la ley requiera u obligue que la información sea presentada o conservada en su forma original, este requisito quedará cumplido con un mensaje de datos, si siendo requerido conforme a la ley, puede comprobarse que ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos.

Se considera que un mensaje de datos permanece integro, si se mantiene completo e inalterable su contenido, salvo algún cambio de forma, propio del proceso de comunicación, archivo o presentación.

Por acuerdo de las partes y cumpliendo con todas las obligaciones previstas en esta ley, se podrán desmaterializar los documentos que por ley deban ser instrumentados físicamente.

Los documentos desmaterializados deberán contener las firmas electrónicas correspondientes debidamente certificadas ante una de las entidades autorizadas según lo dispuesto en el artículo 29 de la presente ley, y deberán ser conservados conforme a lo establecido en el artículo siguiente.

Art. 8.- Conservación de los mensajes de datos.- Toda información sometida a esta ley, podrá ser conservada; este requisito quedará cumplido mediante el archivo del mensaje de datos, siempre que se reúnan las siguientes condiciones:

a) Que la información que contenga sea accesible para su posterior consulta;

b) Que sea conservado con el formato en el que se haya generado, enviado o recibido, o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida;
c) Que se conserve todo dato que permita determinar el origen, el destino del mensaje, la fecha y hora en que fue creado, generado, procesado, enviado, recibido y archivado; y,
d) Que se garantice su integridad por el tiempo que se establezca en el reglamento a esta ley.

Toda persona podrá cumplir con la conservación de mensajes de datos, usando los servicios de terceros, siempre que se cumplan las condiciones mencionadas en este artículo.

La información que tenga por única finalidad facilitar el envío o recepción del mensaje de datos, no será obligatorio el cumplimiento de lo establecido en los literales anteriores.

Art. 9.- Protección de datos.- Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.

No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.

Art. 10.- Procedencia e identidad de un mensaje de datos.- Salvo prueba en contrario se entenderá que un mensaje de datos proviene de quien lo envía y, autoriza a quien lo recibe, para actuar conforme al contenido del mismo, cuando de su verificación exista concordancia entre la identificación del emisor y su firma electrónica, excepto en los siguientes casos:

a) Si se hubiere dado aviso que el mensaje de datos no proviene de quien consta como emisor; en este caso, el aviso se lo hará antes de que la persona que lo recibe actúe conforme a dicho mensaje. En caso contrario, quien conste como emisor deberá justificar plenamente que el mensaje de datos no se inició por orden suya o que el mismo fue alterado; y,
b) Si el destinatario no hubiere efectuado diligentemente las verificaciones correspondientes o hizo caso omiso de su resultado.

Art. 11.- Envío y recepción de los mensajes de datos.- Salvo pacto en contrario, se presumirá que el tiempo y lugar de emisión y recepción del mensaje de datos, son los siguientes:

a) Momento de emisión del mensaje de datos.- Cuando el mensaje de datos ingrese al sistema de información o red electrónica que no esté bajo control del emisor o de la persona que envió el mensaje en nombre de éste o del dispositivo electrónico autorizado para el efecto;
b) Momento de recepción del mensaje de datos.- Cuando el mensaje de datos ingrese al sistema de información o red electrónica señalado por el destinatario. Si el destinatario designa otro sistema de información o red electrónica, el momento de recepción se presumirá aquel en que se produzca la recuperación del mensaje de datos. De no haberse señalado un lugar preciso de recepción, se entenderá que ésta ocurre cuando el mensaje de datos ingresa a un sistema de información o red electrónica del destinatario, independientemente de haberse recuperado o no el mensaje de datos; y,
c) Lugares de envío y recepción.- Los acordados por las partes, sus domicilios legales o los que consten en el certificado de firma electrónica, del emisor y del destinatario. Si no se los pudiere establecer por estos medios, se tendrán por tales, el lugar de trabajo, o donde desarrollen el giro principal de sus actividades o la actividad relacionada con el mensaje de datos.

Art. 12.- Duplicación del mensaje de datos.- Cada mensaje de datos será considerado diferente. En caso de duda, las partes pedirán la confirmación del nuevo mensaje y tendrán la obligación de verificar técnicamente la autenticidad del mismo.

TÍTULO II

DE LAS FIRMAS ELECTRÓNICAS, CERTIFICADOS DE FIRMA ELECTRÓNICA, ENTIDADES DE CERTIFICACIÓN DE INFORMACIÓN, ORGANISMOS DE PROMOCIÓN DE LOS SERVICIOS ELECTRÓNICOS, Y DE REGULACIÓN Y CONTROL DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS

CAPÍTULO I

DE LAS FIRMAS ELECTRÓNICAS

Art. 13.- Firma electrónica.- Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos.

Art. 14.- Efectos de la firma electrónica.- La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba enjuicio.

Art. 15.- Requisitos de la firma electrónica.- Para su validez, la firma electrónica reunirá los siguientes requisitos, sin perjuicio de los que puedan establecerse por acuerdo entre las partes:

a) Ser individual y estar vinculada exclusivamente a su titular;
b) Que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta ley y sus reglamentos;
c) Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado;
d) Que al momento de creación de la firma electrónica, los datos con los que se creare se hallen bajo control exclusivo del signatario, y,
e) Que la firma sea controlada por la persona a quien pertenece.

Art. 16.- La firma electrónica en un mensaje de datos.- Cuando se fijare la firma electrónica en un mensaje de datos, aquélla deberá enviarse en un mismo acto como parte integrante del mensaje de datos o lógicamente asociada a éste. Se presumirá legalmente que el mensaje de datos firmado electrónicamente conlleva la voluntad del emisor, quien se someterá al cumplimiento de las obligaciones contenidas, en dicho mensaje de datos, de acuerdo a lo determinado en la ley.

Art. 17.- Obligaciones del titular de la firma electrónica.- El titular de la firma electrónica deberá:

a) Cumplir con las obligaciones derivadas del uso de la firma electrónica;
b) Actuar con la debida diligencia y tomar las medidas de seguridad necesarias, para mantener la firma electrónica bajo su estricto control y evitar toda utilización no autorizada;
c) Notificar por cualquier medio a las personas vinculadas, cuando exista el riesgo de que su firma sea controlada por terceros no autorizados y utilizada indebidamente;
d) Verificar la exactitud de sus declaraciones;
e) Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización,

salvo que el destinatario conociere de la inseguridad de la firma electrónica o no hubiere actuado con la debida diligencia;
f) Notificar a la entidad de certificación de información los riesgos sobre su firma y solicitar oportunamente la cancelación de los certificados; y,
g) Las demás señaladas en la ley y sus reglamentos.

Art. 18.- Duración de la firma electrónica.- Las firmas electrónicas tendrán duración indefinida. Podrán ser revocadas, anuladas o suspendidas de conformidad con lo que el reglamento a esta ley señale.

Art. 19.- Extinción de la firma electrónica.- La firma electrónica se extinguirá por:

a) Voluntad de su titular;
b) Fallecimiento o incapacidad de su titular;
c) Disolución o liquidación de la persona jurídica, titular de la firma; y,
d) Por causa judicialmente declarada.

La extinción de la firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso.

CAPÍTULO II

DE LOS CERTIFICADOS DE FIRMA ELECTRÓNICA

Art. 20.- Certificado de firma electrónica.- Es el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad.

Art. 21.- Uso el certificado de firma electrónica.- El certificado de firma electrónica se empleará para certificar la identidad del titular de una firma electrónica y para otros usos, de acuerdo a esta ley y su reglamento.

Art. 22. - Requisitos del certificado de firma electrónica.- El certificado de firma electrónica para ser considerado válido contendrá los siguientes requisitos:

a) Identificación de la entidad de certificación de información;
b) Domicilio legal de la entidad de certificación de información;
c) Los datos del titular del certificado que permitan su ubicación e identificación;
d) El método de verificación de la firma del titular del certificado;
e) Las fechas de emisión y expiración del certificado;
f) El número único de serie que identifica el certificado;
g) La firma electrónica de la entidad de certificación de información;
h) Las limitaciones o restricciones para los usos del certificado; e,
i) Los demás señalados en esta ley y los reglamentos.

Art. 23.- Duración del certificado de firma electrónica.- Salvo acuerdo contractual, el plazo de validez de los certificados de firma electrónica será el establecido en el reglamento a esta ley.

Art. 24.- Extinción del certificado de firma electrónica.- Los certificados de firma electrónica, se extinguen, por las siguientes causas:

a) Solicitud de su titular;
b) Extinción de la firma electrónica, de conformidad con lo establecido en el artículo 19 de esta ley; y,
c) Expiración del plazo de validez del certificado de firma electrónica.

La extinción del certificado de firma electrónica se producirá desde el momento de su comunicación a la entidad de certificación de información, excepto en el caso de fallecimiento del titular de la firma electrónica, en cuyo caso se extingue a partir de que acaece el fallecimiento. Tratándose de personas secuestradas o desaparecidas, se extingue a partir de que se denuncie ante las autoridades competentes tal secuestro o desaparición. La extinción del certificado de firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso.

Art. 25.- Suspensión del certificado de firma electrónica.- La entidad de certificación de información podrá suspender temporalmente el certificado de firma electrónica cuando:

a) Sea dispuesto por el Consejo Nacional de Telecomunicaciones, de conformidad con lo previsto en esta ley;
b) Se compruebe por parte de la entidad de certificación de información, falsedad en los datos consignados por el titular del certificado; y,
c) Se produzca el incumplimiento del contrato celebrado entre la entidad de certificación de información y el titular de la firma electrónica.

La suspensión temporal dispuesta por la entidad de certificación de información deberá ser inmediatamente notificada al titular del certificado y al organismo de control, dicha notificación deberá señalar las causas de la suspensión.

La entidad de certificación de información deberá levantar la suspensión temporal una vez desvanecidas las causas que la originaron, o cuando mediare resolución del Consejo Nacional de Telecomunicaciones, en cuyo caso, la entidad de certificación de información está en la obligación de habilitar de inmediato el certificado de firma electrónica.

Art. 26.- Revocatoria del certificado de firma electrónica.- El certificado de firma electrónica podrá ser revocado por el Consejo Nacional de Telecomunicaciones, de conformidad con lo previsto en esta ley, cuando:

a) La entidad de certificación de información cese en sus actividades y los certificados vigentes no sean asumidos por otra entidad de certificación; y,
b) Se produzca la quiebra técnica de la entidad de certificación judicialmente declarada.

La revocatoria y sus causas deberán ser inmediatamente notificadas al titular del certificado.

Art. 27.- Tanto la suspensión temporal, como la revocatoria, surtirán efectos desde el momento de su comunicación con relación a su titular; y, respecto de terceros, desde el momento de su publicación que deberá efectuarse en la forma que se establezca en el respectivo reglamento, y no eximen al titular del certificado de firma electrónica, de las obligaciones previamente contraídas derivadas de su uso.

La entidad de certificación de información será responsable por los perjuicios que ocasionare la falta de comunicación, de publicación o su retraso.

Art. 28.- Reconocimiento internacional de certificados de firma electrónica.- Los certificados electrónicos emitidos por entidades de certificación extranjeras, que cumplieren con los requisitos señalados en esta ley y presenten un grado de fiabilidad equivalente, tendrán el mismo valor legal que los certificados acreditados, expedidos en el Ecuador. El Consejo Nacional de Telecomunicaciones dictará el reglamento correspondiente para la aplicación de este artículo.

Las firmas electrónicas creadas en el extranjero, para el reconocimiento de su validez en el Ecuador se someterán a lo previsto en esta ley y su reglamento.

Cuando las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas y certificados, se reconocerá que ese acuerdo es suficiente en derecho.

Salvo aquellos casos en los que el Estado, en virtud de convenios o tratados internacionales haya pactado la utilización de medios convencionales, los tratados o convenios que sobre esta materia se suscriban, buscarán la armonización de normas respecto de la regulación de mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico, la protección a los usuarios de estos sistemas, y el reconocimiento de los certificados de firma electrónica entre los países suscriptores.

CAPÍTULO III

DE LAS ENTIDADES DE CERTIFICACIÓN DE INFORMACIÓN

Art. 29.- Entidades de certificación de información.- Son las empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica, autorizadas por el Consejo Nacional de Telecomunicaciones, según lo dispuesto en esta ley y el reglamento que deberá expedir el Presidente de la República.

Art. 30.- Obligaciones de las entidades de certificación de información acreditadas.- Son obligaciones de las entidades de certificación de información acreditadas:

a) Encontrarse legalmente constituidas, y estar registradas en Consejo Nacional de Telecomunicaciones;
b) Demostrar solvencia técnica, logística y financiera para prestar servicios a sus usuarios;
c) Garantizar la prestación permanente, inmediata, confidencial, oportuna y segura del servicio de certificación de información,
d) Mantener sistemas de respaldo de la información relativa a los certificados;
e) Proceder de forma inmediata a la suspensión o revocatoria de certificados electrónicos previo mandato del Superintendente de Telecomunicaciones, en los casos que se especifiquen en esta ley;
f) Mantener una publicación del estado de los certificados electrónicos emitidos;
g) Proporcionar a los titulares de certificados de firmas electrónicas un medio efectivo y rápido para dar aviso que una firma electrónica tiene riesgo de uso indebido;
h) Contar con una garantía de responsabilidad para cubrir daños y perjuicios que se ocasionaren por el incumplimiento de las obligaciones previstas en la presente ley, y hasta por culpa leve en el desempeño de sus obligaciones. Cuando certifiquen límites sobre responsabilidades o valores económicos, esta garantía será al menos del 5% del monto total de las operaciones que garanticen sus certificados; e,
i) Las demás establecidas en esta ley y los reglamentos.

Art. 31.- Responsabilidades de las entidades de certificación de información acreditadas.- Las entidades de certificación de información serán responsables hasta de culpa leve y responderán por los daños y perjuicios que causen a cualquier persona natural o jurídica, en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone esta ley o actúen con negligencia, sin perjuicio de las sanciones previstas en la Ley Orgánica de Defensa del Consumidor. Serán también responsables por el uso indebido del certificado de firma electrónica acreditado, cuando éstas no hayan consignado en dichos certificados, de forma clara, el límite de su uso y del importe de las transacciones válidas que pueda realizar. Para la aplicación de este artículo, la carga de la prueba le corresponderá a la entidad de certificación de información.

Los contratos con los usuarios deberán incluir una cláusula de responsabilidad que reproduzca lo que señala el primer inciso.

Cuando la garantía constituida por las entidades de certificación de información acreditadas no cubra las indemnizaciones por daños y perjuicios, aquellas responderán con su patrimonio.

Art. 32.- Protección de datos por parte de las entidades de certificación de información acreditadas.- Las entidades de certificación de información garantizarán la protección de los datos personales obtenidos en función de sus actividades, de conformidad con lo establecido en el artículo 9 de esta ley.

Art. 33.- Prestación de servicios de certificación por parte de terceros.- Los servicios de certificación de información podrán ser proporcionados y administrados en todo o en parte por terceros. Para efectuar la prestación, éstos deberán demostrar su vinculación con la Entidad de Certificación de Información.

El Consejo Nacional de Telecomunicaciones, establecerá los términos bajo los cuales las Entidades de Certificación de Información podrán prestar sus servicios por medio de terceros.

Art. 34.- Terminación contractual.- La terminación del contrato entre las entidades de certificación acreditadas y el suscriptor se sujetará a las normas previstas en la Ley Orgánica de Defensa del Consumidor.

Art. 35.- Notificación de cesación de actividades.- Las entidades de certificación de información acreditadas, deberán notificar al Organismo de Control, por lo menos con noventa días de anticipación, la cesación de sus actividades y se sujetarán a las normas y procedimientos establecidos en los reglamentos que se dicten para el efecto.

CAPÍTULO IV

DE LOS ORGANISMOS DE PROMOCIÓN Y DIFUSIÓN DE LOS SERVICIOS ELECTRÓNICOS, Y DE REGULACIÓN Y CONTROL DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS

Art. 36.- Organismo de promoción y difusión.- Para efectos de esta ley, el Consejo de Comercio Exterior e Inversiones, "COMEXI", será el organismo de promoción y difusión de los servicios electrónicos, incluido el comercio electrónico, y el uso de las firmas electrónicas en la promoción de inversiones y comercio exterior.

Art. 37.- Organismo de regulación, autorización y registro de las entidades de certificación acreditadas.- El Consejo Nacional de Telecomunicaciones "CONATEL", o la entidad que haga sus veces, será el organismo de autorización, registro y regulación de las entidades de certificación de información acreditadas. En su calidad de organismo de autorización podrá además:

a) Cancelar o suspender la autorización a las entidades de certificación acreditadas, previo informe motivado de la Superintendencia de Telecomunicaciones;
b) Revocar o suspender los certificados de firma electrónica, cuando la entidad de certificación acreditada los emita con inobservancia de las formalidades legales, previo informe motivado de la Superintendencia de Telecomunicaciones; y
c) Las demás atribuidas en la ley y en los reglamentos.

Art. 38.- Organismo de control de las entidades de certificación de información acreditadas.- Para efectos de esta ley, la Superintendencia de Telecomunicaciones, será el organismo encargado del control de las entidades de certificación de información acreditadas.

Art. 39.- Funciones del organismo de control.- Para el ejercicio de las atribuciones establecidas en esta ley, la Superintendencia de Telecomunicaciones tendrá las siguientes funciones:

a) Velar por la observancia de las disposiciones constitucionales y legales sobre la promoción de la competencia y las prácticas comerciales restrictivas, competencia desleal y protección al consumidor, en los mercados atendidos por las entidades de certificación de información acreditadas;
b) Ejercer el control de las entidades de certificación de información acreditadas en el territorio nacional y velar por su eficiente funcionamiento;
c) Realizar auditorias técnicas a las entidades de certificación de información acreditadas;
d) Requerir de las entidades de certificación de información acreditadas, la información pertinente para el ejercicio de sus funciones;
e) Imponer de conformidad con la ley sanciones administrativas a las entidades de certificación de información acreditadas, en caso de incumplimiento de las obligaciones derivadas de la prestación del servicio;
f) Emitir los informes motivados previstos en esta ley;
g) Disponer la suspensión de la prestación de servicios de certificación para impedir el cometimiento de una infracción; y,
h) Las demás atribuidas en la ley y en los reglamentos.

Art. 40.- Infracciones administrativas.- Para los efectos previstos en la presente ley, las infracciones administrativas se clasifican en leves y graves.

Infracciones leves:

1. La demora en el cumplimiento de una instrucción o en la entrega de información requerida por el organismo de control; y,
2. Cualquier otro incumplimiento de las obligaciones impuestas por esta ley y sus reglamentos a las entidades de certificación acreditadas.

Estas infracciones serán sancionadas, de acuerdo a los literales a) y b) del artículo siguiente.

Infracciones graves:

1. Uso indebido del certificado de firma electrónica por omisiones imputables a la entidad de certificación de información acreditada;
2. Omitir comunicar al organismo de control, de la existencia de actividades presuntamente ilícitas realizada por el destinatario del servicio;
3. Desacatar la petición del organismo de control de suspender la prestación de servicios de certificación para impedir el cometimiento de una infracción;

4. El incumplimiento de las resoluciones dictadas por los Organismos de Autorización Registro y Regulación, y de Control; y,
5. No permitir u obstruir la realización de auditorias técnicas por parte del organismo de control.

Estas infracciones se sancionarán de acuerdo a lo previsto en los literales c) y d) del artículo siguiente.

Las sanciones impuestas al infractor, por las infracciones graves y leves, no le eximen del cumplimiento de sus obligaciones.

Si los infractores fueren empleados de instituciones del sector público, las sanciones podrán extenderse a la suspensión, remoción o cancelación del cargo del infractor, en cuyo caso deberán observarse las normas previstas en la ley.

Para la cuantía de las multas, así como para la gradación de las demás sanciones, se tomará en cuenta:

a) La gravedad de las infracciones cometidas y su reincidencia;
b) El daño causado o el beneficio reportado al infractor; y,
c) La repercusión social de las infracciones.

Art. 41.- Sanciones.- La Superintendencia de Telecomunicaciones, impondrá de oficio o a petición de parte, según la naturaleza y gravedad de la infracción, a las entidades de certificación de información acreditadas, a sus administradores y representantes legales, o a terceros que presten sus servicios, las siguientes sanciones:

a) Amonestación escrita;
b) Multa de quinientos a tres mil dólares de los Estados Unidos de Norteamérica;
c) Suspensión temporal de hasta dos años de la autorización de funcionamiento de la entidad infractora, y multa de mil a tres mil dólares de los Estados Unidos de Norteamérica; y,
d) Revocatoria definitiva de la autorización para operar como entidad de certificación acreditada y multa de dos mil a seis mil dólares de los Estados Unidos de Norteamérica;

Art. 42.- Medidas cautelares.- En los procedimientos instaurados por infracciones graves. Se podrá solicitar a los órganos judiciales competentes, la adopción de las medidas cautelares previstas en la ley que se estimen necesarias, para asegurar la eficacia de la resolución que definitivamente se dicte.

Art. 43.- Procedimiento.- El procedimiento para sustanciar los procesos y establecer sanciones administrativas, será el determinado en la Ley Especial de Telecomunicaciones.

TÍTULO III

DE LOS SERVICIOS ELECTRÓNICOS, LA CONTRATACIÓN ELECTRÓNICA Y TELEMÁTICA, LOS DERECHOS DE LOS USUARIOS, E INSTRUMENTOS PÚBLICOS

CAPÍTULO I

DE LOS SERVICIOS ELECTRÓNICOS

Art. 44.- Cumplimiento, de formalidades.- Cualquier actividad, transacción mercantil, financiera o de servicios, que se realice con mensajes de datos, a través de redes electrónicas, se someterá a los requisitos y solemnidades establecidos en la ley que las rija, en todo lo que fuere aplicable, y tendrá el mismo valor y los mismos efectos jurídicos que los señalados en dicha ley.

CAPÍTULO II

DE LA CONTRATACIÓN ELECTRÓNICA Y TELEMÁTICA

Art. 45.- Validez de los contratos electrónicos.- Los contratos podrán ser instrumentados mediante mensajes de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos.

Art. 46.- Perfeccionamiento y aceptación de los contratos electrónicos.- El perfeccionamiento de los contratos electrónicos se someterá a los requisitos y solemnidades previstos en las leyes y se tendrá como lugar de perfeccionamiento el que acordaren las partes.

La recepción, confirmación de recepción, o apertura del mensaje de datos, no implica aceptación del contrato electrónico, salvo acuerdo de las partes.

Art. 47.- Jurisdicción.- En caso de controversias las partes se someterán a la jurisdicción estipulada en el contrato; a falta de ésta, se sujetarán a las normas previstas por el Código de Procedimiento Civil Ecuatoriano y esta ley, siempre que no se trate de un contrato sometido a la Ley Orgánica de Defensa del Consumidor, en cuyo caso se determinará como domicilio el del consumidor o usuario.

Para la identificación de la procedencia de un mensaje de datos, se utilizarán los medios tecnológicos disponibles, y se aplicarán las disposiciones señaladas en esta ley y demás normas legales aplicables.

Cuando las partes pacten someter las controversias a un procedimiento arbitral en la formalización del convenio de arbitraje como en su aplicación, podrán emplearse medios telemáticos y electrónicos, siempre que ello no sea incompatible con las normas reguladoras del arbitraje.

CAPÍTULO III

DE LOS DERECHOS DE LOS USUARIOS O CONSUMIDORES DE SERVICIOS ELECTRÓNICOS

Art. 48.- Consentimiento para aceptar mensajes de datos.- Previamente a que el consumidor o usuario exprese su consentimiento para aceptar registros electrónicos o mensajes de datos, debe ser informado clara, precisa y satisfactoriamente, sobre los equipos y programas que requiere para acceder a dichos registros o mensajes.

El usuario o consumidor, al otorgar o confirmar electrónicamente su consentimiento, debe demostrar razonablemente que puede acceder a la información objeto de su consentimiento.

Si con posterioridad al consentimiento del consumidor o usuario existen cambios de cualquier tipo, incluidos cambios en equipos, programas o procedimientos, necesarios para mantener o acceder a registros o mensajes electrónicos, de forma que exista el riesgo de que el consumidor o usuario no sea capaz de acceder o retener un registro electrónico o mensaje de datos sobre los que hubiera otorgado su consentimiento, se le deberá proporcionar de forma clara, precisa y satisfactoria la información necesaria para realizar estos cambios, y se le informará sobre su derecho a retirar el consentimiento previamente otorgado sin la imposición de ninguna condición, costo alguno o consecuencias. En el caso de que estas modificaciones afecten los derechos del consumidor o usuario, se le deberán proporcionar los medios necesarios para evitarle perjuicios, hasta la terminación del contrato o acuerdo que motivó su consentimiento previo.

Art. 49.- Consentimiento para el uso de medios electrónicos.- De requerirse que la información relativa a un servicio electrónico, incluido el comercio electrónico, deba constar por escrito, el uso de medios electrónicos para proporcionar o permitir el acceso a esa información, será válido si:

a) El consumidor ha consentido expresamente en tal uso y no ha objetado tal consentimiento; y,
b) El consumidor en forma previa a su consentimiento ha sido informado, a satisfacción, de forma clara y precisa, sobre:

1. Su derecho u opción de recibir la información en papel o por medios no electrónicos;
2. Su derecho a objetar su consentimiento en lo posterior y las consecuencias de cualquier tipo al hacerlo, incluidas la terminación contractual o el pago de cualquier tarifa por dicha acción;
3. Los procedimientos a seguir por parte del consumidor para retirar su consentimiento y para actualizar la información proporcionada; y,
4. Los procedimientos para que, posteriormente al consentimiento, el consumidor pueda obtener una copia impresa en papel de los registros electrónicos y el costo de esta copia, en caso de existir.

Art. 50.- Información al consumidor.- En la prestación de servicios electrónicos en el Ecuador, el consumidor deberá estar suficientemente informado de sus derechos y obligaciones, de conformidad con lo previsto en la Ley Orgánica de Defensa del Consumidor y su Reglamento.

Cuando se tratare de bienes o servicios a ser adquiridos, usados o empleados por medios electrónicos, el oferente deberá informar sobre todos los requisitos, condiciones y restricciones para que el consumidor pueda adquirir y hacer uso de los bienes o servicios promocionados.

La publicidad, promoción e información de servicios electrónicos, por redes electrónicas de información, incluida la internet, se realizará de conformidad con la ley, y su incumplimiento será sancionado de acuerdo al ordenamiento jurídico vigente en el Ecuador.

En la publicidad y promoción por redes electrónicas de información, incluida la Internet, se asegurará que el consumidor pueda acceder a toda la información disponible sobre un bien o servicio sin restricciones, en las mismas condiciones y con las facilidades disponibles para la promoción del bien o servicio de que se trate.

En el envío periódico de mensajes de datos con información de cualquier tipo, en forma individual o a través de listas de correo, directamente o mediante cadenas de mensajes, el emisor de los mismos deberá proporcionar medios expeditos para que el destinatario, en cualquier tiempo, pueda confirmar su suscripción o solicitar su exclusión de las listas, cadenas de mensajes o bases de datos, en las cuales se halle inscrito y que ocasionen el envío de los mensajes de datos referidos.

La solicitud de exclusión es vinculante para el emisor desde el momento de la recepción de la misma. La persistencia en el envío de mensajes periódicos no deseados de cualquier tipo, se sancionará de acuerdo a lo dispuesto en la presente ley.

El usuario de redes electrónicas, podrá optar o no por la recepción de mensajes de datos que, en forma periódica, sean enviados con la finalidad de informar sobre productos o servicios de cualquier tipo.

CAPÍTULO IV

DE LOS INSTRUMENTOS PÚBLICOS

Art. 51.- Instrumentos públicos electrónicos.- Se reconoce la validez jurídica de los mensajes de datos otorgados, conferidos, autorizados o expedidos por y ante autoridad competente y firmados electrónicamente.

Dichos instrumentos públicos electrónicos deberán observar los requisitos, formalidades y solemnidades exigidos por la ley y demás normas aplicables.

TÍTULO IV

DE LA PRUEBA Y NOTIFICACIONES ELECTRÓNICAS

CAPÍTULO I

DE LA PRUEBA

Art. 52.- Medios de prueba.- Los mensajes de datos, firmas electrónicas, documentos electrónicos y los certificados electrónicos nacionales o extranjeros, emitidos de conformidad con esta ley, cualquiera sea su procedencia o generación, serán considerados medios de prueba. Para su valoración y efectos legales se observará lo dispuesto en el Código de Procedimiento Civil.

Art. 53.- Presunción.- Cuando se presentare como prueba una firma electrónica certificada por una entidad de certificación de información acreditada, se presumirá que ésta reúne los requisitos determinados en la ley, y que por consiguiente, los datos de la firma electrónica no han sido alterados desde su emisión y que la firma electrónica pertenece al signatario.

Art. 54.- Práctica de la prueba.- La prueba se practicará de conformidad con lo previsto en el Código de Procedimiento Civil y observando las normas siguientes:

a) Al presentar un mensaje de datos dentro de un proceso judicial en los juzgados o tribunales del país, se deberá adjuntar el soporte informático y la transcripción en papel del documento electrónico, así como los elementos necesarios para su lectura y verificación, cuando sean requeridos;
b) En el caso de impugnación del certificado o de la firma electrónica por cualesquiera de las partes, el juez o tribunal, a petición de parte, ordenará a la entidad de certificación de información correspondiente, remitir a ese despacho

los certificados de firma electrónica y documentos en los que se basó la solicitud del firmante, debidamente certificados; y,

c) El facsímile, será admitido como medio de prueba, siempre y cuando haya sido enviado y recibido como mensaje de datos, mantenga su integridad, se conserve y cumpla con las exigencias contempladas en esta ley.

En caso de que alguna de las partes niegue la validez de un mensaje de datos, deberá probar, conforme a la ley, que éste adolece de uno o varios vicios que lo invalidan, o que el procedimiento de seguridad, incluyendo los datos de creación y los medios utilizados para verificar la firma, no puedan ser reconocidos técnicamente como seguros.

Cualquier duda sobre la validez podrá ser objeto de comprobación técnica.

Art. 55.- Valoración de la prueba.- La prueba será valorada bajo los principios determinados en la ley y tomando en cuenta la seguridad y fiabilidad de los medios con los cuales se la envió, recibió, verificó, almacenó o comprobó si fuese el caso, sin perjuicio de que dicha valoración se efectúe con el empleo de otros métodos que aconsejen la técnica y la tecnología. En todo caso la valoración de la prueba se someterá al libre criterio judicial, según las circunstancias en que hayan sido producidos.

Para la valoración de las pruebas, el juez o árbitro competente que conozca el caso deberá designar los peritos que considere necesarios para el análisis y estudio técnico y tecnológico de las pruebas presentadas.

Art. 56.- Notificaciones Electrónicas.- Todo el que fuere parte de un procedimiento judicial, designará el lugar en que ha de ser notificado, que no puede ser otro que el casillero judicial y/o el domicilio judicial electrónico en un correo electrónico, de un abogado legalmente inscrito, en cualquiera de los Colegios de Abogados del Ecuador.

Las notificaciones a los representantes de las personas jurídicas del sector público y a los funcionarios del Ministerio Público que deben intervenir en los juicios, se harán en las oficinas que estos tuvieren o en el domicilio judicial electrónico en un correo electrónico que señalaren para el efecto.

TÍTULO V

DE LAS INFRACCIONES INFORMÁTICAS

CAPÍTULO I

DE LAS INFRACCIONES INFORMÁTICAS

Art. 57.- Infracciones informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.

Reformas al Código Penal:

Art. 58.- A continuación del artículo 202, inclúyanse los siguientes artículos innumerados:

"Art...- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Art...- Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.".

Art. 59.- Sustitúyase el artículo 262 por el siguiente:

"Art...- 262.- Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados sin razón de su cargo".

Art. 60.- A continuación del artículo 353, agréguese el siguiente artículo innumerado:

"Art….- Falsificación electrónica.- Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio; alteren o modifiquen mensajes de datos, o la información incluida en éstos,

que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

1. Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;
2. Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;
3. Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.
4. El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este Capítulo.".

Art. 61.- A continuación del artículo 415 del Código Penal, inclúyanse los siguientes artículos innumerados:

"Art...- Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

La pena de prisión será de tres a cinco años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculada con la defensa nacional.

Art...- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica.".

Art. 62.- A continuación del artículo 553 del Código Penal, añádanse los siguientes artículos innumerados:

"Art...- Apropiación ilícita.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

Art...- La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:

1. Inutilización de sistemas de alarma o guarda;
2. Descubrimiento o descifrado de claves secretas o encriptadas;
3. Utilización de tarjetas magnéticas o perforadas;

4. Utilización de controles o instrumentos de apertura a distancia; y,
5. Violación de seguridades electrónicas, informáticas u otras semejantes.".

Art. 63.- Añádase como segundo inciso del artículo 563 del Código Penal, el siguiente:

"Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos.".

Art. 64.- A continuación del numeral 19 del artículo 606 añádase el siguiente:

"... Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.".

DISPOSICIONES GENERALES

Primera.- Los certificados de firmas electrónicas, emitidos por entidades de certificación de información extranjeras y acreditados en el exterior, podrán ser revalidados en el Ecuador siempre que cumplan con los términos y condiciones exigidos por la ley. La revalidación se realizará a través de una entidad de certificación de información acreditada que garantice en la misma forma que lo hace con sus propios certificados, dicho cumplimiento.

Segunda.- Las entidades de certificación de información acreditadas podrán prestar servicios de sellado de tiempo. Este servicio deberá, ser acreditado técnicamente por el Consejo Nacional de Telecomunicaciones. El reglamento de aplicación de la ley recogerá los requisitos para este servicio.

Tercera.- Adhesión.- Ninguna persona está obligada a usar o aceptar mensajes de datos o firmas electrónicas, salvo que se adhiera voluntariamente en la forma prevista en esta ley.

Cuarta.- No se admitirá ninguna exclusión, restricción o limitación al uso de cualquier método para crear o tratar un mensaje de datos o firma electrónica, siempre que se cumplan los requisitos señalados en la presente ley y su reglamento.

Quinta.- Se reconoce el derecho de las partes para optar libremente por el uso de tecnología y por el sometimiento a la jurisdicción que acuerden mediante convenio, acuerdo o contrato privado, salvo que la prestación de los servicios electrónicos o uso de estos servicios se realice de forma directa al consumidor.

Sexta.- El Consejo Nacional de Telecomunicaciones tomará las medidas necesarias, para que no se afecten los derechos del titular del certificado o de terceros, cuando se produzca la revocatoria del certificado, por causa no atribuible al titular del mismo.

Séptima.- La prestación de servicios de certificación de información por parte de entidades de certificación de información acreditadas, requerirá de autorización previa y registro.

Octava.- El ejercicio de actividades establecidas en esta ley, por parte de instituciones públicas o privadas, no requerirá de nuevos requisitos o requisitos adicionales a los ya establecidos, para garantizar la eficiencia técnica y seguridad jurídica de los procedimientos e instrumentos empleados.

Novena.- Glosario de términos.- Para efectos de esta ley, los siguientes términos serán entendidos conforme se definen en este artículo:

Mensaje de datos: Es toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio. Serán considerados como mensajes de datos, sin que esta enumeración limite su definición, los siguientes documentos electrónicos, registros electrónicos, correo electrónico, servicios web, telegrama, télex, fax e intercambio electrónico de datos.

Red electrónica de información: Es un conjunto de equipos y sistemas de información interconectados electrónicamente.

Sistema de información: Es todo dispositivo físico o lógico utilizado para crear, generar, enviar, recibir, procesar, comunicar o almacenar, de cualquier forma, mensajes de datos.

Servicio electrónico: Es toda actividad realizada a través de redes electrónicas de información.

Comercio electrónico: Es toda transacción comercial realizada en parte o en su totalidad, a través de redes electrónicas de información.

Intimidad: El derecho a la intimidad previsto en la Constitución Política de la República, para efectos de esta ley, comprende también el derecho a la privacidad, a la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros, a la no divulgación de los datos personales y a no recibir información o mensajes no solicitados.

Datos personales: Son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta ley.

Datos personales autorizados: Son aquellos datos personales que el titular ha accedido a entregar o proporcionar de forma voluntaria, para ser usados por la persona, organismo o entidad de registro que los solicita, solamente para el fin para el cual fueron recolectados, el mismo que debe constar expresamente señalado y ser aceptado por dicho titular.

Datos de creación: Son los elementos confidenciales básicos y necesarios para la creación de una firma electrónica.

Certificado electrónico de información: Es el mensaje de datos que contiene información de cualquier tipo.

Dispositivo electrónico: Instrumento físico o lógico utilizado independientemente para iniciar o responder mensajes de datos, sin intervención de una persona al momento de dicho inicio o respuesta.

Dispositivo de emisión: Instrumento físico o lógico utilizado por el emisor de un documento para crear mensajes de datos o una firma electrónica.

Dispositivo de comprobación: Instrumento físico o lógico utilizado para la validación y autenticación de mensajes de datos o firma electrónica.

Emisor: Persona que origina un mensaje de datos.

Destinatario: Persona a quien va dirigido el mensaje de datos.

Signatario: Es la persona que posee los datos de creación de la firma electrónica, quien, o en cuyo nombre, y con la debida autorización se consigna una firma electrónica.

Desmaterialización electrónica de documentos: Es la transformación de la información contenida en documentos físicos a mensajes de datos.

Quiebra técnica: Es la imposibilidad temporal o permanente de la entidad de certificación de información, que impide garantizar el cumplimiento de las obligaciones establecidas en esta ley y su reglamento.

Factura electrónica: Conjunto de registros lógicos archivados en soportes susceptibles de ser leídos por equipos electrónicos de procesamiento de datos que documentan la transferencia de bienes y servicios, cumpliendo los requisitos exigidos por las Leyes Tributarias, Mercantiles y más normas y reglamentos vigentes.

Sellado de tiempo: Anotación electrónica firmada electrónicamente y agregada a un mensaje de datos en la que conste como mínimo la fecha, la hora y la identidad de la persona que efectúa la anotación.

Décima.- Para la fijación de la pena en los delitos tipificados mediante las presentes, reformas al Código Penal, contenidas en el Título V de esta ley, se tomarán en cuenta los siguientes criterios: el importe de lo defraudado, el quebranto económico causado, los medios empleados y cuantas otras circunstancias existan para valorar la infracción.

DISPOSICIONES TRANSITORIAS

Primera.- Hasta que se dicte el reglamento y más instrumentos de aplicación de esta ley, la prestación del servicio de sellado de tiempo, deberá cumplir con los requisitos de seguridad e inalterabilidad exigidos para la firma electrónica y los certificados electrónicos.

Segunda.- El cumplimiento del artículo 56 sobre las notificaciones al correo electrónico se hará cuando la infraestructura de la Función Judicial lo permita, correspondiendo al organismo competente de dicha Función organizar y reglamentar los cambios que sean necesarios para la aplicación de esta ley y sus normas conexas.

Para los casos sometidos a Mediación o Arbitraje por medios electrónicos, las notificaciones se efectuarán obligatoriamente en el domicilio judicial electrónico en un correo electrónico señalado por las partes.

DISPOSICION FINAL

El Presidente de la República, en el plazo previsto en la Constitución Política de la República, dictará el reglamento a la presente ley.

La presente ley entrará en vigencia a partir de su publicación en el Registro Oficial.

REGLAMENTO A LA LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS DEL ECUADOR.

No. 3496

Gustavo Noboa Bejarano
PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

Considerando:

Que mediante Ley No. 67, publicada en el Registro Oficial Suplemento No. 557 de 17 de Abril del 2002 se expidió la Ley de Comercio Electrónico, Firmas y Mensajes de Datos;

Que la disposición final de la citada ley dispone que el Presidente de la República debe expedir el correspondiente reglamento; y,

En ejercicio de la facultad prevista en el artículo 171 numeral 5 de la Constitución Política de la República,

Decreta:

Expedir el siguiente REGLAMENTO GENERAL A LA LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS.

Art. 1.- Incorporación de archivos o mensajes adjuntos.- La incorporación por remisión a la que se refiere el Art. 3 de la Ley 67, incluye archivos y mensajes incorporados por remisión o como anexo en un mensaje de datos a cuyo contenido se accede indirectamente a partir de un enlace electrónico directo incluido en el mismo mensaje de datos y que forma parte del mismo.

La aceptación que hacen las partes del contenido por remisión deberá ser expresada a través de un mensaje de datos que determine inequívocamente tal aceptación. En el caso de contenido incorporado por remisión a través de un enlace electrónico, no podrá ser dinámico ni variable y por tanto la aceptación expresa de las partes se refiere exclusivamente al contenido accesible a través del enlace electrónico al momento de recepción del mensaje de datos.

En las relaciones con consumidores, es responsabilidad del proveedor asegurar la disponibilidad de los remitidos o anexos para que sean accedidos por un medio aceptable para el consumidor cuando éste lo requiera. En las relaciones de otro tipo las partes podrán acordar la forma y accesibilidad de los anexos y remitidos.

Los anexos o remisiones referidas a garantías, derechos, obligaciones o información al consumidor deberán observar lo establecido en la Ley Orgánica de Defensa del Consumidor y su reglamento.

Toda modificación a un anexo o remitido en un mensaje de datos se comunicará al receptor del mismo, a través de un mensaje de datos o por escrito, resaltando las diferencias entre el texto original y el modificado. En el texto modificado se deberá incluir en lugar visible y

claramente accesible un enlace al contenido anterior. La comunicación al consumidor acerca de modificaciones no constituye indicación de aceptación de las mismas por su parte. Dicha aceptación deberá ser expresa y remitida por cualquier medio, ya sea éste físico o electrónico.

Cuando las leyes así lo determinen, cierto tipo de información deberá estar directamente incluida en el mensaje de datos y no como anexo o remitido.

Art. 2.- Accesibilidad de la información.- Se considerará que un mensaje de datos, sus anexos y remitidos, son accesibles para consulta posterior cuando se puede recuperar su contenido en forma íntegra en cualquier momento empleando los mecanismos y procedimientos previstos para el efecto, los cuales deberán detallarse y proporcionarse independientemente del mensaje de datos a fin de garantizar el posterior acceso al mismo.

Art. 3.- Información escrita.- Se entiende que la información contenida en un mensaje de datos es accesible para su posterior consulta cuando:

- Ha sido generada y puede ser almacenada en un lenguaje electrónico/informático y formato entendibles por las partes involucradas en el intercambio de información y sus respectivos sistemas informáticos de procesamiento de la información, pudiéndose recuperar su contenido y el de los remitidos o anexos correspondientes en cualquier momento empleando los mecanismos previstos y reconocidos para el efecto; y,

- Se puede recuperar o se puede acceder a la información empleando los mecanismos previstos al momento de recibirlo y almacenarlo, y que deberán detallarse y proporcionarse independientemente el mensaje de los datos a fin de garantizar el posterior acceso al mismo.

Las publicaciones que las leyes exijan por escrito, sin perjuicio de lo establecido en dichas leyes, podrán adicionalmente efectuarse en medios electrónicos en forma de mensaje de datos.

Cumplidos los requisitos de accesibilidad, el mensaje de datos tiene iguales efectos jurídicos que los documentos que consta por escrito.

Art. 4.- Información original y copias certificadas.- Los mensajes de datos de los documentos desmaterializados, cuando las leyes así lo determinen y de acuerdo al caso, deberán ser certificados ante un Notario, autoridad competente o persona autorizada a través de la respectiva firma electrónica, mecanismo o procedimiento autorizado.

Los documentos desmaterializados se considerarán para todos los efectos, copia idéntica del documento físico a partir del cual se generaron y deberán contener adicionalmente la indicación de que son desmaterializados o copia electrónica de un documento físico. Se emplearán y tendrán los mismos efectos que las copias impresas certificadas por autoridad competente.

Art. 5.- Desmaterialización.- El acuerdo expreso para desmaterializar documentos deberá constar en un documento físico o electrónico con las firmas de las partes aceptando tal desmaterialización y confirmado que el documento original y que el documento

desmaterializado son idénticos. En caso que las partes lo acuerden o la ley lo exija, las partes acudirán ante Notario o autoridad competente para que certifique electrónicamente que el documento desmaterializado corresponde al documento original que se acuerda desmaterializar. Esta certificación electrónica se la realiza a través de la respectiva firma electrónica del Notario o autoridad competente.

Los documentos desmaterializados deberán señalar que se trata de la desmaterialización del documento original. Este señalamiento se constituye en la única diferencia que el documento desmaterializado tendrá con el documento original.

En el caso de documentos que contengan obligaciones, se entiende que tanto el documento original cono el desmaterializado son la expresión de un mismo acuerdo de las partes intervinientes y por tanto no existe duplicación de obligaciones. De existir multiplicidad de documentos desmaterializados y originales con la misma información u obligación, se entenderá que se trata del mismo, salvo prueba en contrario.

La desmaterialización de los documentos de identificación personal estará sujeta a las disposiciones especiales y procedimiento que las entidades competentes determinen.

Art. 6.- Integridad de un mensaje de datos.- La consideración de integridad de un mensaje de datos, establecida en el inciso segundo del Art. 7 de la Ley 67, se cumple si dicho mensaje de datos está firmado electrónicamente. El encabezado o la información adicional en un mensaje de datos que contenga exclusivamente información técnica relativa al envío o recepción del mensaje de datos, y que no altere en forma alguna su contenido, no constituye parte sustancial de la información.

Para efectos del presente artículo, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún cambio que sea inherente al proceso de comunicación, archivo o presentación.

Art. 7.- Procedencia e identidad de un mensaje de datos.- La verificación de la concordancia entre el emisor del mensaje de datos y su firma electrónica se realizará comprobando la vigencia y los datos del certificado de firma electrónica que la respalda. En otros tipos de firmas o sistemas de identificación y autentificación, esta verificación se realizará mediante la verificación de los registros acordados o requeridos.

El aviso de un posible riesgo sobre la vulnerabilidad o inseguridad de una firma, su certificado o el mensaje de datos y los anexos relacionados podrá ser realizado por el titular de los mismos, mediante cualquier tipo de advertencia que permita, de manera inequívoca a quien realiza la verificación o recibe un mensaje de datos, tomar las precauciones necesarias para evitar perjuicios y prevenir fallas de seguridad. Este aviso deberá ser realizado antes de iniciar cualquier proceso de transacción comercial negociación o contratación electrónica.

De acuerdo a las leyes, se podrá recurrir a peritos para determinar la procedencia y otro tipo de relaciones de un mensaje de datos con quien lo remite de modo directo o indirecto.

Art. 8.- Responsabilidad por el contenido de los mensajes de datos.- La prestación de servicios electrónicos de cualquier tipo por parte de terceros, relacionados con envío y recepción de comunicaciones electrónicas, alojamiento de sitios en medios electrónicos o servicios similares o relacionados, no implica responsabilidad sobre el

contenido de los mensajes de datos por parte de quien presta estos servicios, siendo la responsabilidad exclusivamente del propietario de la información.

De acuerdo a la ley y por orden de la autoridad competente, el órgano regulador podrá ordenar la suspensión del acceso a cualquier información en redes electrónicas que se declare ilegal y/o que atente contra las leyes o la seguridad nacionales. El proveedor de servicios electrónicos deberá cumplir con la orden de suspender el acceso al contenido en forma inmediata, y en caso de no hacerlo será sancionado con sujeción a la ley por el CONATEL.

Art. 9.- Prestación de servicios de conservación de mensajes de datos.- La conservación, incluido el almacenamiento y custodia de mensajes de datos, podrá realizarse a través de terceros, de acuerdo a lo que establece el Art. 8 de la Ley 67. Los sistemas, políticas y procedimientos que permiten realizar las funciones de conservación de mensajes de datos se denominan Registro Electrónico de Datos. Una vez cumplidos los requisitos establecidos en las leyes, cualquier persona puede prestar servicios de Registro Electrónico de Datos que incluyen:

- Conservación, almacenamiento y custodia de la información en formato electrónico con las debidas seguridades;
- Preservación de la integridad de la información conservada;
- Administración del acceso a la información y la reproducción de la misma cuando se requiera;
- Respaldo y recuperación de información; y,
- Otros servicios relacionados con la conservación de los mensajes de datos.

La prestación de servicios de Registro de Datos se realizará bajo el régimen de libre competencia y contratación. Las partes que intervengan en la contratación de este tipo de servicios, podrán determinar las condiciones que regulan su relación.

La prestación del servicio de Registro Electrónico de Datos deberá observar todas las normas contempladas en la Ley 67, este reglamento y demás disposiciones legales vigentes.

En los procesos de conservación de los mensajes de datos, se debe garantizar la integridad de los mismos al menos por el mismo tiempo que las leyes y reglamentos exijan su almacenamiento.

Por orden de autoridad competente, podrá ordenarse a los proveedores de servicios de Registro Electrónico de Datos mantener en sus sistemas respaldos de los mensajes de datos que tramite por el tiempo que se considere necesario.

Art. 10.- Elementos de la infraestructura de firma electrónica.- La firma electrónica es aceptada bajo el principio de neutralidad tecnológica. Las disposiciones contenidas en la Ley 67 y el presente reglamento no registren la autonomía privada para el uso de otras firmas electrónicas generadas fuera de la infraestructura de llave pública, ni afecta los pactos que acuerden las partes sobre validez y eficacia jurídica de la firma electrónica conforme a lo establecido en la ley y este reglamento.

Los principios y elementos que respaldan a la firma electrónica son:

- No-discriminación a cualquier tipo de firma electrónica, así como a sus medios de verificación o tecnología empleada;
- Prácticas de certificación basadas en estándares internacionales o compatibles a los empleados internacionalmente;
- El soporte lógico o conjunto de instrucciones para los equipos de computo y comunicaciones, los elementos físicos y demás componentes adecuados al uso de las firmas electrónicas, a las prácticas de certificación y a las condiciones de seguridad adicionales, comprendidas en los estándares señalados en el literal b);
- Sistema de gestión que permita el mantenimiento de las condiciones señaladas en los literales anteriores, así como la seguridad, confidencialidad, transparencia y no-discriminación en la prestación de sus servicios; y,
- Organismos de promoción y difusión de los servicios electrónicos, y de regulación y control de las entidades de certificación.

Art. 11.- Duración del certificado de firma electrónica.- La duración del certificado de firma electrónica se establecerá contractualmente entre el titular de la firma electrónica y la entidad certificadora de información o quien haga sus veces. En caso de que las partes no acuerden nada al respecto, el certificado de firmas electrónicas se emitirá con una validez de dos años a partir de su expedición. Al tratarse de certificados de firma electrónica emitidos con relación al ejercicio de cargos públicos o privados, la duración del certificado de firma electrónica podrá ser superior a los dos años pero no podrá exceder el tiempo de duración de dicho cargo público o privado a menos que exista una de las prórrogas de funciones establecidas en las leyes.

Art. 12.- Listas de revocación.- Las entidades de certificación de información proporcionarán mecanismos automáticos de acceso a listas de certificados revocados o suspendidos de acuerdo al Art. 26 de la Ley 67. Cuando la verificación de la validez de los certificados de firma electrónica no sea posible de realizar en tiempo real, la entidad de certificación de información comunicará de este hecho tanto al emisor como al receptor del mensaje de datos.

Los periodos de actualización de las listas de certificados suspendidos, revocados o no vigentes por cualquier causa se establecerán contractualmente.

Art. 13.- Revocación del certificado de firma electrónica.- Establecidas las circunstancias determinadas en la Ley 67, se producirá la revocación, que tendrá también como consecuencia la respectiva publicación y la desactivación del enlace que informa sobre el certificado.

En caso de que las actividades de certificación vayan a cesar, la entidad de certificación deberá notificar con por lo menos noventa días de anticipación a los usuarios de los certificados de firma electrónica y a los organismos de regulación control sobre la terminación de sus actividades.

La cesión de certificados de firma electrónica de una entidad de certificación a otra, contará con la autorización expresa del titular del certificado.

La entidad de certificación que asuma los certificados deberá cumplir con los mismos requisitos tecnológicos exigidos a las entidades de certificación por la ley 67 y este reglamento.

Art. 14.- De la notificación por extinción, suspensión o revocación del certificado de firma electrónica.- La notificación inmediata al titular del certificado de firma electrónica, de acuerdo al Art. 26 de la Ley 67, se hará a la dirección electrónica y a la dirección física que hubiere señalado en el contrato de servicio, luego de la extinción, suspensión o revocación del certificado.

Art. 15.- Publicación de la extinción, revocación y suspensión de los certificados de firma electrónica y digital.- La publicación a la que se refiere el Art. 27 de la Ley 67, se deberá hacer por cualquiera de los siguientes medios:

Siempre a la página electrónica determinada por el CONATEL en la que se reporta la situación y la validez de los certificados, así como en la página WEB de la entidad certificadora; y,

Mediante un aviso al acceder al certificado de firma electrónica desde el hipervínculo de verificación, sea que éste forme parte de la firma electrónica, que conste en un Directorio electrónico o por cualquier procedimientos por el cual se consulta los datos del certificado de firma electrónica.

Opcionalmente en caso de que la entidad certificadora o la entidad de registro relacionada crean conveniente, se podrá hacer la publicación en uno de los medios de comunicación pública.

Art. 16.- Reconocimiento internacional de certificados de firma electrónica.- Los certificados de firma electrónica emitidos en el extranjero tendrán validez legal en Ecuador, una vez obtenida la revalidación respectiva emitida por el CONATEL, el deberá comprobar el grado de fiabilidad de los certificados y la solvencia técnica de quien los emite.

Art. 17.- Régimen de acreditación de entidades de certificación de información.- Para obtener autorización de operar directamente o a través de terceros relacionados en Ecuador, las entidades de certificación de información deberán registrarse en el CONATEL.

Los certificados de firma electrónica emitidos por las entidades de certificación de información que, además de registrarse, se acrediten voluntariamente en el CONATEL, tienen carácter probatorio.

Las entidades que habiéndose registrado y obtenido autorización para operar, directamente o a través de terceros relacionados en Ecuador, no se acreditan en el CONATEL, tendrán la calidad de entidades de certificación de información no acreditadas y están obligados a informar de esta condición a quienes soliciten o hagan uso de sus servicios, debiendo también, a solicitud de autoridad competente, probar la suficiencia técnica y fiabilidad de los certificados que emiten.

Art. 18.- Responsabilidades de las entidades de certificación de información.- Es responsabilidad de la entidad certificadora de información o de la

entidad de Registro que actúe en su nombre, verificar la autenticidad y exactitud de todos los datos que consten en el certificado de firma electrónica.

El CONATEL, podrá requerir en cualquier momento de la entidad de certificación de información, de la entidad de Registro que actúe en su nombre, o del titular del certificado de firma electrónica los documentos de respaldo que confirmen la autenticidad y exactitud de los datos que contiene.

Art. 19.- Obligaciones del titular de firma electrónica.- A más de las consideradas en la Ley 67 y su reglamento, serán las mismas previstas en las leyes por el empleo de la firma manuscrita.

El órgano que ejerce las funciones de control previsto en la Ley 67, desarrollará los mecanismos, políticas y procedimientos para auditar técnicamente la actividad de las entidades bajo su control.

Art. 20.- Información al usuario.- La información sobre los programas o equipos que se requiere para acceder a registros o mensajes de datos deberá ser proporcionada mediante medios electrónicos o materiales. En el caso de uso de medios electrónicos se contará con la confirmación de recepción de la información por parte del usuario, cuando se usen medios materiales, los que formarán parte de la documentación que se le deberá entregar al usuario.

Para demostrar el acceso a la información el usuario deberá manifestar expresamente que conoce la información objeto de su consentimiento y que sus sistemas le permiten el acceso tecnológico a la misma.

Art. 21.- De la seguridad en la prestación de servicios electrónicos.- La prestación de servicios electrónicos que impliquen el envío por parte del usuario de información personal, confidencial o privada, requerirá el empleo de sistemas seguros en todas las etapas del proceso de prestación de dicho servicio. Es obligación de quien presta los servicios, informar en detalle a los usuarios sobre el tipo de seguridad que utiliza, sus alcances y limitaciones, así como sobre los requisitos de seguridad exigidos legalmente y si el sistema puesto a disposición del usuario cumple con los mismos. En caso de no contar con seguridades se deberá informar a los usuarios de este hecho en forma clara y anticipada previo al acceso a los sistemas o a la información de instruir claramente sobre los posibles riesgos en que pueden incurrir por la falta de dichas seguridades.

Se consideran datos sensibles del consumidor sus datos personales, información financiera de cualquier tipo como números de tarjetas de crédito o similares que involucren transferencias de dinero o datos a través de los cuales puedan cometerse fraudes o ilícitos que le afecten.

Por el incumplimiento de las disposiciones contenidos en el presente artículo o por falta de veracidad o exactitud en la información sobre seguridades, certificaciones o mecanismos para garantizar la confiabilidad de las transacciones o intercambio de datos ofrecida al consumidor o usuario, el organismo de control podrá exigir al proveedor de los servicios electrónicos la rectificación necesaria y en caso de reiterarse el incumplimiento o la publicación de información falsa o inexacta, podrá ordenar la suspensión del acceso al sitio

con la dirección electrónica del proveedor de servicios electrónicos mientras se mantengan dichas condiciones.

Art. 22.- Envió de mensajes de datos no solicitados.- El envío periódico de información, publicidad o noticias promocionando productos o servicios de cualquier tipo observará las siguientes disposiciones:

- Todo mensaje de datos periódico deberá incluir mecanismos de suscripción y de suscripción;

- Se deberá incluir una nota indicando el derecho del receptor a solicitar se le deje de enviar información no solicitada;

- Deberá contener información clara del remitente que permita determinar inequívocamente el origen del mensaje de datos;

- A solicitud del destinatario se deberá eliminar toda información que de él se tenga en bases de datos o en cualquier otra fuente de información empleada para el envió de mensajes de datos periódicos u otros fines no expresamente autorizados por el titular de los datos; y,

- Inmediatamente de recibido por cualquier medio la solicitud del destinatario para suscribirse del servicio o expresando su deseo de no continuar recibiendo mensajes de datos periódicos, el emisor deberá cesar el envío de los mismos a la dirección electrónica correspondiente.

Las solicitudes de no envío de mensajes de datos periódicos, se harán directamente por parte del titular de la dirección electrónica de destino.

Los proveedores de servicios electrónicos o comunicaciones electrónicas, a solicitud de cualquiera de sus titulares de una dirección electrónica afectado por el envió periódico de mensajes de datos no solicitados, procederán a notificar al remitente de dichos correos sobre el requerimiento del cese de dichos envíos y de comprobarse que el remitente persiste en enviar mensajes de datos periódicos no solicitados podrá bloquear el acceso del remitente a la dirección electrónica afectada.

Art. 23.- Sellado de tiempo.- Para la prestación de los servicios de sellado de tiempo, el mensaje de datos debe ser enviado a través de la entidad certificadora o un tercero debidamente registrado en el CONATEL para prestar este servicio. El sellado de tiempo únicamente establecerá para los fines legales pertinentes, la hora y fecha exacta en que el mensaje de datos fue recibido por la entidad certificadora o el tercero registrado por el CONATEL; y la fecha y hora exacta en dicho mensaje de datos fue entregado al destinatario.

Para efectos legales el servicio de sellado de tiempo se prestará tomando como referencia el huso horario del territorio continental ecuatoriano.

La prestación de servicios de sellado de tiempo se realizará en régimen de libre competencia y contratación. Las partes que intervengan en la contratación de este tipo de servicios podrán determinar las condiciones que regulen su relación.

Artículo Final.- El presente reglamento entrará en vigencia a partir de su publicación en el Registro oficial.

Dado en el Palacio Nacional, en Quito, a 12 de Diciembre del 2002.

f.) Gustavo Noboa Bejarano, Presidente Constitucional de la República.

Es fiel copia del original.- Lo certifico.

f.) Marcelo Santos Vera, Secretario General de la Administración Pública.

BIOGRAFÍA:

VARELA NUÑEZ JUAN FRANCISCO

1. DATOS PERSONALES

Fecha de nacimiento: 18 de Diciembre de 1974
Estado civil: Casado
Número de cédula: 1710165554

2. EDUCACIÒN

a. Primaria

Escuela “La Salle”, Quito

b. Secundaria

Colegio “La Salle”, Quito.

Bachiller en Ciencias, especialización Físico – Matemáticas, Junio, 1992

c. Superior

- Escuela Superior Militar “Eloy Alfaro”, Parcayacu.
  Subteniente del Ejército Ecuatoriano, Agosto 10, 1996

- Escuela Politécnica del Ejército, Sangolquí. Carrera de Ingeniería en Sistemas e Informática 2001 – 2007

- Escuela Politécnica del Ejército, Sangolquí. Diploma en Suficiencia en el idioma Inglés 2004 - 2005

GUAIGUA GUANOPATIN SINTHIA ELIZABETH

3. DATOS PERSONALES

Fecha de nacimiento: 02 Julio de 1983
Estado civil: Soltera
Número de cédula: 1718431032

4. EDUCACIÒN

a. Primaria

Colegio “LA INMACULADA”, Sangolquí

b. Secundaria

Colegio Experimental “24 DE MAYO”, Quito.
Bachiller en Ciencias, especialización Físico – Matemáticas, Julio, 2001

c. Superior

- Escuela Politécnica del Ejército, Sangolquí. Carrera de Ingeniería en Sistemas e Informática 2002 – 2007

- Escuela Politécnica del Ejército, Sangolquí. Diploma en Suficiencia en el idioma Inglés 2004 - 2005

d. Otros

- Certificación Internacional: Academia Cisco, Sangolquí, 2005-2007

HOJA DE LEGALIZACION DE FIRMAS

ELABORADO POR

_____
Sinthia Elizabeth Guaigua Guanopatin

_____
Capt. Varela Núñez Juan Francisco

COORDINADOR DE LA CARRERA

_____
Ing. Ramiro Delgado

Lugar y fecha: Sangolquí, Septiembre de 2007