U N I V E R S I D A D L A T I N A, S.C.
INCORPORADA A LA
UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

LICENCIATURA EN INFORMÁTICA

"Criptografía Asimétrica con la Implementación de Cifrado y Firma Digital en Correo Electrónico en la Comisión Nacional Bancaria y de Valores"

T E S I S

PARA OBTENER EL TITULO DE LICENCIADO EN INFORMÁTICA

P R E S E N T A

Ernesto Alejandro Cruz Villela

ASESOR: L. I. CLAUDIA AGUIRRE SALAZAR

MÉXICO D.F. **DICIEMBRE 2009.**

AGRADECIMIENTOS

***Mamá**:*

Gracias por el apoyo que me has dado porque hoy veo llegar a su fin una de las metas de mi vida, por el amor, la confianza, por formarme y educarme, creando un hombre con buenos principios, forjando siempre en la familia la solidaridad y la justicia.

***Papá**:*

Gracias por brindarme todo el apoyo moral y estímulos con mucho amor y confianza, por infundir en mi, ese camino que inicio con total responsabilidad y que representa el término de mi carrera profesional, y por enseñarme a tener siempre presente la justicia, el respeto y la responsabilidad en todos los actos de mi vida.

***Eric**:*

Te expreso mi profundo agradecimiento por estar a mi lado, por compartir momentos inolvidables y bellos, por ser tú y saber que siempre cuento contigo, te estaré eternamente agradecido, hermano.

***Alita**:*

A la peque de la familia, gracias hermanita por estar conmigo en este momento tan importante en mi vida, por tu apoyo incondicional, por tu amor, la confianza y por ser una inspiración para seguir siempre adelante en todos mi propósitos.

***Familia y Amigos**:*

Por existir y ser parte de este logro, por su comprensión y confianza, por su amor y amistad incondicional, por lo que ha sido y será, mil gracias.

Doy gracias a Dios por haberme permitido terminar esta meta y darme vida para compartir con mi familia este feliz momento.

Papá, Mamá, Eric y Ale: Por el sacrificio y esfuerzo de todos nosotros, solo quiero decirles que este logro no es sólo mío, es de todos, los amo.

PRÓLOGO

En el universo de la informática, la seguridad es un tema muy complejo y difícil de entender, pero es necesario tener segura la información y su intercambio.

Por lo anterior se requiere el uso de técnicas que permitan evitar o disminuir el índice de ataques a la información, tales como:

- El uso de cifrado para garantizar la confidencialidad e integridad
- La firma digital para la autenticación y el no repudio.

Esta tesis expone el tema basado en el sistema cifrado asimétrico o sistema de cifrado de llave pública con la implementación de firma digital en el correo electrónico.

La aplicación de este tipo de criptografía puede utilizarse en el sector público y privado para el intercambio de información de alta confidencialidad.

Existe una constante preocupación de la información que es procesada en los diferentes sistemas de información, en nuestro caso el correo electrónico y que tiene un alcance a nivel organizacional o simplemente a nivel personal, ya que la seguridad de la información juega un papel cada vez más importante.

El problema existe en aplicaciones como el comercio electrónico, el uso de transacciones de tipo venta y compra de mercancías, la protección de activos personales e institucionales, transacciones bancarias, entre otras.

Se puede decir que la criptografía es un métoñdo práctico que nace de la necesidad de proteger la información. Hay dos acciones cuando hablamos de criptografía una de ellas es el cifrado y otra el descifrado.

El cifrado me permite transformar un mensaje entendible en algo que no lo es y que solo personas que conocen la llave puedan tener acceso a la información y hace que la información sea más segura.

La firma manuscrita es todavía la forma más utilizada y confiable para relacionar un documento con una persona en particular, de manera legal. Sin embargo, este método ha adolecido y sigue adoleciendo de diversas imperfecciones, entre ellas la posibilidad de falsificación y las dificultades en el proceso de verificación de la firma.

La firma en sí, involucra dos acciones: la acción de firmar y la acción de verificación de la firma. La acción de firmar, en el caso de la firma manuscrita, consiste en que una persona deje su rúbrica; mientras que la acción de verificación es más complicada ya que se requiere en algunos casos la utilización de tecnología altamente sofisticada y siempre con probabilidad de error.

Como solución a estos problemas nace una nueva tecnología que puede reemplazar a la firma manuscrita, y que se ha denominado firma digital.

La tecnología de firma digital y cifrado va llegando poco a poco a todo el mundo, y cada vez más se promueve su uso y de cómo implementarlos, y para concientizar a todos de las ventajas que esta nos brinda.

De esta manera, quedarían resueltos los problemas de seguridad dentro del entorno del correo electrónico, con técnicas como el cifrado de llave pública y la firma digital.

ÍNDICE

INTRODUCCIÓN

La segunda aplicación más utilizada en Internet es el correo electrónico, además del explorador. Un problema considerable es que no se le da el nivel de importancia a los ataques existentes derivados del uso del correo electrónico y por consecuente a la privacidad, el mal uso del e-mail estriba en comprometer y/o divulgar el contenido de mensajes. El propósito de éste trabajo es proporcionar la información referente al funcionamiento de la criptografía asimétrica, sus diversos algoritmos de cifrado, la firma digital, así como también implementarlas en el correo electrónico, además de usar protocolos para asegurar servicios de seguridad como: confidencialidad, autenticación, integridad y no repudio.

La mayoría de las personas utilizan el correo electrónico, y para sorpresa de muchos, puede ser utilizado en su contra. El correo no deberá ser manejado como una tarjeta postal, en donde cualquiera puede leer el contenido. Siempre es recomendable evitar colocar información que no se deseé que sea vista por personas ajenas. Se dice que existen estrategias para asegurar el correo. En el presente trabajo se considera la utilización segura del correo y cómo proteger la privacidad.

El correo electrónico exige mucho más que el solo hecho de transferir información, requiere que se proporcione a las partes interesadas una seguridad sobre la información transferida y sus efectos; no solo tecnológica, sino también jurídica. Para lograr atender esta necesidad nace la firma digital, que en términos legales es el equivalente a una firma manuscrita y debe cumplir las mismas funciones principales, como son: la autenticación de la identidad del firmante, la integridad de la información, la confidencialidad de los datos y el no repudio de la información.

Generalmente, la seguridad de la información consiste en garantizar que la información importante de una persona u organización cumpla con el fin para lo que les fue destinado y que personas ajenas o sin suficientes privilegios no tengan acceso a ella y así poder evitar un mal uso, es en si la protección de la información de accesos no autorizados, en el capítulo 1 se habla de la criptografía como un elemento de seguridad para la información, antecedentes, cifrado de llave pública y el proceso de firma digital incluyendo los certificados digitales con la finalidad de utilizarlos en nuestro correo electrónico.

En el mundo se han adoptado legislaciones orientadas a permitir, contribuir y fomentar el uso de la firma digital con la finalidad de promover el uso de correo electrónico seguro en el sector público y privado.

El capitulo 2 habla de todo el funcionamiento de la criptografía asimétrica, el intercambio de llaves, algoritmos y estándares más utilizados, finalmente todo el proceso que abarca la firma digital así como sus aplicaciones.

Posteriormente el capítulo 3 contiene la información referente a la infraestructura de red de la Comisión Nacional Bancaria y de Valores para tener el conocimiento de cómo están interconectados todos los equipos, con que servidores se cuentan, cuantos nodos de red hay y cuantos usuarios tiene la Institución. Finalmente en el capítulo 4 se realiza la implementación del sistema de cifrado y firma digital para correo electrónico, desde su configuración hasta su utilización.

En la actualidad el buen uso de la información y su seguridad consiste en salvaguardar y proteger los datos personales como pueden ser la información, dinero, privacidad y la criptografía es una herramienta que permite garantizarla.

Para que la información se considere segura debe contener las siguientes propiedades: autenticidad, confidencialidad, integridad y disponibilidad.

JUSTIFICACIÓN

Implementar un esquema de firma digital y cifrado asimétrico en correo electrónico, haciendo uso de la infraestructura adecuada que permita firmar y cifrar correos teniendo la certeza de que la información es segura.

El propósito es proveer la información necesaria para utilizar el correo electrónico de una manera segura y aplicar los métodos antes mencionados para conseguirlo.

Hacer que el sistema de cifrado de llave pública y firma digital nos otorgue un alto grado de seguridad y confidencialidad para tener alternativas de protección contra las amenazas que pongan en riesgo la información.

Lo que se implementa es lo siguiente:

- Firma digital dentro y fuera de la institución.
- Validación de las firmas digitales por medio de certificados digitales.
- Implementar un esquema de cifrado de llave pública.
- Expedir los certificados digitales para cada usuario.

Utilizar este esquema para garantizar la integridad, confidencialidad, autenticación y no repudio en el envío de mensajes vía correo electrónico.

CAPITULO 1: CRIPTOGRAFÍA COMO ELEMENTO DE SEGURIDAD DE LA INFORMACIÓN

1.1 INTRODUCCIÓN

En los últimos años el término “Seguridad de la Información” ha evolucionado de manera considerable, esto es por el constante avance de los sistemas informáticos y de la necesidad de desarrollar herramientas automáticas para proteger los archivos y la información que se almacena o se envía. De estas necesidades ha surgido la tarea de proteger la información, su autenticidad e integridad, y de permitir el acceso solo a personal autorizado.

A través del tiempo, desde antiguo Egipto a la era digital, los mensajes cifrados han jugado un papel destacado en la historia. Son la mejor defensa de las comunicaciones y datos que viajan por Internet o cualquier red local donde se intercambie información por un canal público o privado.

Hoy en día, en plena era de la información y gracias a la implementación de tecnologías de comunicación, que convergen cada vez más a una conectividad global, las cuestiones planteadas y estudiadas por la criptografía adquieren una importancia vital y despiertan mayor interés para el público en general. Lo que se pretende con este trabajo es introducirse en el fascinante mundo de la criptografía y seguridad de la información

1.2 SEGURIDAD DE LA INFORMACIÓN

Tiene como objetivo fundamental proteger la información, controlar el acceso a ella, evitar modificaciones y que no se comprometa o sufra algún daño.

Otros de los objetivos, es el de minimizar y gestionar los riesgos y detectar los posibles problemas y amenazas de seguridad. Garantizar la adecuada utilización de la información. Es en sí, asegurar la integridad, confidencialidad y disponibilidad de los activos de información, salvaguardarlos de un uso no autorizado, revelación, modificación, ya sea por daño o pérdida accidental o intencional.

Para comprender el tema de seguridad de la información, es necesario conocer las características de la información, que es lo que se pretende proteger.

Así que, dato es la unidad con la que se compone cierta información y la información es un conjunto de datos que tiene un significado específico más allá de cada uno de estos y tendrá un sentido particular según de la manera como sea procesada. Por ejemplo: C, R, U y Z son datos, en su conjunto es información, CRUZ.

El valor de la información no es fácil de establecer, porque constituye un recurso, que muchas veces no se valora adecuadamente debido a su intangibilidad.

Existe información que es, o debe de ser pública, significa que puede ser visualizada por cualquier persona; y también la información que debe ser privada y solo puede ser visualizada por personas que tengan acceso autorizado a ella. La información privada se debe mantener así, para preservarla de este modo, se debe tomar en cuenta lo siguiente:

- Crítica: es indispensable para garantizar la continuidad operativa.
- Valiosa: es un activo con valor en sí misma.
- Sensitiva: debe ser conocida por los usuarios que la procesan y solo por ellos, como puede ser información bancaria, contraseñas, en fin, datos personales.

La Seguridad de la información envuelve tres características fundamentales: confidencialidad, integridad y disponibilidad.

Todos los controles, salvaguardas, amenazas, vulnerabilidades y procedimientos relacionados con la seguridad de la información se basan en estos tres principios, su definición es la siguiente:

- Confidencialidad: Mediante este servicio o función de seguridad se garantiza que el contenido de cada mensaje transmitido o información en general solo podrá ser leído por el destinatario legítimo, en caso de que la información caiga en manos de otras personas, éstas no podrán tener acceso al contenido del mensaje. “Previene el descubrimiento no autorizado de la información”[1].
- Integridad: Este servicio se encarga de asegurar que no se realicen modificaciones a la información desde su creación o durante su transmisión, por personal o procesos no autorizados. “Previene una modificación no autorizada”[2].
- Disponibilidad: Este servicio es un poco complejo ya que es muy difícil poder garantizarla en su totalidad. La disponibilidad asegura que el acceso a la información se produzca correctamente y en tiempo. Es decir la disponibilidad da la garantía que los sistemas funcionan cuando se les necesita. “Previene la negación de acceso autorizado”[3].

Estos tres servicios de seguridad en su conjunto forman el llamado triangulo de oro de la seguridad de la información.

[1] Pfleeger, Charles P., Security in Computing, (2006), Data Confidentiality.
[2] Pfleeger, Charles P., Security in Computing, (2006), Data Integrity.
[3] Pfleeger, Charles P., Security in Computing, (2006), The meaning of Computer Security.

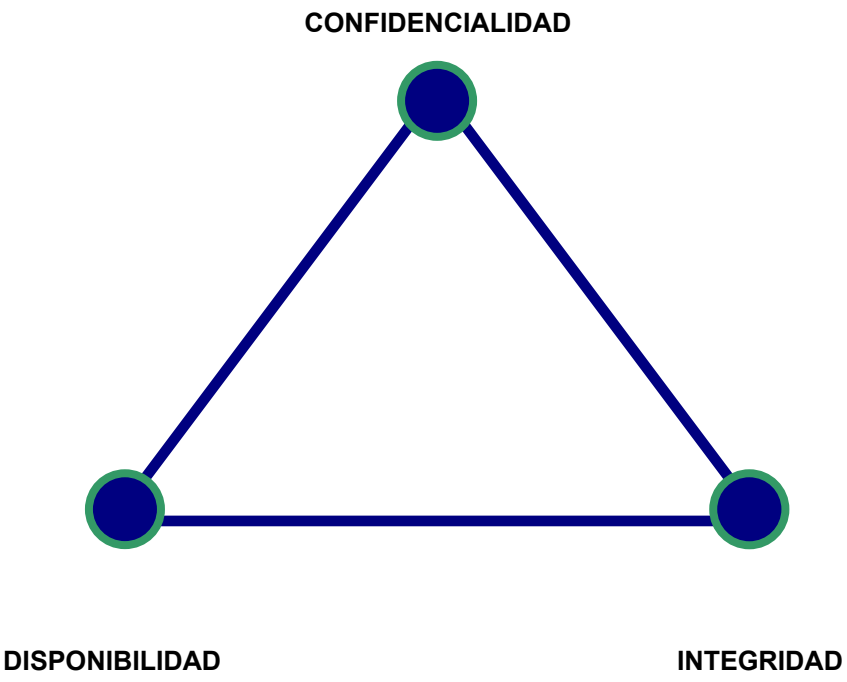

Figura 1. Triangulo de Oro de la Seguridad de la información.

No todas estas características deben estar vigentes al mismo tiempo, ni tampoco todas tienen la misma importancia en todas las circunstancias. Existen circunstancias en donde la confidencialidad es esencial, como en la guerra, en otros casos se requiere que la información sea auténtica como puede ser en inversiones, siempre se debe determinar cuáles de las propiedades son necesarias o importantes.

Se considera muy importante la integración de otros dos servicios que entrarían en un nuevo esquema que sería la pirámide de la seguridad de la información y son el control de acceso y a la autenticación.

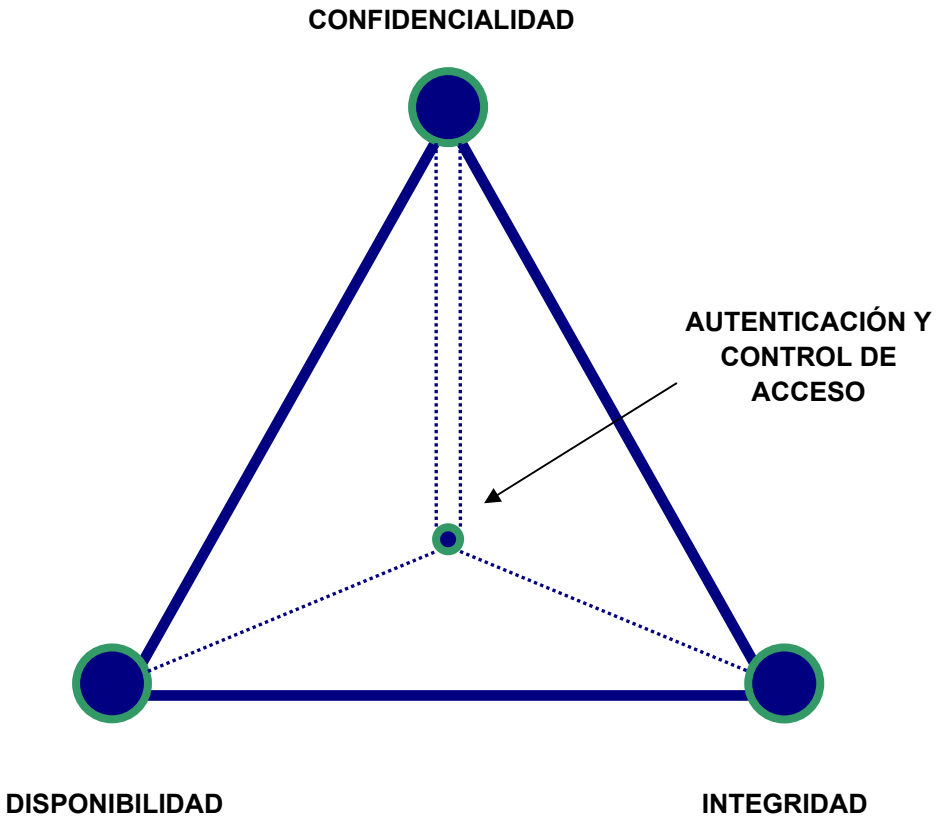

Figura 2. Pirámide de la seguridad de la Información.

La definición de estos dos servicios de seguridad es la siguiente:

- Autenticación: Garantiza que la identidad del emisor o creador de un mensaje sea legitimo, es decir, que el emisor es quien dice ser y el destinatario del mensaje esté seguro que el creador es la persona que figura como remitente del mensaje. "Por lo general la autenticación implica una combinación de algo que es, algo que se sabe y algo que se tiene"[4].

- Control de acceso: Después de la identificación y autenticación de un usuario, controlar la manera de acceder a los recursos, para esto se definen listas de control de acceso, con relación de usuarios y grupos de usuarios y los permisos de acceso a los recursos del sistema. "Es la capacidad de controlar y conocer quién y cuándo acceden a una zona, servicio o determinada información"[5].

[4] Hughes, Larry J., Actually Useful Internet Security Techniques, (1995), Capítulo 1, Encryption and Authentication, (p. 10).
[5] Aceituno, Vicente, SEGURIDAD DE LA INFORMACIÓN: Expectativas, riesgos y técnicas de protección, (2007), Capítulo 3, Control de accesos lógico y físico, (p. 74).

Se debe tomar en cuenta que una definición más amplia de seguridad de la información y sus servicios debe incluir: la seguridad física y seguridad del personal, esta última con relación a los usuarios que tienen relación directa con la información.

Siempre existe una gran cantidad de preocupaciones de quien puede tener acceso a la información y darle un mal uso, de usuarios que intentan acceder de manera no autorizada a la información, si la desean comercializar, en fin. Las respuestas a estas interrogantes varían porque el motivo puede ser por distintos factores como: vandalismo, ganancia monetaria, terrorismo o simplemente curiosidad por poner un ejemplo.

Para llevar a cabo una buena seguridad, se debe considerar independientemente de las razones que el intruso o atacante tenga, qué características de seguridad pueden ser violadas y cómo.

Por poner un ejemplo, las violaciones a la confidencialidad, pueden llevarse a cabo por medio de la intervención o monitoreo de canales o líneas; para la autenticación, un método simple de violarla es pidiendo la contraseñas de acceso a la información, es decir persuadir al dueño de la llave para obtenerla, estos es conocido como ingeniería social. En el caso de la disponibilidad puede ser por una denegación de servicios, que impide utilizar los recursos y la información. Una vía o camino para llegar a tener la información segura, es la criptografía, que me permite implementar diferentes servicios de seguridad de manera separada o en su conjunto para implementar un alto nivel de seguridad de la información, ya sea personal u organizacional.

1.3 CRIPTOGRAFÍA

La criptografía está teniendo un gran auge últimamente ante el miedo de que una transmisión en Internet pueda ser interceptada y algún atacante pueda enterarse de alguna información que no debería. Y no estamos hablando de un correo electrónico en el que nos ponemos de acuerdo para ir al cine, nos referimos, por ejemplo, una transacción comercial de cientos de miles de pesos o una información sobre determinados temas críticos de una organización. Y el uso de la criptografía permite proteger esos datos que son importantes y garantizar que la información estará segura.

El cifrado es una herramienta sumamente importante para la seguridad de la información y que ha demostrado su utilidad desde hace miles de años.

1.3.1 Antecedentes

Desde la antigüedad los mensajes cifrados han jugado un papel importante, ya que surge la necesidad de transmitir y almacenar la información de tal manera que tenga confidencialidad y de esta necesidad surge la criptografía.

Cronología

1500 a. C.	Una tableta en Mesopotamia contiene una fórmula cifrada para producir un vidriado para cerámica.
500 – 600 a. C.	Un escribano hebreo que trabajó en el libro de Jeremías, usó un cifrado sencillo invirtiendo el alfabeto, conocido como cifrado de sustitución.
487 a. C.	Los griegos inventan un dispositivo llamado SCYTALE, es un bastón donde se enrolla un listón de cuero y se escribe sobre él, sólo alguien con el bastón del mismo diámetro podría leer el escrito.

Fuente: http://en.wikipedia.org/wiki/File:Skytale.png

Figura 3. Scytale.

50 -60 a. C.	Julio César usa un sistema simple de sustitución, desplazando el alfabeto unos cuantos caracteres, para cifrar la información.
855 d. C.	Aparece el primer libro de criptografía en Arabia.
1412	En Arabia se escribe una enciclopedia con 14 tomos donde se explican los conceptos de criptografía, contiene también

	las técnicas de sustitución y transposición, además se da la explicación del método de sustituciones repetidas de cada carácter del texto en claro.
1500	En Italia se produce un gran interés por la criptografía debido al desarrollo de la vida diplomática.
1518	Se hace la impresión del primer libro de criptografía llamado “Polygraphia libri sex”, escrito por Trithemius en alemán, en este libro se muestran cifrados monoalfabéticos con nuevas tablas de sustitución rectangulares.
1585	El francés Blaise de Vigenere publica su libro “Tractie de chiffre”, se presenta un sistema polialfabético con autoclave, conocido como “Le chiffre indechiffrable”, después se le cambio el nombre a cifrado de Vigenere. La autoclave se mantiene presente durante mucho tiempo y se aplica en estándares como DES (Data Encryption Standard), en los modos de cifrado de bloques y cifrado de flujo.
1795	Thomas Jefferson diseña el primer dispositivo de de cifrado cilíndrico, conocido como “Rueda de Jefferson”.
1854	Charles Wheatstone inventa un cifrado que utiliza una matriz de 5x5 como llave, posteriormente Lyon Playfair lo publica en ambientes militares y diplomáticos y se le conoce como cifrado Playfair.
1863	Friedrich Kasiski, desarrolla métodos estadísticos de criptoanálisis que rompen el cifrado de Vigenere.
1883	Auguste Kerckhoff publica “La Cryptographie militaire”, contiene los principios de Kerckhoff, la seguridad radica en un método de cifrado que se basa en la privacidad de la llave y no en el algoritmo.
1917	Gilbert Vernam desarrolla la cinta aleatoria de un solo uso, el único sistema criptográfico seguro.
1923	La máquina de rotores Enigma, diseñada por el alemán Arthur Scherbius y funda la compañía "Chiffriermaschinen AG" para comercializar Enigma en todo el mundo.
1929	Lester Hill publica el artículo "Cryptography in an Algebraic Alphabet". El cifrado de Hill aplica álgebra (multiplicación de matrices), para cifrar.

1973	David Bell y Len LaPadula desarrollan el modelo Bell-LaPadula que formaliza las normas de acceso a la información clasificada, con la intención de lograr la confidencialidad de los datos.
	Ellis, Cocks y Williamson desarrollan un algoritmo de cifrado de llave pública para el gobierno de la Gran Bretaña (GCHQ). Este descubrimiento se conoció públicamente hasta 1997. Debido a esto, los métodos de cifrado asimétrico serán nuevamente reconstruidos de forma independiente y, esta vez sí, públicamente por Diffie, Hellman, Rivest, Shamir y Adleman, que son considerados los descubridores de la criptografía de clave pública.
1975	Diffie y Hellman describen que los procedimientos de llave pública son teóricamente posibles, aunque se desee demostrar lo contrario.
1976	Diffie y Hellman publican "New Directions in Cryptography".
	Que es una introducción a un nuevo método de distribución de llaves criptográficas, lo que era hasta la fecha uno de los problemas fundamentales de la criptografía. Este mecanismo será conocido como el protocolo Diffie-Hellman de intercambio de claves.
1977	El algoritmo inventado por IBM en 1975, DES (Data Encryption Standard), es elegido por el NIST (National Institute od Standards and Technology, FIPS PUB-46) como el algoritmo de cifrado estándar de Estados Unidos de América.
	Ronald Rivest, Adi Shamir y Leonard Adleman desarrollan y publican el algoritmo RSA (Rivest, Shamir, Adleman). Este es el primer procedimiento de llave pública utilizado en la práctica y es considerada la contribución criptográfica más innovadora del siglo.
1979	Los primeros cajeros automáticos ATM (Automatic Teller Machines), utilizan DES para cifrar los códigos PIN.
1982	Richard Feynman diseña el modelo teórico de una computadora cuántica.
1984	Charles Bennett y Gilles Brassard describen la criptografía cuántica.
1986	Neal Koblitz y Victor Miller proponen usar curvas elípticas como modelo de criptografía de llave pública.

1991	Xueija y Massey desarrollan el algoritmo IDEA (International Data Encryption Algorithm), que se usará en el software criptográfico PGP (Pretty Good Privacy). DSA (Digital Signature Algorithm) es elegido por el NIST como algoritmo estándar para las firmas digitales. PGP es diseñado por Phil Zimmermann como un software gratuito y de código libre, cuya finalidad es cifrar e intercambiar archivos con un alto nivel seguridad. En este programa para usuarios finales es aplicada la criptografía híbrida, que es la combinación de criptografía simétrica y asimétrica.
1994	El protocolo de cifrado SSL (Secure Socket Layer), es publicado por Netscape Communications y todos los navegadores Web lo soportan.
1995	S/MIME (Secure/Multipurpose Internet Mail Extensions), es un estándar para firmado de correo y criptografía de llave pública para la seguridad del correo electrónico, y es apoyado por todos los clientes de correo. Se basa en el estándar de Internet MIME.
1998	Deep Crack, rompe una clave DES con un ataque de texto claro conocido, posteriormente los laboratorios de RSA lanzan el desafío 2DES.
1999	Nuevamente Deep Crack con la colaboración de Distributed.net rompen una clave DES con un ataque basado en texto claro conocido, por consiguiente RSA lanza el desafío 3DES.
2000	Después de una competencia de 5 años el NIST elige al sucesor del DES, el algoritmo Rijndael es el ganador y se denomina AES (Advanced Encryption Standard).

Los métodos clásicos no son muy confiables en la actualidad, en algunos casos basta con hacer cálculos simples para descubrir los mensajes ocultos o simplemente la intuición que es un arma esencial de todos aquellos que descifran información, llamados criptoanalistas.

En escritos medievales se encontraron anagramas, por ejemplo, términos como: otsenre, aquellos que escribían libros a manos utilizaban anagramas alterando el uso de las letras (es este caso otsenre, anagrama de ernesto).

La criptografía antigua y hasta mediados del siglo pasado se consideraba una era pre – científica de la criptografía, esto no es porque carezca de interés actual o no funcione ya, sino que ese tipo de criptografía fue practicada y entendida como un arte y no como una ciencia.

Es una ciencia porque se rige por reglas matemáticas, pero también es un arte porque no hay forma de saber cuándo un sistema de cifrado es bueno.

1.3.2 Definición

La palabra criptografía "de las voces griegas ***kryptos***, escondido y ***graphein***, escribir, es el arte de escribir con signos convencionales y con objeto de impedir que el que no posea la clave de los mismos, puede penetrar su significado"[6].

La criptografía es el arte para ocultar la información, transforma la información legible en información ilegible con un elemento único conocido como llave, de tal modo que solo el poseedor de la llave pueda leerla.

1.3.3 Objetivo

El objetivo de la criptografía es proporcionar los servicios de seguridad que son confidencialidad, autenticación, integridad y no repudio. Asimismo garantizar el secreto en la comunicación entre dos partes (personas, organizaciones, etc.) también, asegurar que la información que se envía es auténtica en un doble sentido: que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado, habitualmente denominado criptograma, no haya sido modificado en su tránsito.

1.3.4 Clasificación

En la criptografía se pueden distinguir dos tipos que son: simétrica y asimétrica, dependiendo de la llave que se utiliza.

En el cifrado simétrico (también llamado cifrado de llave privada o cifrado de llave secreta) se emplea la misma llave en el proceso de cifrado y descifrado, mientras tanto en el cifrado asimétrico (también llamado cifrado de llave pública) utilizan dos llaves distintas pero que tienen relación entre sí, una para el cifrado y otra para el descifrado.

[6] ENCICLOPEDIA VNIVERSAL ILVSTRADA, (1995), Tomo 16, Criptografía, (p. 205).

1.3.4.1 Criptografía Simétrica

Es llamada también criptografía clásica, ya que fue la única que se utilizó hasta 1970. Funciona usando la misma llave para el proceso de cifrado y descifrado. La llave secreta debe ser acordada con anterioridad a través de un canal seguro, una vez acordada debe mantenerse secreta porque de ello depende la confidencialidad y la seguridad del cifrado en los mensajes que se envían.

Se implementa predeterminando un algoritmo de cifrado y así asignar a cada una de las partes una llave secreta, esta llave secreta se emplea para cifrar y descifrar los mensajes. “El término llave secreta implica que la seguridad de un mensaje cifrado radica en la capacidad de engañar al remitente y el receptor para mantener la llave en secreto”[7].

Dado que toda la seguridad se centra en la llave, esta tiene que ser difícil de adivinar.

Algunos algoritmos simétricos son: AES, DES, 3DES, IDEA.

Uno de los principales inconvenientes del cifrado simétrico, es que no está ligado a los algoritmos, sino al intercambio de llaves y el secreto de las mismas. El canal utilizado para el intercambio debe ser lo suficientemente seguro. Una vez que el remitente y el destinatario hayan intercambiado las llaves pueden usarlas para comunicarse con seguridad. Cabe mencionar que este sistema no es recomendable en grupos grandes de personas porque el número de llaves sería enorme, para solucionar este tipo de problema existe la criptografía asimétrica y criptografía híbrida.

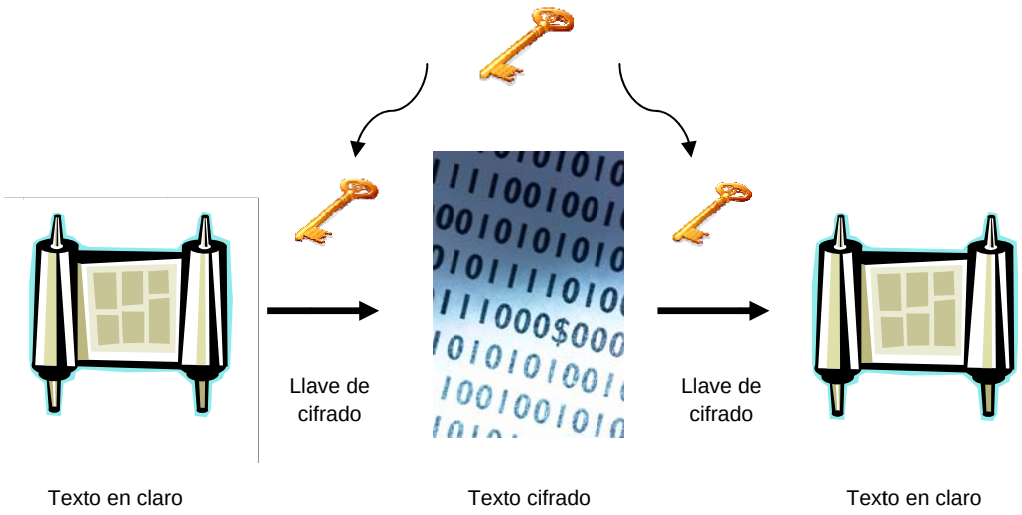

Figura 4. Proceso de cifrado simétrico.

[7] Hughes, Larry J., Actually Useful Internet Security Techniques, (1995), Capítulo 2, Data Confidentiality and Integrity, (p. 47).

1.3.4.2 Criptografía Asimétrica

En este tipo de criptografía cada usuario tiene 2 llaves, una pública que todo el mundo conoce y otra privada que solamente él conoce. “La criptografía de llave pública siempre usa diferentes llaves para el cifrado y descifrado, con la característica esencial que una llave no puede ser sacada de la otra”[8].

Aquel que desee enviar información a una entidad, cifra esa información usando la llave pública de esa entidad. Por su parte la entidad receptora es la única que puede descifrar ese mensaje y lo hace usando su llave privada. Los mensajes que son cifrados con una llave pública no se pueden descifrar con esa llave pública.

Este tipo de sistema de criptografía asimétrica se basa en la construcción de funciones matemáticas cuyo inverso sea computacionalmente imposible de determinar. Lo que quiere decir que es imposible deducir la llave privada a partir de la llave pública.

Los estándares utilizados para este tipo de criptografía son: RSA, ElGamal, Diffie – Hellman, criptografía de curvas elípticas.

Las llaves públicas y privadas son otorgadas por una autoridad de certificación, aunque ambas llaves son propias de cada persona. Para que todo funcione de manera correcta la llave pública se debe hacer pública, la llave privada debe mantenerse en secreto, si se compromete, no habrá seguridad.

Al cifrar con la llave pública se logra autenticación y confidencialidad.

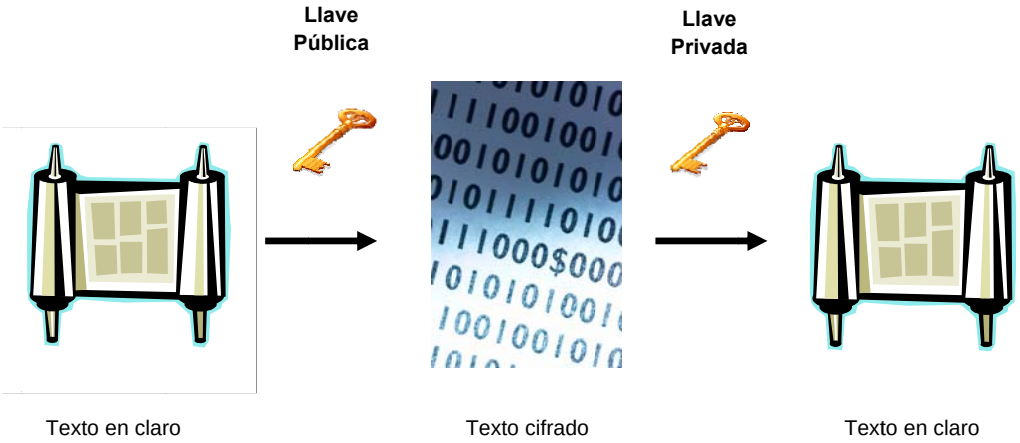

Figura 5. Proceso de Cifrado Asimétrico con Llave Pública.

[8] Hughes, Larry J., Actually Useful Internet Security Techniques, (1995), Capítulo 2, Data Confidentiality and Integrity, (p. 48).

También, se puede cifrar con la llave privada y descifrar con la llave pública, la diferencia es que no proporciona confidencialidad ya que cualquiera puede descifrar un mensaje cifrado con una llave privada ya que se puede obtener siempre la llave pública.

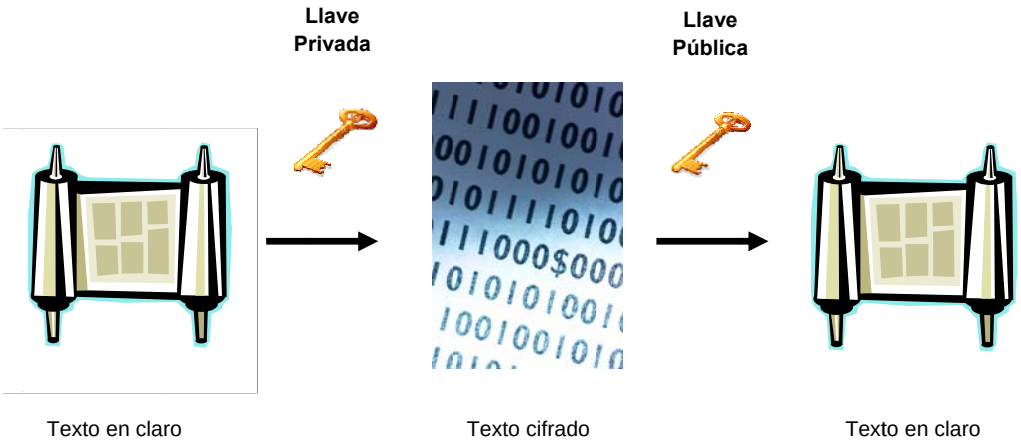

Figura 6. Proceso de Cifrado Asimétrico con Llave Privada.

RSA es el algoritmo de llave pública más utilizado, este algoritmo es reversible, es decir, además de permitir cifrar con la clave pública y descifrar con la privada, permite cifrar con la llave privada y descifrar con la llave pública.

Algunas de las características cruciales es que la llave secreta ya no se transmite entre las entidades y tampoco es necesario tener llaves diferentes para cada pareja de entidades, es suficiente con que cada usuario tenga su pareja de llaves.

1.4 FIRMAS DIGITALES

La firma digital es la información cifrada que identifica al autor de un documento y autentica su identidad, también lo relaciona con una llave, esta debe ser la privada.

La firma digital no implica que el mensaje esté cifrado, es decir, que este no pueda ser leído por otras personas, al igual que cuando se firma un documento en papel, este sí puede ser visualizado por otras personas.

La firma digital es un fragmento de información confidencial y propia de cada usuario, que se utiliza para asegurar y autorizar un documento. “El receptor o terceras personas pueden verificar que el documento y la firma corresponden a la persona que lo firma y que el documento no ha sido alterado”[9].

1.4.2 Firmas autógrafas y sus propiedades

La Real Academia de la Lengua define firma como: Nombre y apellido, o titulo, que una persona escribe de su propia mano en un documento, para darle autenticidad o expresar que aprueba su contenido.

La firma autógrafa contiene las siguientes características:

- Auténtica: El receptor del documento firmado debe estar convencido que el firmante voluntariamente firmó el documento.
- No reusable: La firma es parte del documento, es decir, no se puede mover a otro documento.
- Infalsificable: Probar que el firmante, nadie más, firmó el documento.
- Inalterable: Después de firmado el documento no podrá modificarse.
- No Repudio: El firmante no puede negar la firma.

Trasladar todas estas características al mundo digital, no fue sencillo, como es conocido, los documentos y archivos son fáciles de copiar y pegar, el texto puede ser copiado y pegado en otro documento y en general los documentos son fáciles de modificar. Este problema no tuvo solución hasta 1976 con la aparición de la criptografía de llave pública.

1.4.3 Procesos de la firma digital

La firma digital consta de dos procesos que son: el proceso de firma y el proceso de verificación de firma.

Una vez aplicada la función de firma al documento, se obtiene como resultado la firma digital; la firma se envía junto con el documento a la parte interesada. Por su parte el receptor debe verificar la validez de la firma, usando otra llave (esta es la llave pública o de verificación de firma). Si la verificación es válida, la firma se considera como auténtica, de lo contrario no es válida y se rechaza.

[9] Echenique, José, Auditoría en Informática, (2001), Capítulo 6, Encriptamiento, (p. 216).

Figura 7. Proceso de firma digital (Firmado y Verificación).

Aunque la firma digital se basa en esquemas de criptografía de llave pública, la función de firma no es un proceso de cifrado y la verificación de firma tampoco es un proceso de descifrado.

La firma digital produce el mismo efecto que una firma autógrafa, ya que es una marca que solo el firmante puede hacer y que los demás pueden reconocer, esto porque todos conocen la llave publica correspondiente.

Una firma digital proporciona los siguientes servicios de seguridad:

- Autenticación de identidad.
- Autenticación de origen de datos.
- Integridad.
- No Repudio.

Algunos algoritmos para firma digital son: ElGamal, DSA, DSS.

Se debe tener en cuenta que la firma digital es dependiente del documento y la firma autógrafa es independiente del documento.

1.5 CERTIFICADOS DIGITALES

Un certificado es un documento electrónico público y con la capacidad de que puede ser verificado, contiene información acerca de su propietario y es emitido por una tercera parte confiable denominada "Autoridad Certificadora" qué garantiza la vinculación entre la identidad de un sujeto o entidad y su llave pública, además esta entidad posee su correspondiente llave privada.

Los mecanismos que son usados en la generación de los certificados digitales garantizan que sólo la asociación certificadora pudo emitirlo.

"En el mundo digital, un certificado de llave pública, (también conocido como certificado digital, ID Digital o certificado), es un identificador que funciona como un medio para probar la identidad en transacciones electrónicas"[10].

Contiene información referente a:

- La llave pública del dueño.
- Nombre.
- Fecha de expiración.
- Nombre del emisor (Autoridad Certificadora que generó el certificado).
- Numero de serie.
- La firma digital del emisor, esta firma garantiza su autenticidad.

Para emitir un certificado digital la autoridad certificadora valida la identidad del suscriptor, firma digitalmente el certificado e incorpora su firma.

La seguridad del certificado digital radica en la generación del mismo, porque involucra algoritmos criptográficos para firmas digitales, esto hace imposible la falsificación, porque el falsificador necesita conocer la llave privada de la autoridad certificadora.

La confianza que un certificado digital otorga respecto a la identidad de un sujeto o entidad depende de, qué tan confiable sea la autoridad certificadora y de los mecanismos que esta utilice para proteger su llave privada.

[10] Daltabuit, Enrique, La seguridad de la información, (2007), Capítulo 4, Aplicaciones criptográficas, (p. 161).

1.5.1 Autoridad Certificadora

Es una entidad de confianza que certifica, emite certificados, autentica aplicaciones y mantiene información acerca de las entidades o sujetos. Estos certificados se utilizan para hacer posible el uso de las firmas digitales.

La autoridad certificadora posee su propio par de llaves y firma digitalmente los certificados con su llave privada, de tal manera que si se confía en la firma digital de la autoridad certificadora, entonces se puede confiar de igual manera en los certificados que genera.

Las autoridades certificadoras pueden tener un alcance interno o local, o pueden ser organizaciones que se dedican comercialmente a emitir certificados. Algunas autoridades certificadoras comerciales son:

- Verisign.
- Cyber Trust.
- CertCo.

1.5.2 Aplicaciones de los Certificados Digitales

Por la fácil adaptación y sus características de seguridad, pueden ser utilizados en una gran cantidad de aplicaciones como:

- Forma segura para la distribución de llaves públicas en grandes comunidades.
- Como un mecanismo de no repudio.
- Implementación de servicios de autenticación e identificación.

Las aplicaciones más populares en donde pueden utilizarse son:

- Código Seguro.
- Correo Electrónico (e-mail).
- Seguridad en servidores.
- Control de acceso.

1.5.3 Estándares PKCS

Es un grupo de estándares de criptografía asimétrica (de sus siglas en inglés, **P**ublic **K**ey **C**ryptography **S**tandards).

Facilitan el desarrollo y compatibilidad de la infraestructura para el manejo de certificados digitales.

Son independientes del ambiente de la aplicación y definen lo siguiente:

- Mecanismos de seguridad.
- Mensajes.
- Estructura de datos.
- Procedimientos de manejo de información para firmas digitales y certificados.

Los elementos de los certificados digitales que se han estandarizado son los siguientes:

- Formato de certificados (X.509).
- Solicitudes de Certificación (PKCS#10).
- Formato para enviar el certificado al solicitante (PKCS#7).
- Formato para transferir y almacenar certificados de llave privada (PKCS#12).

1.5.4 Certificados X.509

Un certificado digital es representado como una estructura de datos definida por el estándar X.509. “Este estándar fue publicado por primera vez en 1988 por la International Telecommunication Union – Telecommunications Standarization Sector (ITU-T) e ISO / International Electromechanical Commision”[11].

En el año de 1996 se publicó la versión 3, la cual es utilizada en la actualidad.

[11] Daltabuit, Enrique, La seguridad de la información, (2007), Capítulo 4, Aplicaciones criptográficas, (p. 170).

El certificado X.509 tiene la siguiente estructura:

- Versión: Este campo contiene el número de versión del certificado, los valores válidos actualmente son: 1, 2 y 3.

- Número de serie del certificado: Es un número de serie asignado por una autoridad certificadora. Cada certificado emitido debe tener un número de serie único.

- Identificador del algoritmo de firma: Este campo identifica el algoritmo de firma utilizado por la autoridad certificadora para firmar el certificado, por ejemplo: RSA o DSA.

- Nombre del emisor: Identifica la autoridad certificadora que firmó y emitió el certificado.

- Periodo de validez: Contiene el intervalo de tiempo durante el cual el certificado es considerado válido. Está formado por la fecha en la que el certificado comienza a ser válido y la fecha en la que el certificado deja de ser válido.

- Nombre del sujeto: Este campo identifica a la entidad cuya llave pública está siendo certificada. El nombre del sujeto debe ser único para cada sujeto certificado por una autoridad certificadora. Sin embargo, una autoridad certificadora puede emitir más de un certificado para el mismo nombre de sujeto, asumiendo que se trata de la misma entidad.

- Información de la llave pública del sujeto: Contiene la llave pública, parámetros y el identificador del algoritmo con el que la llave es usada.

- Identificador único del emisor: Este es un campo opcional, que permite reutilizar los nombres de emisor.

- Identificador único del sujeto: Este es un campo opcional, que permite reutilizar los nombres de sujeto.

- Extensiones: Proporcionan una manera de asociar información adicional para sujetos, llaves públicas, administración de la jerarquía de certificación y administración de listas de revocación. Un campo de extensión tiene tres partes:

    - Tipo de extensión: Es un identificador de objeto que proporciona la semántica y el tipo de información como: cadena de texto, fecha u otra estructura de datos.

    - Valor de la extensión: Contiene el valor actual del campo.

    - Indicador de importancia: Indica a una aplicación si es seguro ignorar el campo de extensión si no reconoce el tipo de extensión.

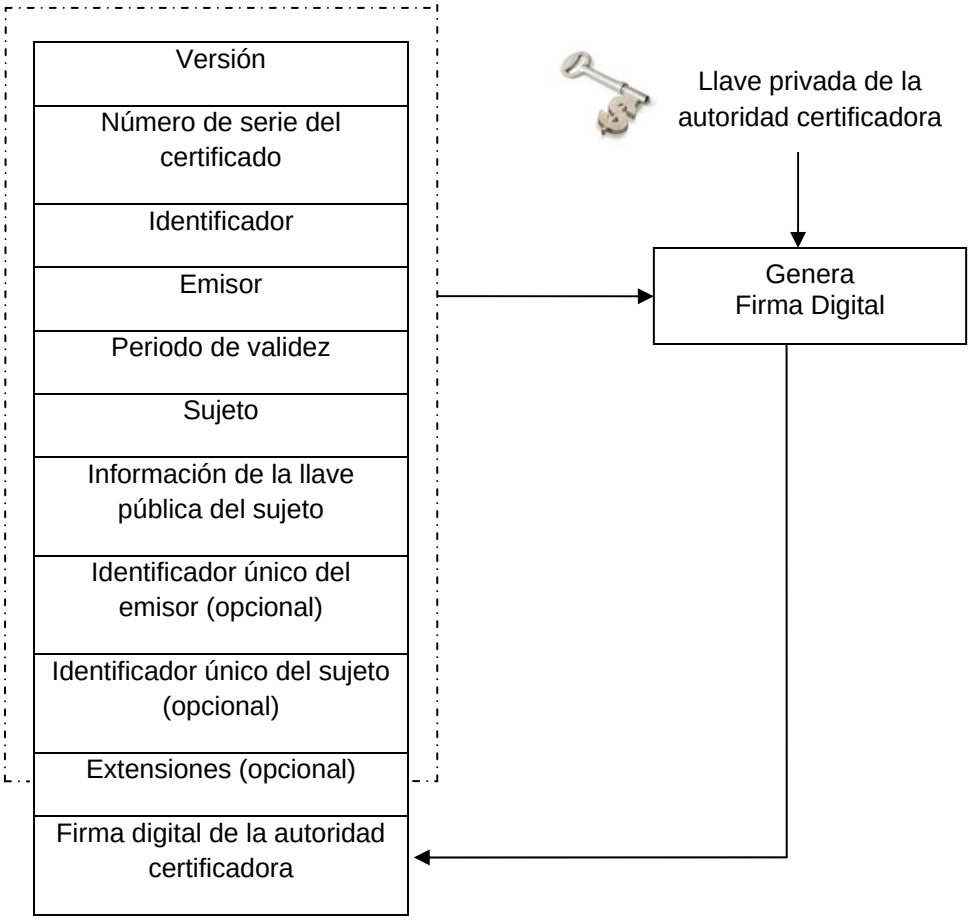

Figura 8. Estructura de un certificado X.509.

1.6 CORREO ELECTRÓNICO SEGURO

Uno de los servicios más conocidos y utilizados en internet es el correo electrónico, que permite a los usuarios tener una comunicación rápida y de bajo costo, para enviar y recibir mensajes.

El correo electrónico tiene origen el 1 de octubre de 1971, cuando el investigador Ray Tomlinson, escribió el primer mensaje entre dos ordenadores conectados en red.

Actualmente el correo electrónico no solo me permite enviar texto, sino todo tipo de documentos digitales, por ello en muchos casos este tipo de correo está desplazando al correo convencional, por su facilidad de uso y eficiencia.

Debido al gran uso de este servicio de internet, se tiene problemas de confidencialidad e integridad de los mensajes que enviamos a diario, por tal motivo se tuvo que llegar a la utilización de correo electrónico seguro.

Existen distintas maneras de poder asegurar nuestra información, la utilización de la criptografía es una de ellas, así como también la implementación de firmas y certificados digitales.

Para garantizar la seguridad en un correo electrónico en una red es necesario contar con un sistema seguro desde el emisor hasta el receptor.

La implementación de seguridad en el correo electrónico de remitente a destinatario, necesita:

- Usar criptografía de llave secreta para garantizar la confidencialidad.
- Usar criptografía de llave pública para autenticación y no repudio.
- Y una infraestructura formal de llave pública para asignar responsabilidades.

Entre los protocolos de correo electrónico seguro, se encuentran:

- Pretty Good Privacy (PGP).
- Secure / Multipurpose Internet Mail Extensions (S/MIME).

1.6.1 S/MIME

S/MIME es un proceso que me permite intercambiar correo electrónico de manera segura y garantiza la confidencialidad y autenticación de los mensajes.

Se basa en estándares de llave pública, es decir, permite cifrar el contenido del mensaje pero no la comunicación.

"S/MIME es un sistema desarrollado por RSA en 1995, como una variante del formato de correo MIME, basándose en el estándar de tecnología de llave pública PKCS#7 (estándar que define la sintaxis para los mensajes criptográficos)"[12].

Para crear mensajes, S/MIME debe basarse en la especificación PKCS#7, que hace referencia a la sintaxis del mensaje.

[12] Gómez, Álvaro, (2007), Enciclopedia de la Seguridad Informática, Capítulo 22, Utilización segura del correo electrónico, (p. 500).

S/MIME implementa los siguientes servicios:

- Autenticación del origen del mensaje: Firma digital.
- Verificación de integridad del mensaje: Firma digital.
- No repudio de origen: Firma digital.
- Confidencialidad del mensaje: Cifrado.

1.6.2 PGP

Es un software que proporciona funciones criptográficas y de gestión de llaves, fue desarrollado inicialmente por Philip Zimmermann en 1991. Este software de puede utilizar para proteger cualquier tipo de datos como:

- Archivos.
- Discos duros.
- Conversaciones.
- Correo electrónico.

Una de las características que distingue a PGP es el método que utiliza para certificar la autenticidad de las llaves públicas. En lugar de acudir a autoridades de certificación, como lo hace S/MIME, cada uno de los usuarios puede certificar de forma directa las llaves que está convencido que son auténticas. Y puede tomar decisiones respecto a una llave desconocida en función de quienes sean los usuarios que hayan certificado esa llave.

Otra característica propia de PGP es la eficiencia en el intercambio de los mensajes, ya que siempre que sea posible los datos se comprimen antes de cifrarlos y/o después de firmarlos.

La principal diferencia entre S/MIME y PGP es el método de intercambio de llaves. Básicamente PGP depende de intercambio de llaves de cada usuario con todos los beneficiarios potenciales y el establecimiento de un círculo de destinatarios de confianza, sino que también requiere el establecimiento de un grado de confianza en la autenticidad de las llaves para los beneficiarios.

S/MIME utiliza jerárquicamente certificados validados, por lo general representado en formato X.509, para el intercambio de llaves.

Así, “con S/MIME, el remitente y el destinatario no es necesario que se hayan intercambiado las llaves de antemano, debido que tienen una autoridad certificadora en común que brinda la confianza”[13].

[13] Pfleeger, Charles P., Security in Computing, (2006), Secure E – Mail, S/MIME.

CAPITULO 2: SISTEMA DE CRIPTOGRAFÍA ASIMÉTRICA Y PROCESO DE FIRMA DIGITAL

2.1 INTRODUCCIÓN

El objetivo real de una infraestructura de seguridad es la aplicación de tecnologías, políticas y procedimientos que hagan valer los principios de integridad, confidencialidad, autenticación y disponibilidad. Una infraestructura segura me permite tener la información sensible bien protegida.

Las tecnologías de cifrado asimétrico y las infraestructuras de llaves públicas son ejemplos de tecnologías y políticas que surgen para la seguridad en el intercambio de información.

La criptografía de llave pública me permite implementar seguridad en las comunicaciones de tal manera que la información que necesite ser confidencial, pueda ser protegida con técnicas de cifrado, cuando dicha información sea enviada a otras personas a nivel local o público. Estas técnicas también me permiten asegurar que la información enviada no sufra modificaciones durante su transmisión, de tal manera que también puedo confirmar quien envió la información y saber que es autentica.

Otra posibilidad que me da el uso de la criptografía de llave pública son las firmas digitales, para poder firmar documentos o correo electrónico. La naturaleza las firmas digitales es igual que las firmas autógrafas y su autenticidad no puede repudiarse o negarse.

Los certificados digitales también forman parte de la criptografía asimétrica, con ellos enviamos nuestras llaves públicas, en fin estas distintas técnicas hacen posible una infraestructura de llave pública.

2.2 INFRAESTRUCTURA DE LLAVE PÚBLICA

Permite a los usuarios poner en práctica criptografía asimétrica, PKI (de sus siglas en inglés, **P**ublic **K**ey **I**nfrastructure), es una combinación de software, hardware, tecnologías de cifrado y servicios que permiten proteger las transmisiones de información.

PKI es un sistema para la gestión de certificados digitales y aplicaciones de firma digital, es la integración de criptografía simétrica, asimétrica y funciones de digestión o Hash.

PKI ofrece a cada uno de los usuarios un conjunto de servicios relacionados con la identificación y el control de acceso, como:

- Crear certificados que asocian la identidad de un usuario con una llave pública.
- Dar a conocer certificados desde una base de datos.
- Agregar credibilidad a la autenticidad del certificado.
- Confirmar o negar que el certificado sea válido.
- Invalidar certificados para los usuarios que no tengan acceso permitido o si llave privada ha sido expuesta.

Una PKI debe garantizar lo siguiente:

- Integridad.
- Confidencialidad.
- Autenticación.
- No repudiación.

"A menudo PKI, es considerado un estándar, ya que es un conjunto de políticas, productos y procedimientos, que se dejan a la interpretación sin tener un sentido estricto"[14].

Las políticas definen las reglas conforme a los cuales los sistemas criptográficos deberían funcionar, también especifican como manejar llaves y la información valiosa y como igualar el nivel de control al nivel de riesgo. Los procedimientos dictan como las llaves deberían ser generadas, manejadas y usadas. Finalmente, los productos en realidad ponen en práctica las políticas, y ellas generan, almacenan, y manejan las llaves.

El Proceso para construir una PKI deberá siempre partir de la definición de las políticas operativas y contemplar como requerimiento esencial el asegurar la calidad y seguridad de las operaciones que los usuarios finales realizan con sus llaves privadas, por ejemplo en la firma de correo.

[14] Pfleeger, Charles P., Security in Computing, (2006), Network Security Controls, PKI and Certificates.

2.2.1 Componentes

La infraestructura de llave pública está constituida por:

Figura 9. Componentes de una PKI.

- Autoridades de Certificación (AC):
  - Es la fuente de confianza de una infraestructura de llave pública.
  - Son quienes emiten los certificados digitales y los firman con su llave privada.
  - Almacenan los certificados en un repositorio público.
  - Certifican que la llave pública asignada en un certificado digital de una entidad o usuario final, corresponda realmente a dicha entidad o usuario final.
  - Gestiona la caducidad y revocación de los certificados. Esto significa que, tiene la facultad de verificar si un certificado tiene

aún vida útil o ha caducado y también puede revocar un certificado cuando se ha comprometido la llave privada.

- La fiabilidad de una autoridad certificadora radica en que nunca sea violada su llave privada.

- Autoridades de Registro (AR):
  - Realiza el proceso de registro de los usuarios o entidades.
  - Valida que los datos de un solicitante sean correctos para el certificado.
  - Verifica el enlace entre la identidad de su titular y la llave pública del certificado.
  - Genera el par de llaves (Pública y Privada).

- Repositorios
  - Guarda información de la PKI, como son los certificados y las listas de revocación de certificados.

- Listas de revocación de certificados:
  - Son listas de certificados que han dejado de ser válidos por algún motivo y por tanto en los que no se puede confiar.
  - Se pueden revocar en casos como: la llave privada ha sido comprometida o hayan cambiado los datos del certificado.

- Aplicaciones:
  - Es el software capaz de operar con los certificados digitales.
  - Estas aplicaciones son las que dan el valor real de la infraestructura de llave pública hacia el usuario.
  - Hacen posible por poner algún ejemplo, el uso de cifrado y firma digital en documentos o correo electrónico.

2.2.2 Propósito

La infraestructura de llave pública permite a los usuarios autenticarse frente a otros usuarios y usar la información de sus certificados, por ejemplo, cuando utilizan las llaves públicas de otros usuarios para cifrar y descifrar.

Un usuario puede firmar digitalmente mensajes usando su llave privada, y otro usuario puede validar que dicha firma (usando la llave pública del usuario, que está contenida en el certificado que ha sido emitido por una autoridad certificadora). Esto permite establecer una comunicación que garantiza la confidencialidad y la integridad de un mensaje y la autenticación de los usuarios sin tener que intercambiar previamente ninguna información secreta.

2.3 CRIPTOLOGÍA

La criptología es la ciencia para el ocultamiento de información y es un tema muy importante de investigación.

La palabra Criptología "de las voces griegas ***Kryptos***, oculto y ***logos***, tratado. Investigación de efectos producidos por causas ocultas"[15]. Se divide en dos áreas: Criptografía y Criptoanálisis.

2.3.1 Criptografía

La criptografía busca métodos para asegurar la confidencialidad, integridad y autenticación de los mensajes, transformando la información con un elemento llamado llave, de tal manera que una persona con malas intenciones o que no le pertenezca no pueda entenderla y que solo aquel que posea la llave pueda revertir esa transformación y sea entendible.

Siempre se debe tener en cuenta el valor y la vida útil de la información, que el costo de romper la seguridad exceda el valor de la información asegurada y que el tiempo requerido para romper la seguridad no exceda el tiempo de vida útil de la información.

Una cifra o algoritmo de cifrado es un método que convierte un texto en claro (normal), "**M**", en un texto secreto (cifrado), "**C**". El proceso de convertir "**M**" en "**C**" se le llama cifrado y el proceso inverso se le llama descifrado. El elemento esencial de ambos procesos es lo que se conoce como llave, "**K**".

[15] ENCICLOPEDIA VNIVERSAL ILVSTRADA, (1995), Tomo 16, Criptografía, (p. 220).

La base de la criptografía son los algoritmos de cifrado, que son funciones matemáticas usadas para cifrar y descifrar mensajes.

Un criptosistema es un sistema o implementación de un algoritmo de cifrado que incluye:

- Mensaje en claro, "**M**".
- Llave de cifrado, "$\mathbf{K_c}$".
- Proceso de cifrado.
- Texto cifrado, "**C**".
- Proceso de descifrado.
- Llave de descifrado, "$\mathbf{K_d}$".

La seguridad de un cifrado puede basarse en el secreto de su algoritmo, esto es común pero inseguro, se le denomina "seguridad por oscuridad".

La seguridad debe basarse en el algoritmo y la llave, el algoritmo y los detalles de su implementación, deber ser conocidos públicamente.

El espacio de llaves, es un aspecto muy importante y es utilizado en la criptografía de nuestros tiempos y se basa en usar llaves seleccionadas de un gran espacio, por ejemplo:

- Una llave de 1024 bits, tiene un espacio de $\mathbf{2^{1024}}$ posibles llaves, la seguridad se basa en el secreto de la llave, no en los detalles del algoritmo.

La notación criptográfica de un mensaje cifrado es:

Para un mensaje en claro "**M**", el cifrado de "**M**", con la llave "**K**", para producir el texto cifrado "**C**", se denota:

$$\mathbf{K_c\,(M) = C}$$

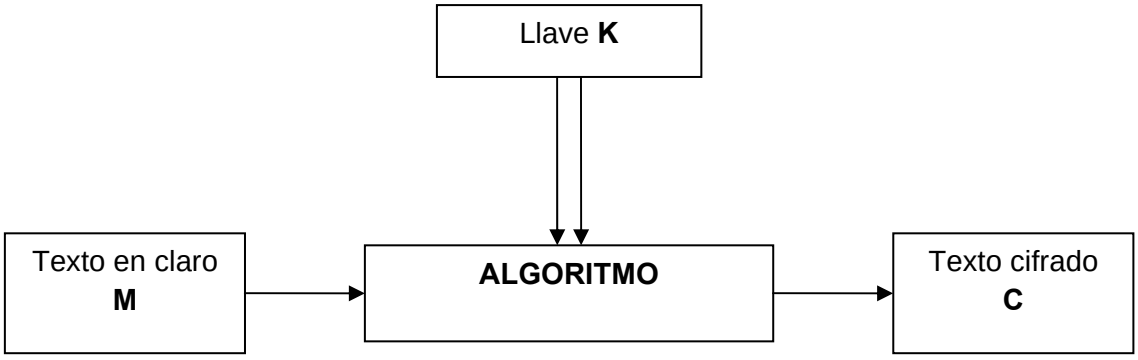

Figura 10. Proceso de cifrado.

Similarmente, el descifrado de "**C**", con la llave "**K**", para recuperar "**M**", se denota:

$$\mathbf{K_d\,(C) = M}$$

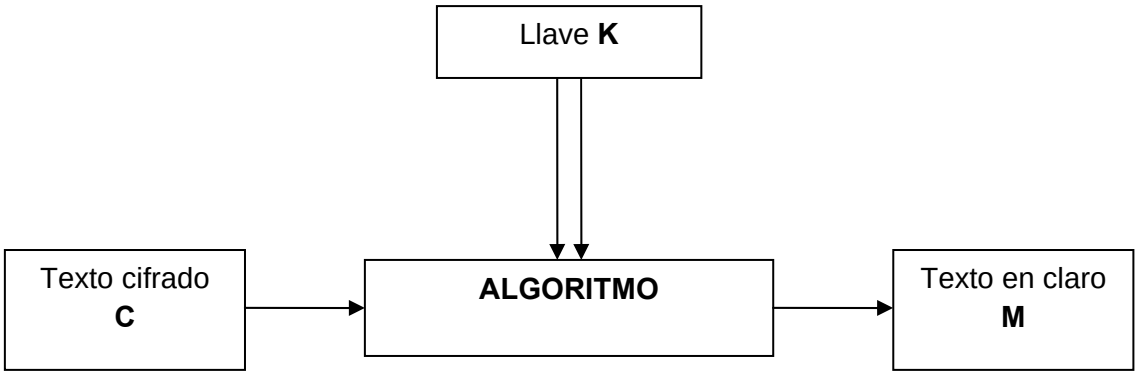

Figura 11. Proceso de descifrado.

Nótese que:

- $K_c\,(K_d\,(M)) = M$, para algoritmos de llave simétrica.
- $K1_c\,(K2_d\,(M)) = M$, para algoritmos de llave asimétrica.

La criptografía se clasifica de la siguiente manera:

- Por el número de llaves
  - Simétrica o de llave secreta: Se usa una única llave para cifrar y descifrar.
  - Asimétrica o de llave pública: Se usan dos llaves, una pública y otra privada, lo que se cifra con una llave, se descifra con la otra y viceversa.
  - Funciones Hash o de resumen: Ninguna llave, entrada variable y salida fija.

- Por el modo de proceso
  - Por bloque: Cifra la información en bloques de longitud fija, es decir, parte la información en pedazos y los va cifrando.

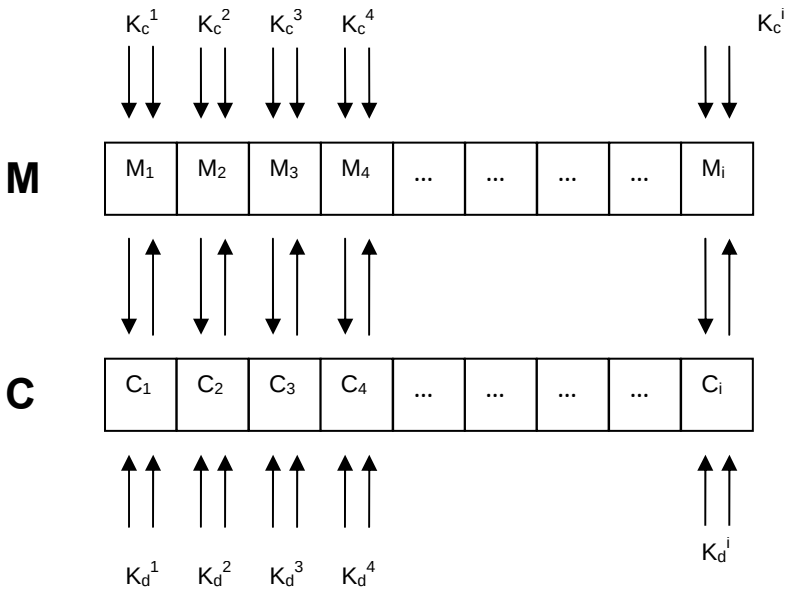

Figura 12. Cifrado por bloques.

- Por flujo: cifra la información como un flujo de bytes, es decir, va uno por uno hasta terminar la cadena.

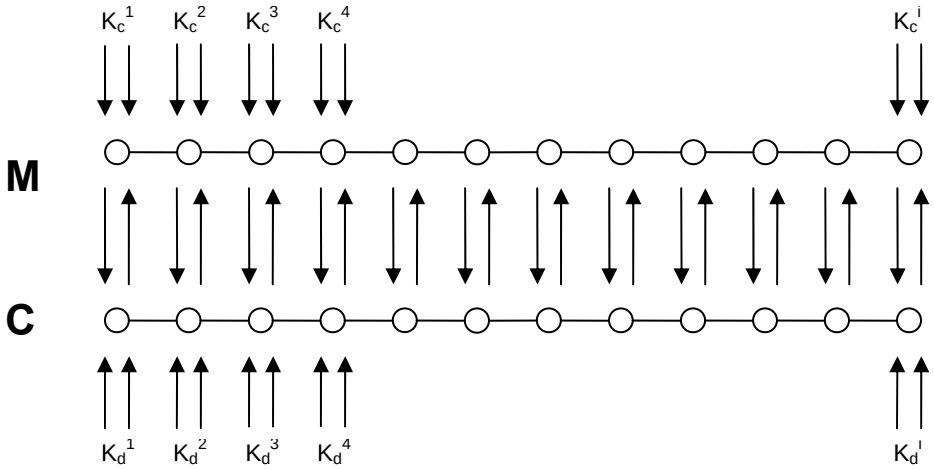

Figura 13. Cifrado por flujo.

o Por el tipo de operaciones

- Sustituciones: Es un mapeo de caracteres, es decir, cada carácter en **M** se reemplaza por un correspondiente carácter en **C**.

  M: a b c d e f g h i j k l m n o p q r s t u v w x y z.
  C: p g h z y t r a m b s n w e k x f l i u q j v c o d.

  Son todas las posibilidades que tiene todos los caracteres, es decir, se pueden mapear en todos los caracteres.

- Corrimientos: Cada carácter de **M** se reemplaza por un carácter de **K** posiciones a la derecha del alfabeto, según una llave.

  Por ejemplo, cuando la llave K=3.

  HOLA = KROD.

- Permutaciones o transposiciones: Es un rearreglo de caracteres, consiste en crear el texto cifrado simplemente desordenando los caracteres que forman el texto original según una llave. Por ejemplo la frase: “de la orden para empezar el ataque”, K=7.

1	***2***	***3***	***4***	***5***	***6***	***7***
D	***E***	***L***	***A***	***O***	***R***	***D***
E	***N***	***P***	***A***	***R***	***A***	***E***
M	***P***	***E***	***Z***	***A***	***R***	***E***
L	***A***	***T***	***A***	***Q***	***U***	***E***

Es igual a: DEML ENPA LPET AAZA ORAQ RARU DEEE

- Producto: Se llama cifrado producto a la aplicación iterativa de cifrados sobre textos ya cifrados, es decir, a la composición de varios cifrados. En general, los cifrados simétricos son cifrados producto de las dos operaciones mencionadas, sustitución y transposición.

Dentro de esta clasificación es importante mencionar las tareas que realizan la difusión y confusión, la primera me permite difundir la influencia de **M** y **K** en **C**, tanto como sea posible. Las permutaciones, son usadas para evitar deducciones de **K** por medio de relaciones estadísticas complicadas entre **M** y **C**. La confusión, oscurece la relación entre **M** y **C**. Con las sustituciones se hace confusión y con las permutaciones difusión.

2.3.2 Criptoanálisis

Es acto de recuperar **M** sin conocer **K**, es decir, busca romper los métodos de la criptografía sin el conocimiento alguno de la llave o bien, construir señales codificadas que puedan ser aceptadas como auténticas. La persona que lleva a cabo esta tarea se le denomina criptoanalista. “El criptoanálisis se ocupa del estudio de las técnicas y métodos que permite romper los algoritmos de encriptación”[16].

Existen distintos ataques por criptoanálisis como:

- Sólo texto cifrado: El atacante sólo cuenta con el texto cifrado **C**, sin conocer nada sobre su contenido.

[16] Gómez, Álvaro, Enciclopedia de la Seguridad Informática, (2007), Fundamentos y aplicaciones de la criptografía, Criptoanálisis, (p. 285).

- Texto en claro conocido: El atacante cuenta con parejas de texto en claro y texto cifrado. A partir de esto el criptoanalista puede descifrar el resto del mensaje cifrado, ya sea deduciendo la llave empleada a la hora de cifrar o aprovechando las palabras que tiene sin cifrar, este ataque es efectivo en sistemas de cifrado simétrico por bloques, ya que éstos cada palabra conserva su longitud inicial al cifrar el mensaje.

- Texto en claro escogido: El atacante puede elegir el texto en claro a cifrar y conocer el correspondiente texto cifrado sin el conocimiento de la llave. Esto permite comparar las transformaciones de diversos textos en claro.

- Texto cifrado escogido: El atacante puede escoger el texto cifrado y conocer el correspondiente texto en claro. De igual manera que el anterior se desconoce la llave empleada en el cifrado.

- Texto escogido adaptativo: El atacante puede escoger el texto, en claro o cifrado y lo adapta a sus necesidades.

- De prueba y ensayo: Es uno de los métodos más simples de todos, consiste en probar cada una de las posibles llaves hasta dar con el que permite descifrar el mensaje. Es un método lento si se realiza en una sola máquina, pero con la aparición de Internet y con ello la posibilidad de poner a trabajar una gran cantidad de equipos en paralelo es rápido.

- Con intermediario: El atacante básicamente usa su intuición en el momento en que las dos partes quieren enviarse información y están intercambiando sus llaves.

  El criptoanalista aprovecha ese momento para enviar a cada parte su propia llave, de esta manera el recibe primero los mensajes y luego los envía al destinatario legítimo, haciendo creer a ambas partes que el proceso de comunicación es seguro. Este método pone en manifiesto uno de los grandes inconvenientes del sistema de cifrado simétrico, que es el intercambio de llaves y se debe de realizar por un medio seguro, de lo contrario el atacante puede tenerlas fácilmente, y puede cifrar y descifrar sin problemas con absoluta transparencia, tanto para el emisor como el receptor.

El criptoanálisis normalmente utiliza las matemáticas como su mejor herramienta y las propiedades redundantes de los lenguajes. Se compone de las siguientes disciplinas:

- Teoría de números.

- Estadística.

- Probabilidad.

- Algebra.
- Teoría de matrices.
- Cálculo no lineal.
- Lenguaje de la comunicación.

Los criptoanalistas tienen el conocimiento sobre los algoritmos de cifrado y los detalles de su implementación, de igual manera cuentan con los recursos de cómputo y el tiempo suficientes, así como también el idioma que se utiliza.

2.3.2.1 Reglas de Kerckohffs

La suposición universal de la criptografía es que el criptoanalista tiene acceso completo al criptograma o texto cifrado **"C"**. Auguste Kerckhoffs, dijo que la seguridad del cifrado debe residir completamente en la llave secreta, dándonos cuenta que el mecanismo y resultado completo del cifrado es conocido por el criptoanalista, excepto el conocimiento de la llave secreta.

Kerckhoffs escribió en el siglo XIX un trabajo titulado, "La criptografía militar", ahí recomendó que todo sistema criptográfico debía cumplir las siguientes reglas, con el objetivo de evitar ser afectado por un ataque criptoanalista. Estas reglas han sido adoptadas por gran parte de la comunidad criptográfica y son las siguientes:

1) No debe de existir ninguna forma de recuperar mediante el texto cifrado, el texto inicial o la llave.
2) Todo sistema criptográfico ha de estar compuesto por dos tipos de información:
    - Pública: Son la serie de algoritmos que lo definen.
    - Privada: Son las llaves, en los sistemas asimétricos parte de la llave también es pública.
3) La llave escogida debe ser fácil de recordar y modificar.
4) La información cifrada ha de poder ser transmitida usando los medios de comunicación habituales.
5) La complejidad del proceso de recuperación del texto original debe corresponderse con el beneficio obtenido.

2.4 CRIPTOGRAFÍA ASIMÉTRICA O DE LLAVE PÚBLICA

En 1976, Whitfield Diffie y Martin Hellman, dos ingenieros electrónicos de la Universidad de Stanford publicaron el artículo, "New Directions in Cryptography", que creó una auténtica revolución en el mundo de la criptografía. Sugieren usar problemas computacionalmente inviables para el diseño de criptosistemas seguros.

La principal característica es que no se basa en una única llave sino en dos: una conocida, llamada llave pública y otra privada. Esto lleva al nacimiento de la criptografía de llave pública, el acuerdo de llave simétrica y la firma digital.

La idea consiste básicamente contar con una sistema de cifrado computacionalmente fácil (o al menos no difícil), de manera que el descifrado sea por el contrario, computacionalmente inviable a menos que se conozca la llave.

Se propuso utilizar distintas llaves para los procesos de cifrado y descifrado. La finalidad era que cualquier persona pudiera cifrar empleando una llave pública, pero que solo el verdadero destinatario pudiera descifrar el mensaje, al aplicar una llave privada. Y que el tiempo necesario para obtener un resultado, aun con las máquinas más potentes fuera tan elevado, que una vez resuelta la información fuera nula y no tuviera ninguna validez o utilidad.

"En pocas palabras se aprovechan de operaciones matemáticas (como potenciación y logaritmos, en un sentido simple, pero una inversa compleja), muy sencillas de realizar en un sentido, pero con una inversa extremadamente difícil de resolver"[17].

Para poder realizarlo, había que usar una transformación criptográfica $\mathbf{T_k}$ de fácil aplicación, pero de tal forma que sea muy difícil hallar la transformación inversa $\mathbf{T^{-1}_k}$, sin la llave de cifrado. La función $\mathbf{T_k}$ es, desde el punto de vista computacional, no invertible sin cierta información adicional (llave de descifrado) y es llamada función unidireccional o función trampa. En este tipo de sistemas de cifrado asimétrico se utiliza una llave de cifrado (llave pública), que determina la función trampa $\mathbf{T_k}$, y una llave de descifrado (llave privada) que permite el cálculo de la inversa $\mathbf{T^{-1}_k}$.

Los sistemas de llave pública más trascendentes: RSA y ElGamal, implementan las siguientes funciones matemáticas: la factorización de números primos grandes (RSA), o el cálculo de logaritmos discretos (ElGamal).

Cualquier usuario puede cifrar usando la llave pública, pero solo aquellos que conozcan la llave privada, pueden descifrar correctamente. Esto evita el problema de distribución de llaves del sistema de cifrado simétrico, y permite la autenticación y la firma digital, además garantizando la confidencialidad.

[17] Diffie, W. y M.E.Hellman. New directions in Cryptography, (1976), IEEE Transactions on Information Theory, Documento electrónico.

Para facilitar la tarea de los sistemas de criptografía asimétrica, las llaves públicas de todos los usuarios se organizan en directorios públicos de acceso libre, mientras que la llave privada sólo está en poder del propietario.

Según Diffie – Hellman en su artículo "New Directions in Cryptography", todo algoritmo de llave pública debe cumplir las siguientes propiedades de complejidad computacional:

1) Cualquier usuario puede calcular sus propias llaves, pública y privada, en tiempo polinomial.

2) El proceso de cifrado, utilizando la llave pública, ha de ser en tiempo polinomial.

3) El proceso de descifrado, utilizando la llave privada, ha de ser en tiempo polinomial.

4) El criptoanalista que intente averiguar la llave privada a partir de la pública, se encontrará con un problema intratable.

5) El proceso de descifrado de un criptograma teniendo la llave pública, se encontrara con un problema intratable.

"En la práctica, los diseñadores de algoritmos asimétricos se encuentran con cinco problemas. Los tres primeros, corresponden a las condiciones 1, 2 y 3, deben pertenecer a la clase polinomial. Los otros dos correspondientes a las condiciones 4 y 5 son problemas complejos"[18].

El funcionamiento de un sistema criptográfico asimétrico es el siguiente:

Un determinado usuario **B**, por poner un ejemplo, genera su pareja de llaves que están relacionadas entre sí, una de estas llaves se hace pública, porque es la que otros usuarios utilizan para cifrar la información al usuario **B**. El otro usuario **A**, por ejemplo, tiene que enviar información confidencial a **B**, debe cifrar la información utilizando la llave pública de **B**:

[18] Diffie, W. y M.E.Hellman. New directions in Cryptography, (1976), IEEE Transactions on Information Theory. Documento Electrónico.

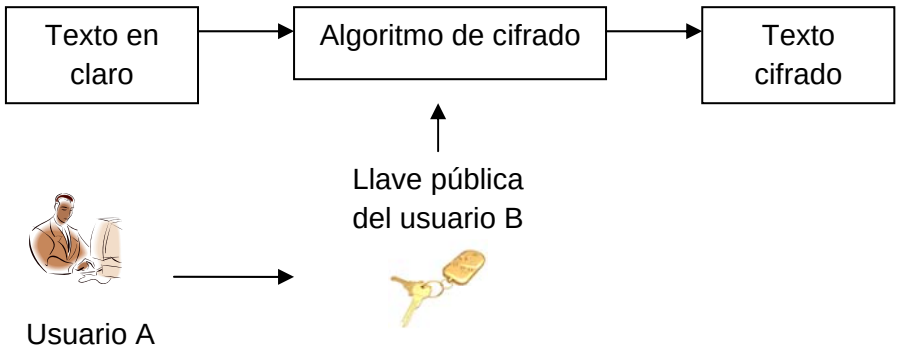

Figura 14. Cifrado mediante un algoritmo asimétrico.

El texto cifrado a partir de la llave pública de **B**, sólo puede ser descifrado utilizando la llave privada de **B** y el correspondiente algoritmo de descifrado.

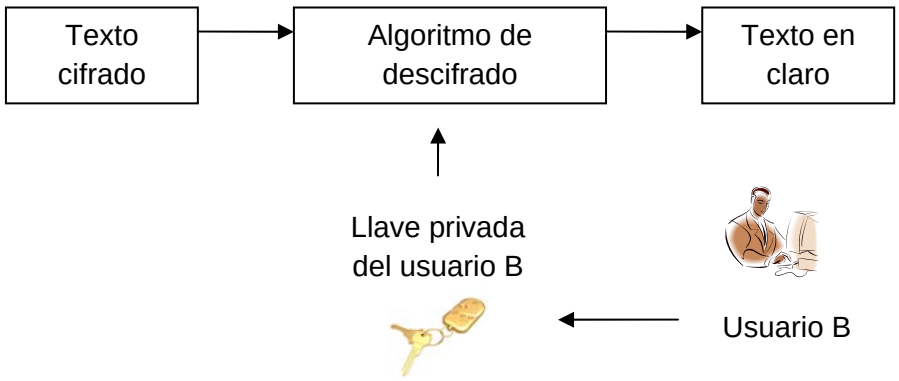

Figura 15. Descifrado mediante un algoritmo asimétrico.

Los algoritmos empleados en la criptografía de llave pública son más lentos y consumen muchos recursos computacionales, esto se debe a que realizan operaciones matemáticas más complejas.

Algunos de los algoritmos más utilizados son: RSA, Diffie – Hellman, ElGamal.

Estos algoritmos emplean llaves mucho más largas para tener un nivel de protección igual que los algoritmos simétricos: 512, 1024 ó 2048 bits, son entre 100 y 1000 veces más lentos que los simétricos.

Actualmente se ha venido investigando sobre algoritmos de llave pública basados en curvas elípticas, estos criptosistemas pretenden reducir el tamaño de las llaves de una manera considerable, por consecuente serían mucho más rápidos, por poner un ejemplo, una llave de 1024 bits sería equivalente a una de 106 bits con criptografía de curvas elípticas.

Los sistemas híbridos son una combinación de cifrado asimétrico con simétrico y cada unos presenta la siguiente funcionalidad:

- Se usa un algoritmo de llave pública para cifrar y descifrar, una llave compartida (como puede ser una llave DES, 3DES o AES).
- Posteriormente se cifra un mensaje con esa llave compartida.
- El mensaje cifrado y la llave compartida se cifran con la llave pública y se envían.
- El receptor usa el algoritmo de llave pública acordado para descifrar la llave compartida y luego usa esa llave descifrada para descifrar el mensaje.

En la práctica se recurre a los dos tipos de criptografía, mediante un sistema asimétrico los usuarios intercambian de forma segura la llave que se utiliza para cifrar y descifrar los datos de un sistema simétrico.

Por ejemplo un usuario **A** utiliza una determinada llave para cifrar el texto en claro y, a su vez, procede a cifrar esta misma llave con la llave pública del usuario **B**, de modo que sólo **B** pueda recuperar la llave necesaria para descifrar el texto en claro, ya que para obtener esta llave, es necesario utilizar la llave privada de **B**. En la siguiente figura se muestra el proceso de cifrado híbrido.

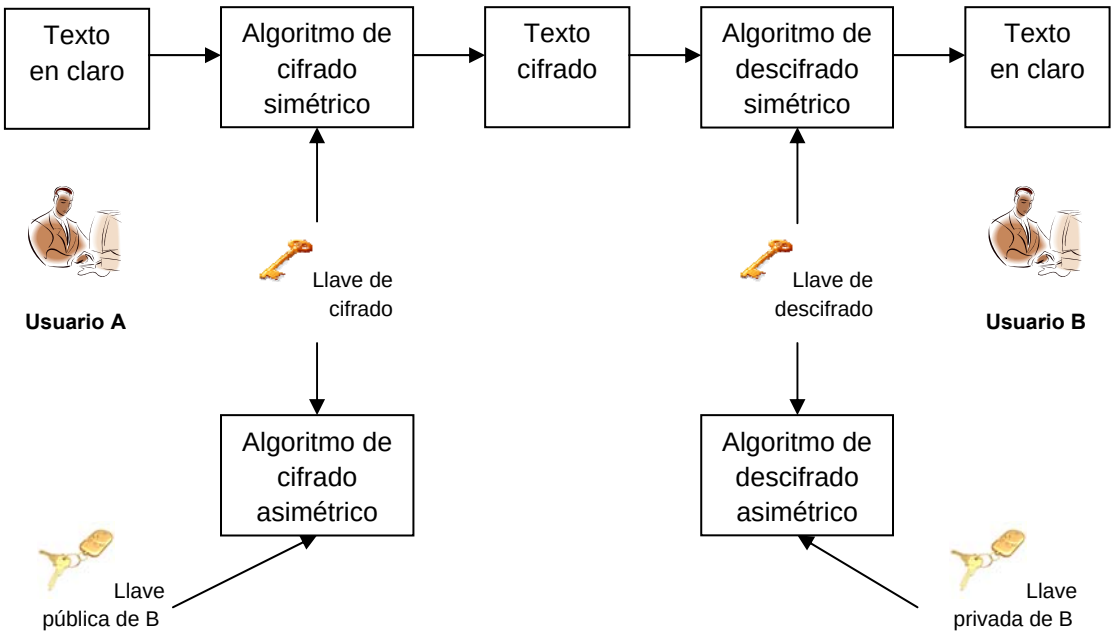

Figura 16. Combinación de sistemas criptográficos simétricos y asimétricos.

Al emplear sistemas híbridos, se garantiza la confidencialidad de la comunicación y agiliza los procesos de cifrado y descifrado.

2.4.1 Algoritmo RSA

Este algoritmo fue desarrollado en 1977 por Ronald **R**ivers, Adi **S**hamir y Leonard **A**dleman "**RSA**", el nombre proviene de cada uno de los apellidos de sus autores.

"El más conocido y sabido algoritmo de cifrado para la implementación de un criptosistema de llave pública es el sistema RSA. Internet para la privacidad del correo electrónico hace empleo del sistema RSA"[19].

La seguridad de RSA se basa en que no existe una forma eficiente de factorizar números que sean productos de dos primos grandes.

- Requerimientos:

[19] Siyan, Karanjit, INTERNET FIREWALLS AND NETWORK SECURITY, (1995), Background Information, Designing a network policy, (p. 135).

- Fácil para un usuario **B** generar su llave pública y privada.
- Fácil para **A**, conociendo la llave publica de **B** y un mensaje **M**, generar el mensaje cifrado **C**.
- Fácil para **B** descifrar **C**, usando su llave privada y recuperar **M**.
- Inviable determinar la llave privada de **B** a partir de conocer la llave pública de **B**.
- Inviable recuperar **M** a partir de la llave pública de **B** y **C**.

Los requerimientos son formidables, se necesita de una función unidireccional (One Way Function), esta mapea todas las entradas en un rango, tal que para todo valor de la función exista en inverso único. "De tal forma que calcular la función sea fácil, pero calcular el inverso sea difícil"[20].

- Características:
  - Algoritmo de llave pública: existen dos llaves, una pública y una privada, lo que se cifra con la llave pública sólo puede ser descifrado por la llave privada y viceversa.
  - Algoritmo considerablemente más seguro que DES, pero es considerablemente más lento que éste.
  - Se utiliza principalmente para la autenticación de mensajes y el intercambio de llaves secretas.

A continuación se mostrarán los procesos que lleva a cabo RSA:

- Proceso de obtención de llaves:

  El proceso de obtención de las dos llaves, pública y privada, es de la siguiente forma, todos los números y operaciones pertenecen al grupo de los enteros:

  - Hallar dos números primos grandes, **p** y **q** (secretos) y calcular el número **n** (público), mediante su producto, **n** = **p***q**.
  - Hallar la llave de descifrado constituida por un gran número entero impar, **d** (secreto), que es primo con el número **F**(**n**) (secreto), obteniendo mediante **F**(**n**) = (**p** – 1) * (**q** – 1).
  - Calcular el entero **e** (público) tal que **e***d** = 1(mod **F**(**n**)).

[20] Pfleeger, Charles P., Security in Computing, (2006), The uses of encryption.

- Hacer pública la llave de cifrado (**e**, **n**).

o Proceso de cifrado y descifrado

Una vez que se obtienen las llaves, el cifrado y descifrado es el siguiente:

- Para cifrar cada bloque $\mathbf{M_i}$ transformándolo en un nuevo bloque de números $\mathbf{C_i}$ de acuerdo con la expresión:

$$\mathbf{C_i = M_i^{\,e} \pmod n}$$

- Para descifrar el bloque $\mathbf{C_i}$ se usa la llave privada **d** según la expresión:

$$\mathbf{M_i = C_i^{\,d} \pmod n}$$

o Ejemplo del funcionamiento de RSA:

- Elegimos dos números primos: **p**=3 y **q**=5 y calculamos su producto:
  - **n** = 3 * 5 = 15
- Calculamos **F**(**n**) = (3-1)*(5-1)= 8
- Elegimos **e** = 3, entonces **d** = 3, ya que:
  - **e*d** mod 8 = 3*3 mod 8= 9 mod 8 = 1
- La llave pública es (**n**, **e**) = (15, 3)
- Supongamos que el mensaje es **m** = 2
- El mensaje cifrado es:
  - $\mathbf{C_i = M_i^{\,e} \pmod n}$, es decir:
  - $\mathbf{2^3 \bmod 15}$, entonces $\mathbf{C_i}$ = 8
- Se envía 8.
- Ahora se descifra el mensaje.
- Se calcula:
  - $\mathbf{M_i = C_i^{\,d} \pmod n = 8^3 \bmod 15}$
- Es decir:

- **M_i = 512 mod 15 = 2**

- Finalmente se obtiene el mensaje original.

El algoritmo RSA es muy seguro y su confiabilidad radica en:

- Debido a los cálculos necesarios, tanto la generación de llaves como el cifrado y descifrado son complejos y cuanto más grandes sean los tamaños de las llaves más lento será el sistema.

- La mayoría de las discusiones sobre el criptoanálisis se han centrado en la tarea de factorizar **n** en sus dos números primos.

- Actualmente, se considera bastante potente un tamaño de llave de 1024 bits (aproximadamente 300 dígitos decimales) para virtualmente todas las aplicaciones.

2.4.2 Aplicaciones criptográficas

El interés por las aplicaciones ha ido en aumento debido al crecimiento de las comunicaciones electrónicas y de la protección de la información.

2.4.2.1 Protocolos

"Es un acuerdo entre dos o más partes, donde se definen reglas para realizar una tarea específica"[21].

Utilizaremos la siguiente notación en el uso de protocolos:

- **A**. Primer participante del protocolo.

- **B**. Segundo participante.

- **J**. Tercera parte confiable.

[21] Daltabuit, Enrique, La seguridad de la información, (2007), Capítulo 3, Criptografía, protocolos, (p. 135).

Sus características son:

- Resuelve un problema y produce un resultado.
- Consiste en una serie de pasos bien definidos.
- Involucra a dos o más partes.
- Todas las partes involucradas conocen el protocolo y están de acuerdo a seguirlo.
- Define de forma clara lo que cada parte gana o expone con su ejecución.

Tipos de protocolos:

- Protocolos Arbitrados. Están basados en una tercera parte confiable, el árbitro no tiene ningún tipo de preferencia por alguna de las partes. En la vida real es el papel que juega un juez.

  Este tipo de protocolo es poco práctico, debido a la dificultad de tener una tercera parte confiable y neutral.

  Por ejemplo: **A** y **B**, desean hacer una compra / venta de una casa usando a **J** como árbitro o juez.

  - **A** entrega los papeles y las llaves de la casa a **J**.
  - **B** entrega el cheque de pago a **A**.
  - **A** deposita el cheque en el banco.
  - Si el cheque es bueno, **J** entrega los papeles y las llaves de la casa a **B**, si el cheque es malo, **J** entrega los papeles y las llaves de la casa a **A**.

  J, sólo es la tercera parte confiable y no tiene ninguna intención de hacer trampa

- Protocolos Adjudicados: Son una variante de los arbitrados, de igual manera se basan en una tercera parte confiable, pero esta parte no siempre se requiere, es decir, si todas las partes respetan el protocolo, el resultado se logra sin la ayuda de la tercera parte confiable que en este caso es el adjudicador.

  Si una de las partes involucradas piensa o cree que las otras partes hacen trampa, se involucra al adjudicador como ayuda, este analiza la

disputa y las reglas, posteriormente dice quien está actuando bien y qué es lo que se debe hacer.

Un ejemplo de este protocolo como el caso anterior:

- **A** entrega las llaves y los papeles de la casa a **B**.
- **B** entrega el cheque de pago a **A**.
- Si el cheque no es bueno o los papeles son falsos, **A** y **B** comparecen frente a un juez y los dos presentan sus evidencias.
- El juez juzga las evidencias y la parte que engaña es penalizada.

o Protocolos Autoimplementados: Son los mejores protocolos y se diseñan de tal manera que hacen virtualmente imposible el engaño, no requieren ni árbitro ni juez y garantizan que si algún participante engaña, el engaño es descubierto de inmediato por el otro y otros participantes.

Por otra parte los protocolos criptográficos son utilizados para implementar servicios de seguridad como son: la confidencialidad, autenticación, integridad y no repudio.

Uno de los servicios más importantes es el de confidencialidad, ya que desde mucho tiempo ha sido requerido, ya sea al usar cifrado de llave secreta o de llave pública. Otro de servicio que se utiliza de manera considerable es la autenticación.

Para implementar el servicio de integridad es necesario emplear funciones resumen o Hash, que son la herramienta esencial para ello y es parte de la criptografía.

El no repudio, se implementa con una herramienta llamada firma digital que es parte de los esquemas de criptografía asimétrica.

A continuación se muestran algunos de los protocolos para implementar estos servicios, con la aplicación de cifrado asimétrico, este tipo de protocolos se conocen como protocolos criptográficos y son los siguientes:

o Confidencialidad con sistemas criptográficos asimétricos:

Un usuario **A** desea enviar de manera secreta, un mensaje **M** al usuario **B** con la utilización de un algoritmo de llave pública:

Se requiere que previamente, cada parte haya generado su pareja de llaves (pública y privada), y que las llaves públicas de ambas partes sean públicamente accesibles. El protocolo es el siguiente:

- **A** cifra **M** por ejemplo usando RSA con llave pública de **B** y produce el texto cifrado **C**.
- **A** envía **C** a **B**.
- **B** descifra **C** usando RSA y su llave privada para obtener **M**.

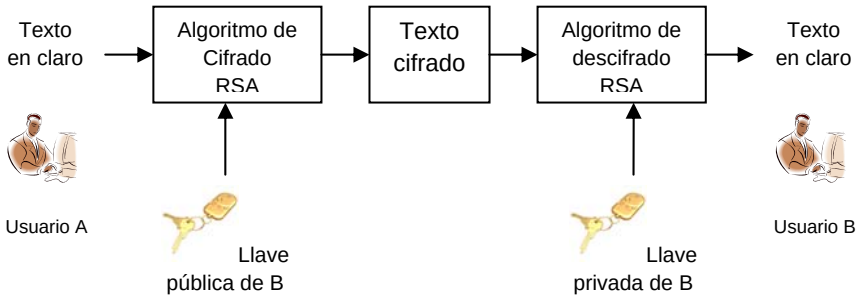

Figura 17. Confidencialidad con cifrado asimétrico.

Por medio de este protocolo se obtiene confidencialidad, porque nadie más que **B** puede descifrar **C** y obtener **M**, ya que sólo **B** tiene su propia llave privada.

Existe un problema en este protocolo, **B** no puede estar seguro que el mensaje **C** lo haya originado **A**, debido a que cualquiera pudo haber usado la llave pública de **B** para cifrar **M** y enviarlo. Así pues, este protocolo proporciona confidencialidad, pero no autenticación.

o Autenticación con sistemas criptográficos asimétricos

La situación es similar a la anterior, pero ahora se desea lograr autenticación. Un usuario **A** quiere enviar mensaje **M** al usuario **B**, pero de tal manera que **B** pueda estar seguro que solamente **A** lo pudo haber originado.

Se requiere que previamente que, cada parte haya generado su pareja de llaves (pública y privada), y que las llaves públicas de ambas partes sean públicamente accesibles. El protocolo es el siguiente:

- **A** cifra **M** usando RSA con su propia llave privada y produce el texto cifrado **C**.
- **A** envía **C** a **B**.

- **B** descifra **C** usando RSA y la llave pública de **A** para obtener **M**.

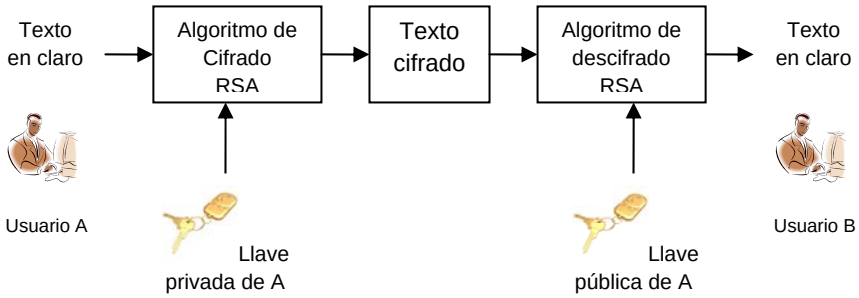

Figura 18. Autenticación con cifrado asimétrico.

Por medio de este protocolo se garantiza el servicio de autenticación, porque, nadie más que **A** pudo haber cifrado **M** con la llave privada de **A** para obtener **C**, ya que el único que conoce la llave privada de **A**, es propiamente **A**.

Sale a luz otro problema, este protocolo no garantiza confidencialidad, puesto que cualquiera puede usar la llave pública de **A**, para conocer el mensaje **M**.

Se llega a la conclusión de qué, ¿será posible integrar los dos protocolos, confidencialidad con autenticación en uno solo?, si es posible.

o Confidencialidad y autenticación con sistemas criptográficos asimétricos

La situación es la siguiente, un usuario **A** quiere enviar mensaje **M** y que solamente **A** lo pudo haber originado. De igual modo supongamos que usamos RSA como algoritmo de cifrado.

Se requiere que previamente que, cada parte haya generado su pareja de llaves (pública y privada), y que las llaves públicas de ambas partes sean públicamente accesibles. El protocolo es el siguiente:

- **A** cifra **M** usando RSA con su propia llave privada y obtiene el texto cifrado **C**, posteriormente **A** cifra **C** con la llave pública de **B** y obtiene $\mathbf{C^1}$.

- **A** envía $\mathbf{C^1}$ a **B**.

- **B** descifra $\mathbf{C^1}$ usando RSA y su propia llave privada para obtener **C**, posteriormente **B** descifra **C** con la llave pública de **A** para obtener **M**.

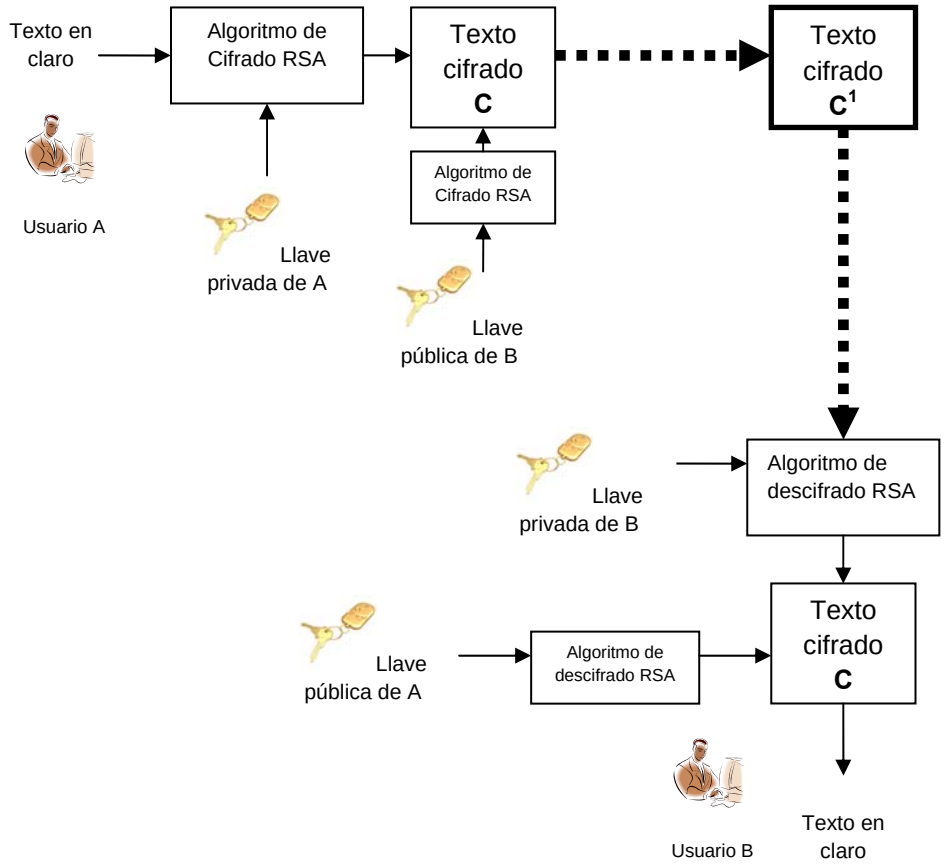

Figura 19. Confidencialidad y Autenticación con cifrado asimétrico.

Este protocolo proporciona confidencialidad y autenticación, para entenderlo de una manera más fácil es como firmar el documento por el emisor con su propia llave privada para brindar autenticación y después poner en un sobre ese mensaje que sería la llave pública del receptor para brindar confidencialidad.

En algunas ocasiones además de confidencialidad y autenticación, se necesita saber que la información no ha sido modificada y se utiliza otro servicio que es el de integridad, y todo esto unificarlo en un mismo protocolo.

o Confidencialidad, autenticación e Integridad con sistemas criptográficos asimétricos

Ahora la situación es la siguiente, un usuario **A** quiere enviar mensaje **M** de manera secreta al usuario **B**, pero de tal manera que **B** pueda estar seguro que solamente **A** lo pudo haber originado, y además que **M** no haya sufrido alteraciones durante el envío. De igual modo supongamos que usamos RSA como algoritmo de cifrado.

Se requiere que previamente que, cada parte haya generado su pareja de llaves (pública y privada), y que las llaves públicas de ambas partes sean públicamente accesibles.

En este protocolo también debe asumirse que las dos partes acuerdan el uso de funciones Hash o de digestión "**H**", por ejemplo (SHA – 1) y que esta función es públicamente disponible. El protocolo es el siguiente:

- **A** calcula el valor Hash de **M**, **H(M)**.
- **A** cifra **H(M)**, con RSA usando su llave privada y produce un equivalente a una firma **S** del **H(M)**.
- **A** cifra **M** con la llave pública de **B** y produce **C**.
- **A** envía **S** y **C** a **B**.
- **B** descifra **C** usando RSA y su propia llave privada para obtener **M**.
- **B** calcula el valor Hash de **M**, **H(M)**.
- **B** descifra **S** usando RSA y la llave pública de **A** para obtener el **H(M)** que genero **A** al inicio.
- **B** compara los resultados Hash, el que él calculó con el que recibió de **A**.

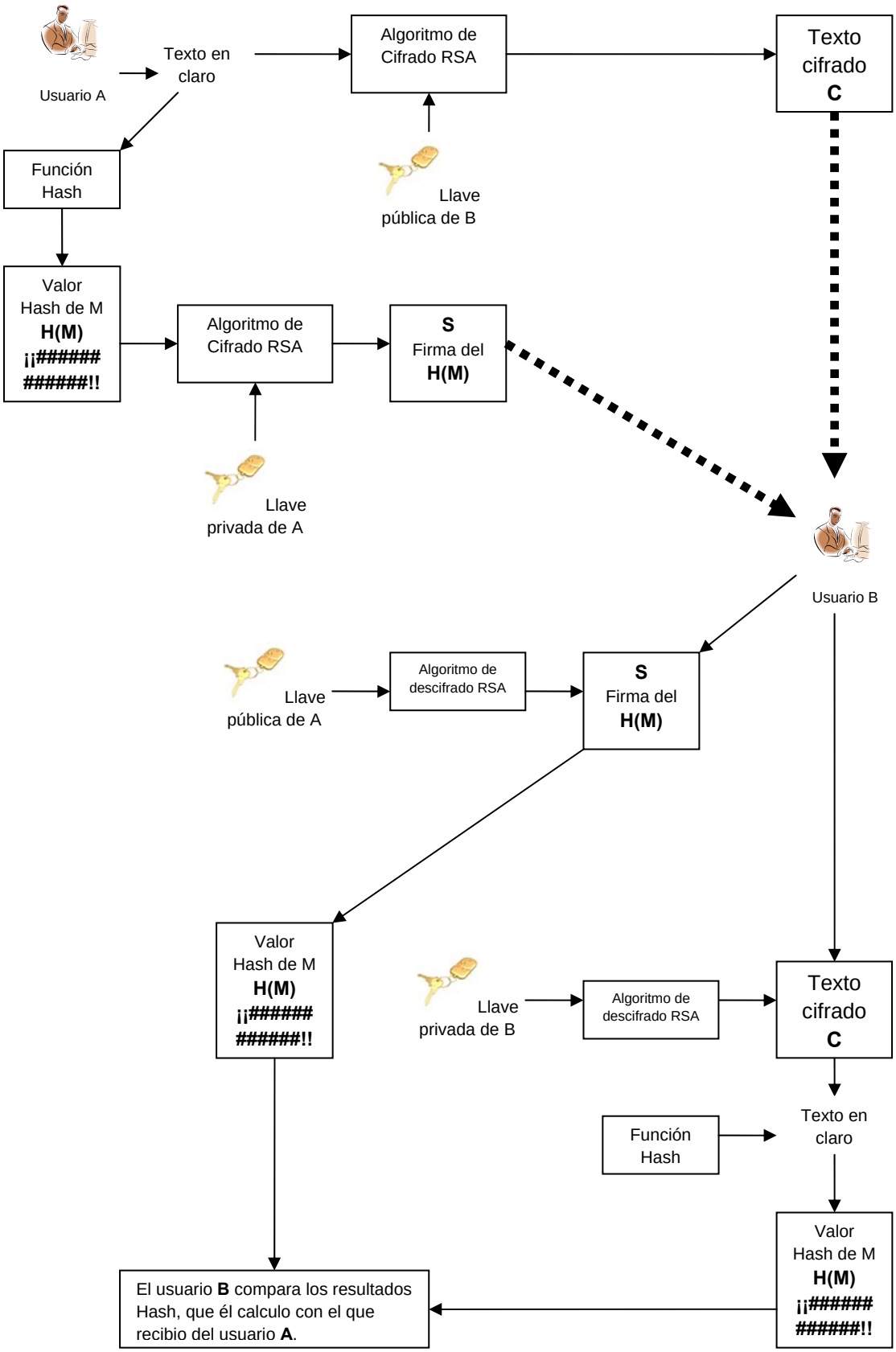

Figura 20. Confidencialidad, autenticación e integridad con sistemas de criptografía asimétrica.

Este protocolo proporciona los servicios de confidencialidad, autenticación e integridad.

- Confidencialidad: **M** viaja cifrado con la llave pública de **B** y nadie más que **B** puede descifrarlo y leerlo.

- Autenticación: Nadie más que **A** pudo haber cifrado (firmado) **H(M)**, ya que es el único que posee su propia llave privada.

- Integridad: **B**, porque al recibir cifrados **M** y **H(M)**, puede descifrarlos y hacer el mismo cálculo sobre **M** y verificar los resultados Hash. Si coinciden, está seguro que el mensaje no ha sido modificado durante el trayecto.

2.4.3 Acuerdo e intercambio de llaves

Existe un gran problema dentro de la criptografía simétrica, esta es incapaz de resolver el problema de acuerdo de llave de cifrado.

La criptografía asimétrica ayuda a resolver este problema en la medida que la llave que se requiere para el cifrado es pública y puede colocarse en un servidor de llaves o directorio público. La criptografía de llave pública genera un nuevo y gran problema conocido como: administración y distribución de llaves.

Hay otros problemas relacionados, las llaves ni las personas son eternas, las llaves pueden ser comprometidas o caducan, por otro lado las personas mueren. La situación se complica más, si las partes que quieren comunicarse son más de dos, es necesario hacer varios acuerdos e intercambios de llaves.

Por poner un ejemplo, en una institución, las computadoras conectadas en red de **n** nodos desean intercambiar un secreto para comunicarse usando cifrado simétrico, el número de intercambios necesarios es: **n (n – 1) / 2**, es decir:

- 2 nodos = 1 comunicación (acuerdo de llave).

- 3 nodos = 3 acuerdos de llave.

- 4 nodos = 6 acuerdos de llave.

- 5 nodos = 10 acuerdos de llave, así sucesivamente.

Tomando el mismo ejemplo, supongamos que la red cuenta con 1500 nodos, el número intercambios necesarios para que los nodos acuerden su llave son más de un millón. Lo que deja la conclusión que no es un problema pequeño.

Con el surgimiento de la criptografía de llave pública ya no se requiere tener que acordar llaves de cifrado para lograr una confidencialidad, sin embargo la llave pública siempre está asociada a una llave privada, y si ésta se compromete hay que generar otro par de llaves y sustituir la nueva llave pública debido a ello. Las llaves públicas tienen caducidad o simplemente se dejan de usar. Esta problemática genera un nuevo escenario que se le conoce como administración de llaves.

El problema de la administración de llaves está relacionado con:

- Autenticidad de la llave pública.
- Distribución.
- Caducidad, revocación, sustitución y cancelación de las llaves.

Un tipo de llave fundamental es la conocida como llave de sesión, solo se utiliza para la sesión actual de trabajo. Por lo regular es este tipo de llaves se acuerda, por medio de un protocolo, inmediatamente después que el proceso de autenticación se ha realizado de manera segura. Muchas veces los protocolos de autenticación llevan implícito el proceso de acuerdo e intercambio de llave de sesión.

2.4.3.1 Llave de sesión

Dentro del proceso de la comunicación, lo normal es acordar una llave que es llamada llave de sesión y que se utiliza para y durante la sesión actual. La llave de sesión se acuerda entre las partes y se utiliza para la sesión actual de trabajo, esta llave debe ser criptográficamente fuerte y su objetivo principal es servir como llave de cifrado de toda la información que se intercambia durante la sesión.

Normalmente se acuerda entre las partes involucradas en un protocolo, inmediatamente después del proceso de autenticación. Los protocolos de autenticación típicamente llevan implícito el establecimiento de acuerdo o intercambio de llave de sesión. Por esto, se les conoce como protocolos de autenticación e intercambio de llave.

Existen distintas maneras para poder establecer las llaves de sesión que pueden ser:

- Servidor de llaves: Crea y distribuye la llave de sesión a las partes interesadas.

- Intercambio de llave: Una de las partes interesadas genera la llave y la distribuye a las otras partes.

- Acuerdo de llave: Las partes intercambian información, a partir de la cual cada parte calcula la misma llave.

2.4.3.2 Ventajas y Desventajas

Cada uno de estos esquemas tiene sus ventajas y sus desventajas, son las siguientes:

- Servidor de llaves:
  - Las partes sólo solicitan la llave.
  - Toda la seguridad depende del servidor.
  - Tiene absoluto control sobre la seguridad en la comunicación de los participantes.

- Intercambio de llave:
  - Las partes no dependen de un servidor.
  - Una de las partes genera la llave y la hace viajar por un canal inseguro.
  - Esto representa un riesgo de seguridad.

- Acuerdo de llave:
  - Es el esquema ideal.
  - Evita la dependencia de la parte confiable.
  - La llave no viaja por el canal.
  - Pero… se tiene que intercambiar información previa.
  - Cada parte debe realizar un proceso computacional para calcular la llave.
  - Pero no siempre las partes cuentan con recursos para ello.

Para cada uno de estos esquemas existen protocolos que realizan esta tarea, un algoritmo muy elegante para el acuerdo de llave es el que diseñaron Diffie y Hellman en 1976, este algoritmo permite a dos o más partes, acordar una llave, aún cuando los intercambios previos al acuerdo sean públicos.

2.4.3.3 Idea de acuerdo de llave Diffie – Hellman

Fue el primer algoritmo asimétrico y solamente se puede utilizar para intercambiar llaves simétricas y que serán utilizadas para cifrar una sesión. Permite a dos partes comunicarse mediante un canal sin cifrar y se pongan de acuerdo en un valor numérico sin que una tercera parte, que tenga acceso completo a la comunicación, pueda conocerlo o calcularlo, al menos en un tiempo práctico. “Permite a dos o más partes acordar una llave, aún cuando los intercambios previos al acuerdo sean públicos”[22].

El algoritmo D – H tiene lo siguiente como idea principal:

- **A** inventa un número $\mathbf{N_A}$, y le aplica una transformación **f**, a ese número $\mathbf{f(N_A)}$ y transmite el resultado a **B**.
- **B** inventa su propio número $\mathbf{N_B}$, y de igual manera aplica una transformación **f** a ese número $\mathbf{f(N_B)}$ y trasmite el resultado a **A**.
- **A** calcula la llave de la sesión utilizando $\mathbf{N_A}$ y $\mathbf{f(N_B)}$.
- **B** calcula la misma llave de la sesión utilizando $\mathbf{N_B}$ y $\mathbf{f(N_A)}$.

Con el uso de este algoritmo no es necesario distribuir llaves, la idea es simple, sólo hay que establecer de manera clara las siguientes cuestiones:

- Que significa “inventar” un número.
- De qué tipo y tamaño tienen que ser $\mathbf{N_A}$ y $\mathbf{N_B}$.
- En qué consiste exactamente la transformación **f**, y que propiedades tiene.
- Qué tipo de cálculo tienen que hacer **A** y **B** con $\mathbf{N_A}$, $\mathbf{f(N_B)}$ y $\mathbf{N_B}$, $\mathbf{f(N_A)}$, respectivamente. De tal modo que obtengan exactamente el mismo resultado.

[22] Daltabuit, Enrique, La seguridad de la información, (2007), Capítulo 4, Aplicaciones Criptográficas, Algoritmo Diffie – Hellman, (p. 135).

Inventar significa generar pseudoaleatoriamente los números y deben ser grandes (más de 512 bits), estos funcionaran como exponentes de números primos públicamente conocidos, que funcionan como la base en una función exponencial (la transformación **f**) y con las propiedades de función exponencial permite a las partes calcular el mismo resultado con los parámetros que conoce cada una de las partes.

Con las dudas aclaradas el algoritmo D – H, puede ser planteado de la siguiente manera:

- **A** y **B** conocen previamente o pueden pactar públicamente 2 números; el número **n** que es un número primo grande (mayor de 512 bits), y el número **g**, elegido de tal manera que **1 < g < n**.

- **A** y **B** generan o seleccionan aleatoriamente, cada uno el suyo, un número grande y los mantienen en secreto; supongamos que **A** selecciona el número "**X**" y **B** selecciona el número "**Y**".

- **A** calcula $\mathbf{X = g^x \pmod n}$

- **B** calcula $\mathbf{Y = g^y \pmod n}$

- **A** y **B** intercambian los resultados **X**, **Y** de tal manera que **A** conozca **Y** y que **B** conozca **X**.

- **A** calcula la llave de sesión $\mathbf{k = Y^x \pmod n}$

- **B** calcula la llave de sesión $\mathbf{k^1 = X^y \pmod n}$

- **A** y **B** tienen $\mathbf{k = Y^x \pmod n = k^1 = X^y \pmod n = g^{xy} \pmod n}$, las **k** calculadas por las dos partes son idénticas.

La seguridad del algoritmo de D – H, depende de la dificultad del cálculo de un logaritmo discreto. Es la imposibilidad matemática de calcular $\mathbf{g^{xy}}$ a partir del conocimiento de $\mathbf{g^x \pmod n}$ y de $\mathbf{g^y \pmod n}$.

Igualmente es computacionalmente infactible poder deducir **X** a partir del conocimiento de $\mathbf{g^x \pmod n}$, esto último se le conoce como problema de los logaritmos discretos.

2.4.4 Gestión de llaves

El tema de gestión de llaves abarca situaciones como la transmisión de las llaves a través de un canal seguro o inseguro y de su adecuada distribución entre los usuarios, el almacenamiento y conservación de las llaves, tiempo de vida, aplicación y destrucción de las llaves.

Dentro del entorno criptográfico se distinguen dos tipos de llaves:

- Llaves de corta duración o llamadas también llaves de sesión: son empleadas para cifrar un único mensaje o para el cifrado de la información intercambiada en una sesión establecida entre dos usuarios.

- Llaves de larga duración, conocidas como llaves de usuario o llaves primarias: que se emplean para el servicio de autenticación, y de esta manera asegurar la confidencialidad de la información, ya sea a la hora de transmitirla o de proteger la que se encuentra almacenada dentro de un medio informático.

Siempre se debe de definir un buen procedimiento para la correcta implementación de los procedimientos relacionados con la gestión de llaves, saber quiénes son los responsables en cada situación.

Se recomienda poner énfasis en cuales llaves se necesita aplicar mayor seguridad y en que procedimientos o tipos de datos emplear determinadas llaves.

2.4.4.1 Generación

La base de la seguridad de un algoritmo radica en la llave, cuando se utilizan llaves criptográficamente débiles el algoritmo resultará débil, cuando se eligen las llaves se debe considerar lo siguiente:

- Espacio de la llave: Es muy importante la longitud de la llave, se debe considerar una llave fuerte aquella que sea lo suficientemente larga, que contenga caracteres especiales, utilizando letras minúsculas y mayúsculas; pero debemos considerar que la llave no debe ser muy grande porque vuelve ineficiente el algoritmo de cifrado.

- Problema de una llave débil: Cuando los usuarios eligen sus llaves suelen hacerlo de manera ineficiente, suelen utilizar su mismo nombre, su fecha de nacimiento o palabras comunes, esto es un problema porque son atacadas por fuerza bruta, que prueba las llaves más comunes.

- Llaves aleatorias: Para la creación de las llaves se puede recurrir a generadores pseudoaleatorios, que generan las llaves de manera automática.

2.4.4.2 Distribución

Uno de los temas principales dentro de la gestión de llaves es la distribución de ellas. La distribución se realiza antes de la comunicación.

Los requisitos específicos en cuanto a seguridad de esta distribución dependerán de para qué y cómo van a ser utilizadas las llaves. Así pues, será necesario garantizar la identidad de su origen, su integridad y, en el caso de llaves secretas, su confidencialidad.

Las consideraciones más importantes para un sistema de gestión de claves son el tipo de ataques que lo amenazan y la arquitectura del sistema.

Normalmente, es necesario que la distribución de llaves se lleve a cabo sobre la misma red de comunicación donde se está transmitiendo la información a proteger. Esta distribución es automática y la transferencia suele iniciarse con la petición de llave por parte de una entidad a un centro de distribución de llaves que es conocida como intercambio centralizado o a la otra entidad involucrada en la comunicación llamada intercambio directo.

La distribución de llaves se lleva siempre a cabo mediante protocolos, muchas de las propiedades de estos protocolos dependen de la estructura de los mensajes intercambiados y no de los algoritmos criptográficos subyacentes. Por ello, las debilidades de estos protocolos provienen normalmente de errores cometidos en los niveles más altos del diseño.

Una vez que las llaves hayan sido distribuidas, se activan y pueden ser utilizadas para distintos propósitos:

- Autenticación de usuarios.
- Cifrado de documentos y ficheros.
- Cifrado de las comunicaciones.
- Generación de firma electrónica, etc.

En la práctica se aconseja que cada llave sólo sea utilizada para un determinado fin y así alcanzar su función de seguridad. Y no se recomienda emplear la misma llave para tratar de garantizar la confidencialidad y al mismo tiempo la integridad de la información.

El desarrollo de los sistemas basados en criptografía de llave pública ha venido a facilitar el intercambio de llaves y su manera de distribuirlas.

2.4.4.3 Almacenamiento

Una de las maneras más fáciles es almacenarla en la memoria del usuario. Pero de forma más sofisticada existen métodos para guardar las llaves, ya sea en el disco duro cuando las llaves son difíciles de memorizar, cifrándolas mediante otro algoritmo y una determinada llave de acceso, por ejemplo, cifrar la llave privada RSA mediante el algoritmo 3DES.

Un método sofisticado de almacenamiento es la utilización de tarjetas con chip ROM donde se grabe la llave, conocidas como "ROM Keys" o tarjetas inteligentes "Smart Card". De tal manera que la llave queda asociada a un dispositivo físico y que usuario debe introducir a un lector para poder utilizar la llave.

Siempre se recomienda disponer de una copia de seguridad centralizada de todas las llaves de los usuarios de una organización, para poderlas recuperar cuando sea necesario.

2.4.4.4 Tiempo de vida

Las llaves por cuestiones de seguridad nunca se deben usar por tiempo indefinido, deben tener una fecha de caducidad, por lo siguiente:

- Entre más tiempo se use una llave es más probable que se comprometa.
- Cuanto más tiempo se usa una llave, mayor será el daño si la llave se compromete, ya que toda la información protegida con esa llave queda al descubierto.
- En general es más fácil realizar criptoanálisis con mucho texto cifrado con la misma clave.

2.4.4.5 Destrucción

En primer lugar se debe tomar en cuenta que las llaves que tengan la caducidad vencida se destruyan de manera segura, ya que por cuestiones de seguridad es importante porque si un atacante decide usar esas llaves puede leer mensajes antiguos. En conclusión, ser destruidas de tal manera que sean irrecuperables.

2.5 FUNCIONES HASH O DE DIGESTIÓN

Es una función unidireccional, lo que significa que es fácil de calcular en una dirección pero infactible en la otra.

"La función de hash tiene características especiales, por ejemplo, algunos cifrados depende de una función que es fácil de entender pero difícil de calcular"[23].

Las funciones hash aceptan entradas arbitrariamente grandes y entrega una salida de longitud fija y pequeña.

Es infactible que dos entadas mapeen al mismo valor hash y también es infactible que dado un valor hash se pueda hallar más de una entrada.

En caso de cambiar un bit de entrada cambia la salida.

Estas funciones también llamadas de digestión o resumen, se usan para verificación de integridad., es decir, cada valor Hash es una huella digital.

Los algoritmos que se utilizan son: MD5, SHA-1, SHA-2.

Un valor Hash **h**, es resultado de aplicar una función **F** one – way (unidireccional), que opera sobre un mensaje **M** de longitud arbitraria y regresa un valor de longitud fija **h**.

$$\mathbf{H = H(M)}$$

Es decir:

- Dado **h**, es difícil calcular **M**, tal que **H(M) = h**.
- Dado un mensaje **M** específico es difícil hallar otro mensaje $\mathbf{M^1}$, tal que $\mathbf{H(M) = H(M^1)}$.
- Dado un espacio grande de **M´**s, es difícil hallar cualquier pareja de **M´**s con el mismo valor Hash.
- Dado un mensaje **M**, es fácil calcular **H(M)**.

A continuación se mostrará un ejemplo de una función Hash aplicada a un mensaje y su respectivo resumen, utilizando el algoritmo SHA-1:

[23] Pfleeger, Charles P., Security in Computing, (2006), Cryptographic Hash Functions.

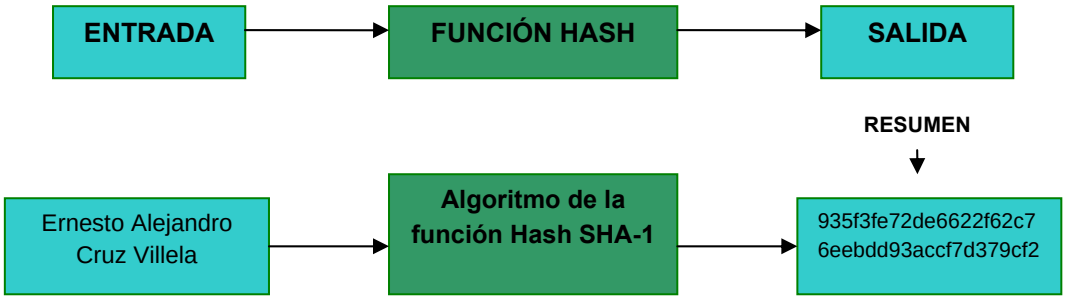

Figura 21. Función Hash.

Las funciones Hash están asociadas con la seguridad, y para evitar que un mensaje tenga el mismo resultado hash de otro mensaje, es necesario dentro de la criptografía, que cumpla con las siguientes características.

2.5.1 Características

El Hash de un mensaje será seguro si cumple con estas características:

- Unidireccionalidad: Conocido un resumen **H(M)**, debe ser computacionalmente imposible encontrar **M** a partir de dicho resumen.
- Comprensión: A partir de un mensaje **M** de cualquier longitud, el resumen **H(M)** debe tener una longitud fija, por lo regular la longitud de **H(M)** es menor que **M**.
- Facilidad de cálculo: Debe ser fácil calcular **H(M)** a partir de **M**.
- Difusión: El resumen **H(M)** debe ser una función compleja de todos los bits del mensaje **M**. Si se modifica un bit del mensaje **M**, el hash **H(M)** debería cambiar aproximadamente la mitad de sus bits.

Las funciones hash tienen distintas aplicaciones:

- Cifrar con llave simétrica **M** y **h**.
- Cifrar sólo **h** con una llave simétrica y enviarla junto con **M**.
- Cifrar sólo **h** con una llave privada y enviarla junto con **M**, que es lo que se conoce como “Firma Digital”.

El objetivo de una función Hash es producir un identificador único de cualquier documento digital, en forma eficiente y segura.

2.5.2 Huellas digitales

Una huella digital es un conjunto de datos asociados a un mensaje que permiten asegurar que el mensaje no fue modificado. La huella digital o resumen de un mensaje, se obtiene aplicando una función Hash a dicho mensaje, como se mencionó anteriormente.

Una función hash tiene las siguientes propiedades:

- Dos mensajes iguales producen huellas digitales iguales.
- Dos mensajes parecidos producen huellas digitales completamente diferentes.
- Una función Hash es irreversible (no se puede deshacer), por tanto su comprobación se realizará aplicando de nuevo la misma función Hash al mensaje.

2.5.3 Algoritmo SHA – 1

El algoritmo SHA – 1, de sus siglas en inglés, (Secure Hash Algorithm) fue diseñado por la Agencia de Seguridad Nacional de los Estados Unidos y publicado por NIST (National Institute of Standards and Technology).

El SHA – 1 toma como entrada un mensaje de longitud máxima 264 bits (más de dos mil millones de Gigabytes) y produce como salida un resumen de 160 bits.

Trabaja con resúmenes de 224, 256 y 512 bits.

Fue diseñado para trabajar con el Algoritmo de Firma Digital (DSA).

SHA – 1 tiene las mismas propiedades de las funciones Hash que son: La primera es que son de sentido único. Esto significa que se puede tomar un mensaje y calcular un valor de Hash, pero no se puede tomar un valor Hash y recrear el mensaje original. También es libre de colisión y, por tanto, no hay dos mensajes Hash con el mismo valor.

SHA – 1 puede ser usado en una variedad de aplicaciones:

- Aplicaciones de seguridad que requieren autenticación.
- Correo electrónico.
- Distribución de software.
- Almacenamiento de datos.

2.6 CERTIFICADO DIGITAL

Es un documento electrónico que lo emite una entidad denominada Autoridad Certificadora que garantiza la vinculación entre la identidad de un sujeto o entidad con su llave pública.

Cabe mencionar que dentro de esta tesis los certificados que se utilizan son X.509 con su versión más reciente que es V3. Todo está relacionado con estos tipos de certificados, ya que son los más utilizados y los que usaremos para implementar la firma digital y el cifrado.

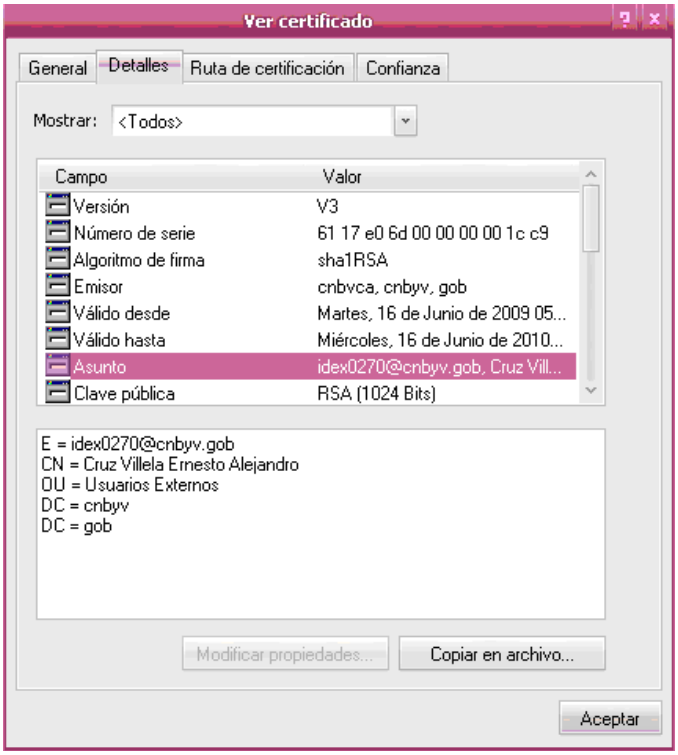

Figura 22. Certificado Digital.

2.6.1 Seguridad de los certificados digitales

Un certificado es seguro por lo siguiente:

- La autoridad certificadora firma digitalmente el certificado calculando su valor Hash y lo firma con su llave privada.

- La generación del certificado involucra algoritmos criptográficos para firmas digitales.

Esto hace imposible la falsificación, ya que el falsificador necesita conocer la llave privada de la autoridad certificadora.

Si un atacante modifica el certificado, el valor Hash cambia y no coincidirá con la firma que la autoridad certificadora generó.

Por estos motivos tenemos que, los certificados digitales de llave pública permiten asegurar que una llave pública pertenece a la entidad certificada y que dicha entidad posee la correspondiente llave privada.

Veremos más adelante de manera gráfica como se genera un certificado, cuando una entidad solicita su certificado a la Autoridad Certificadora.

Los certificados digitales permiten implementar los servicios de identificación y autenticación y como un mecanismo de no repudiación.

2.6.2 Obtención de un certificado

El usuario debe generar su propio par de llaves de manera local y almacenar de forma segura su llave privada, quizá cifrándolo con alguna contraseña y mandar la llave pública junto con la solicitud con la información para la identificación a la autoridad certificadora, finalmente esta comprueba la información proporcionada por el solicitante.

Existen otras opciones para generar las llaves, como puede ser el uso de una tarjeta inteligente, esta es capaz de generar el par de llaves por sí misma, proporciona la llave pública a las aplicaciones externas que lo requieran y mantiene la llave privada guardada de forma segura. Tiene otra gran ventaja la llave privada nunca sale de la tarjeta, se genera, almacena y destruye en la tarjeta.

Otra alternativa, es que las llaves sean generadas por un sistema central propio de la autoridad certificadora; en la actual investigación se hace uso de este

método. Este sistema debe enviar la llave pública a la autoridad certificadora y transmitir de forma segura la llave privada al solicitante.

De cualquier manera, el dueño de las llaves debe tomar las medidas necesarias para proteger su llave privada.

2.6.3 Autenticación del sujeto

Para autenticar a un sujeto, la autoridad certificadora debe realizar una tarea muy importante que es la comprobación de la información dada por el solicitante antes de asociar la llave pública del sujeto con su entidad.

La confirmación es de vital importancia, debido a que si un impostor logra obtener un certificado que relaciona su llave pública con identidad de otra persona, se podrá hacer pasar por dicha persona y hacer actividades fraudulentas.

La autoridad certificadora confirma la identidad del solicitante siempre y cuando el solicitante presente información personal u organizacional válida como: nombre, dirección, número de teléfono, etc.

Dicha autoridad también puede validar información recurriendo a base de datos de clientes de terceros, en la que se mantiene información personal sobre una población. También puede solicitar presencia física, las medidas que una autoridad certificadora toma dependen del nivel de seguridad que pretenda proporcionar el certificado.

Los certificados se clasifican por niveles, en función de las medidas de validación efectuadas para cada clase, y los controles de validación dependen de las políticas establecidas por la autoridad certificadora por cada tipo certificado.

Dependiendo de las validaciones de datos que se realicen se dividen en cuatro clases:

- Clase 1: Son los certificados más fáciles de obtener e involucran pocas verificaciones de los datos, como: el nombre y la dirección de correo electrónico.

- Clase 2: Son también fáciles de obtener y la autoridad certificadora comprueba de igual manera el nombre y el correo electrónico, además otros datos como la licencia, permiso de conducir, fecha de nacimiento y número de seguridad social.

- Clase 3: Aparte de la comprobación de los datos anteriores de la clase 2, se hace la verificación del nivel de crédito de la persona u organización.

- Clase 4: Incluye todas las comprobaciones anteriores y se agrega la información sobre la posición de la persona dentro de una organización.

Entre más alta sea la clase, mayor será el grado de verificación.

2.6.4 Generación de un certificado

Una vez validados los datos, la autoridad certificadora genera el certificado y lo firma con su llave privada. Los certificados pueden distribuirse por diversos mecanismos como:

- Servidores.

- Directorios.

- Correo electrónico.

Esto permite que una persona pueda usar el servicio para buscar el certificado de otra, instalar el certificado y usarlos para enviar correo electrónico seguro.

Las herramientas necesarias para generar un certificado digital son de fácil acceso, lo que permite que una organización puede contar con una entidad generadora de certificados en el caso de que decida utilizarlos de manera interna.

En la siguiente figura se muestra como se genera un certificado:

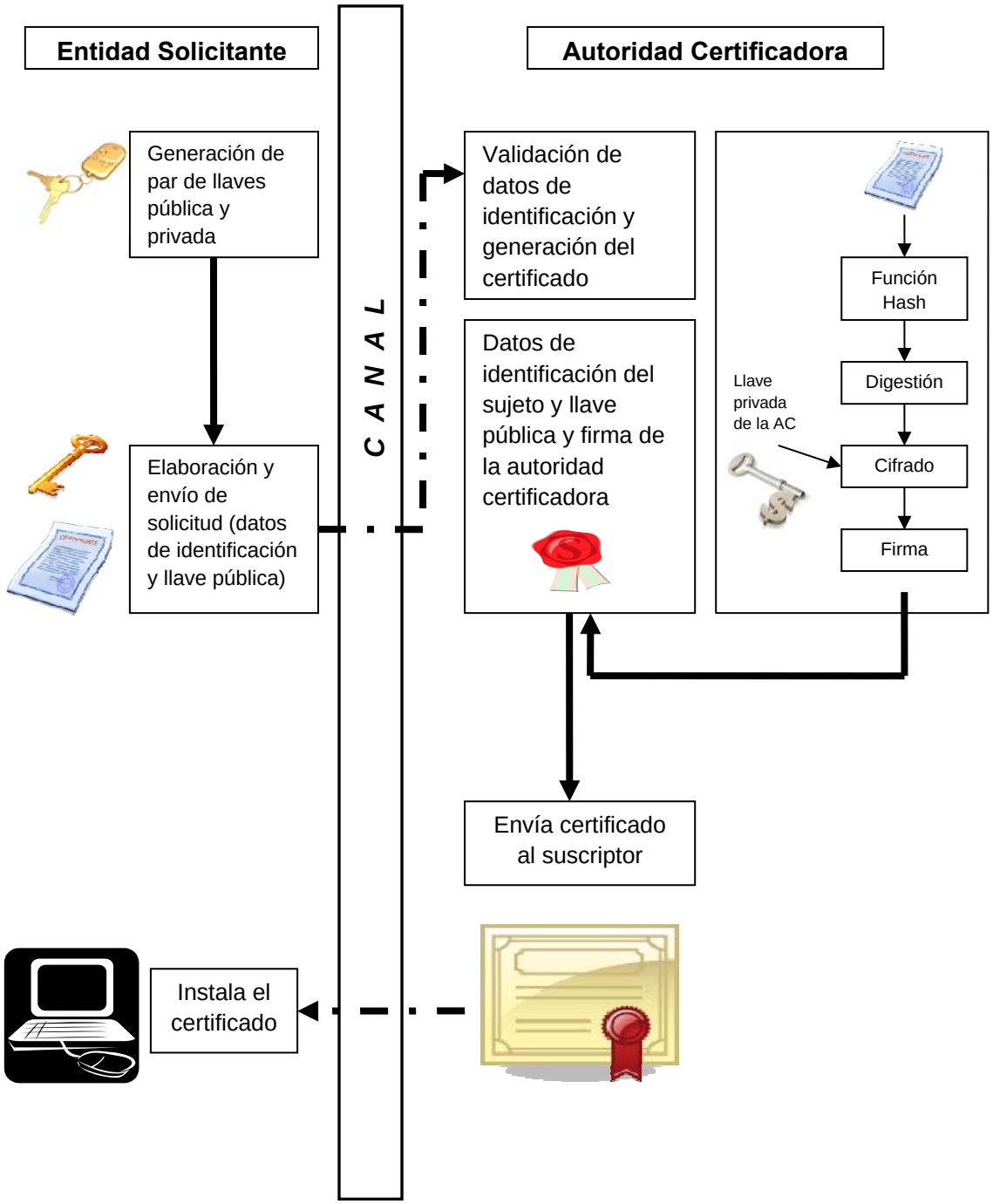

Figura 23. Proceso de generación de un certificado.

2.6.5 Verificación de un certificado

Las aplicaciones que utilizan certificados digitales los verifican o validan mediante el siguiente proceso:

- Se determina la ruta de verificación.
- Verificar cada certificado en la ruta con la llave pública del suscriptor del siguiente certificado en la ruta, si el certificado es el último, debe verificarse con la llave pública de la autoridad certificadora raíz.
- Se valida que ninguno de los certificados en la ruta haya expirado.
- Validan que ningún certificado esté revocado.
- Finalmente se verifican que las extensiones críticas de cada certificado sean reconocidas.

2.6.6 Ruta de certificación

Cuando se utilizan certificados digitales se necesita saber la ruta de validación entre el suscriptor y la autoridad certificadora raíz antes de poder evaluar el nivel de seguridad que tiene el suscriptor del certificado.

La ruta de certificación es una secuencia de uno o más nodos conectados entre los suscriptores y la autoridad certificadora raíz, también indica la forma en que una aplicación puede generar confianza en el certificado del suscriptor.

La autoridad certificadora raíz en la que confía la aplicación que usa certificados digitales es donde la llave pública ha sido importada de forma segura y almacenada previamente por la aplicación.

Por ejemplo para validar el certificado **E**:

- **E** es emitido por **Z**, la llave pública de **Z** se usa para validar **E**.
- En este caso **Z** es el certificado raíz, y se considera confiable.

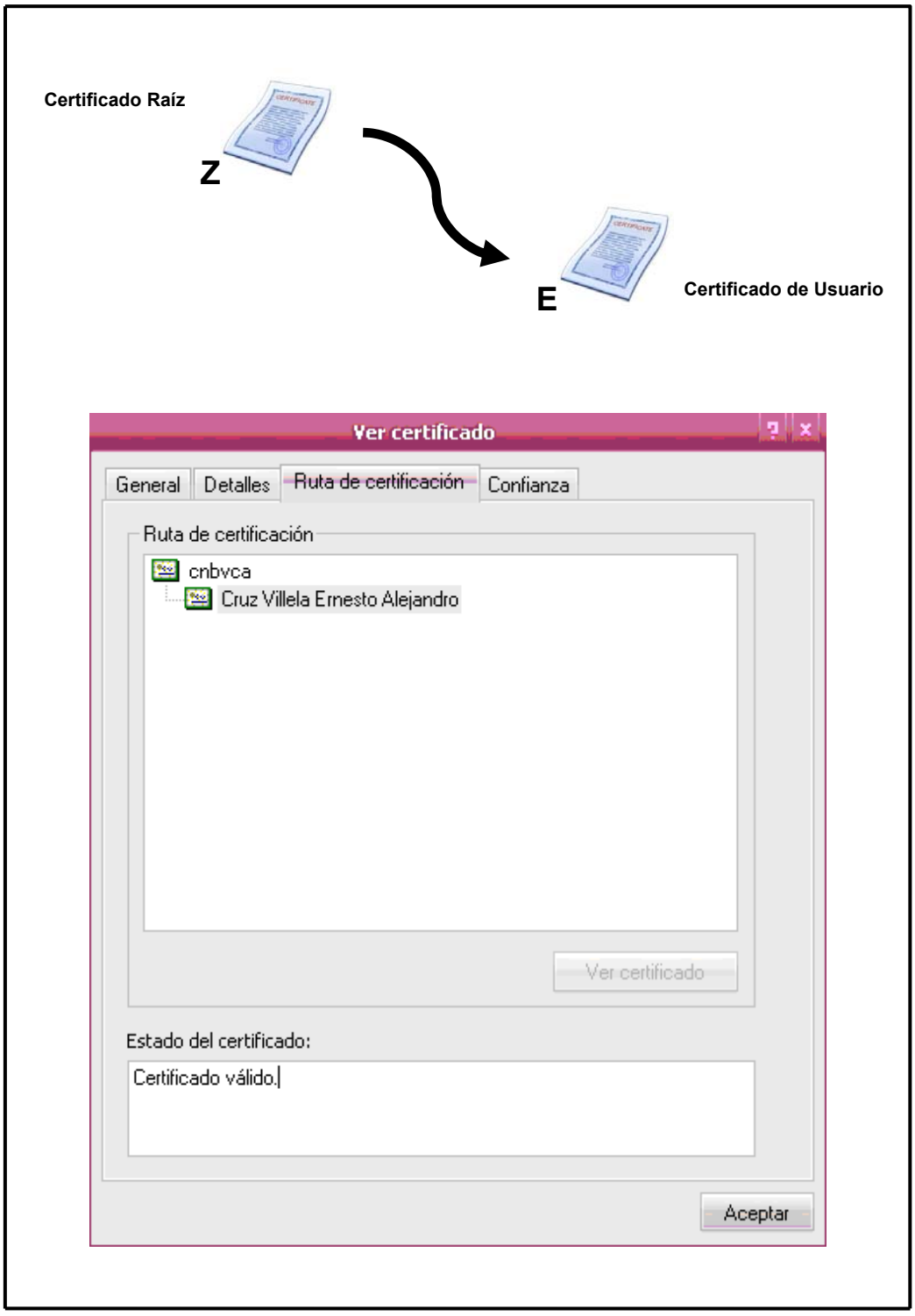

Figura 24. Ruta de Certificación.

2.6.7 Estándares para los certificados

Facilitan el desarrollo y compatibilidad de una infraestructura de certificados, definen los mecanismos de seguridad, mensajes, estructura de los datos y los procedimientos del manejo de la información para firmas y certificados digitales.

Los estándares de criptografía de llave pública, son publicados por RSA Data Security Inc.

Los elementos que se han estandarizado son:

- X.509: Formato de certificados.

- PKCS # 10: Solicitudes de certificación. Describe la sintaxis para solicitudes de certificación. Una solicitud consiste en un nombre y la llave pública.

- PKCS # 7: Formato para enviar el certificado al solicitante. Define y especifica el mecanismo de propósito general para la creación de una especie de sobre firmado digitalmente.

  Para certificados, se usa para firmar el sobre en el que la autoridad certificadora envía al usuario el certificado emitido y las cadenas de certificados requeridas para la validación de éste.

- PKCS # 12: Formato para transferir y almacenar certificados junto con sus llaves privadas. Especifica el formato de intercambio diseñado para transferir los certificados, rutas de certificación y las llaves privadas entre las computadoras.

2.6.8 Tiempo de vida de un certificado

Los certificados X.509, tienen un periodo de validez, desde pocos meses hasta algunos años. Una vez que caduca el certificado, se convierte en no válido, es inseguro seguir confiando en él.

Un certificado deja de ser vigente cuando vence el periodo de validez, en este caso la autoridad certificadora revoca el certificado. Ya sea porque ha sido comprometida la llave privada del usuario o cambiaron algunos datos del usuario.

2.6.9 Listas de revocación de certificados

Son mecanismos que una autoridad certificadora usa para publicar el estado de los certificados.

Una lista de revocación de certificados es una estructura de datos firmado digitalmente por la autoridad certificadora que la emite y contiene la fecha y hora de la publicación de la lista de revocación, el nombre de la autoridad certificadora que la emitió, y los números de serie de todos los certificados revocados que aún no han expirado.

2.7 FIRMAS DIGITALES

La firma digital es una aplicación de la criptografía asimétrica cuya finalidad es asegurar el vínculo del firmante con el mensaje emitido, así como la integridad del mensaje por medio de códigos de verificación, brindar confidencialidad en los datos y finalmente el no repudio de la información.

2.7.1 Características

Las firmas digitales proporcionan los siguientes servicios de seguridad:

- Autenticación de identidad: Que consiste en identificar al emisor del mensaje y asegurar que esa persona sea quien dice ser.
- No repudio: Al ser autenticada la identidad del firmante, se evita que el emisor niegue haber firmado y se puede garantizar que el firmante está de acuerdo con el contenido del mensaje y se vincula a él de alguna forma como algún tipo de autor o simplemente dándose por enterado.
- Integridad: Asegurar que la información no ha sufridos cambios, ya sea de manera accidental o intencionada después de haber firmado.
- Confidencialidad: Impedir que la información de un documento, sea vista por personas no autorizadas

2.7.2 Descripción del proceso de firma digital

El proceso de firma digital involucra varios elementos, todos ellos de gran importancia y son:

- Llave privada.
- Llave pública.
- Certificado.
- Resumen.
- Mensaje o documento original.
- Mensaje o documento cifrado.

La firma digital consiste en dos subprocesos, la realización de la firma y la verificación de la misma.

2.7.2.1 Realización de la firma

El emisor del mensaje, el firmante **A** crea una firma digital **S** para un mensaje **M** de la siguiente manera:

- **A** calcula $\mathbf{S = S_A (M)}$, donde **S** es la firma de **A** sobre el mensaje **M** con la función de firma $\mathbf{S_A}$.
- **A** envía a **B** la firma digital y el mensaje **(M, S)**.

2.7.2.2 Verificación de la firma

El receptor del mensaje, el verificador **B**, verifica que la firma **S** sobre el mensaje **M** la haya creado **A**, de la siguiente manera:

- **B** obtiene la función de verificación $\mathbf{V_A}$ de **A**.
- **B** calcula $\mathbf{V = V_A (M, S).}$

- **B** aceptará la firma creada por **A** siempre y cuando **V = Verdadero**, y será rechazada si **V = Falso**.

Las funciones $\mathbf{S_A}$ y $\mathbf{V_A}$ se caracterizan por su tipo de llave, $\mathbf{S_A}$ es siendo la llave privada y $\mathbf{V_A}$ la llave pública, que son conocidas como llaves de realización y verificación de firma respectivamente.

2.7.3 Seguridad de las firmas digitales

La seguridad se basa en que es computacionalmente infactible para cualquier entidad, distinta de **A**, hallar algún mensaje **M** y una firma **S**, tal que se cumpla $\mathbf{V_A}$ **(M, S) = Verdadero**, es decir, al firmar con mi llave privada un mensaje, a partir de este no se puede obtener la llave privada que es con la que se firma.

La llave privada se usa para firmar y la llave pública se usa para verificar la firma.

Los algoritmos más recomendados para firma digital son: ElGamal y DSA.

2.7.4 Algoritmo ElGamal

En un principio fue diseñado para producir firmas digitales y posteriormente para el cifrado de mensajes. Fue descrito por Taher ElGamal en 1984, este algoritmo no está bajo ninguna patente lo que lo hace de uso libre. Y está basado en el problema de los logaritmos discretos. El algoritmo ElGamal, se basa en los estándares para firmas digitales, requiere que el mensaje **M**, que será firmado sea convertido a una cadena de bits de longitud arbitraria.

ElGamal, usa una función Hash **H**, y un número primo **p** grande, que sea mayor de 512 bits. Ahora veremos los procesos de generación de llaves, firma y verificación del algoritmo ElGamal.

2.7.4.1 Generación de llaves

Las partes involucradas son, el firmante **A** y el verificador **B**, deben hacer lo siguiente para generar las llaves:

- Cada parte debe crear una pareja de llaves, una pública y otra privada.
- **A** debe generar un número primo grande **p**, y un generador **α** del grupo multiplicativo $\mathbf{Z_{p^*}}$.
- **A** debe seleccionar un número entero aleatorio **a** tal que **1 < a < p-2**.
- **A** debe calcular el valor de $\mathbf{y = \alpha^a \pmod p}$.
- La llave pública de **A** es **(p, α, y)**, la llave privada de **A** es **a**.

2.7.4.2 Proceso de firma

- **A** debe elegir aleatoriamente un número entero **K**, tal que **1 < K < p-2**, de tal manera que el máximo común divisor de **(K, p-1) = 1**.
- **A** calcula un primer parámetro de firma $\mathbf{r = \alpha^k \pmod p}$.
- Igualmente **A** calcula $\mathbf{K^{-1} \pmod{p-1}}$.
- **A** calcula $\mathbf{S = K^{-1} (H(M) - ar) \pmod{p-1}}$.
- La firma de **A** para el mensaje **M** es la pareja **(r, S)**.
- **A** envía a **B**, el mensaje y **(r, S)**.

2.7.4.3 Proceso de verificación

Para poder verificar la firma que **A** envío **(r, S)**, el verificador **B** debe hacer lo siguiente:

- Obtener la auténtica llave pública de **A**, **(p, α, y)**.
- Verificar que **r** llegue en el rango **1 < r < p-1**, sino se rechaza la firma.
- Calcular un verificador $\mathbf{V_1 = y^r * r^s \pmod p}$.
- Se calcula el **H (M)** y un segundo verificador $\mathbf{V_2 = \alpha^{H(M)} \pmod p}$.
- Luego se compara si $\mathbf{V_1 = V_2}$, sino es rechazada.

2.7.5 Algoritmo DSA

Es un algoritmo de firma digital, del inglés, (**D**igital **S**ignature **A**lgorithm), fue propuesto en 1991 por el Instituto Nacional de Estándares y Tecnología (NIST), es un estándar federal de procesamiento de información del gobierno de Estados Unidos y conocido como estándar de firma digital (DSS), el algoritmo DSA es una variante de ElGamal, además es el primer esquema de firma digital reconocido por cualquier gobierno y requiere explícitamente usar el algoritmo de Hash seguro (SHA – 1).

2.7.5.1 Generación de llaves

La entidad **A** debe hacer lo siguiente:

- Seleccionar un número primo **q**, tal que $\mathbf{2^{159} < q < 2^{160}}$.
- Escoger **t**, tal que **0 < t < 8**.
- Seleccionar un número primo **p**, donde $\mathbf{2^{511+64t} < p < 2^{512+64t}}$, con la propiedad que **q** divida a **(p-1)**.
- Seleccionar un generador **α** del grupo cíclico único de orden **q** en **Z***.
- Escoger $\mathbf{g \in Z^*_p}$ y calcular $\mathbf{\alpha = g^{(p-1)/q} \pmod p}$.
- Si **α = 1**, entonces regresar elegir otro número **α**.
- Escoger aleatoriamente un entero **a**, tal que **1 < a < q-1**.
- Calcular $\mathbf{y = \alpha^a \pmod p}$.
- La llave pública de **A** es **(p, q, α, y)**.
- La llave privada de **A** es **a**.

2.7.5.2 Proceso de Firma

A debe hacer lo siguiente:

- Seleccionar aleatoriamente un número entero secreto **K**, tal que **0 < K < q**.

- Calcular **$r = (\alpha^k \bmod p) \pmod q$**.
- Calcular **$K^{-1} \pmod q$**.
- Calcular **$S = K^{-1} [H(M) + ar] \pmod q$**.
- La firma de **A** para el mensaje **M**, es la pareja **(r, S)**.

2.7.5.3 Proceso de verificación

Para verificar la firma **(r, S)**, de **A** sobre el mensaje **M**, **B** debe hacer lo siguiente:

- Obtener la llave pública de **A**, **(p, q, α, y)**.
- Verificar que **$0 < r < q$**, y que **$0 < S < q$**, de lo contrario rechaza la firma.
- Calcular **$W = S^{-1} \pmod q$** y **H(M)**.
- Calcular **$U_1 = W * H(M) \pmod q$** y **$U_2 = r * W \pmod q$**.
- Calcular **$V = (\alpha^{U1} y^{U2} \bmod p) \bmod q$**.
- Acepta la firma si y sólo si **V = r**.

2.7.6 Estándar para firmas digitales

DSS, de sus siglas en inglés (**D**igital **S**ignature **S**tandard) es un sistema de firma digital adoptado como estándar por la organización de estándares de los Estados Unidos. (NIST). Utiliza la función Hash SHA y el algoritmo asimétrico DSA (Digital Signature Algorithm). Fue propuesto en 1991, y está basado en SHA – 1 y DSA.

El estándar DSS, solamente es usado para firma digital.

En 1994 se establece como estándar DSA y se le conoce como DSS.

2.7.7 Firmas digitales con cifrado

Dentro de la vida cotidiana es muy común que después de firmar un documento, ya sea por una o varias personas, se guarda en un sobre y se sella. Se protege de miradas indiscretas o no autorizadas brindando confidencialidad.

Ocurre lo mismo con las firmas digitales, después del proceso de firmado, se realice el ocultamiento de la firma, es decir, cifrar la firma.

En las firmas autógrafas, firmar el documento equivale a la firma digital y ponerlo en el sobre sellado equivale al proceso de cifrar la firma. De este modo con la combinación de la firma digital y la criptografía de llave pública se obtiene:

- La seguridad del cifrado.
- La autenticidad de la firma.

La firma proporciona la autoría y el sobre la privacidad o confidencialidad.

Un ejemplo de un protocolo con el uso de cifrado y firma digital sería el siguiente:

- **A** firma el documento **M** con su llave privada para firma.
- **A** cifra la firma con la llave pública de **B** y lo envía a **B**.
- **B** descifra la firma con su privada para cifrado.
- **B** verifica la firma con la llave pública de firma de **A**.

Cabe destacar que este protocolo implementa autenticación y confidencialidad. Con la autenticación garantizo el no repudio, porque solo **A** tiene su llave privada y es con la que firma.

Con la utilización de firmas digitales surge una cuestión, ¿Es mejor firmar antes de cifrar o viceversa?

En las firmas autógrafas, firmar y después cifrar es igual a firmar el documento y luego meterlo en un sobre. Cuando se cifra y luego firma es igual a meter el documento en un sobre y luego firmarlo. Se llega a la conclusión de que firmar antes de cifrar en más natural, es conveniente por consideraciones legales y es más seguro.

2.8 SEGURIDAD EN CORREO ELECTRÓNICO

Hoy en día, el correo electrónico es un servicio ampliamente utilizado en cualquier organización. Pero además es uno de los servicios que más ataques recibe, como son: Los virus, Spyware, Spam, Mal uso, Denegación de servicios, etc.

Por esto, es fundamental disponer de una organización segura y así minimizar los riesgos.

El correo electrónico carece de seguridad, los mensajes y los archivos que se adjuntan y viajan a través de la red pueden ser fácilmente alterados o abiertos. Lo que quiere decir que las partes involucradas no pueden estar seguras de que su comunicación está protegida.

Con la firma digital y el uso de los certificados digitales, es posible implementar un esquema de seguridad entre el remitente de un mensaje y el destinatario y para ello se requiere:

- Usar criptografía de llave secreta para garantizar la confidencialidad.
- Usar criptografía de llave pública para autenticación y no repudio.
- Una infraestructura de llave pública para asignar responsabilidades.

S/MIME es un protocolo de correo seguro y utiliza certificados digitales.

2.8.1 Funcionamiento de S/MIME

S/MIME, de sus siglas en inglés, (Secure / Multipurpose Internet Mail Extensions), Extensiones de Correo de Internet de Propósitos Múltiples / Seguro.

Es un protocolo que emplea criptografía de llave pública y firma para envolver el correo y fue desarrollado por RSA Inc. Data Security.

Con S/MIME tengo la capacidad de emplear cifrado y firmas digitales, de tal manera que se puede asegurar la integridad, autenticación, no repudio y confidencialidad en el correo electrónico.

Se basa en el estándar PKCS #7, para definir el formato y sintaxis necesaria para envolver el mensaje MIME dentro de un objeto PKCS #7 y este a su vez es envuelto en un mensaje MIME para ser transportado a los destinatarios. Por

su parte el receptor extrae el objeto PKCS de la entidad MIME que lo transporto, lo desenvuelve y recupera el mensaje MIME original.

El estándar PKCS #7, describe una sintaxis general para los datos a los que se les haya aplicado alguna función criptográfica, tal como la firma digital o el sobre digital.

PKCS #7, define seis diferentes tipos de contenido para manejar datos criptográficos, de los cuales tres con usados en S/MIME:

- Datos: Sólo datos, usado para enviar datos sin cifrar.
- Contenido Firmado: Datos firmados, usado para la autenticación del remitente. Con una estructura compuesta por los identificadores de algoritmos requeridos, certificados, listas de revocación de certificados y toda la información relacionada con la firma digital.
- Sobre digital: Una estructura de datos para incluir datos cifrados con la llave secreta y esta es cifrada con RSA usando la llave pública de cada unos de los destinatarios del mensaje. La combinación de un mensaje cifrado y la llave secreta usada cifrada es lo que se conoce como sobre digital, debido a que únicamente el destinatario puede abrirlo.

La composición de un mensaje S/MIME de manera gráfica es la siguiente:

S/MIME envuelve un mensaje MIME dentro de un objeto PKCS #7, el cual a su vez es envuelto en un mensaje MIME.

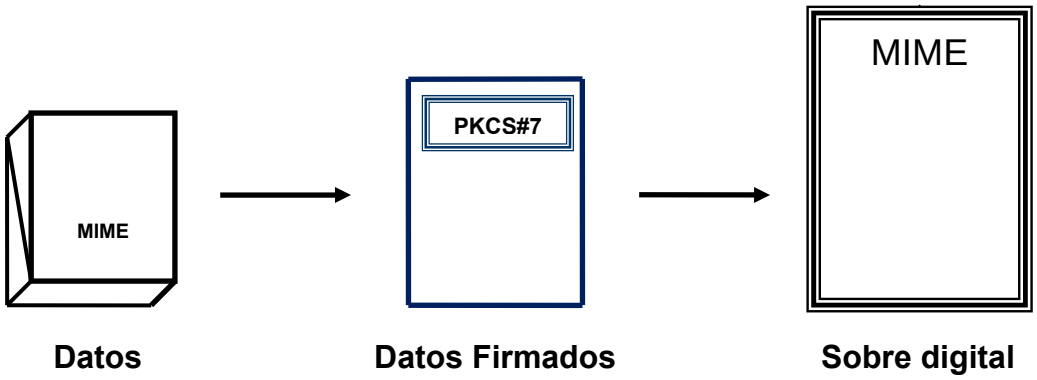

Figura 25. Mensaje S/MIME.

2.8.1.1 Proceso de firma en S/MIME

Las firmas digitales son el servicio más utilizado de S/MIME, cuando se firma un mensaje y es enviado, se le agrega una firma con el formato PKCS #7, que va junto con el mensaje. Esta firma agregada contiene un Hash del mensaje original firmado con la llave privada del emisor y también el certificado.

Para la firma del mensaje se necesita la pareja de llaves RSA, una llave pública y una llave privada y también se necesita en certificado X.509.

El cifrado de datos que utiliza S/MIME es RSA. La autenticidad de origen y de contenido es por medio de DSS / RSA y SHA – 1, la otra forma es por medio de DSS / RSA y MD5.

RSA y SHA – 1, es la forma de autenticidad que se utiliza en la implementación de firma digital de este proyecto. Para la administración de llaves, S/MIME lo hace por medio de RSA.

2.8.1.2 Cifrado de correo electrónico en S/MIME

El cifrado de un mensaje en S/MIME es generado utilizando la llave pública del receptor. El mensaje es cifrado usando una llave simétrica aleatoria, y la llave simétrica es cifrada usando la llave pública del receptor y es enviada junto con el mensaje.

En el caso de que el mensaje sea enviado a varios receptores, la llave simétrica es cifrada separadamente por cada una de las llaves públicas de cada uno de los receptores.

Los mensajes cifrados y todas las llaves simétricas cifradas son empaquetados todos juntos usando el formato PKCS #7. Para el cifrado de mensajes se necesita un certificado X.509 para cada receptor.

Para el cifrado de datos se utilizan los algoritmos: RC2/40 bits, RC2/64 bits, RC2/128 bits, DES, o 3DES.

La autenticidad de origen y contenido es por medio de RSA y SHA – 1, finalmente la administración de llaves es con RSA.

Dentro de las aplicaciones que emplean S/MIME encontramos Microsoft Outlook, que es la aplicación que se usará para implementar cifrado asimétrico y firma digital para correo electrónico seguro.

CAPITULO 3: INFRAESTRUCTURA DE RED EN LA CNBV

3.1 INTRODUCCIÓN

El objetivo principal de la infraestructura de red de la CNBV es mantener y garantizar la disponibilidad de la infraestructura de telecomunicaciones a través de esquemas de: conectividad, comunicación, monitoreo, respaldo y recuperación de la información, soporte y mantenimiento de infraestructura de red para que los usuarios de la CNBV, cuenten con los servicios de correo electrónico, red interna, internet, comunicación y acceso a los servidores.

Las aplicaciones de cifrado y firma digital, que se aplicaron a la Comisión Nacional Bancaria y de Valores con motivo de seguridad en correo electrónico, es a través del cliente de correo Outlook de Microsoft, con el objetivo de brindar seguridad y hacer más confidencial la información que fluye por la red, obteniendo también por otra parte la plena confianza de que el mensaje es auténtico y fue firmado por la persona que realmente lo emitió.

La infraestructura de seguridad de la Comisión Nacional Bancaria y de Valores, está compuesta con canales cifrados, VPN's, detectores de intrusos, filtrado de paquetes y filtros de contenido.

Para el análisis de la estructura, es necesario saber los objetivos que tiene la Institución y principalmente la Dirección General de Informática y poder cumplirlos de manera correcta.

Por otro lado saber también de que manera está constituida la red, cuantas secciones tiene, y poder conocer los alcances de la red cableada e inalámbrica, con cuantos usuarios cuenta la Comisión Nacional Bancaria y de Valores, y la plataforma en que se va a trabajar e implementar la firma digital y cifrado en el correo electrónico.

Cuando se habla de información se debe tener en cuenta que es necesario tener un nivel de seguridad bastante fuerte tanto de manera interna como externa, la información puede ser sensible y no puede llegar a manos de personas que puedan hacer un mal uso de ella o simplemente enterarse de cosas que no deben.

Cabe destacar que los elementos que permitirán dar seguridad a la información en el correo electrónico y de los cuales se hace uso, son el cifrado y la firma digital.

3.2 MISIÓN Y OBJETIVOS DE LA COMISIÓN NACIONAL BANCARIA Y DE VALORES

“Que el país cuente con una autoridad fuerte e independiente, capaz de responder de manera oportuna con regulación y supervisión eficaz, a fin de procurar la estabilidad y correcto funcionamiento de las distintas entidades financieras, evitando incurrir en riesgos sistémicos, al tiempo de ofrecer protección a los inversionistas y al público usuario de sus servicios”.

Para el cumplimiento de esta misión la Comisión Nacional Bancaria y de Valores ha fijado los siguientes objetivos:

- Procurar la estabilidad y solvencia del sistema financiero.
- Proteger los intereses de los ahorradores y del público inversionista.
- Promover el mejoramiento constante de la calidad de la administración de los intermediarios e instituciones bancarias.
- Fomentar la eficiencia y el sano desarrollo del sistema financiero.
- Fortalecer el desarrollo institucional de la Comisión Nacional Bancaria y de Valores.

Para el cumplimiento de sus objetivos la Comisión Nacional Bancaria y de Valores cuenta con las facultades que le otorgan las leyes relativas al sistema financiero, así como su propia Ley, las cuales se ejercen a través de los siguientes órganos: Junta de Gobierno, Presidencia, Vicepresidencias, Contraloría Interna, Direcciones Generales y demás unidades administrativas necesarias.

3.3 DIRECCIÓN GENERAL DE INFORMÁTICA

3.3.1 Visión

“Una Comisión Nacional Bancaria y de Valores que cuente con una función Informática sólida y vanguardista que esté en una constante investigación a nivel nacional e internacional sobre el desarrollo de nuevas prácticas, que a través de sistemas informáticos, modelos y metodologías modernicen y fortalezcan los procesos de supervisión y administración de la Comisión y que

patrocine una actualización tecnológica siempre acorde a las estrategias del Organismo".

3.3.2 Misión

"Implantar sistemas de información que estén acordes y apoyen los procesos sustantivos de supervisión, regulación y coordinación institucional con calidad, oportunidad, seguridad, disponibilidad, optimización, mejor desempeño, niveles de servicio adecuados, apegados a estándares tecnológicos de punta y a criterios de costo-beneficio, con indicadores de desempeño que permitan una administración eficaz y eficiente de los recursos".

3.3.3 Objetivo

"Aplicar la tecnología para participar en la mejora continua de los servicios de la CNBV encaminada a incrementar la eficiencia, productividad y cobertura de los servicios de regulación y supervisión, estableciendo mecanismos que garanticen información disponible, veraz y oportuna, a través de la aplicación de estándares y políticas que se apeguen al marco legal y normativo federal en materia de Tecnología de Información, a fin de brindar apoyo y las facilidades tecnológicas a los usuarios de la CNBV, Autoridades y Entidades Financieras para el intercambio electrónico de información".

3.4 COMPOSICIÓN DE LA RED INTERNA

Una red de computadoras es un conjunto de computadoras interconectadas entre sí. Las formas en que pueden ser conectadas son variadas, se pueden conectar unas cuantas computadoras para formar una red local y también interconectar dos o más redes locales para formar una red amplia.

La red interna dentro de la institución está constituida aproximadamente por 2000 nodos y 1200 usuarios, además de otros nodos extras para servidores, DNS's y firewalls, que por motivos de seguridad no se pueden mencionar con cuantos se cuentan ni de qué manera están conectados. Todos los usuarios están conectados dentro de un dominio llamado:

- "**CONABV.GO**"

La red esta segmentada en ocho partes en las dos torres, la norte y la sur. Esta a su vez está repartida en cuatro segmentos en cada torre. Existe un segmento más que se encuentra ubicado en otra parte de la torre, que sirve como respaldo de datos.

La red cuenta con dos Core's de conexión, uno para cada torre, estos a su vez se encuentran interconectados con fibra óptica a una velocidad de 10 GB, para la transmisión de datos.

A continuación se muestra de manera gráfica como está distribuida la red:

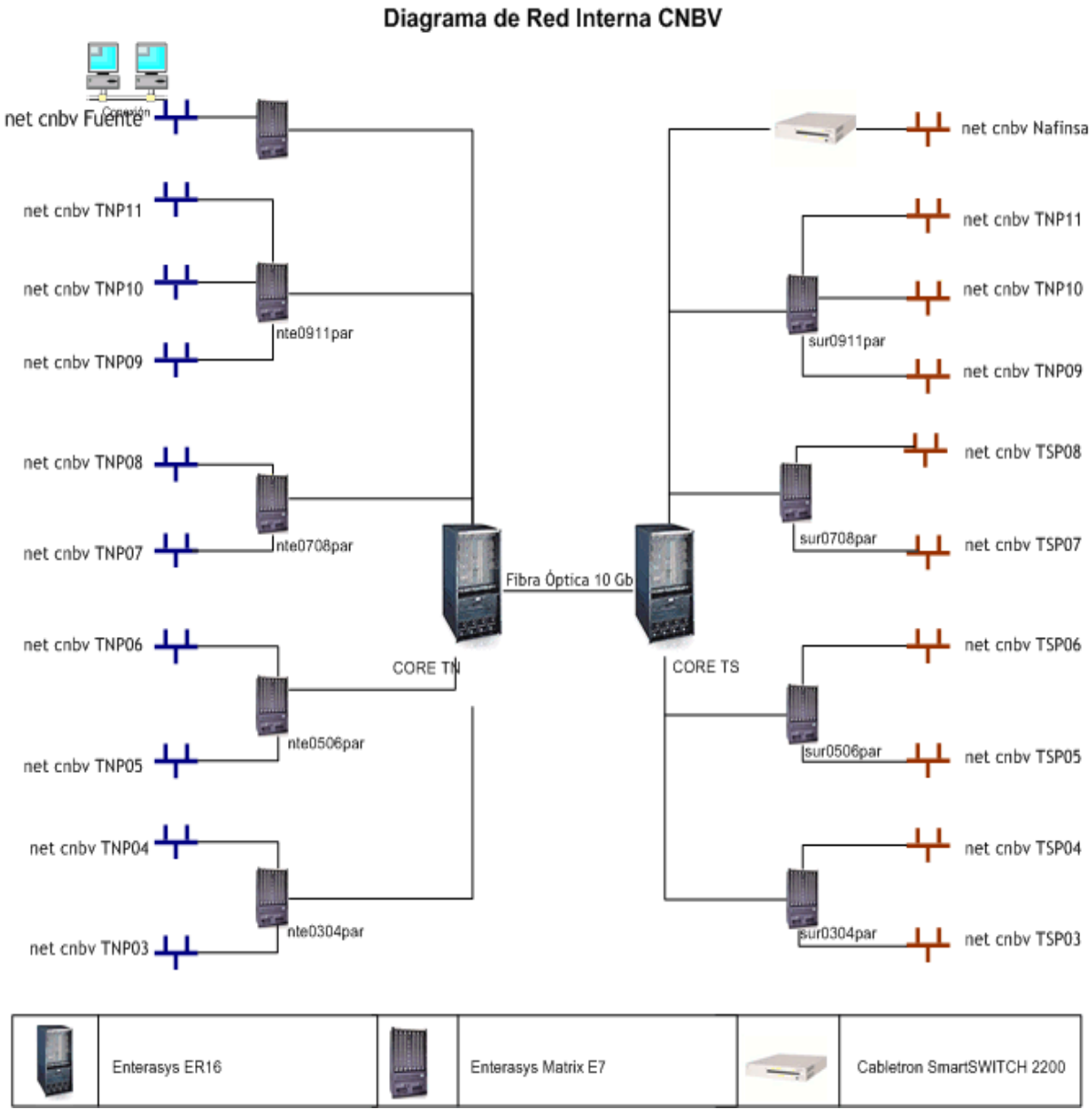

Figura 26. Red Interna.

Para colocar a todos los usuarios dentro del dominio y poderse autenticar, se tiene instalada la herramienta “Active Directory”, con la que se administra y se da permiso a los usuarios para ingresar a diferentes segmentos de la red y servidores. Dicha herramienta está instalada dentro del siguiente servidor: Microsoft Windows Server 2003 Service Pack 2, con las siguientes características:

- 4GB en RAM.
- Disco duro de 100 GB.
- Tarjeta de red con una velocidad de 1 GB.
- Procesador Intel Xenon Quad Core, 3 GHz.

La versión instalada y que se utiliza de Active Directory es la siguiente:

- Active Directory Users and Computers.
- Microsoft Corporation.
- V. 52.23790.3959.

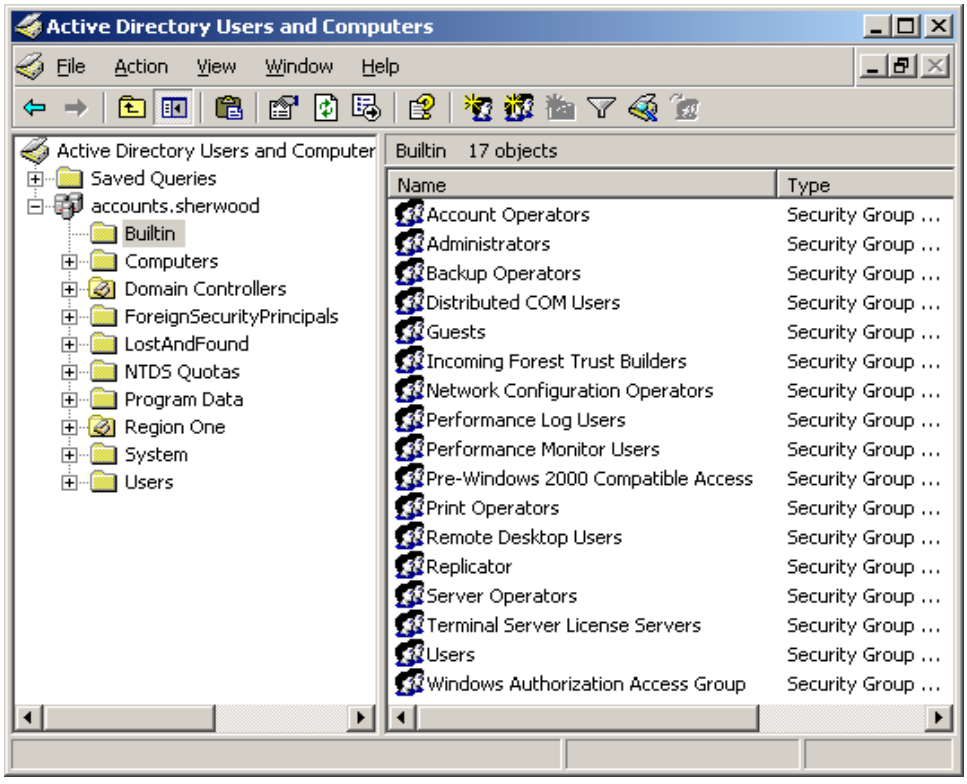

Figura 27. Active Directory Users and Computers.

Active Directory es un componente clave para la implementación de certificados S/MIME. Para distribuir certificados a los usuarios para que los utilicen con los servicios de correo electrónico. Además, Active Directory en Windows Server 2003 ofrece compatibilidad como el directorio PKI para varios clientes de correo electrónico de Microsoft, incluidos Office Outlook, Outlook Express y Outlook Web Access (OWA) con S/MIME y la capacidad de asignar cuentas de usuario a los certificados.

Cabe destacar que Active Directory hace el manejo de todos los usuarios, estos se encuentran clasificados por un identificador "ID" y se agrupan de la siguiente manera:

- ID, más número de nómina para empleados.
- IDXT, para usuarios externos.
- IDSS, para usuarios de servicio social.
- IDHO, para usuarios que trabajan por honorarios.

A los usuarios que no son empleados se les otorga un número consecutivo posterior al ID al que pertenezcan. De esta manera la herramienta maneja a los usuarios y permite que ingresen dentro del dominio.

Para la implementación de la firma digital y cifrado en el correo electrónico se utiliza Active Directory, porque se tiene todos los datos reales de cada uno de los usuarios, sin la posibilidad de alterar o eliminar información de cada uno de los empleados, lo que me da la confianza que los usuarios no pueden poner datos falsos.

3.5 SERVIDORES

Un servidor es un tipo de software que realiza ciertas tareas en nombre de los usuarios. También es utilizado para referirse al ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer datos de modo que otras máquinas puedan utilizar esos datos.

Un servidor sirve información a los ordenadores que se conecten a él. Cuando los usuarios se conectan a un servidor pueden acceder a programas, archivos y otra información del servidor.

Algunos servidores manejan solamente correo o solamente archivos, mientras que otros hacen más de un trabajo, ya que un mismo ordenador puede tener diferentes programas de servidor funcionando al mismo tiempo.

La Comisión Nacional Bancaria y de Valores cuenta con distintos servidores, como son:

- Bases de datos.
- Web.
- Aplicaciones locales.
- Dominio.
- Correo electrónico.
- Acceso Web al correo electrónico.
- DNS.

Los servidores que se usan para implementar cifrado y firma digital en el correo electrónico son:

- Servidor Exchange (Correo Electrónico, Outlook y Outlook Web Access).
- Servidor de Dominio (Active Directory). Sus características ya has sido mencionadas con anterioridad.

El servidor Windows Server Exchange 2007, es con el que cuenta la Institución y tiene las siguientes características:

- Procesador AMD Quad Core 1.7 GHz.
- 8 GB de memoria RAM.
- Disco duro de 250 GB.

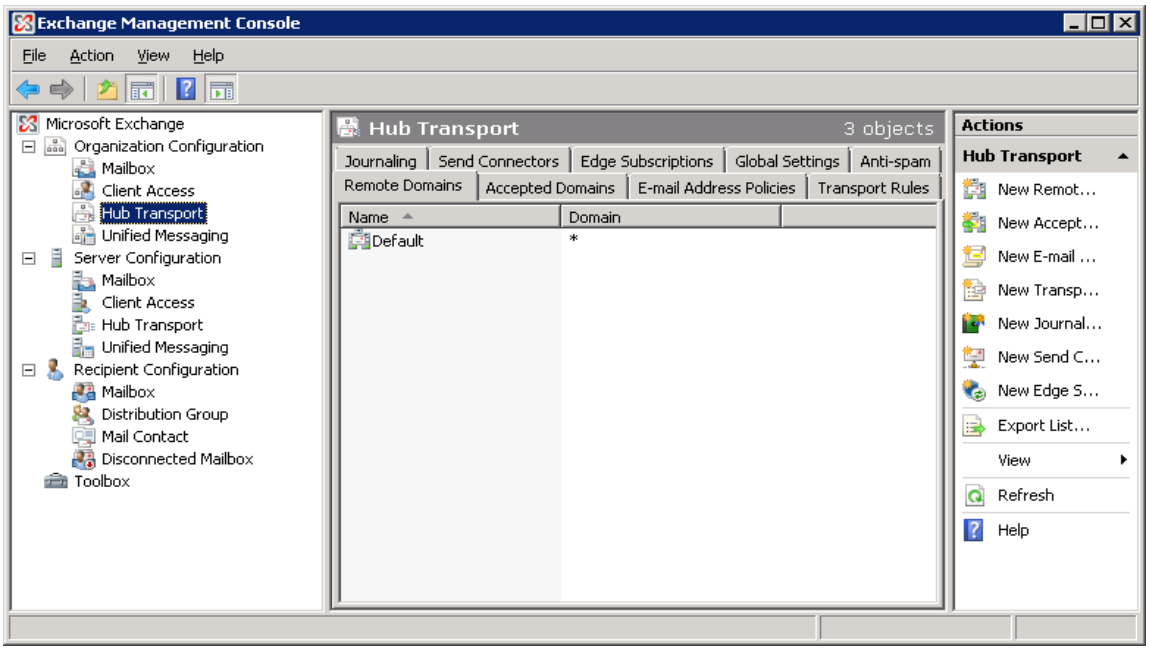

Figura 28. Windows Server Exchange 2007.

Exchange Server 2007 puede personalizar la implementación para que cumpla con la firma digital y el cifrado. S/MIME de Exchange Server 2007 puede admitir clientes de Outlook, de OWA y de Outlook Express. Sin embargo, puesto que el cliente de correo electrónico debe admitir la versión 3 de S/MIME.

S/MIME también se incluye en Exchange Server 2000 y Exchange Server 2003.

Este servidor me permite administrar las cuentas de correo de cada uno de los usuarios y está ligado completamente con el Servidor Windows 2003 con Active Directory, ya que este ingresa a los usuarios al dominio.

También se utiliza la aplicación OWA, de sus siglas en ingles, (Outook Web Access), que permite acceder al correo electrónico vía web. Se puede acceder a él mediante el portal de la Comisión Nacional Bancaria y de Valores en la sección E – MAIL CNBV.

Figura 29. Outlook Web Access.

Outlook Web Access permite acceder al buzón de Exchange Server 2007 vía web y consultar sus datos personales donde quiera que el usuario se encuentre, en cualquier momento podrá examinar su cuenta, por ejemplo:

- Correo electrónico.
- Libro de direcciones.
- Agenda.
- Calendario, etc.

El aspecto gráfico del OWA es muy similar al Outlook estándar, con la única diferencia de ser considerablemente más simple en algunas de sus funciones.

Debido a que esta aplicación es una especie de interfaz no necesita tanto almacenamiento, porque toda la información de los correos se encuentra almacenada en el Servidor Exchange.

Dentro de la CNBV los switches de conexión se encuentran físicamente en los pisos 9, 8, 5 y 3 de la torre norte. En la torre norte se localizan en el piso 9, 7, y dos en el piso 4.

Cada torre alberga muchos usuarios y están distribuidos de la siguiente forma:

- Torre Norte:
  - 288 Nodos en los pisos 11, 10 y 9.
  - 288 Nodos en los piso 8 y 7.
  - 312 Nodos en los pisos 5 y 4.
  - 192 Nodos en el piso 3.

- Torre Sur:
  - 240 Nodos en los pisos 11, 10 y 9.
  - 240 Nodos en los pisos 8 y 7.
  - 240 Nodos en los pisos 6 y 5.
  - 240 Nodos en los pisos 4 y 3.

Cada usuario cuenta con una computadora donde tiene instalado Microsoft Office Outlook 2007, este admite la conectividad basada en MAPI (Interfaz de programación de aplicaciones de mensajería) con Exchange Server 2007.

S/MIME de Exchange Server 2007 se puede utilizar con cualquier versión de Outlook que admita certificados digitales X.509 v3. La compatibilidad total en Outlook para los certificados digitales X.509 v3.

Los certificados con que cuentan los usuarios son X.509 v3.

En el diagrama siguiente se muestra la red completa de todos los ordenadores junto con la granja de servidores, y como esta segmentada dentro de las dos torres.

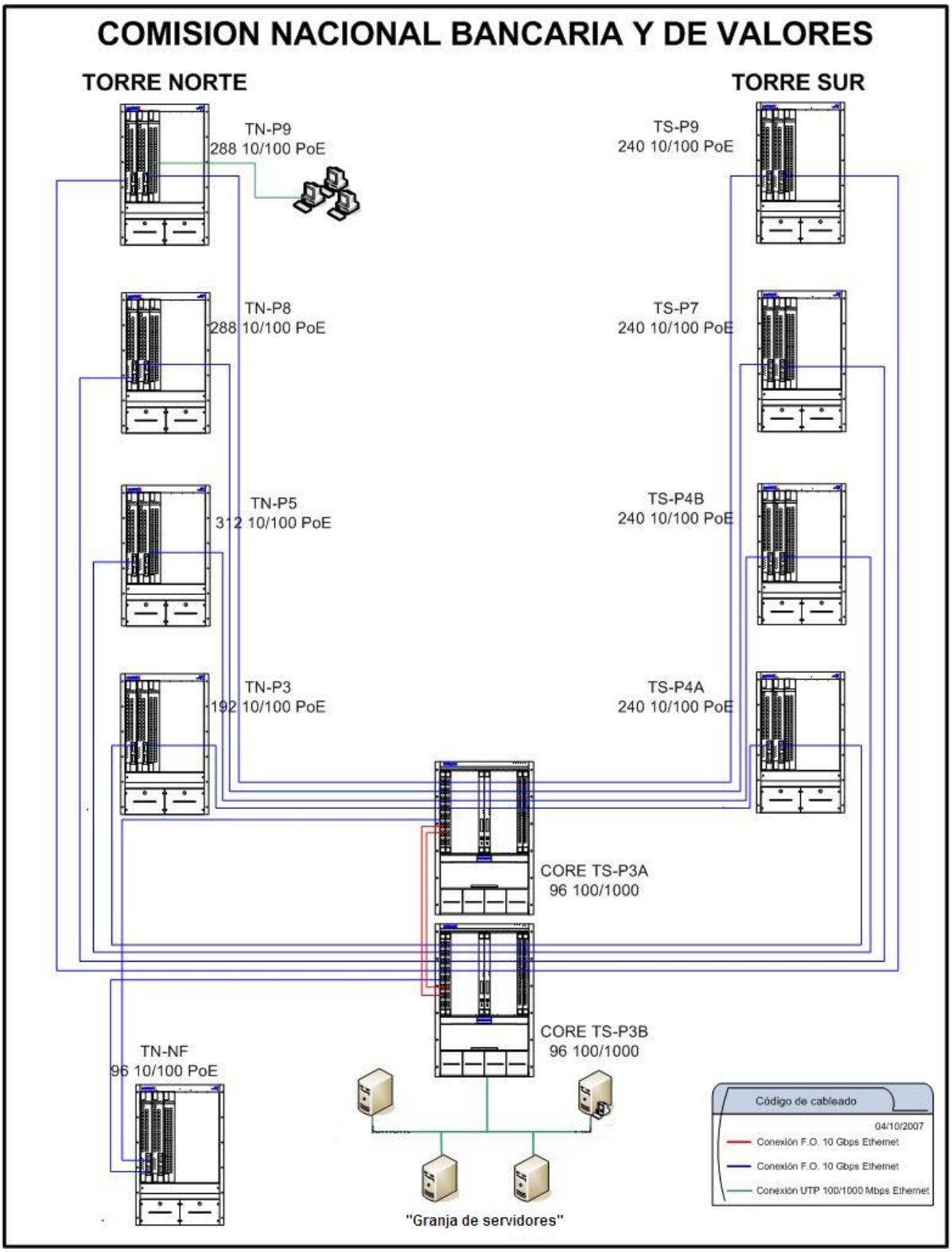

Figura 30. Servidores y Red de la CNBV.

Con el análisis de la estructura de la Institución, se da por hecho que se puede hacer la implementación la firma digital y cifrado de correo en la Comisión Nacional Bancaria y de Valores, con la utilización del servidor de correo (Server Exchange 2007 con OWA) y servidor de dominio (Server 2003 con Active Directory), así como el uso del cliente de correo Microsoft Outlook.

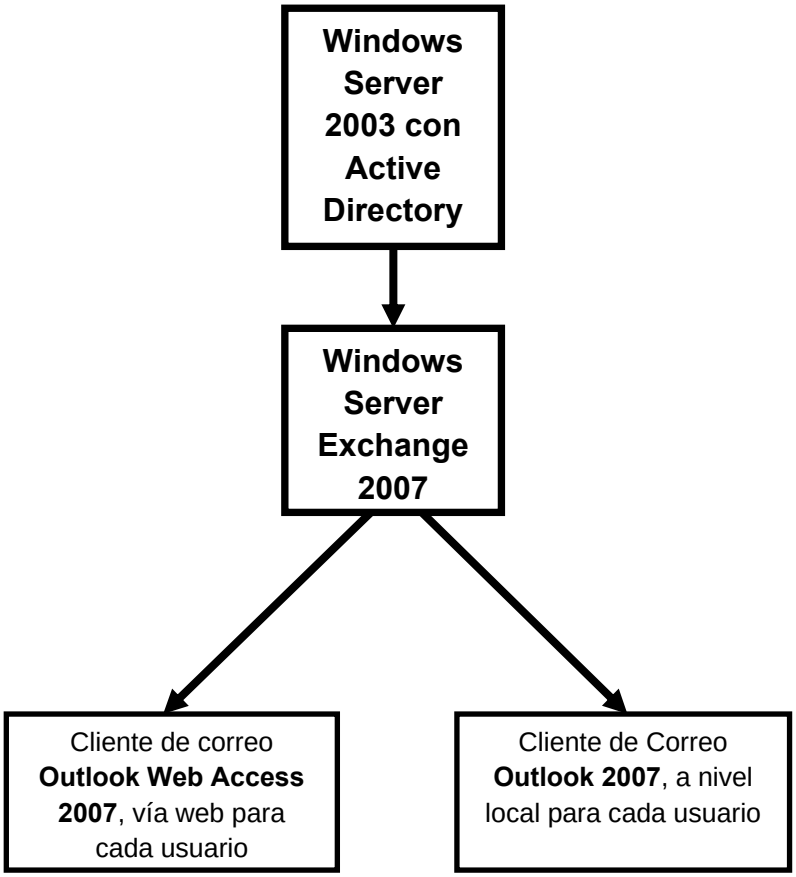

Figura 31. Conexión de servidores y aplicaciones.

El uso del correo electrónico seguro dentro de la CNBV, con cifrado y firma digital, me permite garantizar la confidencialidad, integridad y autenticación.

Para que fuera posible hacer esta tarea se utilizó el estándar S/MIME, que está basado en criptografía de llave pública. Con los servidores que se cuentan y la manera que están conectados permite a cada usuario firmar y cifrar correo electrónico a través del cliente de correo Outlook 2007 y vía Web a través de Outlook Web Access.

CAPITULO 4: IMPLEMENTACIÓN DE CIFRADO Y FIRMA DIGITAL

4.1 INTRODUCCIÓN

Cada vez más, las personas y las organizaciones utilizan el correo electrónico como una herramienta para enviar información confidencial. Dada la naturaleza confidencial de los datos, los sistemas de correo electrónico deben proporcionar mecanismos para impedir que los datos sean modificados, además de garantizar que los mensajes no van a ser interceptados ni leídos por ninguna otra persona que no sea el destinatario al que van dirigidos.

Mediante las llaves privadas y públicas así como también las firmas digitales, estos tres elementos son conocidos también como identificadores digitales. Se puede acreditar la identidad de una persona en las transacciones electrónicas, como cuando se enseña la credencial de elector cuando se tiene que cobrar un cheque. Puede utilizar también un identificador digital para cifrar mensajes de forma que se garantice su confidencialidad. Los identificadores digitales incorporan la especificación S/MIME, para proteger el correo electrónico.

La implementación se basa en el uso de certificados digitales emitidos por la propia Comisión Nacional Bancaria y de Valores para su personal y para uso exclusivo dentro de ella.

La privacidad y veracidad que brinda la propia autoridad emisora de certificados, al enviar el correo electrónico.

4.2 DESCRIPCIÓN GENERAL

Desde hace tiempo las funciones de seguridad en el correo electrónico han estado presentes desde la primera versión de Microsoft Exchange Server, normalmente sólo los usuarios que conocen de seguridad han utilizado estas funciones. Los únicos que necesitaban comprender los conceptos de seguridad en los mensajes de correo electrónico eran los especialistas en seguridad y aquellos usuarios con conocimientos en criptografía.

Gracias al soporte mejorado de S/MIME en Exchange Server 2007 y a la necesidad de una conformidad normativa, los administradores comenzaron a necesitar comprender estos principios y conceptos.

Microsoft Exchange Server 2007 Service Pack 2, ofrece soporte para S/MIME en Microsoft Outlook Web Access y Microsoft Office Outlook 2007.

4.2.1 Ventajas de S/MIME

Con S/MIME, los administradores tienen una opción de correo electrónico que ayuda a ofrecer una gran seguridad, lo que permite una conectividad de correo electrónico generalizada y segura.

S/MIME ofrece dos servicios de seguridad:

- Firmas digitales.
- Cifrado de mensajes.

Estos dos servicios constituyen el núcleo de la seguridad de mensajes en el correo electrónico basada en S/MIME. El resto de conceptos relacionados con la seguridad de mensajes admiten estos dos servicios. Aunque el ámbito completo de la seguridad de mensajes puede parecer complejo, estos dos servicios constituyen la base para alcanzar esa seguridad.

Las firmas digitales y el cifrado de mensajes son servicios que pueden trabajar de manera conjunta. Cada servicio se ocupa de problemas de seguridad específicos. Las firmas digitales se encargan de los problemas de autenticación y no repudio, por su parte el cifrado de mensajes se ocupa de los problemas de confidencialidad.

Debido a que cada servicio se encarga de problemas diferentes, una estrategia de seguridad de mensajes requerirá la presencia de ambos, a menudo al mismo tiempo. Cuando estos dos servicios se utilizan por separado, se utilizan de la siguiente manera, las firmas digitales se encargan de los problemas de seguridad relacionados con los remitentes, mientras que el cifrado se encarga principalmente de los problemas de seguridad relacionados con los destinatarios.

Cuando las firmas digitales y el cifrado de mensajes se utilizan conjuntamente, los usuarios se benefician de ambos servicios. El empleo de ambos servicios en los mensajes no cambia la manera de proceso de cada servicio.

4.2.2 Firmas Digitales

Las firmas digitales son el servicio más utilizado de S/MIME. Como su nombre lo dice, las firmas digitales son la otra cara digital de la firma tradicional de un documento de papel. Las firmas digitales cuentan con las siguientes características:

- Autenticación: Una firma sirve para validar una identidad.

- No repudio: Una firma ayuda a impedir que el propietario de la firma rechace la firma.

- Integridad: Ayuda a garantizar que el mensaje de correo electrónico que se ha recibido es igual al mensaje que se ha firmado y enviado y que no se ha alterado durante el envío.

4.2.3 Cifrado de Mensajes

El cifrado de mensajes ofrece una solución en el intercambio de mensajes.

El correo electrónico de Internet no protege los mensajes. Lo puede leer cualquier usuario que lo vea durante su envío o verlo en el lugar en el que se ha almacenado. Por ejemplo dentro de la Comisión Nacional Bancaria y de Valores el administrador de red puede ver cualquier mensaje, que este enviándose o almacenado en el servidor de correo. S/MIME contribuye a solucionar estos problemas mediante el uso del cifrado.

El cifrado es una forma de cambiar la información para que no se pueda leer o entender hasta que se devuelve a un formato legible y compresible.

A pesar de que el cifrado de mensajes no se utiliza tanto como las firmas digitales, logra solucionar lo que muchas personas perciben como la debilidad más grave del correo electrónico en Internet.

El cifrado de mensajes proporciona dos servicios de seguridad específicos:

- Confidencialidad: Protege el contenido de un mensaje de correo electrónico. Sólo el destinatario deseado puede ver el contenido y éste permanece confidencial y no puede conocerlo nadie más que quien recibirá el mensaje.

  El cifrado permite proporcionar confidencialidad mientras el mensaje se encuentra en tránsito o almacenado.

- Integridad: De la misma manera que con las firmas digitales, el cifrado de mensajes garantiza que el mensaje no haya sufrido modificaciones.

4.3 REQUISITOS PARA LA IMPLEMENTACIÓN

En la Comisión Nacional Bancaria y de Valores para proporcionar, confidencialidad, autenticación, no repudio e integridad en el correo electrónico, se requiere de lo siguiente, tomando en cuenta que en los servidores ya se encuentran instaladas las aplicaciones como son: Active Directory, Outlook Web Access.

4.3.1 Windows Server como controlador de dominio

Ya se encuentra instalado y es administrado con Active Directory.

4.3.2 Conectar estaciones de trabaja al dominio

Todos los usuarios se encuentran conectados al dominio “CONABV.GO”, por medio de Active Directory.

4.3.3 Windows Exchange Server 2007 con servicios de Correo Electrónico

Estos servicios ya se encuentran instalados dentro del servidor, estos servicios de correo electrónico incluyen el servicio Protocolo de Oficina de Correo 3, (POP3, de sus siglas en inglés, Post Office Protocol) y el servicio Protocolo simple de transferencia de correo (SMTP, de sus siglas en inglés, Simple Mail Transfer Protocol), que recuperan y transfieren correo electrónico, respectivamente. Para proporcionar servicios de correo electrónico a los usuarios, como envío y recepción de correo electrónico, los administradores pueden crear buzones en el servidor.

Las características de cada unos de estos servicios son**:**

- El servicio POP3 es un servicio de correo electrónico que recupera correo electrónico. Los administradores pueden utilizar el servicio POP3 para almacenar y administrar cuentas de correo electrónico en el servidor de correo. Cuando el servicio POP3 está instalado en el

servidor de correo, los usuarios pueden conectarse al servidor y recuperar el correo electrónico en su equipo local mediante un cliente de correo electrónico que sea compatible con el protocolo POP3, como Outlook. El servicio POP3 se utiliza con el servicio SMTP, que envía el correo electrónico saliente. "POP3 es una norma de Internet para almacenar mensajes de correo electrónico en un servidor de correo para acceder a él y descargarlos en una computadora"[24].

- SMTP controla el modo en que el correo electrónico se transporta y distribuye a través de una organización o Internet hasta un servidor de destino. SMTP recibe y envía correo electrónico entre servidores. El servicio SMTP se instala automáticamente en el equipo donde está instalado el servicio POP3 para permitir que los usuarios envíen correo electrónico saliente. Cuando se crea un dominio con el servicio POP3, el dominio se agrega también al servicio SMTP para que los buzones del dominio puedan enviar correo electrónico saliente. "El servicio SMTP del servidor de correo recibe el correo entrante y lo transfiere el correo a donde se almacena. Gobierna la transmisión de mensajes de correo electrónico en la redes de computadoras"[25].

4.3.4 Windows Server 2007 con Outlook Web Access

Ya se encuentra instalado y está conectado directamente con Windows Exchange Server 2007 como servidor de correo. Y pueden los usuarios conectarse a él vía Web.

4.4 OBTENCIÓN DE LOS CERTIFICADOS

La CNBV tiene instalada su propia entidad emisora de certificados y envía certificados para sus empleados para crear un entorno informático seguro.

En el dominio de la CNBV el envío de correo electrónico seguro se basará en los certificados emitidos por la entidad certificadora "CNBVCA" que se utiliza dentro de la institución. Por lo tanto cada empleado tiene su certificado personal para firmar y cifrar correo.

---

[24] Cisco Systems, Inc., *Academia de Networking de Cisco Systems Guía del primer año. CCNA 1 y 2*, (2004), TCP Intermedio, (p. 751).

[25] Cisco Systems, Inc., *Academia de Networking de Cisco Systems Guía del primer año. CCNA 1 y 2*, (2004), Conjunto de protocolos TCP/IP y direccionamiento IP, (p. 349).

La solicitud de un certificado debe realizarla el usuario o equipo que tenga acceso a la llave privada asociada a la llave pública que formará parte del certificado. El certificado se solicita mediante un asistente de solicitud de certificados.

El proceso para solicitar un certificado por medio del asistente es el siguiente:

- En el equipo del usuario, hacer clic en el botón Inicio de Windows, en ejecutar, escribir **certmgr.msc** y después clic en aceptar.

- En la ventana certificados en la carpeta personal, hacer clic en el signo de más (**+**), ubicado junto a personal para expandir la carpeta.

- En certificados, dar clic derecho y elegir todas las tareas y finalmente dar clic en solicitar un nuevo certificado. El proceso se muestra en la siguiente figura:

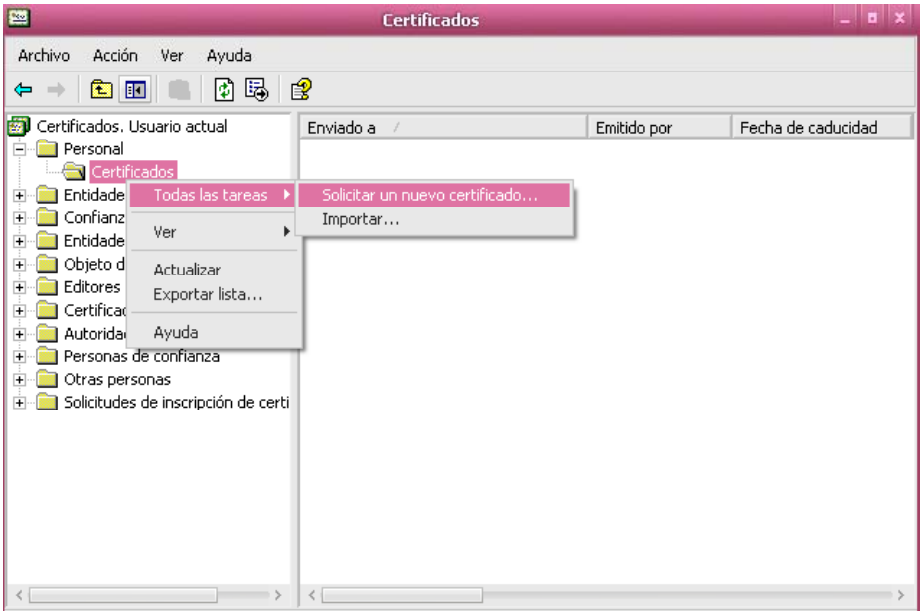

Figura 32. Solicitar un nuevo certificado.

- Posteriormente aparece en la pantalla el asistente para solicitud de certificados, hacer clic en siguiente.

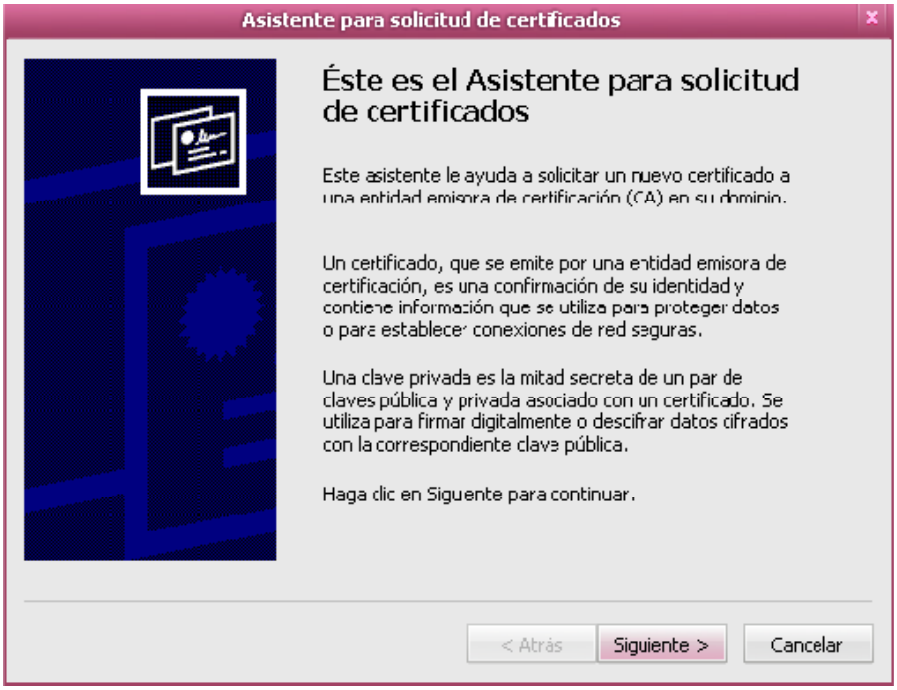

Figura 33. Asistente para solicitud de certificados.

- En tipos de certificados hacer clic en tipo Usuario y verificar la casilla en opciones avanzadas, posteriormente clic en siguiente

- En proveedor de servicios de cifrado escoger Microsoft Enhanced Cryptographic Provider V1.0, la longitud de la llave en 1024 bits, luego se verifica la casilla para habilitar la protección segura de llave privadas y también la de marcar esta clave como exportable, esto sirve para exportarla en algún momento y después importarla para usarla en alguna otra computadora para el uso de Outlook Web Access.

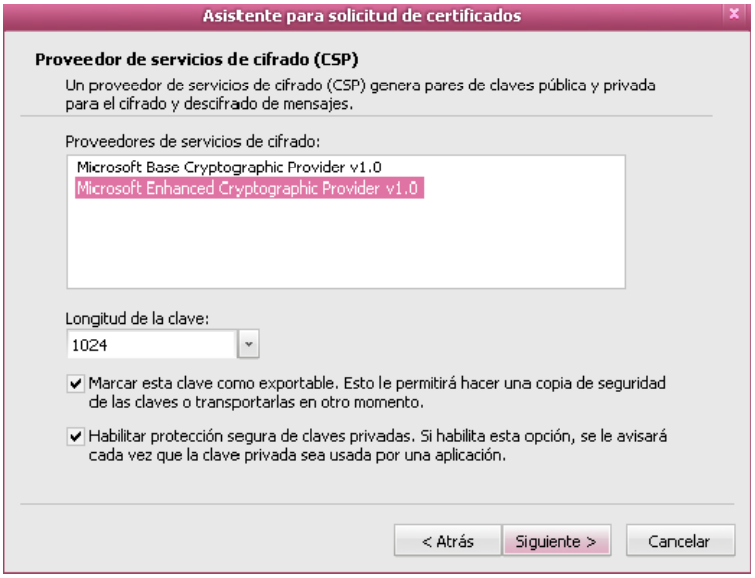

Figura 34. Proveedor de servicios de cifrado, longitud y protección de la llave.

- En la ventana entidad emisora de certificados, nos muestra la autoridad certificadora que es **"CNBVCA",** y el equipo donde se encuentra, por razones de seguridad no se muestra el nombre del servidor. Dar clic en siguiente.

- En descripción y nombre descriptivo del certificado nuevo, poner **"ID Certificado"**, a continuación, clic en siguiente. Comprobar que los datos del certificado sean correctos, como muestra la siguiente figura:

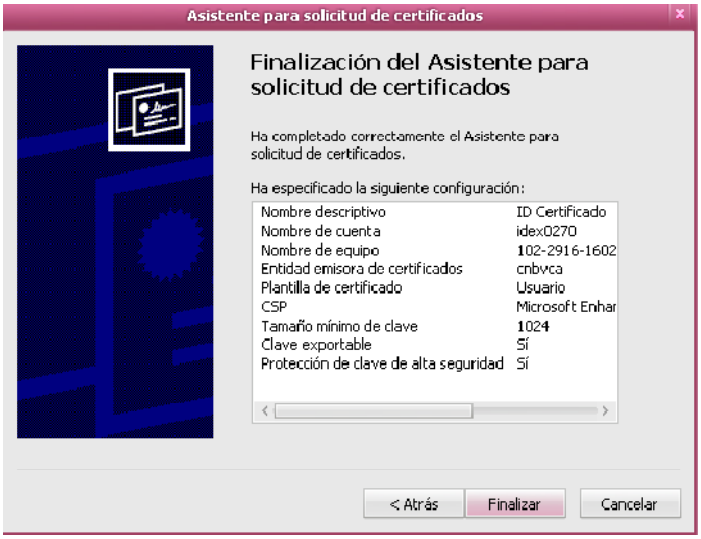

Figura 35. Informe de solicitud de certificado.

- Posteriormente hacer clic en finalizar y nos aparecerá una ventana para crear una contraseña para el intercambio de llaves con RSA.

Figura 36. Creando una nueva clave de intercambio RSA.

- Dar clic en nivel de seguridad, nos aparecerá una nueva ventana, se elige nivel alto de seguridad, con ello nos solicita una contraseña al enviar un mensaje cifrado o firmado, a continuación, clic en siguiente.

Figura 37. Nivel de seguridad para la llave privada.

- Se elige una contraseña segura para proteger la llave privada, se confirma y se da clic en finalizar, a continuación en aceptar.

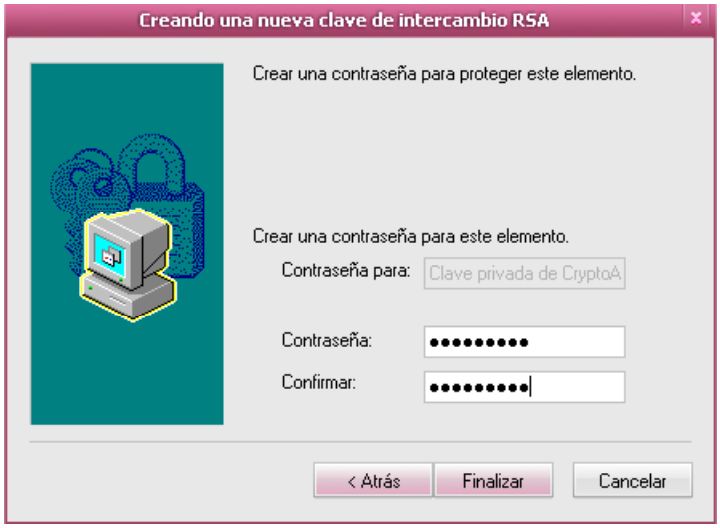

Figura 38. Contraseña para el uso de la llave privada.

- Finalmente aparece una ventana confirmando que todo se realizó correctamente, a continuación, clic en finalizar.

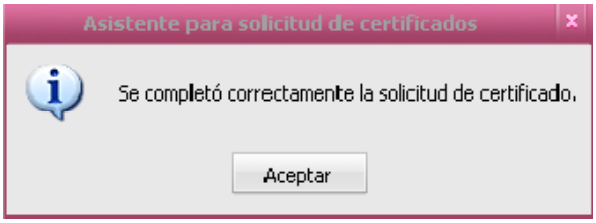

Figura 39. Confirmación de solicitud terminada.

Ahora en la ventana de certificados, en la carpeta personal aparece nuestro certificado con nuestro nombre, por la autoridad certificadora que lo emitió, la fecha de caducidad, las propiedades en este caso para correo seguro, cifrado y autenticación.

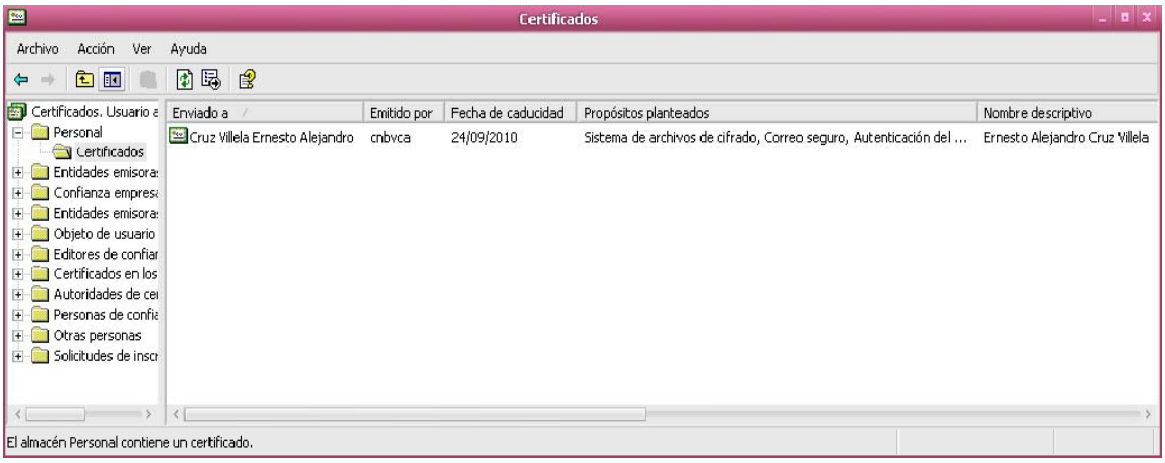

Figura 40. Almacén de certificados personal.

Se puede comprobar los datos dando doble clic en el nombre del certificado, posteriormente nos aparece el certificado personal, como muestra la siguiente figura:

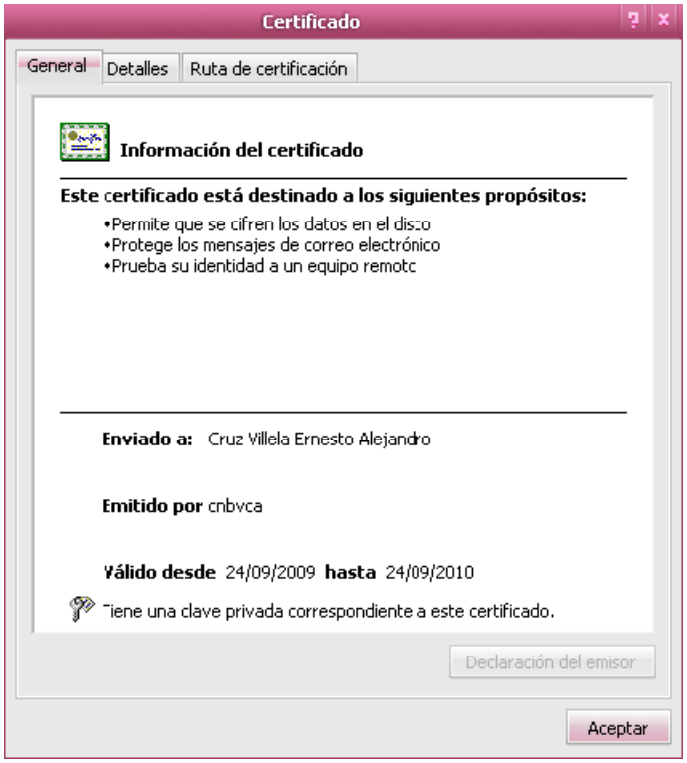

Figura 41. Certificado Digital Personal.

El certificado digital nos muestra información valiosa, como son, el periodo de validez y los propósitos para los que fue hecho:

- Permite que se cifren los datos en el disco.
- Protege los mensajes de correo electrónico.
- Prueba su identidad a un equipo remoto.

Con la realización de todos estos pasos se da por terminado el proceso de obtención de un certificado digital, ahora se configuran las estaciones de trabajo con Windows XP Profesional y Microsoft Outlook 2007, para poder hacer uso de los certificados digitales e implementar cifrado y firma digital.

4.5 CONFIGURACIÓN DE MICROSOFT OUTLOOK 2007 EN ESTACIONES DE TRABAJO

- En el equipo local de cada usuario, hacer clic en el botón de inicio de Windows, seleccionar todos los programas y después hacer clic en Microsoft Office, a continuación, hacer clic en Microsoft Office Outlook 2007.
- Al abrir Outlook, en la CNBV el usuario ya tiene su cuenta configurada en el servidor de correo, Windows Exchange Server 2007, y el servicio de correo listo para utilizar.
- Dentro de Outlook, hacer clic en herramientas y posteriormente clic en centro de confianza.

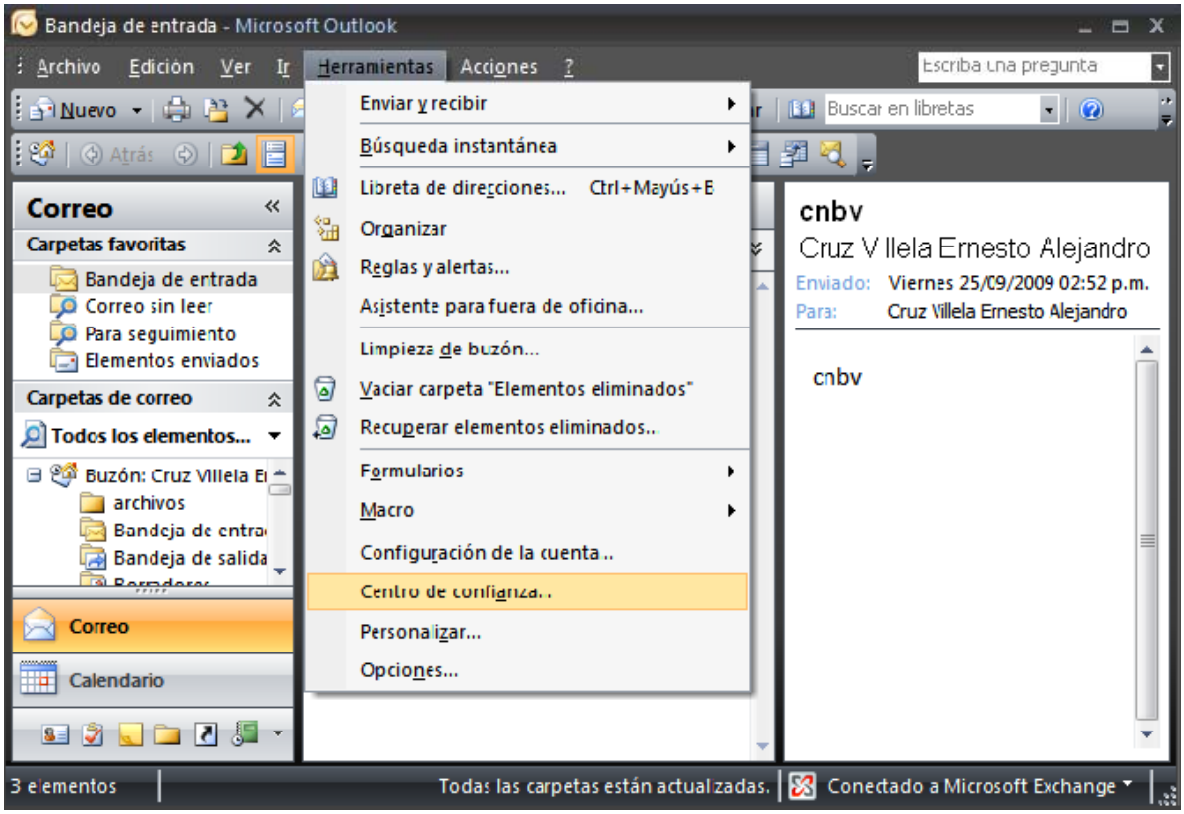

Figura 42. Configuración de Outlook.

- En la ventana Centro de confianza, hacer clic en la ficha Seguridad en correo electrónico.

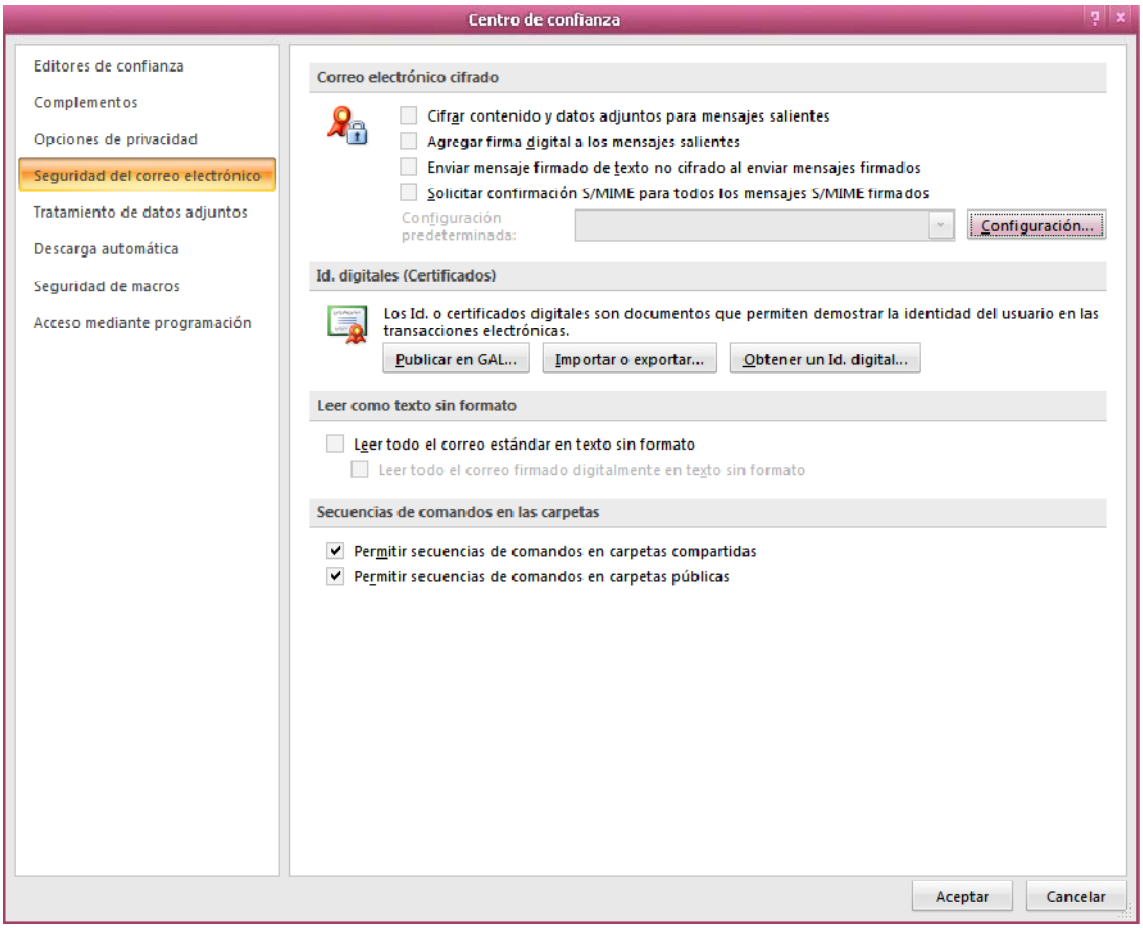

Figura 43. Seguridad en correo electrónico.

- Dar clic en el botón configuración, para elegir el modo de cifrado y el certificado para firmar y cifrar

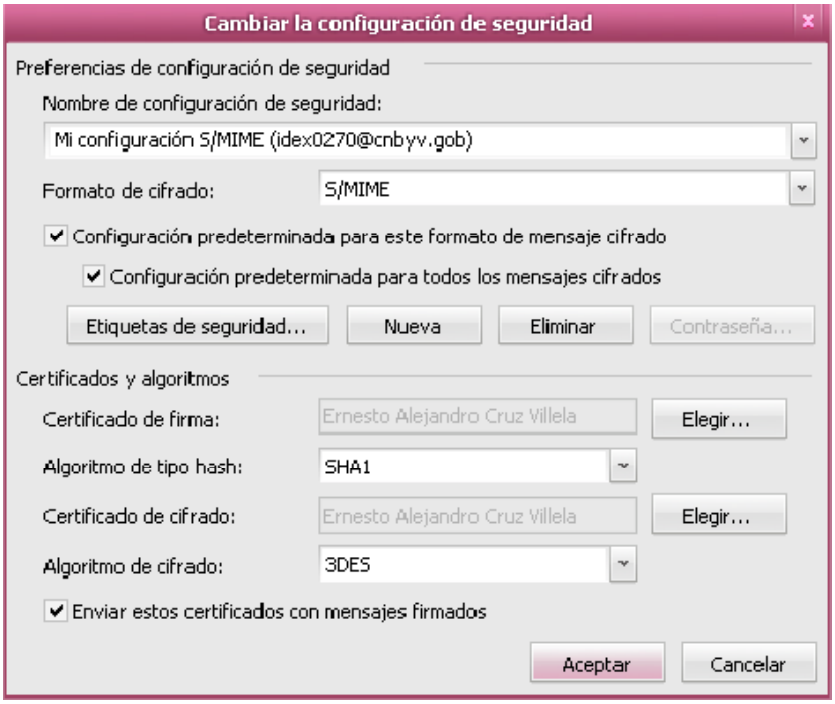

Figura 44. Cambiar la configuración de seguridad.

- Para las preferencias de configuración de seguridad se elige lo siguiente:
  - Nombre de configuración de seguridad: optar por mi configuración S/MIME que viene con el correo electrónico del usuario.
  - En formato de cifrado: elegir S/MIME.
  - Activar las casillas de configuración predeterminada para este formato de mensaje cifrado y para todos los mensajes cifrados, con estas dos opciones, permite cifrar siempre todos los mensajes con S/MIME.

- Ahora en la parte de certificados y algoritmos damos clic en elegir certificado de firma, esto es para escoger el certificado que se creó y del cual se hace uso para firmar los mensajes de correo electrónico, en la ventana seleccionar certificado damos clic en el certificado personal y a continuación aceptar. Se hace lo mismo para certificado de cifrado, estopara hacer solo del certificado creado y cifrar los mensajes de correo electrónico.

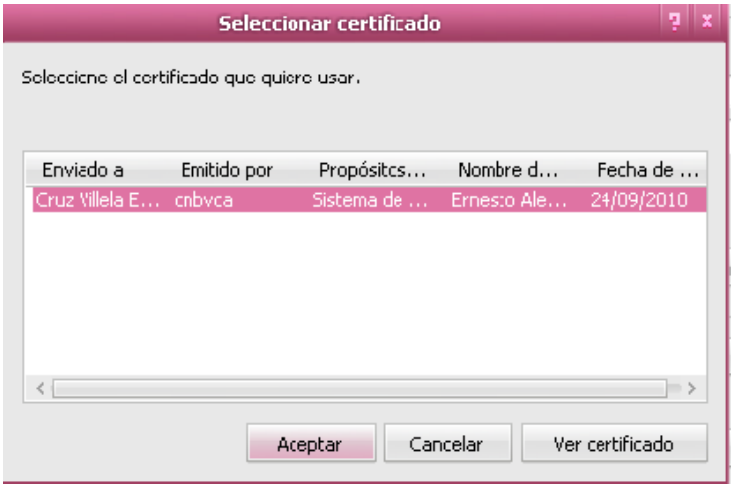

Figura 45. Seleccionar el certificado personal para firmar y cifrar.

- En el algoritmo de tipo hash para el certificado de firma, se da clic en el algoritmo SHA – 1.
- Para el algoritmo de cifrado, se da clic en 3DES, para el certificado de cifrado.
- Posteriormente activamos la casilla, enviar estos certificados con mensajes firmados, esto sirve para que cuando se manden mensajes firmados se envíe con ellos la llave pública del usuario, a continuación, clic en aceptar.
- Finalmente en la ventana Centro de confianza dar clic en aceptar.

Con los pasos anteriores se da por terminada la configuración Outlook 2007, ahora es posible cifrar y firmar digitalmente correos electrónicos en la CNBV.

4.6 EXPORTACIÓN E IMPORTACIÓN DE UN CERTIFICADO DIGITAL PARA FIRMAR Y CIFRAR CORREO VÍA WEB DESDE OUTLOOK WEB ACCESS.

La exportación e importación de un certificado digital en la CNBV, es muy importante, porque con el certificado creado en la estación de trabajo lo puedo exportar para posteriormente importarlo en alguna otra máquina, como puede ser en el hogar del empleado, y utilizar ese certificado para firmar y cifrar correo electrónico vía Web a través de OWA.

El usuario puede acceder a través e la página del portal de la CNBV que es http://www.cnbv.gob.mx y dar clic en parte inferior izquierda donde dice, E-MAIL CNBV.

4.6.1 Exportar un certificado digital

Para exportar un certificado digital se realiza lo siguiente:

- Ir a inicio de Windows y dar clic en ejecutar y escribir, “certmgr.msc”, en la ventana certificados, dar clic secundario en el certificado personal, a continuación, en todas las tareas, elegir exportar.

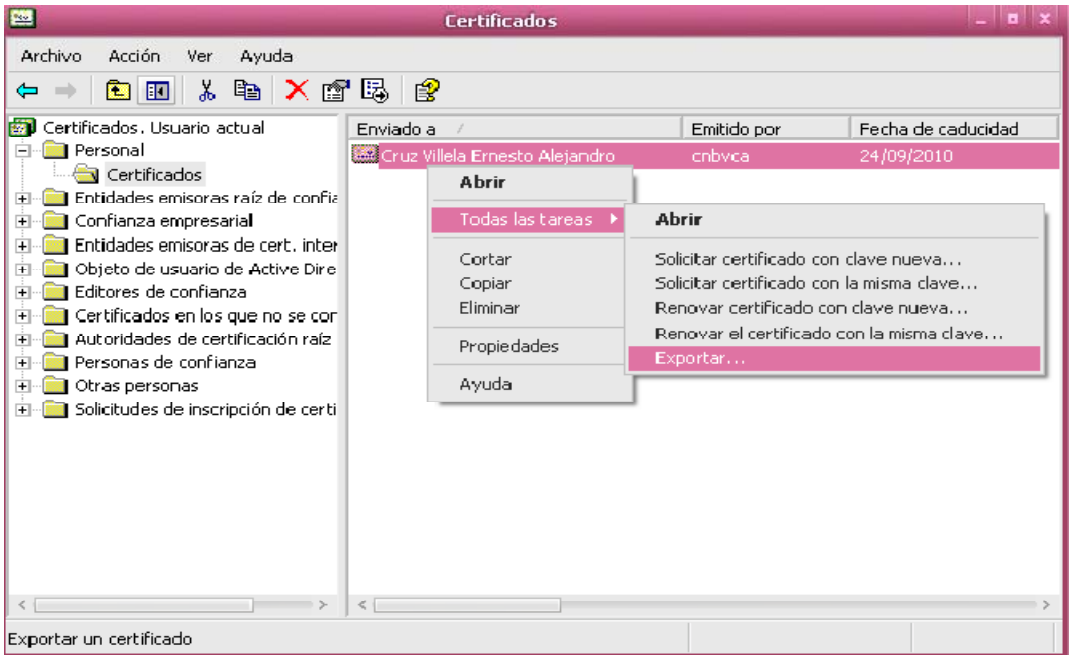

Figura 46. Exportar certificado digital.

- En la ventana del asistente de exportación de certificados, dar clic en siguiente, elegimos exportar la llave privada, para poder cifrar mensajes, a continuación, clic en siguiente.

Figura 47. Asistente para exportación de certificados.

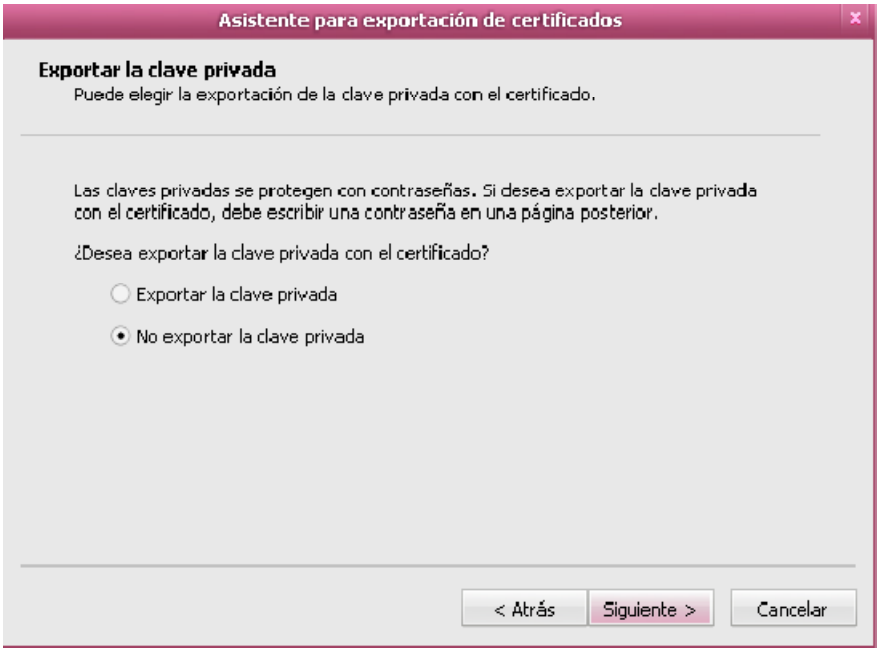

Figura 48. Exportar la llave privada.

- En la ventana formato de archivo de exportación, elegir intercambio de información personal y activar la casilla, permitir protección segura, a continuación dar clic en siguiente.

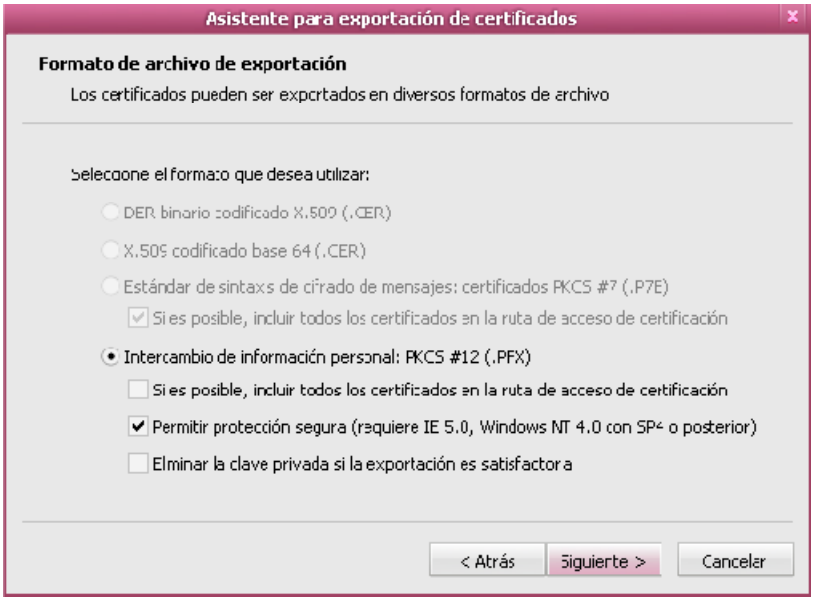

Figura 49. Formato de archivo de exportación.

- La llave privada se debe de proteger con una contraseña para mantenerla segura, elegimos una, se confirma y clic en siguiente.

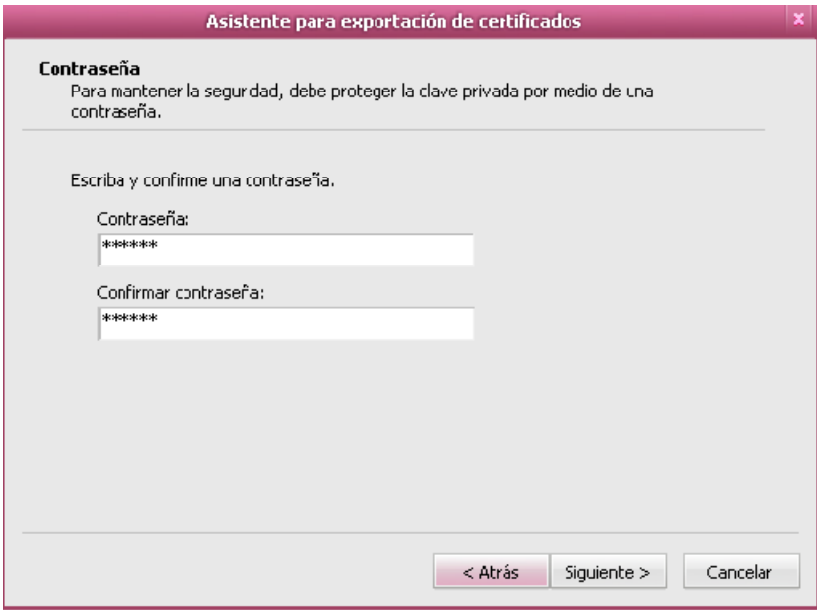

Figura 50. Contraseña para la llave privada.

- Posteriormente se especifica el nombre del archivo que se desea exportar en este caso el certificado y la ruta donde se guardará, se crea un archivo con la extensión **“.pfx”,** elegir un nombre y dar clic en guardar, puede guardarse en una memoria USB, por ejemplo, a continuación dar clic en siguiente.

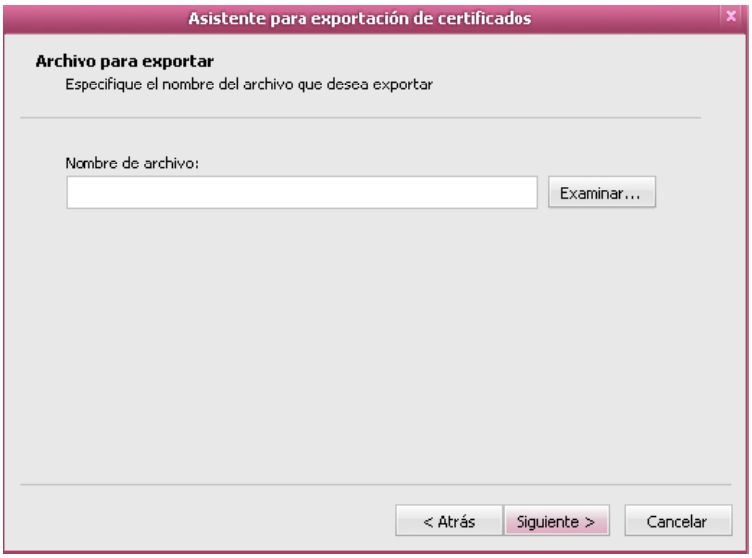

Figura 51. Archivo para exportar.

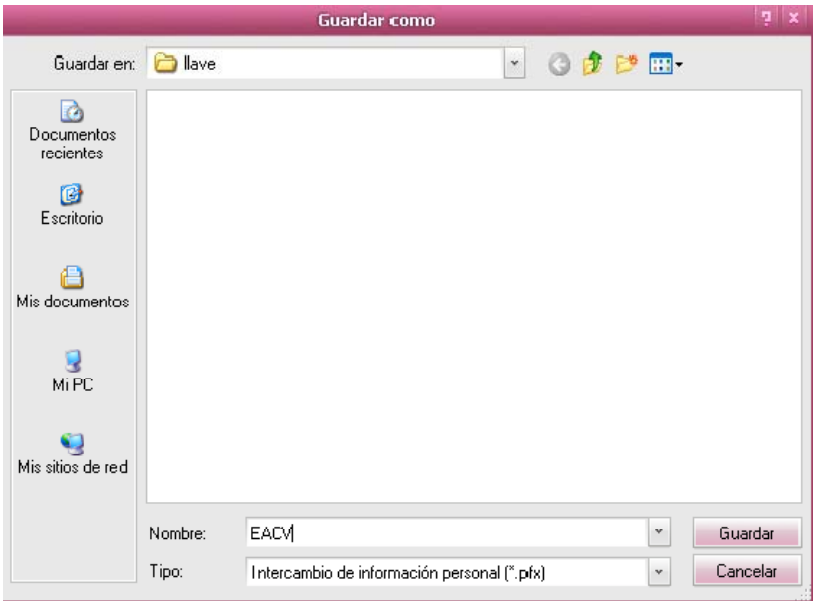

Figura 52. Guardar certificado digital.

- Finaliza el asiste para la exportación de certificados, nos da un informe, se verifica que los datos sean correctos y se da clic en finalizar. Antes de terminar nos aparece una ventana para ingresar la clave para el intercambio de llaves RSA, que se creó en el proceso de obtención de certificados, finalmente dar clic en aceptar.

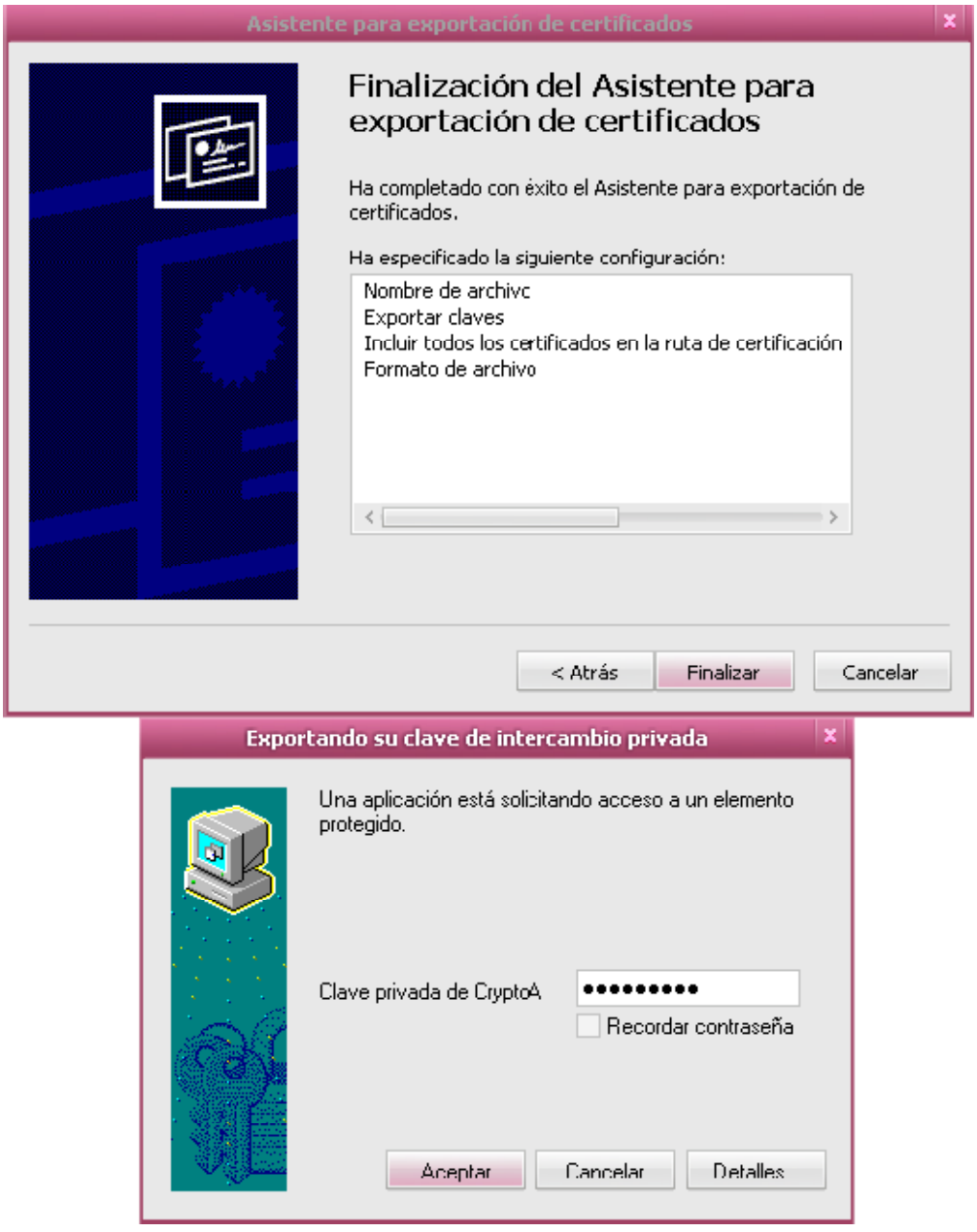

Figura 53. Clave para finalizar la exportación.

- Aparece una venta confirmando, que la exportación del certificado se realizó con éxito.

Figura 54. Confirmación de exportación terminada.

Ya exportado el certificado, ahora es posible importarlo en cualquier computadora para poder hacer uso de él, y así poder firmar y cifrar correo electrónico a través de Outlook Web Access, en cualquier parte del mundo vía Web.

4.6.2 Importar un certificado digital

Un certificado importado en un equipo local diferente a la estación de trabajo, permite firmar digitalmente y cifrar un mensaje de correo electrónico vía Web, la importación se lleva a cabo de la siguiente manera:

- Se ubica el archivo con extensión ".pfx", que se guardó con anterioridad al exportar el certificado, se da doble clic sobre el archivo.

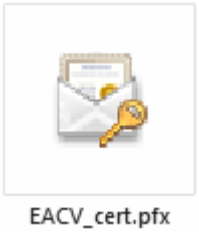

Figura 55. Archivo de certificado digital.

- Aparece un asistente para importación de certificados, dar clic en siguiente.

Figura 56. Asistente para importación de certificados.

- En el asistente se especifica el archivo que se desea importar, aparece la ruta donde tenemos nuestro certificado, que es para el intercambio de información personal, clic en siguiente.

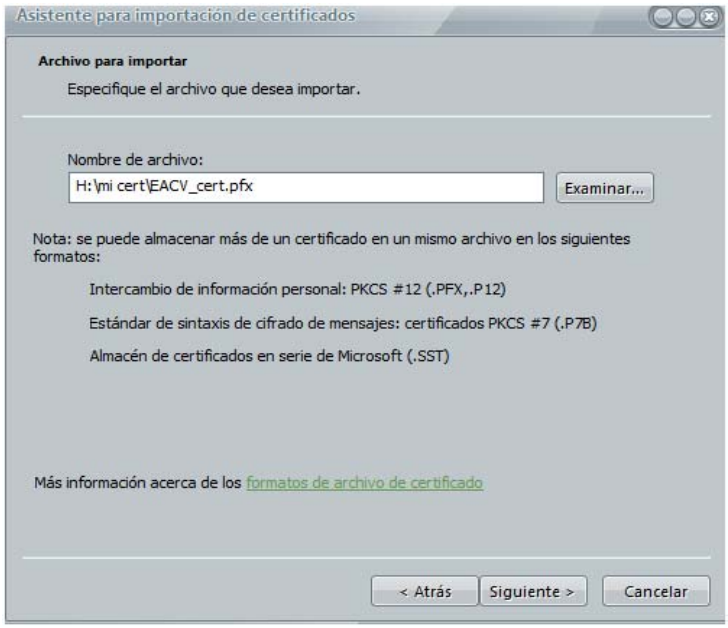

Figura 57. Certificado a importar.

- Ahora se escribe la contraseña de protección de la llave privada, esta es la que se escribió al exportar el certificado, se habilitan todos las casillas, a continuación, clic en siguiente.

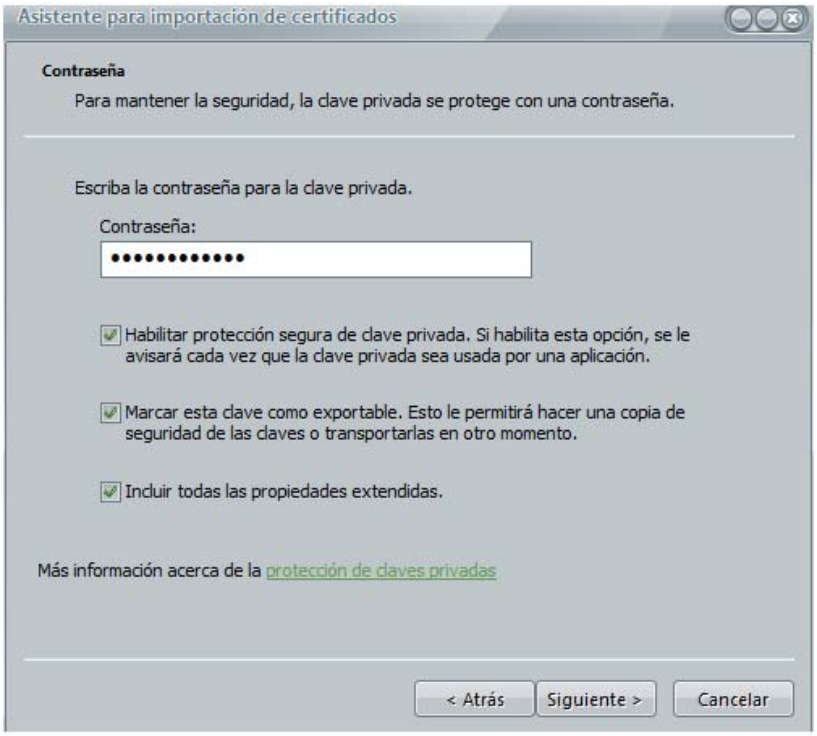

Figura 58. Contraseña para la llave privada.

- En almacén de certificados, se da la ubicación donde se guardan los certificados, seleccionar automáticamente el almacén de certificados en base al tipo de certificado, a continuación, clic en siguiente.

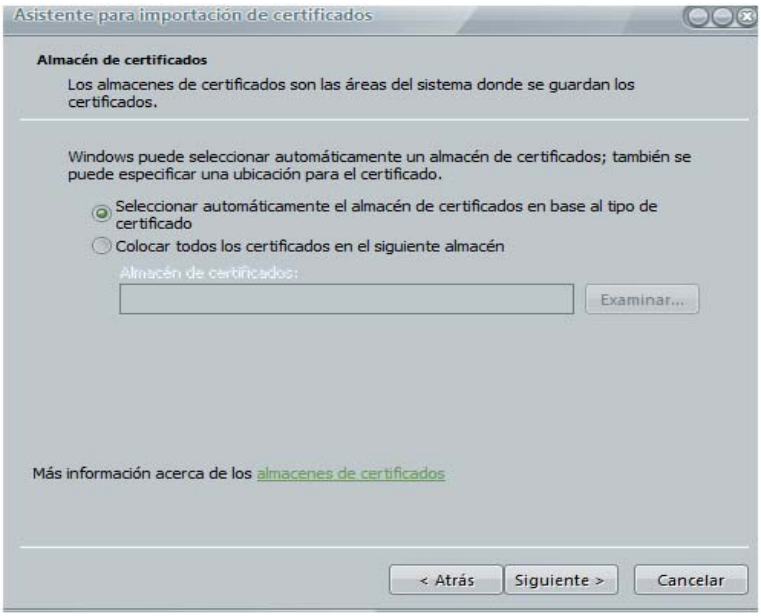

Figura 59. Almacén de certificados.

- Se confirman que los datos sean correctos y se da clic en finalizar el asistente.

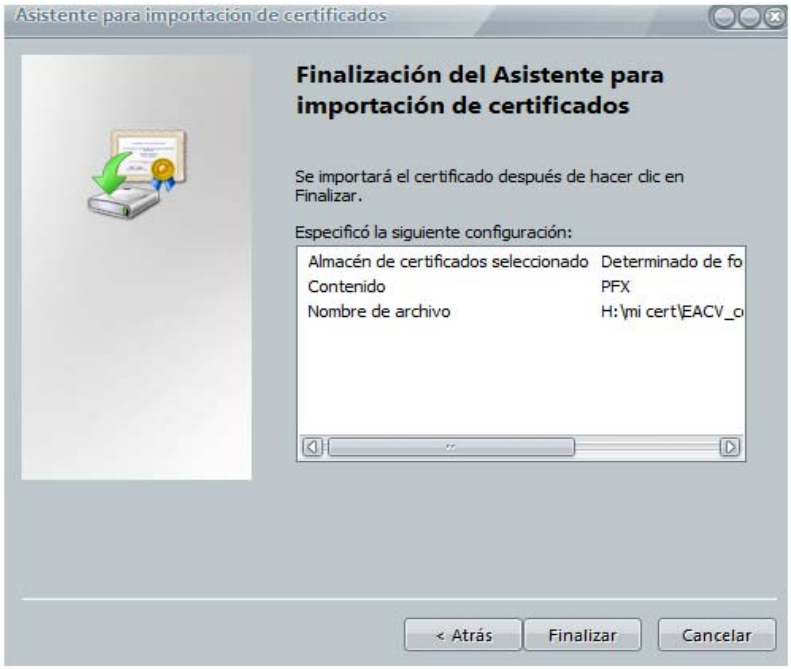

Figura 60. Finalización del asistente de importación de certificados.

- A continuación, en la ventana importando una nueva clave de intercambio, dar clic en nivel de seguridad y elegir nivel alto de seguridad, a continuación, clic en siguiente.

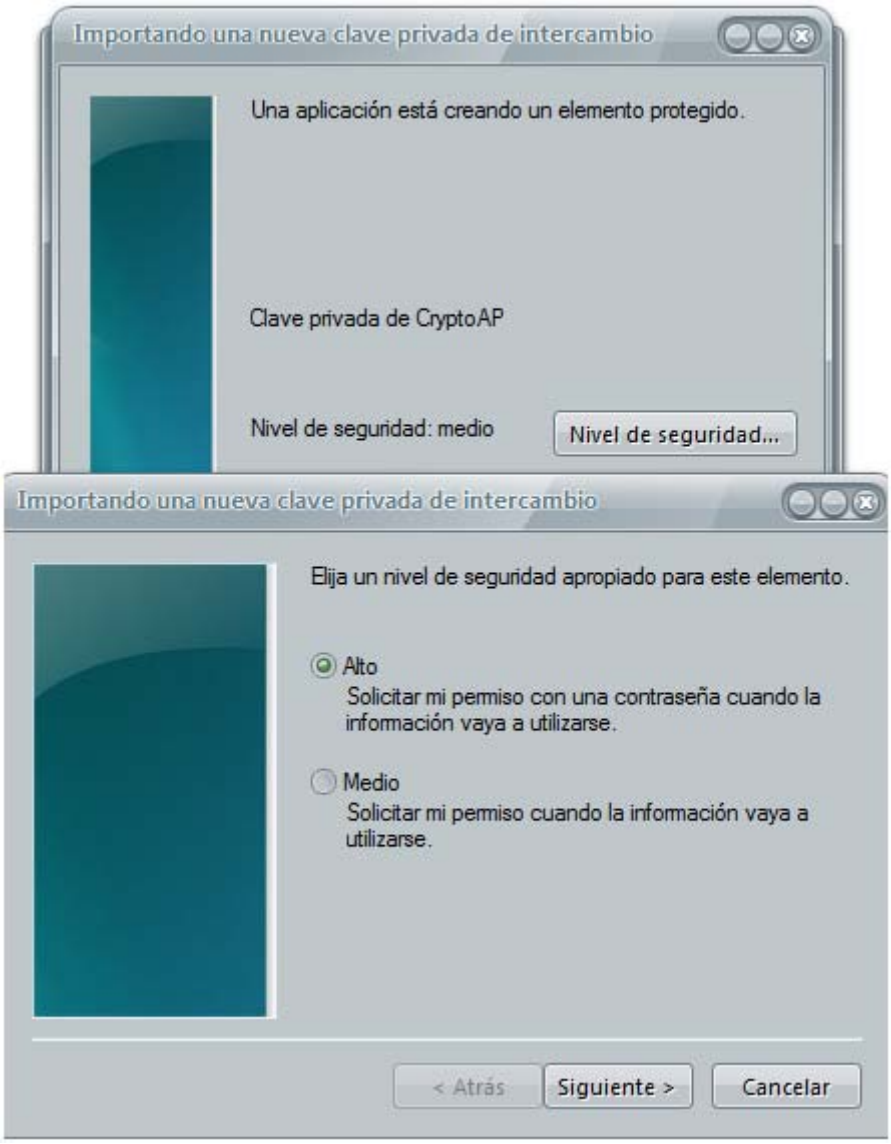

Figura 61. Nivel de seguridad de la llave privada.

- En la ventana siguiente elegimos una contraseña para la llave privada, la confirmamos, dar clic en finalizar y posteriormente clic en aceptar.

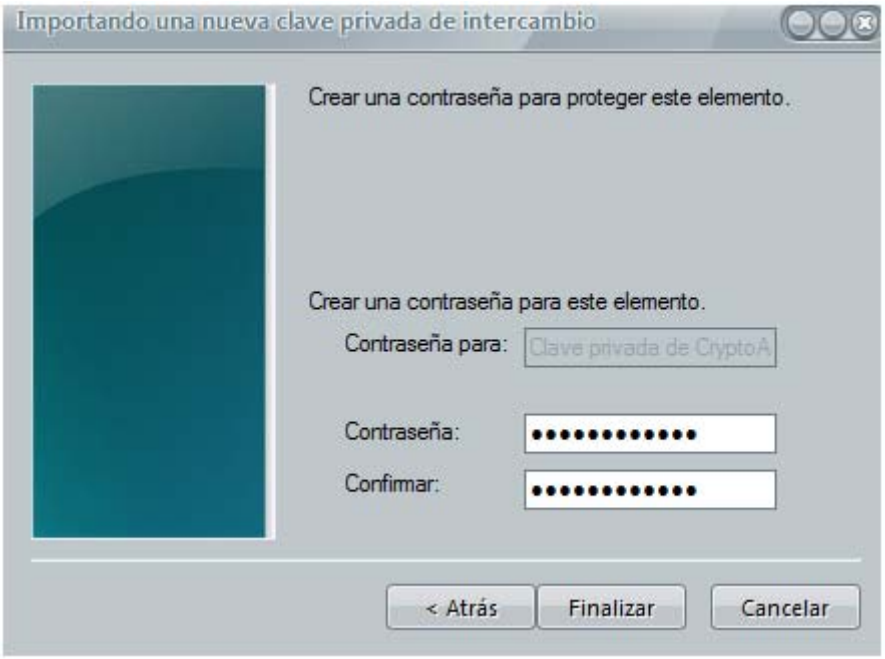

Figura 62. Contraseña para el uso de la llave privada.

- Para terminar aparece una confirmación de que el certificado se importo con éxito, dar clic en aceptar para finalizar el asistente.

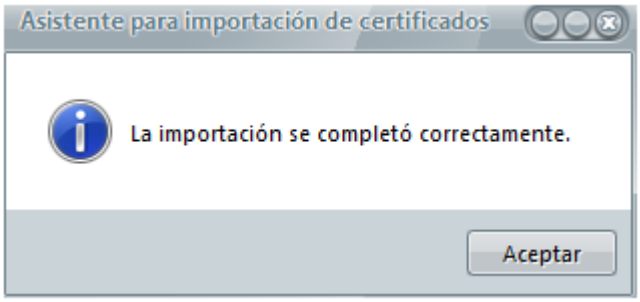

Figura 63. Confirmación de la importación terminada.

Ahora se hace posible la utilización del certificado digital personal fuera del área de trabajo, y con él poder firma y cifrar correo electrónico vía web desde Outlook Web Access.

4.7 PROCESO DE FIRMA Y CIFRADO EN OUTLOOK WEB ACCESS

Para firma un correo electrónico vía Web es necesario, tener una conexión a internet, ingresar a la página Web, https://mail.cnbv.gob.mx, o desde el portal de internet de la Comisión Nacional Bancaria y de Valores, www.cnbv.gob.mx, en la parte inferior izquierda dar clic en E – MAIL EMPLEADOS.

En la página de Outlook Web Access, ingresar usuario y contraseña, estos son con los que se entra normalmente al dominio en el lugar de trabajo.

Una vez ingresado, se tiene acceso al correo electrónico personal de cada empleado.

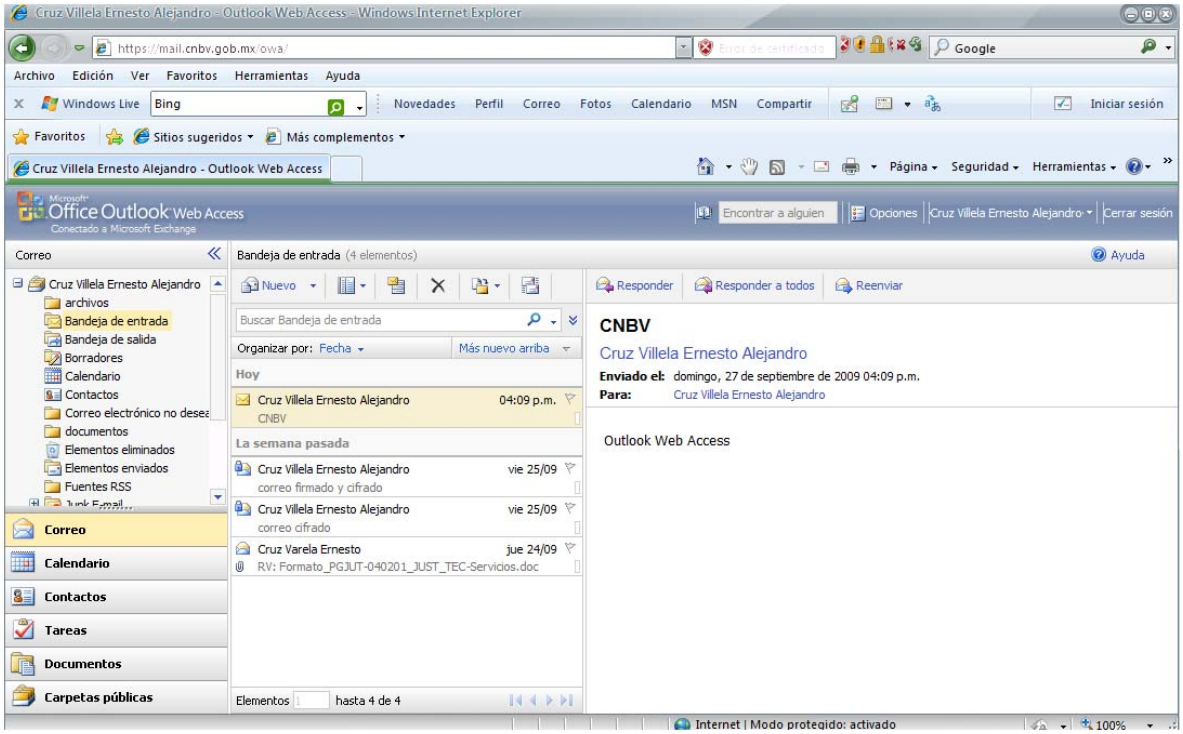

Figura 64. Outlook Web Access.

Outlook Web Access, necesita instalar un complemento de S/MIME para poder firmar y cifrar el correo electrónico, para ello se realiza lo siguiente:

- En la página principal de OWA, en la parte superior derecha hacer clic en opciones, para comenzar la configuración, en el menú de la parte izquierda dar clic en la plantilla seguridad en correo del correo electrónico, y a continuación, clic en descargue el control S/MIME de Outlook Web Access, en la ventana siguiente dar clic en ejecutar.

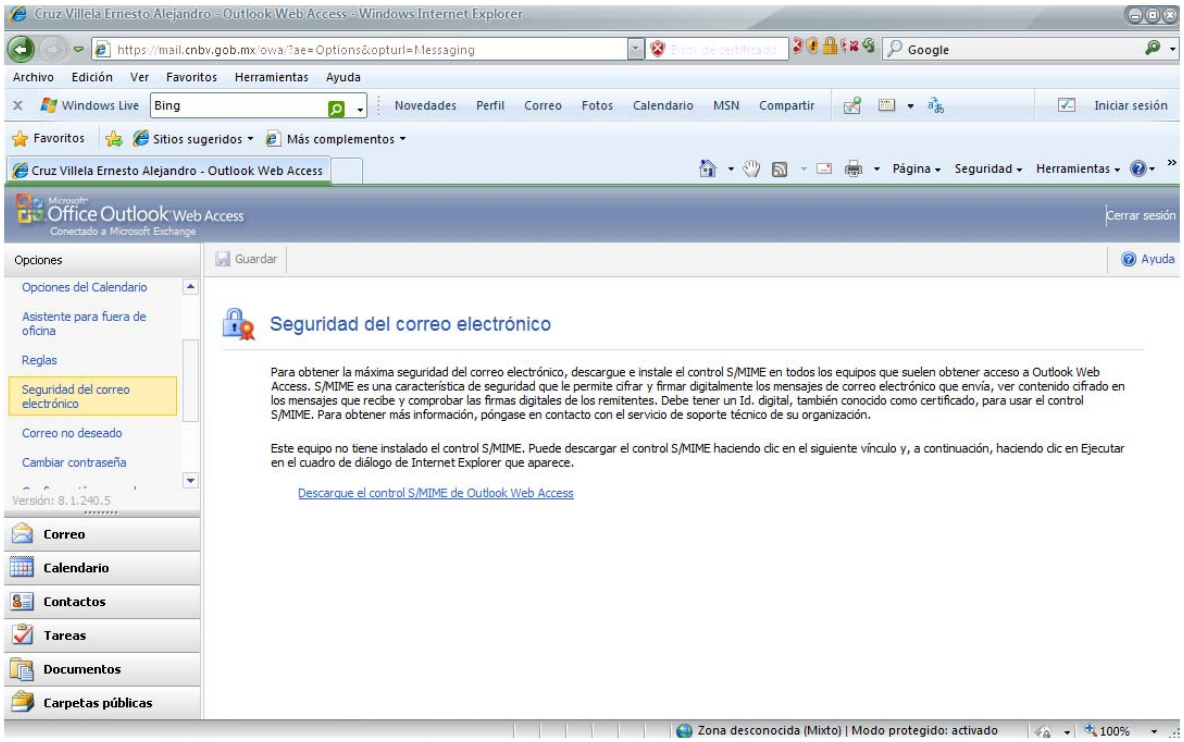

Figura 65. Seguridad del correo electrónico de OWA.

- Una vez instalado, en la página web de OWA, sale un aviso emergente, solicitando que el sitio web necesita ejecutar el complemento MIME, dar clic en ejecutar complemento, a continuación, ejecutar.

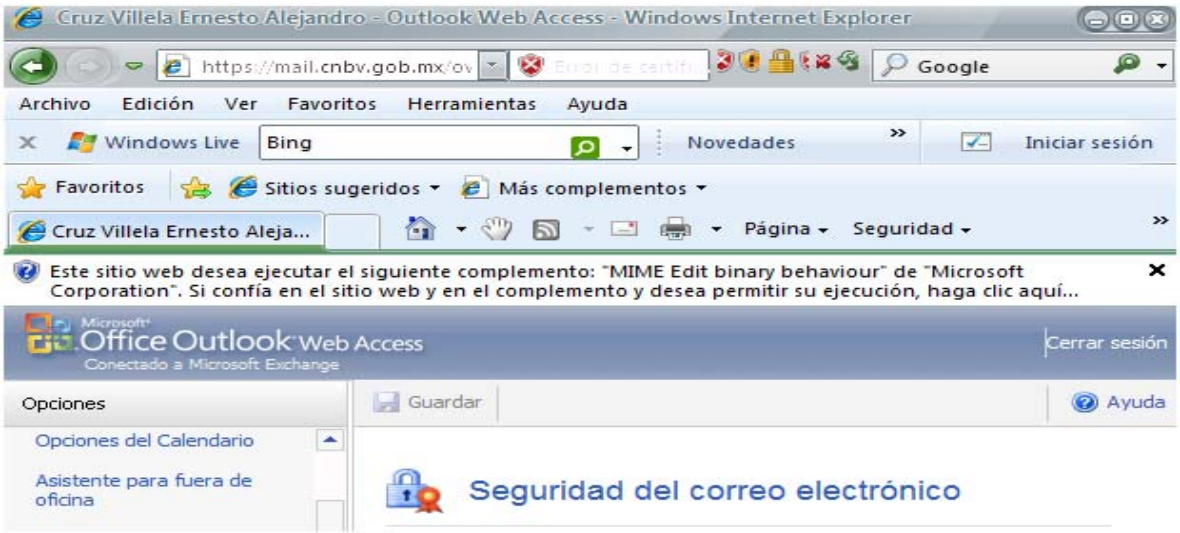

Figura 66. Ejecutar control MIME en OWA.

- Para firmar y cifrar correo electrónico en OWA, dirigirse a seguridad del correo electrónico y activar las casillas:

    - Cifrar el contenido y los datos adjuntos de todos los mensajes salientes.
    - Agregar una firma digital a todos los mensajes salientes.

- Finalmente dar clic en guardar.

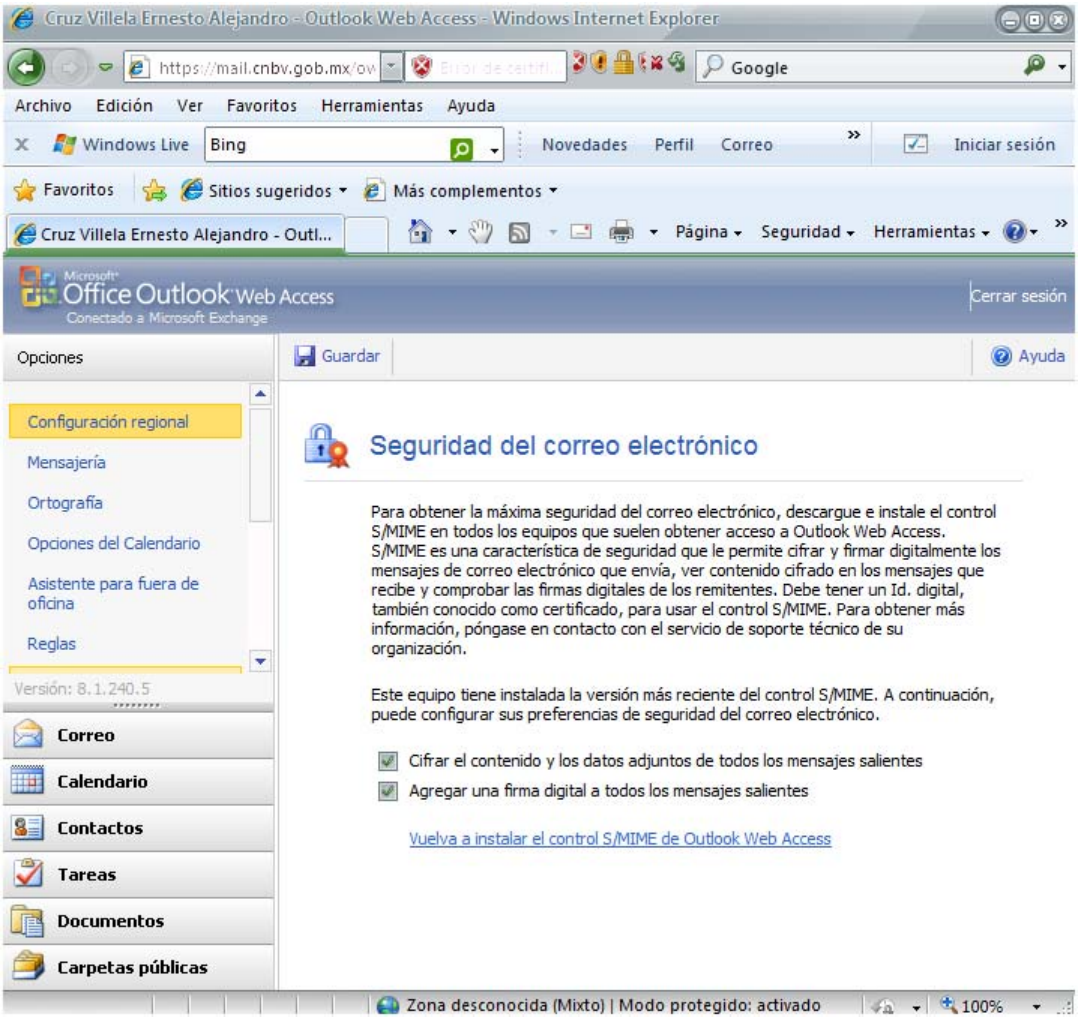

Figura 67. Activar firmar y cifrar mensajes en OWA.

Con esta configuración es posible ahora firmar y cifrar el correo electrónico, para los empleados de la CNBV, que estén fuera de su lugar de trabajo, cabe destacar que el usuario puede activar y desactivar los botones de firma y cifrado, al enviar el mensaje, dependiendo las necesidades del usuario.

4.7.1 Firmar un correo electrónico

Para firmar un correo electrónico dentro de OWA, se hace lo siguiente:

- En la página principal de correo electrónico de OWA, dar clic en nuevo, en la ventana del nuevo mensaje, poner el destinatario a quien se le vaya a enviar el mensaje, a continuación, en asunto poner por ejemplo: correo firmado y en el cuerpo del mensaje: Este es un correo firmado mediante OWA, por poner un ejemplo, a continuación en la parte superior dar clic en el icono , para agregar una firma digital a este mensaje y a continuación, clic en enviar. Automáticamente el correo se firma con el certificado digital personal que se importó.

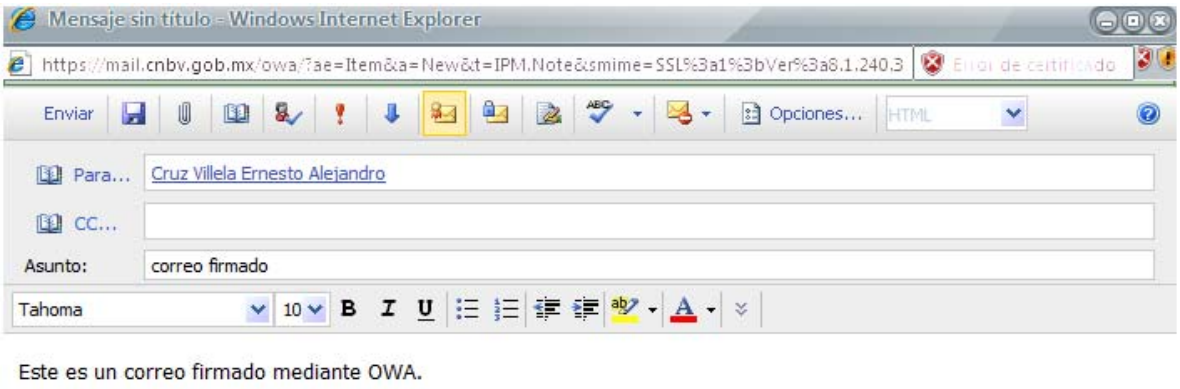

Figura 68. Firmar correo electrónico en OWA.

Cuando se recibe un correo electrónico firmado, aparece el ícono de firma digital, para poder comprobar que la firma es auténtica, en el ícono dar clic, para saber si la firma digital es válida y de confianza.

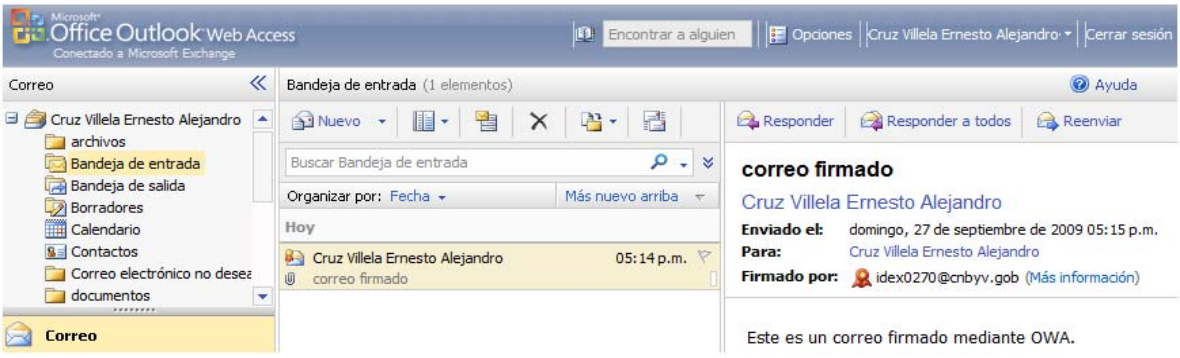

Figura 69. Comprobación de la firma digital en OWA.

- La información que arroja al dar clic en el ícono de firma es, el nombre de usuario, por quien fue firmado y que autoridad certificadora emitió el certificado, si son correctos esos datos, se toma la firma como válida, finalmente, dar clic en aceptar.

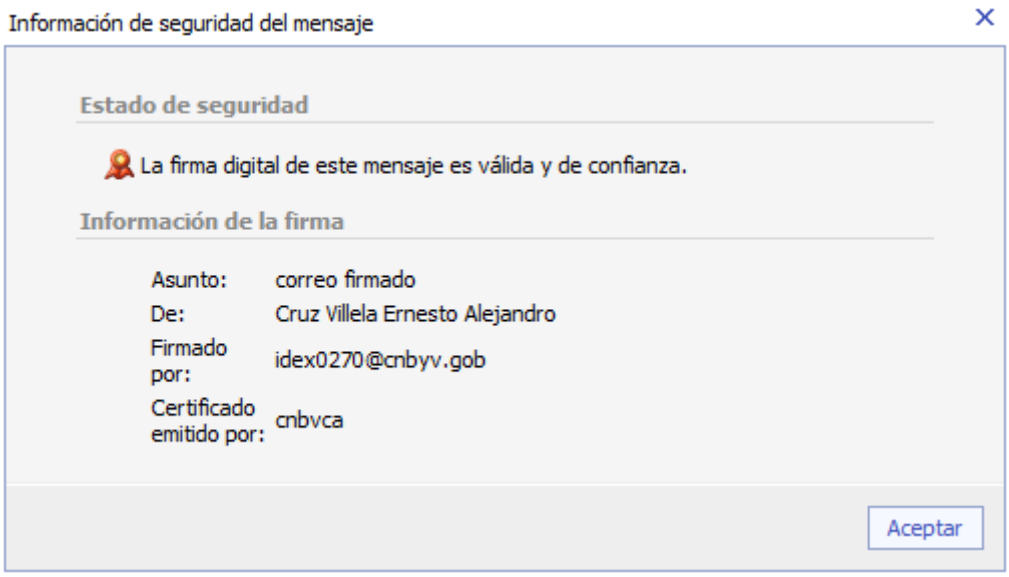

Figura 70. Validación de la firma.

Se da por terminado el proceso de firma digital de un mensaje de correo electrónico por medio de Outlook Web Access.

4.7.2 Cifrar un correo electrónico

Para cifrar un correo electrónico mediante OWA, se realiza lo siguiente:

- En la página principal de correo electrónico de OWA, dar clic en nuevo, en la ventana del nuevo mensaje, poner el destinatario a quien se le vaya a enviar el mensaje, a continuación, en asunto poner por ejemplo: correo cifrado y en el cuerpo del mensaje: Este es un correo cifrado mediante OWA, por poner un ejemplo, a continuación en la parte superior dar clic en el ícono , para cifrar este mensaje y a continuación, clic en enviar. Automáticamente el correo se cifra con el certificado digital personal que se importó.

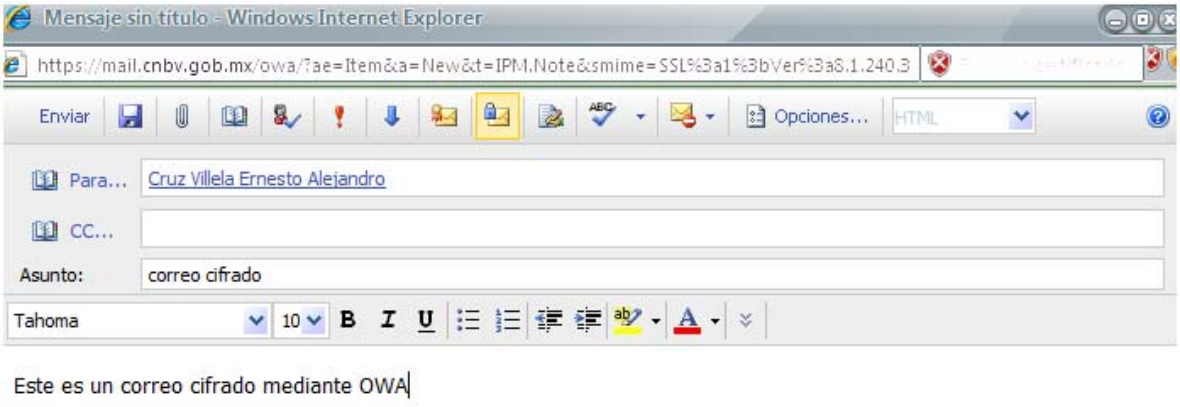

Figura 71. Cifrar correo electrónico en OWA.

Cuando se recibe un correo electrónico cifrado, aparece un mensaje que avisa que el mensaje está cifrado, para descifrarlos solo se da doble clic sobre el mensaje y aparece en claro.

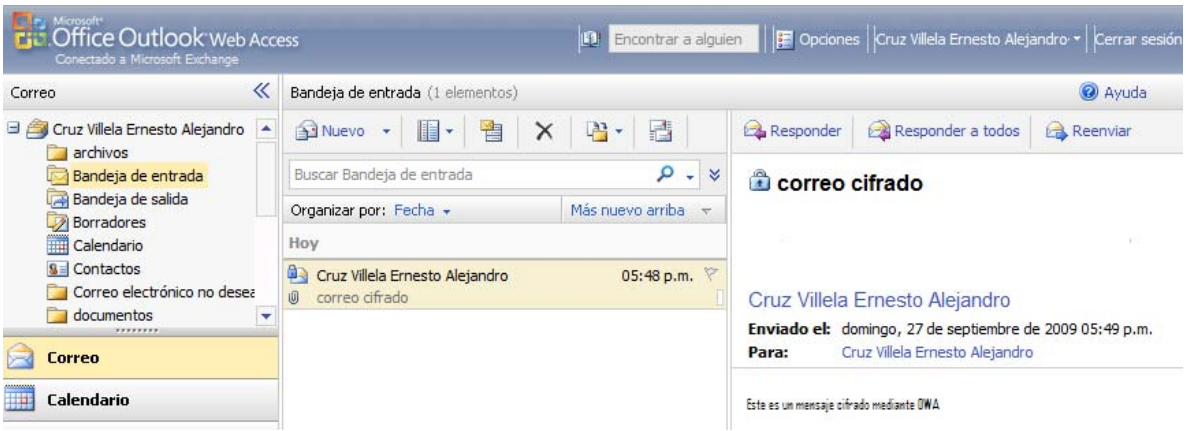

Figura 72. Mensaje cifrado en OWA.

El cifrado de un mensaje de correo electrónico proporciona al propietario del certificado personal la certeza de que únicamente el destinatario podrá abrir y leer dicho mensaje; sin embargo solo se debe utilizar cuando estemos seguros de que el destinatario posea su propio certificado personal.

4.8 PROCESO DE FIRMA Y CIFRADO EN OUTLOOK

La firma de un mensaje de correo electrónico proporciona al destinatario la certeza de que tal mensaje lo ha enviado el propietario del certificado personal y que no ha sido alterado. Para firmar un mensaje de correo electrónico en Outlook, se realiza lo siguiente:

- En el menú herramientas, hacer clic en centro de confianza y a continuación en Seguridad de correo electrónico.

- Activar la casilla, agregar firma digital a los mensajes salientes, a continuación, clic en aceptar.

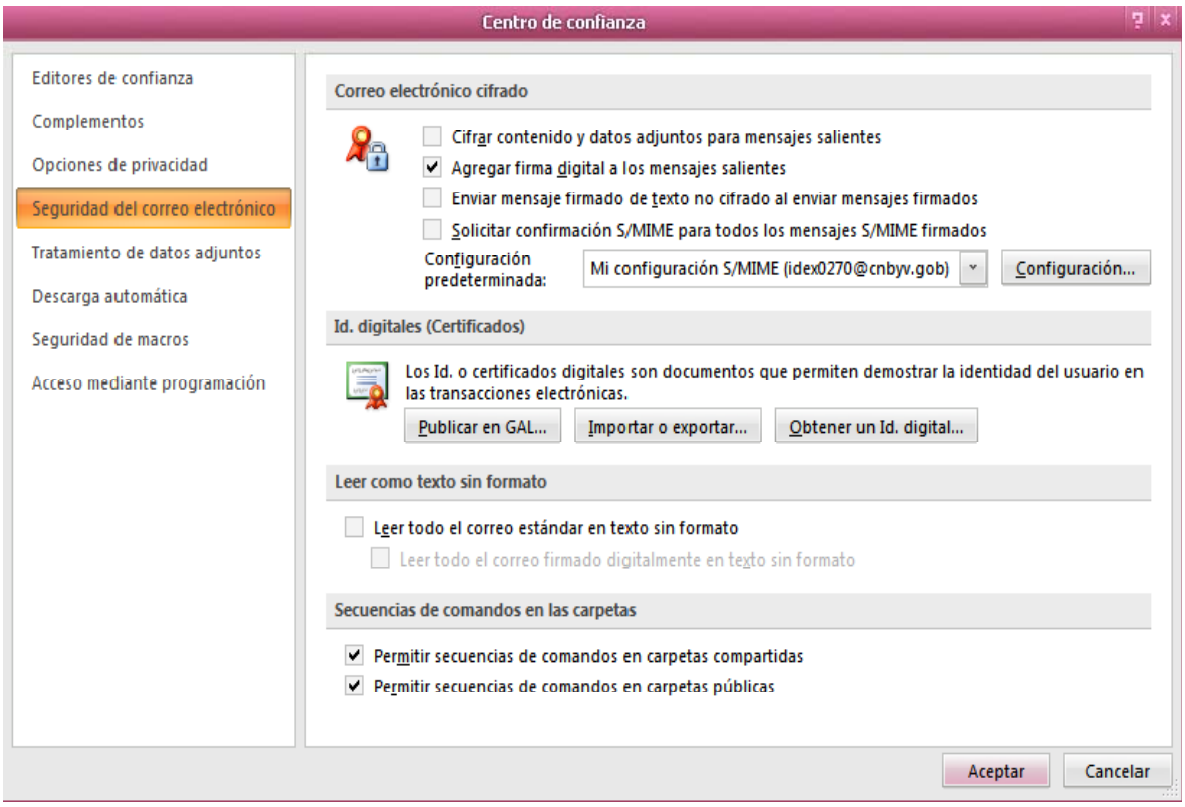

Figura 73. Agregar firma digital a los mensajes.

- Si se desea que los destinatarios que no cuentan con seguridad de correo electrónico S/MIME puedan leer los mensajes, activar la casilla, enviar mensaje firmado de texto no cifrado al enviar mensajes firmados.

- Cuando se quiere comprobar que los destinatarios validan la firma digital y solicitar la confirmación de que el mensaje se ha recibido sin modificaciones además de enviar una notificación con información de

que usuario ha abierto el mensaje y a qué hora lo hizo, activar la casilla, solicitar confirmación S/MIME para todos los mensajes S/MIME firmados.

- Elegir las opciones necesarias y dar clic en aceptar.

4.8.1 Firmar un correo electrónico

Con la configuración anterior automáticamente todos los mensajes que se envíen tendrán una firma digital, el proceso de firma digital a un mensaje de correo electrónico es el siguiente:

- En la página principal de correo electrónico de Outlook, dar clic en nuevo, en la ventana del nuevo mensaje, poner el destinatario a quien se le vaya a enviar el mensaje, a continuación, en asunto poner por ejemplo: correo firmado y en el cuerpo del mensaje: Este es un correo firmado con Outlook, por poner un ejemplo, a continuación en la parte superior dar clic en el icono , para agregar una firma digital a este mensaje y a continuación, clic en enviar. Automáticamente el correo se firma con el certificado digital personal.

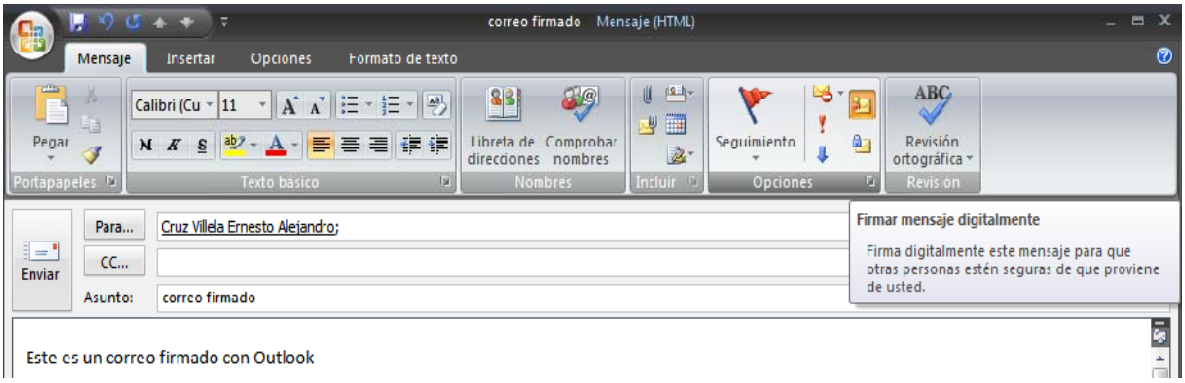

Figura 74. Firmar correo electrónico en Outlook.

Cuando se recibe un correo electrónico firmado en la bandeja de entrada al abrir un mensaje, si se activo la casilla de solicitar confirmación, pregunta al destinatario si desea enviar una confirmación, dar clic en sí, de lo contrario no se enviará ninguna confirmación. Si no se activo esa casilla no aparecerá esa confirmación.

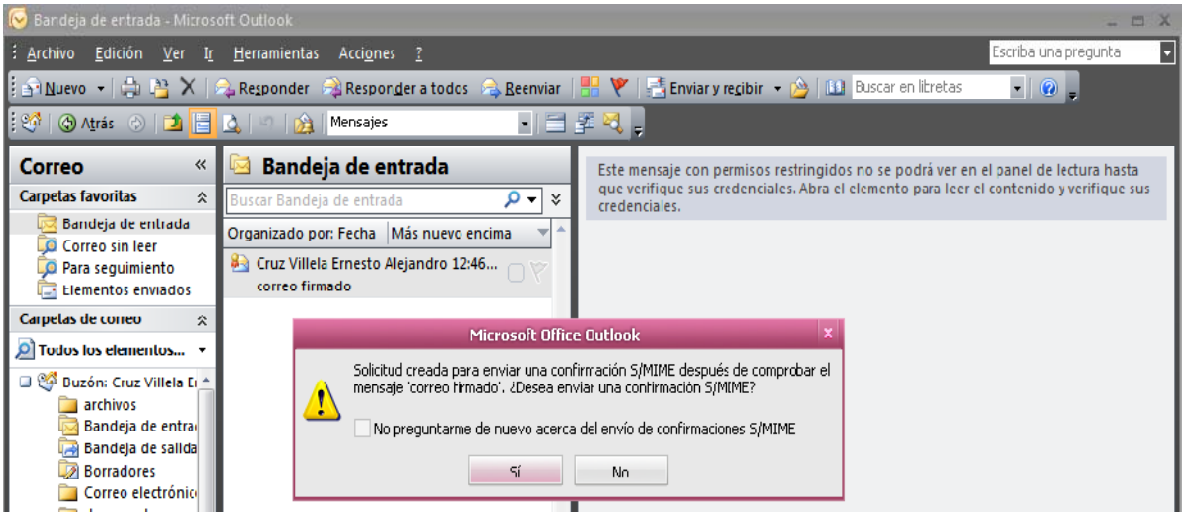

Figura 75. Solicitud de confirmación S/MIME.

En la bandeja de entrada aparece otro mensaje que es la confirmación de que el mensaje fue entregado y a la hora que se abrió.

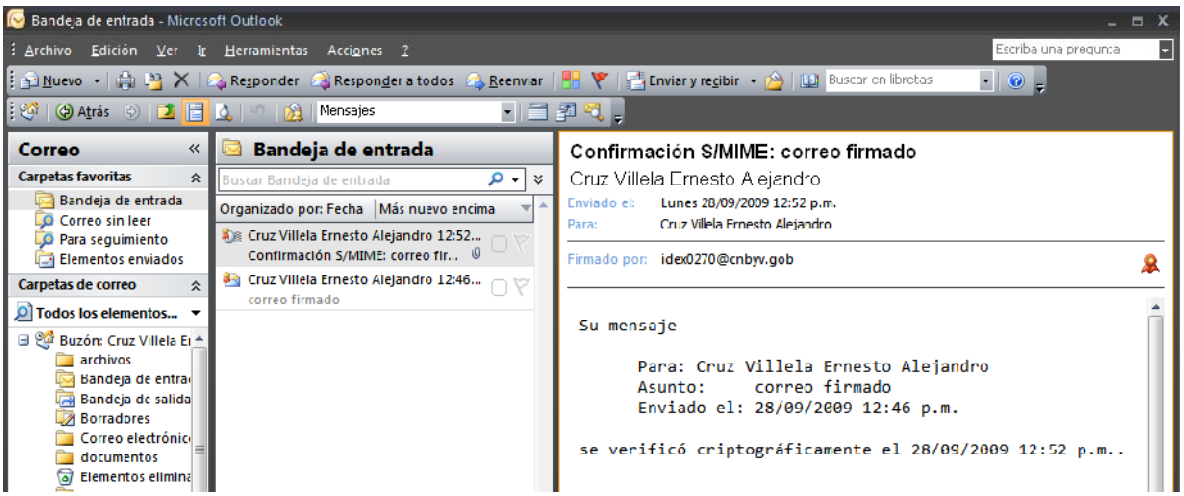

Figura 76. Información de la solicitud de mensaje firmado.

Comprobar la firma digital de un mensaje es necesario para saber si ésta es válida y confiar en el emisor del mensaje, para hacerlo abrimos el mensaje que se encuentra en la bandeja de entrada de Outlook, a continuación, dar clic en el ícono de firma digital , que se ubica en la parte superior derecha del mensaje.

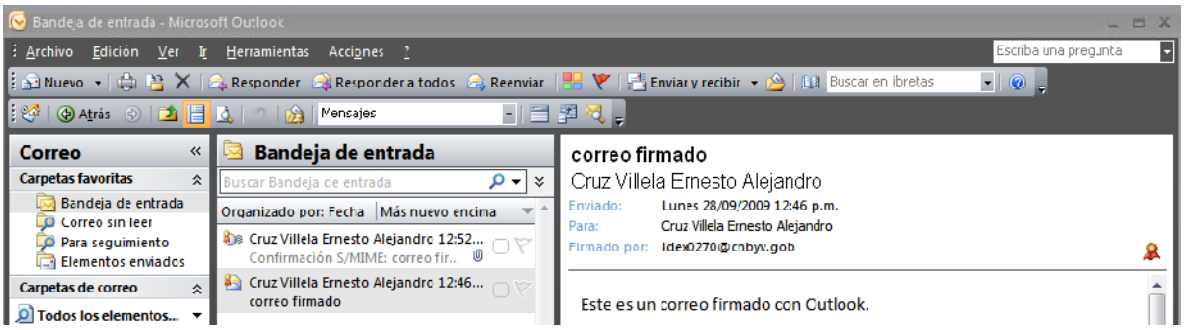

Figura 77. Comprobación de una firma digital en Outlook.

- Al dar clic en el ícono de firma digital, sale una venta con información sobre la firma digital, y si es válida o no. Nos indica el asunto del correo, quien lo emitió y firmó. Si se desea obtener más información acerca del certificado utilizado para firmar el mensaje, dar clic en detalles.

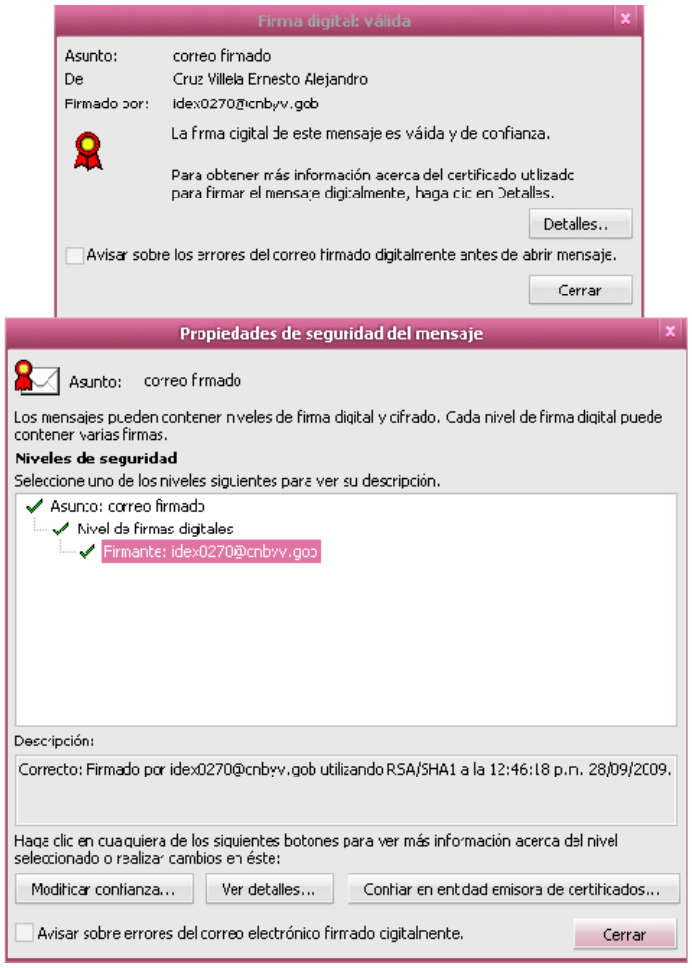

Figura 78. Validación de la firma digital.

- Al dar clic en firmante, se habilita la opción ver detalles, dar clic sobre ese botón y se mostrarán los detalles de la firma digital con los datos del firmante, incluso se puede observar el certificado.

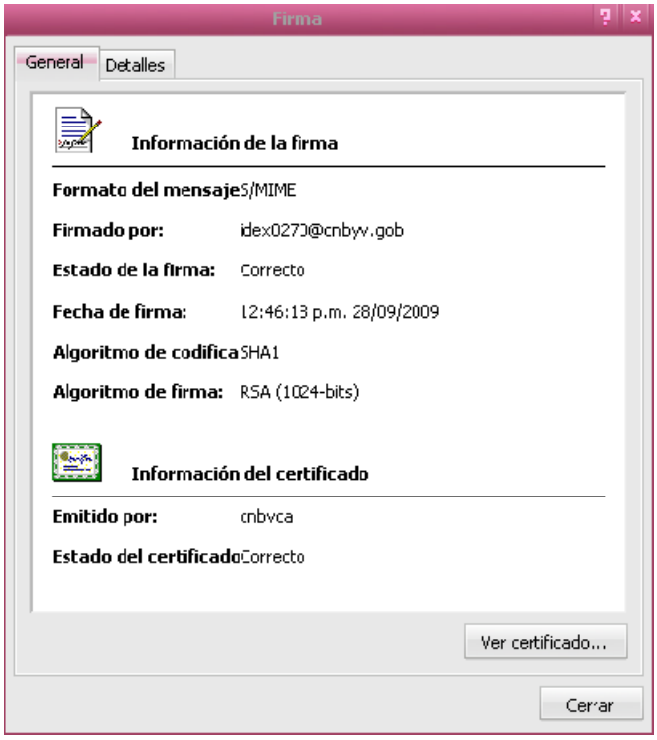

Figura 79. Propiedades de la firma.

4.8.2 Cifrar un correo electrónico

Para cifrar un correo electrónico en Outlook, se realiza lo siguiente:

- En la página principal de correo electrónico de Outlook, dar clic en nuevo, en la ventana del nuevo mensaje, poner el destinatario a quien se le vaya a enviar el mensaje, a continuación, en asunto poner por ejemplo: correo cifrado y en el cuerpo del mensaje: Este es un correo cifrado con Outlook, por poner un ejemplo, a continuación en la parte superior dar clic en el ícono , para cifrar este mensaje y a continuación, clic en enviar.

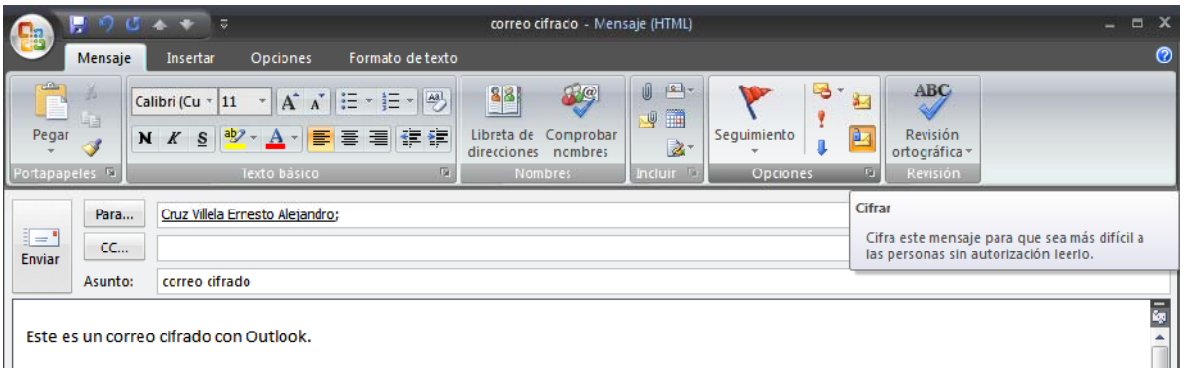

Figura 80. Cifrar correo electrónico en Outlook.

Cuando se recibe un correo electrónico cifrado, aparece un mensaje que avisa que el mensaje está cifrado, para descifrarlos solo se da doble clic sobre el mensaje y aparece en claro, de lo contrario en el panel de lectura no se podrá ver.

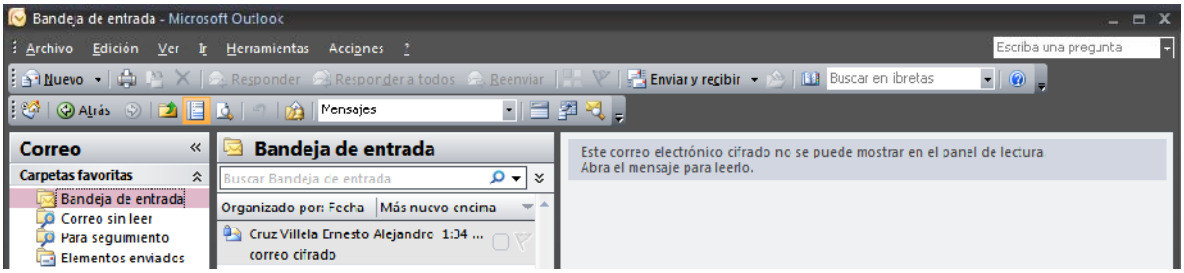

Figura 81. Mensaje cifrado en Outlook.

- Para verificar que el mensaje cifrado del mensaje es correcto, dar doble clic en el mensaje que se encuentra en la bandeja de entrada, al abrir el mensaje dar clic en el ícono de seguridad del correo electrónico .

- En la ventana propiedades de la seguridad del mensaje, dar clic en nivel de cifrado y a continuación ver detalles, donde aparecen los detalles del cifrado, incluso se puede ver el certificado.

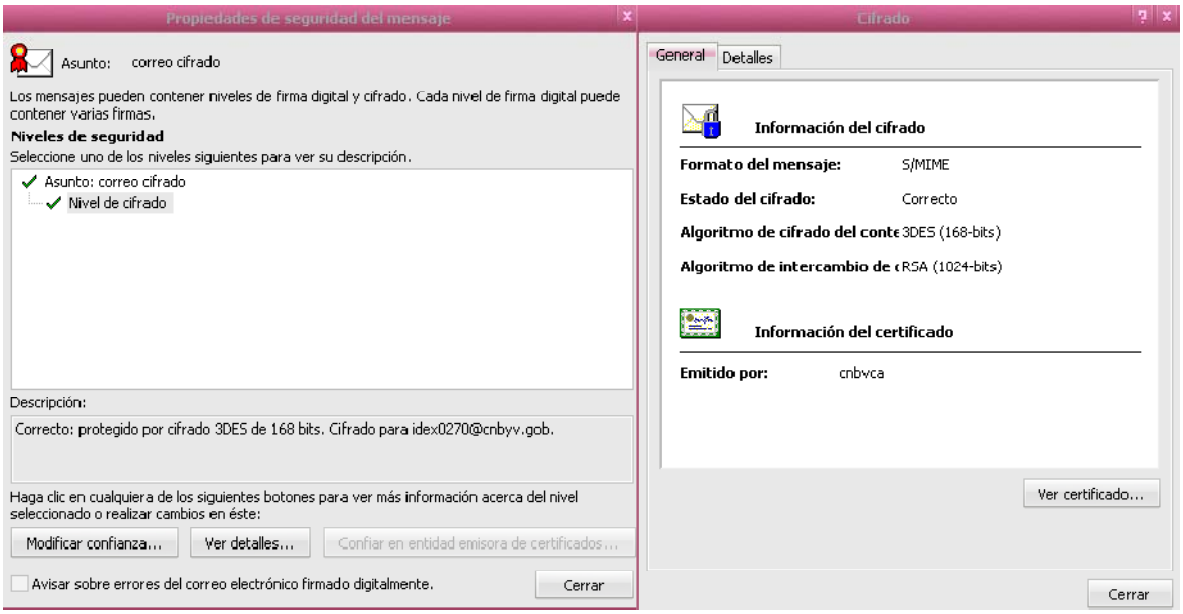

Figura 82. Propiedades de la seguridad del mensaje.

Con la implementación de cifrado y firma digital, obtengo la privacidad y veracidad en los envíos de mensajes:

- La Privacidad para que sólo la persona indicada pueda ver el mensaje y este sea confidencial.

- La Veracidad de la autenticidad e integridad de un mensaje.

Se da por terminada la implementación de cifrado y firma digital en correo electrónico en la Comisión Nacional Bancaria y de Valores, con ello se implementa de igual manera los servicios de Integridad, Confidencialidad, Autenticación y No repudio dentro de la institución.

Como nota final cabe destacar que se hizo uso de los recursos con los que cuenta la institución y no se tuvo que recurrir a otras empresas, comprar software o certificados para la institución y cada unos de los usuarios. Con lo que se hace un uso eficiente y eficaz de los recursos informáticos con los que cuenta la CNBV.

CONCLUSIONES

El proyecto de investigación que se realizó logró el objetivo, se implementó un sistema criptográfico de llave pública, como lo son la firma digital y el cifrado asimétrico y se demostró que hay métodos criptográficos que permite mantener nuestra información segura, aún cuando siempre está latente el riesgo o inseguridad en cualquier red, ya sea local o Internet.

Ahora podemos enviar correos electrónicos con la seguridad de que solo las personas a quien se le envía conocerán el contenido del mismo y tengan la plena certeza que la persona que envió el correo electrónico es quien dice ser. Cabe aclarar que la investigación se basó en los mensajes dentro del dominio en la red local y vía Web por qué es lo que más se ocupa en la actualidad.

La seguridad de la información se ha vuelto cada día más importante dentro de las instituciones y en la vida cotidiana, es necesario tener siempre protegida la información, en ocasiones ya no es una necesidad sino una obligación.

Hoy en día las empresas deben enfocar gran parte de su tiempo en temas de seguridad y herramientas para cumplirla de manera correcta y efectiva, herramientas con las que se les pueda hacer frente a ataques informáticos. El negocio y desarrollo de las actividades de muchas organizaciones dependen de los datos e información almacenados en sus sistemas informáticos. Por esto es necesario hacer llegar a todos los usuarios o por lo menos a mandos directivos, la importancia de proteger la información.

El mundo de la seguridad de la información es muy amplio, la criptografía sólo es una parte de él, esta nos hace posible garantizar la confidencialidad, integridad y autenticación de los mensajes guardados o enviados a través de alguna red. En pocas palabras la criptografía es la ciencia y arte que se ocupa de la construcción de llaves para ocultar mensajes a ojos no autorizados. Existen dos tipos de criptografía, la simétrica y la asimétrica, atendiendo la naturaleza de la llave utilizada y que tipos de servicios son necesarios implementar, para hacer uso de cualquiera de ellas.

Sin duda el servicio de Internet más conocido y utilizado es el correo electrónico, que proporciona una comunicación rápida y barata. En la actualidad millones de personas hacen uso de este servicio y por ende es uno de los que sufren mayor número de ataques. Un correo electrónico puede sufrir distintos ataque como son interceptación, usurpación, repetición y creación de mensajes, para disminuir estos ataques es necesario el uso del cifrado para dar protección a los datos y la firma digital para la autenticidad.

Para mejorar la seguridad en el correo electrónico se propuso utilizar S/MIME, para el uso de correo electrónico seguro. S/MIME utiliza algoritmos de criptografía de llave pública y los certificados digitales de usuario para garantizar la integridad, y autenticidad de los mensajes, así como cifrado simétrico para la confidencialidad.

De esta manera S/MIME, permite garantizar los servicios de seguridad de confidencialidad, integridad, autenticación y no repudio. S/MIME es considerada como la mejor opción para instituciones gubernamentales, por que utiliza menos recursos del modelo de autenticación de la autoridad certificadora, y porque es de fácil implantación a través del cliente de Microsoft Outlook.

Las aplicaciones de firma digital pueden ser muy útiles si lo que se requiere es integridad de la información, autenticación del emisor, si se requiere evitar el no repudio, por otra parte si se requiere confidencialidad en los mensajes, se utiliza el cifrado.

La obtención de datos a partir de una firma digital aplicada en un mensaje de correo electrónico permite asegurar quien en realidad envió el mensaje, el certificado que utilizó para firmar y la autoridad certificadora que lo emitió.

El propósito de la firma digital es doble. El primero es certificar que proviene de la persona que lo envió: que se conoce como no repudio. El segundo es asegurar que el contenido no ha sido alterado, que se conoce como integridad. La manera en que un programa de correo cumple con este cometido es mediante la ejecución de un proceso que, a partir del contenido de tu mensaje, genera un resumen del mismo mensaje, conocido como función hash. Éste último, si el algoritmo matemático que se utiliza es lo suficientemente fuerte, como SHA – 1, posee los siguientes atributos: El mensaje original no puede ser generado a partir del resumen y cada resumen es único.

Por otra parte, el certificado digital es único para cada individuo, como si fuese una licencia para conducir, una credencial de elector o un pasaporte, el cual se compone de dos partes, una llave pública y una privada. El certificado es único para una persona.

El cifrado es como una medida adicional de seguridad, puede cifrar el correo electrónico. El cifrado puede convertir el texto de un correo en un lío mutilado de números y letras que sólo pueden ser interpretados por aquellos que les pertenece. Los secretos personales más profundos pueden estar escondidos para todo el mundo excepto para aquellos ojos en quien se confía.

Se determinó por medio de una encuesta realizada a los usuarios finales de la Comisión Nacional Bancaria y de Valores que la implementación de cifrado y firma digital en el correo electrónico cumplió con las expectativas esperadas debido a que brinda integridad, confidencialidad y autenticación por medio de la criptografía y sus aplicaciones. Ellos valoran su información y opinan que es muy importante la seguridad de la misma y era necesario optar por una medida de seguridad para mantenerle protegida.

En comparación con el uso de correo electrónico tradicional y el utilizado con cifrado y firma digital, los usuarios consideraron que se sienten más seguros al enviar información a través de la red de una manera confiable, ya que la mayoría de los usuarios piensa que su información es observada por personas a las que no les pertenece dicha información.

Los usuarios estimaron que el cifrado y la firma digital en el correo electrónico son fáciles de usar y contienen una mejora de seguridad, además de que es necesario contar con métodos que protejan información valiosa para cada usuario.

Con esto se da por terminado la implementación y de la mejora de seguridad que brinda a cada uno de los usuarios de la Institución.

Antes de terminar, es necesario saber que la a seguridad de la información no debe entenderse como algo que se compra y se instala, en realidad es un proceso que debe estar presente en toda organización, como base de confianza para la privacidad de la información.

La seguridad absoluta tiene un costo infinito, debido a la flexibilidad de los sistemas informáticos, en conclusión debemos desconfiar de soluciones mágicas que garanticen la seguridad de la información sin tener que preocuparnos por nada.

TABLA DE FIGURAS

ANEXO I

Encuesta

Esta encuesta fue realizada a los usuarios de la Comisión Nacional Bancaria y de Valores para valorar la calidad de implementación de cifrado y firma digital en correo electrónico con el fin de saber si cumplió con las expectativas esperadas.

¿Tiene información de carácter personal que envía por correo electrónico?

SI ( )
NO ( )

¿Considera necesario que esa información sea confidencial?

MUY NECESARIA ( )
NECESARIA ( )
NO NECESARIA ( )

¿Qué tan importante es para usted la seguridad de su información?

MUY IMPORTANTE ( )
IMPORTANTE ( )
POCO IMPORTANTE ( )
SIN IMPORTANCIA ( )

¿Considera que su información es observada o modificada por otros usuarios?

SI ( )
NO ( )

¿Ha tenido problemas con algún tipo de correo electrónico por la información que maneja?

SI ( )
NO ( )

¿Qué tan necesarios considera los métodos de cifrado y firma digital en el correo electrónico?

MUY NECESARIOS ( )
NECESARIOS ( )
NO NECESARIOS ( )

¿Cuál es su opinión de la nueva implementación de cifrado y firma digital en el correo electrónico?

EXCELENTE ( )
BUENA ( )
REGULAR ( )
MALA ( )

¿Considera que la firma digital es un método confiable para firmar documentos y correo electrónico?

MUY CONFIABLE ( )
CONFIABLE ( )
POCO CONFIABLE ( )
NADA CONFIABLE ( )

¿Con la implementación de cifrado en el correo electrónico, considera que su información es está más segura y goza de confidencialidad e integridad?

SEGURA ( )
NO SEGURA ( )

¿Considera fácil de usar estos métodos?

FÁCILES ( )
DIFÍCLES ( )

¿Existe una mejora de seguridad en el uso del correo electrónico?

SI ( )
NO ( )

En comparación con el uso de correo electrónico tradicional y el utilizado con cifrado y firma digital ¿Cree usted que es una manera confiable y segura de enviar información a través de la red?

SI ( )
NO ( )

¿Considera usted que se cumplieron las expectativas de tener una manera distinta y fácil de enviar un correo electrónico y que además nos brinde, integridad, confidencialidad, autenticación por medio de la criptografía y sus aplicaciones?

SE CUMPLIERON ( )
NO SE CUMPLIERON ( )

ANEXO II

Petición y aceptación de apoyo de tesis por parte de la Dirección General de Informática en la Comisión Nacional Bancaria y de Valores.

Petición

México, D.F. a 28 de Agosto de 2009

Ing. Jorge Carrillo Alarcon
Dirección General de Informática
Presente

Tengo el gusto de dirigirme a usted, con el fin de solicitar su aprobación para la elaboración de un proyecto de mi tesis, con el propósito de titularme como Licenciado en Informática en la Universidad Latina.

El tema se refiere a la seguridad de la información dentro de la C.N.B.V., básicamente va dirigido al cifrado y firma digital en el correo electrónico.

La tesis llevará por nombre:

"***CRIPTOGRAFÍA ASIMÉTRICA CON LA IMPLEMENTACIÓN DE CIFRADO Y FIRMA DIGITAL EN CORREO ELECTRÓNICO EN LA COMISIÓN NACIONAL BANCARIA Y DE VALORES***"

Sin más por el momento, agradezco su atención y le envió un atento saludo.

Atentamente

Ernesto Alejandro Cruz Villela
Universidad Latina
Campus Sur
México, D.F.

COMISION NACIONAL BANCARIA Y DE VALORES
RECIBIDO
28 AGO. 2009
DIRECCIÓN GENERAL DE INFORMÁTICA

Aceptación

México, D.F. a 28 de Agosto de 2009

Ing. Jorge Carrillo Alarcon
Dirección General de Informática
Presente

Tengo el gusto de dirigirme a usted, con el fin de solicitar su aprobación para la elaboración de un proyecto de mi tesis, con el propósito de titularme como Licenciado en Informática en la Universidad Latina.

El tema se refiere a la seguridad de la información dentro de la C.N.B.V., básicamente va dirigido al cifrado y firma digital en el correo electrónico.

La tesis llevará por nombre:

"***CRIPTOGRAFÍA ASIMÉTRICA CON LA IMPLEMENTACIÓN DE CIFRADO Y FIRMA DIGITAL EN CORREO ELECTRÓNICO EN LA COMISIÓN NACIONAL BANCARIA Y DE VALORES***"

Sin más por el momento, agradezco su atención y le envió un atento saludo.

Atentamente

Ernesto Alejandro Cruz Villela
Universidad Latina
Campus Sur
México, D.F.

COMISIÓN NACIONAL BANCARIA Y DE VALORES
RECIBIDO
28 AGO. 2009
DIRECCIÓN GENERAL DE INFORMÁTICA

GLOSARIO

A

Active Directory	Tecnología de Microsoft, diseñada para permitir a las aplicaciones localizar, usar, gestionar recursos de directorio, por ejemplo nombre de usuario, impresoras de red, permisos; dentro de un entorno informático distribuido.
Algoritmo	Una secuencia finita de pasos para resolver un problema matemático o lógico o para realizar una tarea.
Autenticación	Servicio de seguridad que garantiza que la identidad de un creador de un mensaje o documento es legítima.
Autoridad certificadora	Entidad de confianza del emisor y del receptor de una comunicación. Y es la responsable de emitir y revocar los certificados digitales.
Autoridad de registro	Controla la generación de certificados digitales, se encarga de realizar la petición del certificado y de guardar los datos pertinentes.

B

Bit	Unidad más pequeña de información que puede ser manejada por un equipo informático.
Byte	Unidad de datos compuesta por 8 bits, representa un único carácter, como por ejemplo, una letra, un dígito o un signo de puntuación.

C

Certificado digital	Una tarjeta de identidad de un usuario, es una credencial electrónica que autentica a un usuario.
Certificado .pfx	Un archivo PFX contiene toda la información que compone un Certificado Digital X.509**.**
Cifrar	Proceso para codificar los datos para impedir el acceso no autorizado.
Cifrado asimétrico	Método criptográfico que utiliza un pareja de llave para el cifrado, la llave pública permite cifrar datos y su correspondiente llave secreta permite descifrarlos y viceversa.
Cifrado simétrico	Método criptográfico, el cual usa una misma llave para cifrar y descifrar datos.
Confidencialidad	Servicio de seguridad que garantiza que cada mensaje transmitido o almacenado es un sistema informático sólo pueda ser leído por su legítimo destinatario.
Contraseña	Cadena de caracteres introducida por un usuario para verificar su identidad.
Control de acceso	Mecanismos para limitar el acceso a ciertos elementos de información, basándose en las identidades de los usuarios.
Core de conexión	Núcleo por donde se encuentran conectados los segmentos de red.
Correo electrónico	Un mensaje de texto electrónico, es el intercambio de mensajes de texto y archivos electrónicos a través de una red de comunicaciones.
Criptoanálisis	La decodificación de información cifrada electrónicamente con el

	propósito de comprender las técnicas de cifrado utilizadas.
Criptografía	La utilización de códigos para convertir los datos de modo que sólo un receptor específico sea capaz de leerlos utilizando una llave.
Criptología	Ciencia genérica de ocultamiento de información.

D

DES	Data Encryption Standard, sistema de cifrado de datos adoptado por el gobierno de Estados Unidos como estándar en 1976, utiliza una llave de 56 bits.
Disponibilidad	Garantizar que los sistemas informáticos tengan un correcto funcionamiento y estén en permanente disposición de los usuarios que deseen acceder a sus servicios.
Dominio	Es un conjunto de equipos conectados a una red que confían a un equipo de dicha red la administración de los usuarios y los privilegios de cada uno de ellos en la red.
DSA	Digital Signature Algorithm, algoritmo de firma digital, está basado en un estándar de cifrado que utiliza una llave privada y otra llave pública.

E

ElGamal	Se refiere a un esquema de cifrado basado en problemas matemáticos de

	algoritmos discretos. Es un algoritmo de criptografía asimétrica.
Estándar	Son una serie de lineamientos técnicos detallados, destinados a establecer uniformidad.

F

Firewall	Un sistema de seguridad que trata de proteger la red de un usuario u organización con amenazas externas procedentes de otra red.
Función Hash	Algoritmo de digestión de mensajes, que realiza una serie de operaciones matemáticas sobre un mensaje para calcular un tamaño fijo de bits, llamado hash o huella digital.

H

Huella digital	Es el resultado que produce una función hash, es de tamaño variable.

I

Infraestructura	Es el conjunto de servicios e instalaciones básicas para la creación y el correcto funcionamiento de una organización
Integridad	Servicio de seguridad que garantiza que un mensaje o fichero no ha sido modificado desde su creación o durante su transmisión a través de una red informática.

Internet	Colección mundial de redes, que utilizan protocolos TCP/IP para comunicarse entre sí, llamada también red de redes.
ISO	Organización Internacional de Estandarización, establece estándares globales para las comunicaciones y el intercambio de información.
ITU – T	División de Estandarización de la Unión Internacional de Telecomunicaciones, desarrolla recomendaciones para todo tipo de comunicaciones.

L

Llave privada	En un sistema de cifrado asimétrico, es la llave que solo el emisor del mensaje conoce para cifrar o descifrar un mensaje.
Llave pública	En un sistema de cifrado asimétrico, es la llave que todos conocen para cifrar o descifrar un mensaje.
Lista de revocación de certificados	Es una lista de certificados (más exactamente: sus números de serie), los cuáles se han revocado, no son válidos, y no se debe confiar en ellos, por ningún usuario del sistema.

N

NIST	National Institute of Standards and Technology, Instituto Nacional de estándares y tecnología, desarrolla y promueve estándares para aplicaciones científicas y tecnológicas, con el fin de promover el comercio y mejorar la productividad del mercado.

No repudio	Consiste en demostrar la autoría y envío de un determinado mensaje, de tal manera que el usuario que lo ha creado y enviado, no puede posteriormente negar esta circunstancia, situación que también se aplica al destinatario que se envío.

O

Outlook	Software de aplicación de Microsoft para mensajería y trabajo en colaboración, es parte del paquete Microsoft Office.
Outlook Web Access	Es una aplicación parecida a Outook, que permite acceder al buzón de Microsoft Server Exchange 2007 vía web.

P

PGP	Programa de cifrado de llave pública basado en el algoritmo RSA y desarrollado por Philip Zimmermann.
PKCS	Public Key Cryptographic Standards, Estándares Criptográficos de llave pública, son una serie de estándares, utilizados en firma digital, criptografía de llave pública y servicios de certificación electrónica.
PKI	Public Key Infrastructure, Infraestructura de Llave Pública, es la forma común de referirse a un sistema complejo necesario para la gestión de certificados digitales y aplicación de firma digital.
POP3	Protocolo para servidores de Internet que permite recibir, almacenar y transmitir correo electrónico. Permite a los programas cliente cargar y

	descargar correo electrónico.
Protocolo	Es un acuerdo entre dos o más partes para realizar algo específico.

R

RC2	Es un algoritmo de cifrado simétrico por bloques de llave de tamaño variable diseñado por Ron Rivest de RSA Data Security.
RSA	Algoritmo de llave pública ampliamente utilizado, con longitud de llave bastante considerable, hasta 2048 bits.
Ruta de certificación	Es una secuencia de uno o más puntos conectados entre el suscriptor de un certificado y una autoridad certificadora raíz.

S

S/MIME	Secure / Multipurpose Internet Mail Extensions, extensiones multipropósito de correo de Internet seguro, es un protocolo de internet de correo electrónico con funciones de seguridad que añade cifrado de llave pública y soporte para firmas digitales.
Servidor	Una computadora que ejecuta software administrativo encargado de controlar el acceso a red y a sus recursos.
Servidor DNS	Una computadora que puede responder a consultas de servidores de nombre de dominio, mantiene una base de datos de computadoras host y de sus correspondientes direcciones IP.
Servidor Exchange	Una computadora que proporciona un sistema de mensajería confiable, con protección integrada contra correo no

	deseado y virus. Los usuarios de la organización pueden tener acceso al correo electrónico, el correo de voz, los calendarios y los contactos desde una amplia variedad de dispositivos y desde cualquier ubicación.
SHA – 1	Secure Hash Algorithm – 1, Algoritmo de Hash Seguro – 1. El SHA – 1 toma como entrada un mensaje de longitud máxima 264 bits y produce como salida un resumen de 160 bits.
SMTP	Simple Mail Transfer Protocol, Protocolo Simple de Transferencia de Correo, protocolo TCP/IP, para enviar mensajes de una computadora a otra a través de una red. En Internet se utiliza para distribuir correo electrónico.

T

Triple – DES	Algoritmo que hace triple cifrado DES, también conocido como: TDES o 3DES.

X

X.509	Estándar para infraestructura de llave pública, especifica los formatos para los certificados digitales y da la validación de las rutas de certificación.

BIBLIOGRAFÍA

Gómez, Álvaro, (2007), ***Enciclopedia de la Seguridad Informática***, Primera Edición, Alfaomega, México.

Dalatabuit, Enrique, (2007), ***La Seguridad de la Información***, Primera Edición, Limusa, México.

Echenique García, José Antonio, (2001), ***AUDITORIA EN INFORMÁTICA***, Primera Edición, McGraw – Hill / Interamericana Editores, México.

Cisco Systems, Inc., (2004), ***Academia de Networking de Cisco Systems Guía del primer año. CCNA 1 y 2***, Tercera Edición, Pearson Educación, Madrid.

Hughes, Larry J., (1995), ***Actually Useful Internet Security Techniques***, First Edition, New Riders Publishing, United States of America.

Siyan, Karanjit and Hare, Chris, (1995), ***INTERNET FIREWALLS AND NETWORK SECURITY***, Second Edition, New Riders Publishing, United States of America.

Aiken, Peter, (2005), ***Diccionario de Informática e Internet***, Segunda Edición, McGraw – Hill / Interamericana de España, Madrid.

Aceituno, Vicente, (2007), ***SEGURIDAD DE LA INFORMACIÓN: Expectativas, riesgos y técnicas de protección***, Primera Edición, Limusa, México.

Pfleeger, Charles P., (2006), ***Security in Computing***, Fourth Edition, Prentice Hall, United States of America. E – book.

Diffie, W. y M.E.Hellman, ***New directions in Cryptography***, (1976), IEEE Transactions on Information Theory.

ENCICLOPEDIA VNIVERSAL ILVSTRADA UEROPEO AMERICANA, (1995), 63 Tomos, Espasa Calpe, Madrid, España.

WEBGRAFÍA

http://www.rsa.com

http://www.microsoft.com/security

http://www.nist.gov

http://insecure.org

http://www.verisign.com/mx

http://www.kriptopolis.org

http://www.iec.csic.es/criptonomicon

http://www.segu-info.com.ar

http://www.textoscientificos.com/criptografia

http://es.wikipedia.org

http://www.foromsn.com/Version_Imprimible.php?Id=75160

http://www.seguridaddigital.info

http://criptosec.unizar.es/teoria.php

http://www.criptored.upm.es

http://williamstallings.com/Crypto3e.html

http://www.xombra.com/articulos.php

http://icaix.com/front/21

http://www.dragonjar.org/video-tutoriales-seguridad-informatica.xhtml