UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TÍTULO DEL TRABAJO DE TITULACIÓN:

INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI) PARA UNA PYME

Previa a la obtención del Grado Académico de Magíster en Telecomunicaciones

ELABORADO POR:

Ing. José Rodolfo López Garzón

DIRECTOR:

MSc. Luis Córdova Rivadeneira

Guayaquil, Enero de 2015

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el Magíster José Rodolfo López Garzón como requerimiento parcial para la obtención del Grado Académico de Magíster en Telecomunicaciones.

Guayaquil, Enero de 2015

DIRECTOR DE TESIS

_____

MSc. Luis Córdova Rivadeneira

REVISORES:

_____

MSc. María Luzmila Ruilova Aguirre

_____

MSc. Orlando Philco Asqui

DIRECTOR DEL PROGRAMA

_____

MSc. Manuel Romero Paz

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

DECLARACIÓN DE RESPONSABILIDAD

YO, ING. JOSÉ RODOLFO LÓPEZ GARZÓN

DECLARO QUE:

El Trabajo de Titulación "Infraestructura de clave pública (PKI) para una PYME", previa a la obtención del grado Académico de Magíster, ha sido desarrollado en base a una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del Trabajo de Titulación del Grado Académico en mención.

Guayaquil, Enero de 2015

EL AUTOR

_____

Ing. José Rodolfo López Garzón

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

AUTORIZACIÓN

YO, ING. JOSÉ RODOLFO LÓPEZ GARZÓN

Autorizo a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del Trabajo de Titulación de Maestría: "Infraestructura de clave pública (PKI) para una PYME", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, Enero de 2015

EL AUTOR

_____

Ing. José Rodolfo López Garzón

Dedicatoria

A mis padres José y Mariana, quienes con su apoyo moral y económico han sido un pilar fundamental en todo momento desde el inicio hasta la finalización de la maestría, por las palabras de aliento y empuje que me dedicaban con el objetivo de motivar la culminación de éste trabajo.

A mi esposa Karem quién ha sido mi compañera y amiga, por su amor y comprensión en los momentos de flaqueza y por el tiempo que no estuve presente.

A mi hijo Joaquín quién por sus escasos dos añitos no entendía porque no dedicaba mucho tiempo para jugar con él.

A mi director de tesis MSc. Luis Córdova R. quien supo guiarme en la elaboración de éste trabajo, por su entrega y ayuda, de igual manera al director de la Maestría MSc. Manuel Romero quien ha sido una persona que ha estado siempre dispuesta al diálogo y a ser un soporte del estudiante.

Agradecimiento

En primer lugar agradezco a Dios por haberme dado la vida y por ponerme en el lugar y momento correcto, para poder concretar éste logro tan importante en mi vida profesional.

Gracias infinitas a mis padres por siempre inculcarme el camino del bien y la superación profesional, siendo un ejemplo para sus hijos, estoy seguro que no me alcanzará esta vida para compensar todo lo que han hecho por mí.

Gracias a mi esposa por soportar mis malos momentos y por comprender que todo esfuerzo de hoy tiene su recompensa mañana.

Gracias a mi hermana porque indirectamente con su ejemplo de superación ha sido un modelo a seguir, por ser una mujer luchadora y que siempre obtiene lo que se propone.

Gracias a todos mis familiares, amigos y compañeros de trabajo, por compartir momentos de la vida cotidiana y por sus ideas manifestadas para la elección del tema de tesis.

RESUMEN

En este trabajo se estudió el desarrollo de la criptografía, destacándose la criptografía asimétrica como la vía más práctica para certificar las comunicaciones en una PYME. Se realizó una investigación acerca del funcionamiento de una Infraestructura de clave pública así como de los elementos que la conforman. Se investigó el estado de las infraestructuras de clave pública en el país y se hizo un estudio de las características de la red de la PYME. Se propuso el diseño de una infraestructura de clave pública para la empresa. Se configuró una infraestructura de clave pública en Ubuntu 12.04 y Windows Server 2003. Se investigó las plataformas de código abierto que permiten la implementación de una infraestructura de clave pública y se escogió el software OpenSSL que está incluido en el repositorio de Ubuntu 12.04.

Palabras clave: infraestructura de clave pública, certificado digital, firma digital, Ubuntu.

ABSTRACT

In this work the development of the cryptography was studied, standing out the asymmetric cryptography like the most practical road in order to certify the communications on SME. It was carried out an investigation about the operation of an infrastructure of public key (PKI) as well as of the elements that conform it. It was investigated the state of the infrastructures of public key in the country and it became a study of the characteristics of the data network of one SME. It is proposed the design of a PKI for the company. Also how to configure an PKI in Ubuntu 12.04 and Windows Server 2003. It was investigated the platforms of open code that permit the implementation of a infrastructure of public key and it was chosen the OpenSSL software that is included in the repository of Ubuntu 12.04.

Keywords**:** *infrastructure of public key, digital certificate, digital signature, Ubuntu.*

ÍNDICE

ÍNDICE DE FIGURAS.

Capítulo 1.

Capítulo 2.

ÍNDICE DE TABLAS.

Capítulo 2.

INTRODUCCIÓN

La necesidad de la criptología durante siglos permaneció solo estrechamente vinculada a entornos militares por la necesidad y la importancia que tiene la preservación de la integridad de la información y su confidencialidad. En la actualidad la situación ha cambiado debido al incremento de las comunicaciones electrónicas. Cualquier actividad cotidiana se traduce en un intercambio de datos entre personas, dispositivos o instituciones y se hace necesario proteger ese intercambio de información; así es como la criptografía se vuelve una necesidad de toda la población como una vía para proteger su información privada.

La criptología es una ciencia que abarca tanto la criptografía como el criptoanálisis. Se define la criptografía como la ciencia de usar las matemáticas para cifrar datos. Cuando una información ha sido encriptada puede ser almacenada en un medio inseguro o enviada a través de una red insegura, Internet por ejemplo y aun así permanecer secreta (Ordoñez & zambrano). El criptoanálisis se ocupa de descifrar los datos encriptados con el objetivo de recuperar la información original sin emplear la clave (CryptoForge, 2013), (Fuster, Hernández, Montoya, Muñoz, & Martín, 2012), (Lucena, 2002).

Para descifrar, el algoritmo hace un cálculo combinando los datos encriptados con una clave provista, siendo el resultado de esta combinación los datos descifrados (exactamente igual a como estaban antes de ser encriptados si se usó la misma clave). Si la clave o los datos son modificados el algoritmo produce un resultado diferente. El objetivo de un algoritmo criptográfico es hacer tan difícil como sea posible desencriptar los datos sin utilizar la clave. Si se usa un algoritmo de encriptación realmente bueno, entonces no hay ninguna técnica significativamente mejor que intentar metódicamente con cada clave posible. Incluso para una clave de sólo 40 bits, esto significa 2^{40} (poco más de 1 trillón) de claves posibles (CryptoForge, 2013).

Existen dos tipos fundamentales de criptografía: la criptografía simétrica y la criptografía asimétrica. La criptografía simétrica utiliza esa clave para codificar y decodificar, su desventaja es que al usarse al transmitir, dicha clave debe ser incluida en

emisor y receptor, debiendo transmitir la clave de forma segura (Montoya, 2010), (Lucena, 2002).

Si se emplea el cifrado asimétrico van a existir una clave pública conocida por todo el mundo y una privada que debe conocerla solo el propietario; y lo que se cifra con una clave, solo puede descifrarse con la otra. En este caso cualquier persona puede cifrar un mensaje con la clave pública, pero solo el propietario de la clave privada puede descifrarlo (Alvarez, 2010).

Si el propietario de la clave privada cifra con ella un mensaje, cualquiera puede descifrarlo con la correspondiente clave pública, lo que es equivalente a que el propietario de la clave privada estampe su firma digital (Alvarez, 2010).

Los algoritmos de clave pública son poderosos por lo que pueden usarse en medios inseguros de propagación, por ejemplo Internet. A partir del conocimiento de la clave pública o del texto cifrado no se puede obtener la clave privada. Este tipo de cifrado proporciona confidencialidad y brinda integridad, autenticación y no repudio. Una desventaja que presentan estos algoritmos es que generalmente se basan en claves muy grandes, así una clave de 128 bits es segura en algoritmos simétricos, en cambio en los asimétricos debe tener mínimo 1024 bits (Lucena, 2002), (Vallejos & Zelaya).

Las infraestructuras de clave pública tienen su surgimiento como tecnología en el mundo a partir del año 1989, con el PEM (*Privacy Enhanced Mail*) (Menezes, vanOorshot, & Vanstone, 2011), de Internet, (el medio natural que lo constituiría). Es en la década del 90 que comienza a tomar fuerza, este concepto, con el uso de modelos jerárquicos, pero en sus inicios, solo se desarrollaron algunos de sus componentes, fundamentalmente se hablaba de la creación de una tercera parte confiable o Autoridad de Certificación encargada de firmar estos certificados digitales y de una Autoridad de Registro que dicta las políticas para llevarlo a cabo (López, 2008), (Zanoletti, Jústiz, Díaz, & Nuñez, 2008).

Por esta fecha, algunas Autoridades de Certificación, que se dedicaban nada más que a aspectos relacionados con certificados digitales, encargados de crear las claves de los usuarios, como *Verisign*, tomaron mucha fuerza. Tres regiones que marcaron un

desarrollo significativo de Autoridades de Certificación son: Europa, América Latina y Estados Unidos, desarrollando numerosas empresas que implementan y brindan soluciones PKI flexibles y confiables para operaciones de comercio electrónico, negocios electrónicos, transacciones en la red y otros fines en la web (López, 2008) (Zanoletti, Jústiz, Díaz, & Nuñez, 2008).

El Ecuador ha alcanzado hoy un notable desarrollo en la utilización de las tecnologías de la información y las comunicaciones y de las redes telemáticas, lo cual requiere de un soporte tecnológico que garantice la confianza y seguridad en el intercambio de la información digital. La infraestructura de clave pública es una tecnología sustentada en un conjunto de sistemas informáticos y criptográficos, *hardware*, políticas y procedimientos que permite desplegar servicios seguros basados en el uso de un certificado digital de clave pública y claves criptográficas, garantizando confidencialidad, integridad, autenticidad y no repudio en las redes informáticas (López, 2008) (Zanoletti, Jústiz, Díaz, & Nuñez, 2008).

A nivel internacional, la utilización de la firma electrónica es el nuevo medio para dar autenticidad al documento electrónico, regulado de forma cosmopolita por la mayoría de los Estados que la han acogido.

Para la protección de esta información de una PYME como institución, se va a implementar una infraestructura de clave pública por lo que se utilizará un software de código abierto. El empleo de un software de código abierto permite que la detección y corrección de errores se lleve a cabo de forma eficiente y evita el uso de puertas traseras (*backdoor*) lo que previene la fuga de información (Lucena, 2002).

Antecedentes del problema

Una PYME hace un amplio uso de la red de computadoras, y generalmente la prioridad de sus redes de datos es mantener la seguridad en las comunicaciones pues manejan información sensible que debe mantener su confidencialidad. Algunos de los usos que tiene la red es el acceso a servidores de bases de datos, información que debe ser protegida, acceso a páginas web, correo electrónico, ftp y acceso a Intranet e Internet.

Para garantizar la seguridad de las comunicaciones de datos generalmente las PYMEs tienen implementados *firewall* como única estrategia de seguridad.

Problema a resolver

El problema que motivó el desarrollo de esta investigación es: La carencia de un mecanismo que permita certificar las comunicaciones de datos en algunas PYME.

Objeto de estudio

El objeto de estudio es la seguridad en las comunicaciones.

Campo de acción

Sistemas de Infraestructuras de Clave Pública.

Objetivo General

Implementar una Infraestructura de Clave Pública (PKI) en un ambiente virtualizado.

Objetivos específicos:

1. Desarrollar un estudio del marco teórico general de los principales aspectos relacionados con la criptografía enfatizando en la rama de la criptografía asimétrica.
2. Establecer un análisis comparativo de las diferentes herramientas que permiten la implementación de una infraestructura de clave pública.
3. Configurar un servidor Linux con distribución Ubuntu 12.04 y realizar las configuraciones necesarias para implementar una infraestructura de clave pública.
4. Configurar un servidor con Windows Server 2003 y configuración de la infraestructura de clave pública.
5. Seleccionar el método idóneo para implementar una infraestructura de clave pública en una PYME.

Tareas

1. Búsqueda bibliográfica acerca de la criptografía.
2. Profundización del funcionamiento de las infraestructuras de clave pública.
3. Análisis comparativo de las herramientas para implementar una infraestructura de clave pública.
4. Estudio de las características de la red de datos de una PYME.
5. Elaboración de una propuesta de una infraestructura de clave pública para una PYME.
6. Virtualización y configuración de un servidor Linux con distribución Ubuntu 12.04 y se realiza las configuraciones necesarias para implementar una infraestructura de clave pública.
7. Virtualización de un servidor con Windows Server 2003 y configuración de la infraestructura de clave pública.
8. Selección del método idóneo para implementar una infraestructura de clave pública en una PYME.

Hipótesis

Si se implementa una infraestructura de clave pública con el uso de una plataforma de código abierto es posible obtener un mecanismo para la certificación de las comunicaciones de datos para una PYME.

Metodología de la Investigación

En este trabajo de titulación se utilizó la investigación explicativa en razón de que se trata de averiguar la razón del objeto de estudio, es decir la infraestructura de clave pública (PKI) para una PYME para establecer las causas y efectos mediante una investigación del tipo Ex post facto, demostrando el avance de esta aplicación y mostrar la relación causa–efecto. En este trabajo se explica la aplicación de la clave pública (PKI) para una PYME y su importancia mediante la revisión de la información existente y la infraestructura que permite su aplicación exitosa en los sistemas de seguridad informáticos.

El paradigma corresponde al Empírico-Analítico y se tiene un enfoque cuantitativo por la utilización de expresiones matemáticas y cálculo de parámetros para demostrar las ventajas de la aplicación de una clave pública (PKI) para una PYME.

El diseño de la investigación es no experimental transversal, ya que no se manipulan las variables estudiadas y únicamente se analiza su ejecución en las aplicaciones.

CAPÍTULO 1: GENERALIDADES DE LA CRIPTOGRAFÍA Y LAS INFRAESTRUCTURAS DE CLAVE PÚBLICA

La seguridad en la transferencia de información por una red es muy importante para cualquier usuario. Los ataques a una red pueden ser pasivos o activos. En los ataques pasivos el atacante no altera la comunicación sino que la escucha o monitoriza para obtener la información que se transmite. Estos ataques son muy difíciles de detectar ya que no provocan ninguna alteración en los datos sin embargo es posible evitar su éxito mediante el cifrado de la información. Los ataques activos conllevan un cambio en el flujo de información o la creación de un falso flujo de datos (Valdiviezo, 2013).

Una forma de proteger la información que se intercambia por una red de datos es el empleo de la criptografía.

1.1 Criptosistemas.

Un Criptosistema está constituído por cinco elementos (Lucena, 2002):

- M son los datos sin codificar, un texto simple, posible de remitir (Lucena, 2002).
- C son los datos codificados o criptogramas (Lucena, 2002).
- K son las claves a utilizarse en el criptosistema (Lucena, 2002).
- E son las innovaciones de codificación o conjunto de ocupaciones de los componentes de M para conseguir un C. Hay una innovación distinta E_k generada por cada K (Lucena, 2002).
- D son las innovaciones de codificación, similar a E (Lucena, 2002).

Un criptosistema tiene la función de que si se tiene un mensaje M, este se cifra empleando la clave K y luego se descifra empleando la misma clave se debe obtener el mismo mensaje M (Fischer, 2008).

1.2 Tipos de criptografía.

El tipo particular de transformación aplicada sobre el texto claro y las características de las claves utilizadas marcan la diferencia entre los diversos procedimientos criptográficos (Fuster, Hernández, Montoya, Muñoz, & Martín, 2012).

1.2.1 Cifrado simétrico.

Los sistemas simétricos o de claves privadas usan una sola clave secreta para codificar y decodificar. Su desventaja es que para aplicarlos en telecomunicaciones se necesita tener conocimiento de la clave en el transmisor y en el receptor lo que conlleva a la disyuntiva de cómo transmitir la clave de forma totalmente segura o que exista un centro de distribución de claves que por medio de un canal seguro haga llegar las claves a ambas partes (Lucena, 2002), (Paar & Pelzl, 2011), (StDenis & Johnson, 2006).

1.2.2 Cifrado asimétrico.

Los sistemas de clave pública, o sistemas de cifrado asimétrico, son aquellos en que cada usuario posee un par de claves: una clave pública *Pk* para cifrar y una clave privada *Sk* para descifrar. Suponiendo que una persona X tiene un par de claves (*Pk* ,*Sk*) y otra persona S quiere enviar un mensaje a X, S va a cifrar el mensaje aplicando una función de encriptación E empleando la clave pública *Pk* de X (Delfs & Knebl, 2007):

$$c = E(p_k\ , m\ ) \qquad (1.1)$$

Para descifrar el mensaje el algoritmo calcula mediante la combinación de los datos encriptados con la clave privada S_k de X, por lo que X es la única persona que podrá conocer el contenido del mensaje (CryptoForge, 2013), (Ordoñez & zambrano).

$$m = D_k\ (S_k\ , E) \qquad (1.2)$$

Algoritmos de cifrado asimétrico: RSA.

RSA es un algoritmo criptográfico que se basa en las propiedades de los números primos. Un número primo solo es divisible por sí mismo y por 1. Ronald Rivest, Adi Shamir, y Leonard Adleman encontraron una interesante y práctica aplicación para estos números; esta aplicación se basa en la propiedad más importante de los números primos. Cualquier entero positivo puede ser representado como el producto de números primos en una sola forma. En otras palabras cualquier entero tiene una única factorización

prima. Por ejemplo el número 65535 puede ser representado como el producto de números enteros diferentes formas pero la única forma de representarlo como el producto de números primos es 3, 15, 17 y 257 cuyo producto es 65535.

La idea principal del algoritmo RSA es seleccionar dos números primos largos p y q que juntos constituirán la clave privada. La clave pública N va a ser su producto (Ver ecuación 1.3). Es relativamente fácil multiplicar enteros largos pero es prácticamente imposible, por lo menos empleando poco tiempo, encontrar factores primos de un entero largo con cientos de dígitos. Actualmente, después de un milenio de búsqueda no se ha encontrado un método eficiente de descomponer números que han sido descubiertos. Los algoritmos de descomposición que existen son lentos y puede llevar años descomponer un número entero constituido por unas pocos cientos de dígitos decimales (Salomon, 2005).

$$N = p \times q \qquad (1.3)$$

A modo de resumen se conoce que la clave pública N tiene una única factorización prima y que esos factores primos constituyen la clave privada. Si N es lo suficiente largo no es posible descomponerlo en factores incluso con computadoras rápidas (Salomon, 2005).

DSA.

El algoritmo DSA es una modificación del sistema ElGamal y fue propuesto como algoritmo estándar de firma digital dentro del DSS por el NIST en 1991. Esta medida fue muy criticada sobre todo por RSA Data Security, ya que esta compañía quería que su algoritmo se convirtiera en el estándar (Valdiviezo, 2013).

Dentro de los inconvenientes de DSA y en los que se basaron las críticas de RSA se encuentran que este sistema es solamente un estándar para firma digital, por lo tanto no se puede utilizar en el cifrado de información y por ende para distribuir claves. Otra desventaja de DSA es su lentitud en comparación con RSA en cuanto a la verificación de la firma digital sin embargo realiza la acción de generar las firmas digitales con mayor agilidad (Valdiviezo, 2013).

Curvas Elípticas Criptográficas.

Las Curvas Elípticas Criptográficas (ECC) fueron propuestas independientemente por Víctor Miller y Neal Koblitz en 1985 y ganó interés como un algoritmo de cifrado asimétrico porque empleando claves pequeñas mantiene el mismo nivel de seguridad que métodos como RSA con claves extensas. Esto se traduce en implementaciones rápidas y reducción del consumo de energía y ancho de banda (Koç, 2009).

La seguridad de ECC proviene de la dificultad que representa resolver el problema del logaritmo discreto en el grupo de las curvas elípticas. El problema del logaritmo discreto es encontrar el menor número e positivo que satisfaga la ecuación 1.4.

$$\mathbb{q} = e \times \mathbb{p} = \mathbb{p} + \mathbb{p} + \cdots + \mathbb{p} \qquad (1.4)$$

Donde $\mathbb{p}$ y $\mathbb{q}$ son puntos de una curva elíptica.

Esto envuelve adiciones, multiplicaciones e inversión de enteros los cuales están en las coordenadas de los puntos.

ECC tiene la ventaja con respecto a RSA que solo usa 80 bits para ofrecer la misma seguridad que RSA con 1024 así como también las claves RSA de 2048 bits son equivalentes en seguridad a 210 bits de ECC. Los requerimientos de memoria y CPU para realizar las operaciones criptográficas son también bastante inferiores por lo que este sistema es muy adecuado para ambientes restringidos en recursos donde el poder de computo es reducido y requiera una alta velocidad de procesamiento y grandes volúmenes de transacciones, lo que permite su uso por ejemplo en tarjetas inteligentes y celulares. Su desventaja fundamental es que muchas de sus variantes están patentadas por lo que no pueden utilizarse de forma libre (Valdiviezo, 2013).

1.3 Infraestructura de clave pública.

Las infraestructuras de clave pública hacen uso de criptografía asimétrica que consiste en el uso de dos claves pertenecientes a un usuario: una clave pública que puede ser

leída y una clave privada guardada en un dispositivo seguro (por ejemplo una *smartcard*). La relación matemática entre las dos claves es tal que una acción realizada con una clave puede estar relacionada a la otra clave pero sin revelar los datos de la clave privada. La seguridad del sistema se basa en que la clave privada se mantenga en secreto y que la clave pública se pueda relacionar con esta clave privada. Esto se consigue mediante el manejo del proceso de registro por el cual las claves son emitidas y utilizando un esquema de certificación que confirme la validez de la identidad de la clave pública (Cánovas, Gómez-Skarmeta, López, & Martínez, 2003), (Blanco, 2014).

Una infraestructura de los sistemas de información debe incluir los siguientes puntos:
Protección de la privacidad personal: es necesario garantizar la confidencialidad de las personas que acceden a servicios de información vía redes públicas como Internet. Existe información que solo debe ser disponible para personas autorizadas (StDenis & Johnson, 2006), (ongei.gob.pe, 2002).

Integridad de la información: la información que es publicada y compartida no puede ser alterada, ya que esto afectaría a otros procesos o sistemas, que al utilizar dicha información errónea producirán información no válida (StDenis & Johnson, Cryptography for Developers, 2006), (ongei.gob.pe, 2002).

Disponibilidad de la Información: la información de las entidades públicas debería estar disponible en el momento que se necesite. La seguridad de la información típicamente abarca los principios de confidencialidad, integridad y disponibilidad. Una infraestructura de seguridad se encarga que la información precisa esté disponible para los usuarios autorizados cuando estos son requeridos para propósitos legítimos. La meta de una infraestructura segura es aplicar la tecnología y las políticas administrativas que soporten estos principios (StDenis & Johnson, 2006), (ongei.gob.pe, 2002).

Se puede transformar un canal inseguro en uno confidencial con la ayuda de una infraestructura de clave pública y un canal extra con el objetivo de transmitir la clave pública. Es importante resaltar que el carácter requerido para este canal extra no es confidencial, la autenticación consiste en que el transmisor que envía un mensaje encriptado debe asegurarse que la clave pública que usa sea la apropiada. El cifrado y descifrado ocurren de forma asimétrica: solo el receptor del texto cifrado necesita tener

acceso a la clave privada con el propósito de realizar el descifrado del mensaje (Vaudenay, 2006). En la figura 1.1 se muestra el modelo de Shanon adaptado a la encriptación asimétrica para una Infraestructura de clave pública.

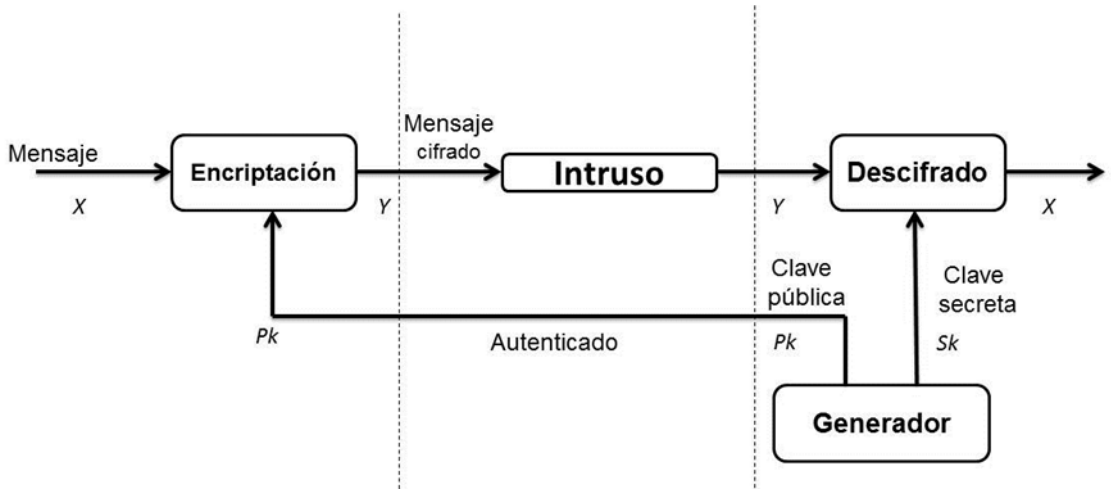

Figura 1. 1 Encriptación asimétrica
Realizado por el Autor

1.3.1 Definición de Infraestructura de clave pública.

Existen múltiples definiciones de infraestructura de clave pública. Adams and Lloyd [2002], Choudhury et al. [2002], Raina [2003], la Recomendación X.509 de la ITU-T11, en [X50, 1997], definen la infraestructura de clave pública de disímiles formas y finalmente todas las definiciones confluyen en que una infraestructura de clave pública es una infraestructura (o marco de trabajo), compleja dado los elementos que la componen, hardware, software, políticas y procedimientos que son requeridos para administrar las claves en un sistema de criptografía de clave pública con el fin de proveer privacidad, autenticación, integridad y no repudio (Ramos & Lamadrid, 2013).

Una infraestructura de clave pública es un sistema de entrega de certificados y claves criptográficas que brinda seguridad en servicios financieros y el intercambio de información importante entre usuarios relativamente desconocidos (ongei.gob.pe, 2002). Además, ofrece privacidad, control de acceso, integridad, autenticación y soporte para el no repudio en aplicaciones informáticas y servicios de comercio electrónico (ongei.gob.pe, 2002). Una infraestructura de clave pública administrará la generación y distribución de claves públicas y privadas y publicará las claves públicas con la

identificación de los usuarios en tablas electrónicas públicas (es decir servicios de directorio x.500) (ongei.gob.pe, 2002). Una infraestructura de clave pública provee un alto grado de confianza, manteniendo las claves privadas seguras, las claves públicas se conectan a sus respectivas claves privadas, y el par de claves (pública y privada) aseguran la veracidad de la persona quien dice ser (ongei.gob.pe, 2002). Mediante sus servicios, un usuario podrá realizar cualquier tipo de operación desde su propio navegador: solicitar un certificado, renovarlo, revocarlo, buscar el certificado de otro usuario con el que se desea establecer una comunicación segura (Cánovas, Gómez-Skarmeta, López, & Martínez, 2003). Una infraestructura de clave pública representa la integración de la criptografía de clave pública para el uso de firmas digitales y el manejo de claves y la criptografía de clave privada usada para cifrado. La base de una infraestructura de clave pública está definida en la recomendación ITU-T X.509 (ongei.gob.pe, 2002), (Cánovas, Gómez-Skarmeta, López, & Martínez, 2003) (Blanco, 2014).

La recomendación X.509 es parte de la serie de recomendaciones X.500 que define un servicio de directorio. Un directorio es un servidor que mantiene una base de datos de información sobre los usuarios. El protocolo X.509 define un marco para proveer servicios de autenticación y define una estructura de certificado y protocolos de autenticación que se usan en una gran variedad de contextos (Blanco, 2014).

En la figura 1.2 se muestran los componentes de una infraestructura de clave pública basada en lo que se describe en la recomendación RFC5280 del PKIX del IETF**:**

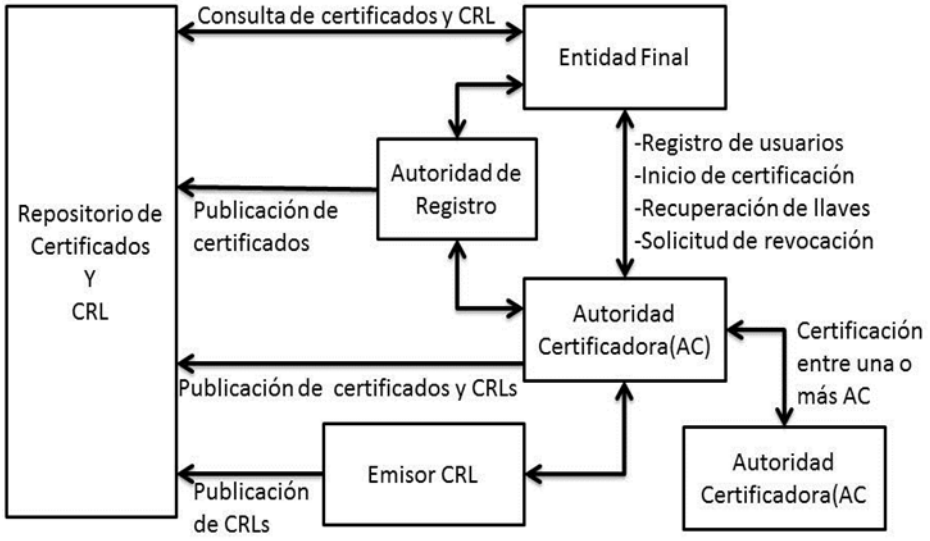

Figura 1. 2 Componentes de una infraestructura de clave pública
Realizado por el Autor

Dónde:

- Autoridad de Certificación (CA): es el componente esencial de una infraestructura de clave pública. Una CA es un conjunto de hardware, software y el personal que los opera (Valdiviezo, 2013). Es la entidad encargada de tramitar las solicitudes de servicio realizadas por ciertas entidades del sistema. Es la encargada de emitir los certificados digitales del sistema, las listas de revocación, firmar las políticas de certificación, y publicar la información en los repositorios de datos tanto internos como públicos (Cánovas, Gómez-Skarmeta, López, & Martínez, 2003). La confianza de los usuarios en la autoridad de certificación es fundamental para el buen funcionamiento del servicio. El entorno de seguridad (control de acceso, cifrado, etc.) de la CA ha de ser muy fuerte, en particular en lo que respecta a la protección de la clave privada que utiliza para firmar sus emisiones. Si este secreto se viera comprometido, toda la infraestructura de clave pública se vendría abajo (ongei.gob.pe, 2002), (Cánovas, Gómez-Skarmeta, López, & Martínez, 2003), (Valdiviezo, 2013).

  Las autoridades de certificación realizan las siguientes tareas (ongei.gob.pe, 2002):

- Emisión de certificados de usuarios registrados y validados por la Autoridad de Registro (RA) (ongei.gob.pe, 2002).
- Revocación de certificados no válidos (CRL-lista de certificados revocados). Un certificado puede ser revocado porque los datos han dejado de ser válidos, la clave privada ha sido comprometida o el certificado ha dejado de tener validez dentro del contexto para el que había sido emitido (ongei.gob.pe, 2002).
- Renovación de certificados (ongei.gob.pe, 2002).
- Publicar certificados en el directorio repositorio de certificados (ongei.gob.pe, 2002).

❖ Autoridad de Registro (RA): es una colección de *hardware, software* y las personas que lo operan (Valdiviezo, 2013). Es la primera entidad de contacto con la infraestructura de certificación. Su función principal es la de validar e identificar a los usuarios que solicitan alguno de los servicios que ofrece la infraestructura. Para realizar sus funciones toma en consideración las opciones determinadas por la política de certificación del sistema (Cánovas, Gómez-Skarmeta, López, & Martínez, 2003). Una persona puede encargarse de las responsabilidades de una RA. Todo el proceso de verificación de la identidad puede ser un conjunto de procedimientos manuales (Ramos & Lamadrid, 2013). Cada CA mantiene una lista de autoridades de registro acreditadas y verificando la firma de una RA en un mensaje una CA puede estar segura de que una RA acreditada proporcionó la información y, por tanto, es fiable. Por consiguiente, es importante que una RA proporcione protección adecuada para su clave privada. Hay dos modelos básicos para que una RA verifique el contenido de un certificado. En el primer modelo la RA recoge y verifica la información antes de presentar a la CA la solicitud para el certificado. En el segundo modelo, la CA recibe una solicitud de certificado que envía a la RA. La RA revisa el contenido y determina si la información es correcta. La RA responde a la petición de la CA con un simple ’Sí’ o ’No’ (Valdiviezo, 2013).

❖ Repositorio público de certificados: esta entidad almacena los certificados digitales y las listas de revocación emitidas por la autoridad de certificación (Cánovas, Gómez-Skarmeta, López, & Martínez, 2003). Los repositorios se diseñan para proporcionar máxima disponibilidad y rendimiento, ya que los

mismos datos establecen su integridad. Los repositorios necesitan restringir el conjunto de usuarios que pueden actualizar la información, ya que, de lo contrario, un atacante podría sustituir los certificados con basura y provocar un ataque de denegación de servicio (Valdiviezo, 2013).

- Tarjetas inteligentes: algunas infraestructuras soportan el uso de tarjetas inteligentes, como es el caso de PKIv6, en las entidades RA y CA y también en entorno web. Los usuarios podrán tener esas tarjetas inteligentes para almacenar su certificado, su clave privada y el certificado de la CA (Cánovas, Gómez-Skarmeta, López, & Martínez, 2003).

1.3.2 Funcionamiento de una infraestructura de clave pública.

Una infraestructura de clave pública se basa en distintos procedimientos de Autoridades de Certificación, las cuales se establecen de manera lógica en una organización de varios rangos. Cada identificación y clave pública de un usuario son localizadas en un mensaje (certificado) (ongei.gob.pe, 2002). Los usuarios de las autoridades de certificación firmarán digitalmente cada certificado y harán disponibles sus certificados y su clave pública mediante tablas electrónicas públicas (servicios de directorio x.500) junto con todos los certificados del resto de usuarios. Por lo tanto cualquier usuario podrá obtener cualquier clave pública de otro usuario de las tablas electrónicas públicas y verificar que esta es auténtica usando la clave pública de la CA, para verificar la firma de la CA sobre el certificado. La CA en el nivel más alto de la jerarquía firmará los certificados que contienen las claves públicas de las CAs subordinadas directamente a estas, y estas CAs firmarán los certificados de cualquier otra CA debajo de la jerarquía de las mismas. Este proceso entrega claves públicas que son firmadas por otras CAs en la infraestructura para ser verificadas, desde una cadena de confianza que ha sido previamente configurada entre las CAs. La confianza en una tercera parte se refiere a la situación en la cual dos entidades o personas individuales implícitamente confían uno del otro, aunque no tengan ningún tipo de relación previamente establecida (ongei.gob.pe, 2002). La confianza en una tercera parte es un requerimiento fundamental para las implementaciones a gran escala de servicios de seguridad basados en criptografía de claves públicas. Ver figura 1.3 (ongei.gob.pe, 2002).

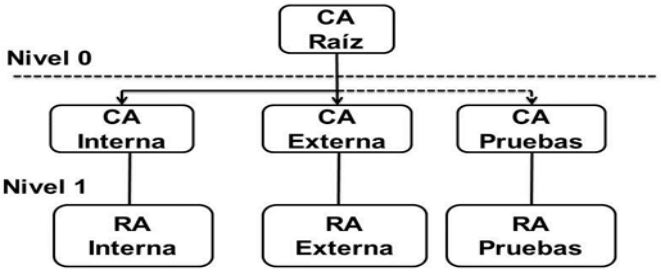

Figura 1. 3 Ejemplo de una jerarquía de certificación de 2 niveles
Realizado por el Autor

Nivel 0: En este nivel se encuentra una autoridad de certificación (CA Raíz) cúspide de la jerarquía de confianza y la base necesaria para crear nuevas jerarquías de certificados independientes. Esta CA emite un certificado autofirmado que la distinguirá como CA Raíz, así como certificados para cada una de las CA subordinadas del siguiente nivel. Esta CA podría establecer relaciones de confianza con CAs de dominios de certificación externos (Indra, 2005).

Nivel 1: En este nivel se ubican las CAs subordinadas (Indra, 2005).

• CA Subordinada Interna: es la encargada de gestionar los certificados de ámbito interno.
• CA Subordinada Externa: es la encargada de gestionar los certificados proporcionados al exterior.
• CA Subordinada de Pruebas: se emplea para realizar las pruebas antes de su paso a las CA de producción y proporcionar certificados al entorno de pruebas (Indra, 2005).
Cada CA del nivel 1 tiene asociada su correspondiente Autoridad de Registro (RA).

1.4 Arquitectura de una infraestructura de clave pública.

La arquitectura de una infraestructura de clave pública describe la organización de sus autoridades de certificación y sus relaciones de confianza. Cada arquitectura tiene sus ventajas y sus inconvenientes y es apropiada para algunos entornos, mientras que para otros no lo es (Valdiviezo, 2013).

1.4.1 CA única.

La arquitectura de clave pública básica es la formada por una CA única que proporciona todos los certificados y listas de revocación de certificados para una comunidad de usuarios. Todos los usuarios confían en la CA que emitió su propio certificado (Valdiviezo, 2013). Por definición, no pueden añadirse nuevas autoridades de certificación a la infraestructura de clave pública y puesto que solo hay una única CA no se establecen relaciones de confianza con otras CA. Es la arquitectura más simple de implementar. Los caminos de certificación constan de un único certificado y hay una única lista de revocación de certificados (Valdiviezo, 2013). Esta arquitectura no es escalable y presenta un único punto de fallo si se compromete la CA se invalidan todos los certificados emitidos y cada usuario debe ser informado inmediatamente. Para restablecer la confianza se debe volver a emitir todos los certificados y la información sobre el nuevo punto de confianza debe ser distribuida a todos los usuarios. Esta arquitectura solo es aplicable a una empresa que no necesita comunicarse con el mundo exterior (Valdiviezo, 2013), (Ponce, Peñafiel, & Cobeña, 2005).

1.4.2 Jerárquica.

La arquitectura jerárquica es la más tradicional. En esta arquitectura varias autoridades de certificación, con una relación superior-subordinado, proporcionan servicios a la infraestructura de clave pública. En esta arquitectura todos los usuarios confían en la CA raíz. Con la excepción de la CA raíz, todas las autoridades tienen una única CA superior. Una CA puede emitir certificados a autoridades de certificación, usuarios o ambos. Cada relación de confianza entre autoridades de certificación se representa por un único certificado. El emisor es la CA superior y el sujeto es la CA subordinada. Para añadir una nueva CA a la infraestructura de clave pública, una CA existente emite un certificado a la nueva CA. La nueva CA se injerta bajo la CA existente y se convierte en una CA subordinada de la CA emisora. Dos infraestructuras de clave pública jerárquicas pueden fusionarse de la misma manera. Las autoridades de certificación superiores pueden imponer restricciones a las CA subordinadas. Estas restricciones pueden implementarse con procedimientos o en los propios certificados (Valdiviezo, 2013). Para verificar un certificado este debe ser validado por las autoridades de certificación en sentido ascendente hasta llegar a la CA raíz (Ponce, Peñafiel, & Cobeña, 2005).

La arquitectura jerárquica proporciona varias ventajas que contribuyen a hacer de ella uno de los modelos más ampliamente desplegados hasta la fecha. En primer lugar, los

caminos de certificados son relativamente cortos. Además, puesto que todos los usuarios confían en la misma CA raíz, hay un único camino para alcanzar un usuario específico. Esto permite a la entidad final (usuario) distribuir los certificados de cualquier CA intermedia en la cadena junto con su propio certificado. La desventaja más significativa de este modelo radica en la misma razón que su simplicidad y éxito: la existencia de una CA raíz en la que todos confían. En una comunidad pequeña es posible acordar una única CA raíz, pero en comunidades grandes es imposible que todos acuerden una única CA raíz (Valdiviezo, 2013).

Si se compromete una CA, diferente de la autoridad de certificación raíz, su CA superior simplemente revoca su certificado. Una vez se ha restablecido, la CA emite certificados a todos sus usuarios (Valdiviezo, 2013).

1.5 Beneficios de una infraestructura de clave pública.

Una infraestructura de clave pública es una solución global de seguridad que puede ser usada en los entornos más heterogéneos. Presenta ventajas técnicas que se traducen en ventajas en entornos de negocios.

Ventajas técnicas:

- Gestión de *passwords* y *Single-Sign-On.* Hay muchos problemas ocasionados por el sistema tradicional de *usernames* y *passwords.* Una infraestructura de clave pública resuelve estos problemas de una manera consistente y sencilla para los usuarios y administradores (Valdiviezo, 2013).
- Firmas digitales: una infraestructura de clave pública permite firmar digitalmente documentos. Las firmas tienen un reconocimiento legal. En conjunto se consigue sustituir el papel con formularios electrónicos, más velocidad y trazabilidad en los procesos de negocios y una seguridad mejorada en las transacciones electrónicas (Valdiviezo, 2013).
- Cifrado: fácil cifrado de datos para cada individuo (sin intercambio previo de información) mediante el acceso al certificado que contiene la clave pública (Valdiviezo, 2013).

- Comodidad del usuario debido a que van a haber menos *passwords* (Valdiviezo, 2013).
- Administración coherente de seguridad en la empresa. Emisión y revocación centralizada de credenciales de usuario. Identificación consistente de usuario cuando se emiten las credenciales. Idéntico mecanismo de autenticación para todas las aplicaciones o servicios de red. Aprovechamiento de la inversión en *smartcards* o *tokens* USB al ser usados por muchas aplicaciones (Valdiviezo, 2013).
- Interoperabilidad con otras instituciones. La confianza entre organizaciones y/o empresas permite firmar y cifrar correos, firmar documentos, autenticación en aplicaciones compartidas (Valdiviezo, 2013).
- Solución basada en estándares. Los estándares proporcionan interoperabilidad entre fabricantes diferentes y que haya código libre (Valdiviezo, 2013).
- Amplio soporte en diferentes sistemas operativos como Windows, Linux, UNIX (Valdiviezo, 2013).
- Almacenamiento de claves en software y hardware. En aplicaciones: Apache, IIS, Oracle, SSL, Código abierto y comercial (Valdiviezo, 2013).

Ventajas de negocios:

- Se pueden conseguir ahorros significativos de tiempo mediante el manejo electrónico de documentos (Valdiviezo, 2013).
- Optimización de los recursos humanos: el usuario puede centrarse en su trabajo en lugar de gastar tiempo en detalles asociados con la infraestructura de seguridad (Valdiviezo, 2013).
- Reducción de los recursos humanos: la operación de una arquitectura unificada en lugar de múltiples soluciones puntuales requiere menos recursos administrativos (Valdiviezo, 2013).
- Reducción del papel: se puede ahorrar en costos de material, en el espacio necesario para almacenarlo, en reducción de residuos y en menor intrusión ambiental (Valdiviezo, 2013).
- Reducción de pérdidas por robo electrónico: los datos corporativos están protegidos, lo que reduce el riesgo de que sean revelados sin autorización (Valdiviezo, 2013).

1.6 Certificados digitales.

Un certificado digital es un equivalente electrónico del pasaporte. Este contiene información que puede ser usada para verificar la identidad del dueño. Una parte principal del contenido de la información del certificado digital es la clave pública del usuario. Una clave pública puede ser usada para poder realizar una comunicación encriptada en dos usuarios que tengan certificados digitales (Vaudenay, 2006), (ongei.gob.pe, 2002).

Los certificados electrónicos son documentos digitales que sirven para asegurar la veracidad de la clave pública perteneciente al propietario del certificado o de la entidad, con la que se firman digitalmente documentos que puedan proporcionar la más absoluta garantía de seguridad respecto a cuatro elementos fundamentales (ongei.gob.pe, 2002):

- La autentificación del usuario/entidad (es quien asegura ser).
- La confidencialidad del mensaje (que sólo lo podrá leer el destinatario).
- La integridad del documento (nadie los ha modificado).
- El no repudio (el mensaje una vez aceptado, no puede ser rechazado por el emisor).

Es, por tanto, muy importante estar realmente seguros de que la clave pública que se maneja es de quien se cree que es el dueño (ongei.gob.pe, 2002).

1.6.1 Certificados X.509

El formato de estos certificados corresponde a un estándar de la ITU-T (*International Telecommunication Union-Telecommunication Standarization Sector*) y el ISO/IEC *(International Standards Organization /International Electrotechnical Commission*) publicado en 1988. En la figura 1.4 se muestra la estructura de un certificado x509 (Hernandez, 2009), (Talens-Oliag, 2003).

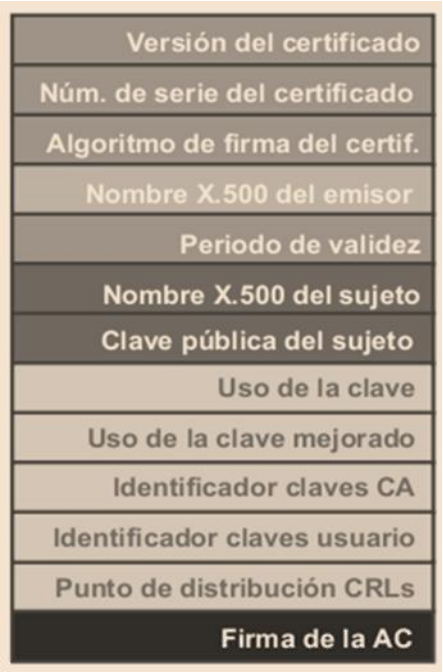

Figura 1. 4 Certificados X509
Realizado por el Autor

- Versión: el campo de versión contiene el número de versión del certificado codificado. Los valores aceptables son 1, 2 y 3 (Talens-Oliag, Seguridad en Java, 1999).
- Número de serie del certificado: este campo es un entero asignado por la autoridad certificadora. Cada certificado emitido por una CA debe tener un número de serie único (Talens-Oliag, Seguridad en Java, 1999).
- Identificador del algoritmo de firmado: este campo identifica el algoritmo empleado para firmar el certificado (como por ejemplo el RSA o el DSA) (Talens-Oliag, Seguridad en Java, 1999).
- Nombre del emisor: este campo identifica la CA que ha firmado y emitido el certificado (Talens-Oliag, Seguridad en Java, 1999).
- Período de validez: este campo indica el período de tiempo durante el cual el certificado es válido y la CA está obligada a mantener información sobre el estado del mismo. El campo consiste en una fecha inicial, la fecha en la que el certificado empieza a ser válido y la fecha después de la cual el certificado deja de serlo (Talens-Oliag, Seguridad en Java, 1999).
- Nombre del sujeto: este campo identifica la identidad cuya clave pública está certificada en el campo siguiente. El nombre debe ser único para cada entidad certificada por una CA dada, aunque puede emitir más de un

certificado con el mismo nombre si es para la misma entidad (Talens-Oliag, Seguridad en Java, 1999).

- Información de clave pública del sujeto: este campo contiene la clave pública, sus parámetros y el identificador del algoritmo con el que se emplea la clave (Talens-Oliag, Seguridad en Java, 1999).
- Identificador único del emisor: este es un campo opcional que permite reutilizar nombres de emisor (Talens-Oliag, Seguridad en Java, 1999).
- Identificador único del sujeto: este es un campo opcional que permite reutilizar nombres de sujeto (Talens-Oliag, Seguridad en Java, 1999).
- Extensiones (Talens-Oliag, Seguridad en Java, 1999).

1.6.2 Proceso de obtención de un certificado.

El proceso para obtener un certificado digital es el siguiente (Valdiviezo, 2013):

1. El solicitante se dirige a una empresa o entidad que tenga el carácter de Prestador de Servicios de Certificación y solicita de ellos las claves y el certificado digital correspondiente a las mismas. Este trámite generalmente se puede realizar presencialmente, acudiendo a dicha entidad o virtualmente, por medio de Internet, utilizando la página Web del Prestador de Servicios de Certificación (Valdiviezo, 2013).
2. El prestador de Servicios de Certificación comprobará la identidad del solicitante, bien sea directamente o por medio de entidades colaboradoras (Autoridades Locales de Registro), para lo cual se deberá mostrar el D.N.I. y si se trata de un representante de una sociedad (administrador, apoderado, etc.) o de cualquier otra persona jurídica, deberá acreditar documentalmente el cargo y las facultades del mismo (vigencia de poderes) (Valdiviezo, 2013).
3. El prestador de Servicios de Certificación mediante los dispositivos técnicos adecuados crea las claves pública y privada que le corresponde al solicitante, y genera el certificado digital correspondiente a dichas claves (Valdiviezo, 2013).

Aplicaciones que emplean certificados digitales (Valdiviezo, 2013)**.**

Existen varias aplicaciones basadas en protocolos que manejan certificados digitales durante los procesos de autenticación; entre las principales aplicaciones se pueden mencionar (Valdiviezo, 2013):

- Establecimiento de sitios web seguros: este tipo de aplicaciones utilizan protocolos que permiten una autenticación del lado del servidor; es decir, el servidor posee un certificado digital que le permite autenticarse y establecer sesiones seguras a través de una red. Entre los protocolos más utilizados para crear sitios web seguros se tiene a SSL (*Secure Sockets Layer*) y TLS (*Transport Layer Security*) (Valdiviezo, 2013)
- Creación de correos electrónicos seguros.

1.6.3 Revocación de certificados digitales

En ocasiones puede ser necesario deshacer la asociación entre entidad y clave pública que establece un certificado antes de que expire. En tal caso se procede a revocar el certificado. Las circunstancias que obligan a revocar un certificado son muy variadas y, entre ellas, se pueden citar que se halla comprometido la clave privada o compromiso de la CA. Las formas más comunes de implementar la revocación de certificados son mecanismos de publicación periódicos, tales como Listas de Revocación de Certificados (*Certificate Revocation Lists*), o mecanismos de consulta *on-line* tales como el *Online Certificate Status Protocol* (OCSP) (Valdiviezo, 2013).

1.6.4 Listas de Revocación de Certificados

Las listas de revocación de certificados son estructuras de datos firmadas que contienen una lista de certificados revocados. La firma digital agregada en la CRL proporciona mecanismos de autenticidad e integridad. Siempre que las políticas lo permitan las Listas de revocación de certificados pueden ser almacenadas en memoria y facilitar la verificación de certificados *off-line*. Normalmente el emisor del certificado y de la CRL es la misma autoridad (Valdiviezo, 2013).

Existen dos adaptaciones de listas de revocación de certificados en el estándar X.509. La versión 1 presenta varios defectos: problemas de escalabilidad, posibilidad de ataques de sustitución que remplazan una CRL por otra sin ser detectado. La versión 2

(Ver figura 1.5) corrige estos problemas mediante el mecanismo de las extensiones (Valdiviezo, 2013).

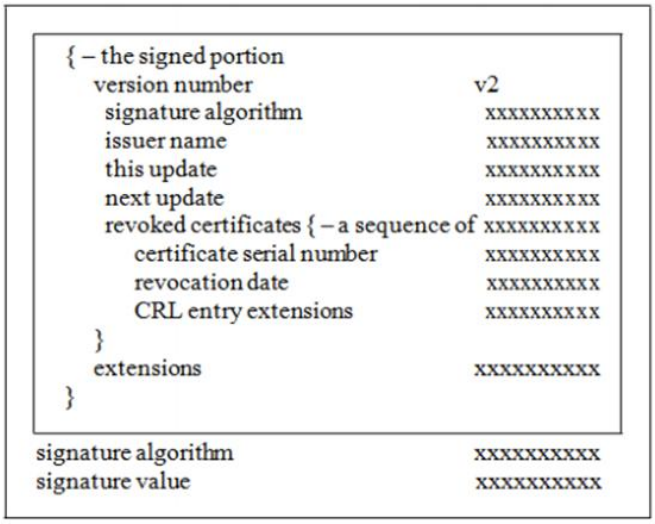

Figura 1. 5 Versión 2 de CRL
Fuente: (Valdiviezo, 2013)

Dónde:

- *Versión*: indica la versión de la CRL. Si el campo no está presente indica que se trata de una CRL v1; si el campo está presente su valor debe ser el entero 1, indicando que se trata de una CRL v2.
- *Signature Algorithm*: indica el OID del algoritmo usado para calcular la firma digital de la CRL. Debe coincidir con el campo *Signature Algorithm* perteneciente a la porción no firmada.
- *Issuer Name*: se trata del DN del emisor de la CRL, es decir, quién firma la CRL. Debe estar siempre presente y ser único.
- *This Update*: indica la fecha y hora en la que se emitió la CRL.
- *Next Update*: campo opcional según X.509 que indica la fecha y hora en la que se emitirá la siguiente CRL.
- *Revoked Certificates*: se trata de la lista de los certificados revocados. Cada entrada contiene el *Serial Number* del certificado revocado, la fecha y hora en la que se revocó el certificado y, opcionalmente, puede incluir extensiones aplicables a la entrada concreta de la lista.
- *Extension*: son las extensiones aplicables a la CRL globalmente.

El estándar X.509 define varias extensiones aplicables a una entrada de la lista. Estas extensiones permiten agregar información adicional a cada revocación. Algunas extensiones son:

- *Reason Code*: razón por la cual el certificado fue revocado (compromiso de la clave privada, compromiso de la CA, cambio de algún dato).
- *Certificate Issuer*: es el nombre del emisor del certificado.
- *Hold Instruction*: permite soportar la suspensión temporal de un certificado.
- *Invalidity Date*: es la fecha y hora en la que el certificado deja de ser válido.

Las Autoridades de Certificación emiten los certificados y sus propias CRL. Periódicamente la CA emite una única CRL que cubre toda su población de certificados, estas se denominan CRL completas (Valdiviezo, 2013).

1.7 Firma digital.

Se define firma digital como un sonido, símbolo o proceso electrónico, adjuntado o asociado lógicamente a un contrato u otro tipo de archivo y ejecutado o adoptado por una persona con la intención de firmar tal archivo (Ponce, Peñafiel, & Cobeña, 2005).

Con la invención de la criptografía de claves públicas, es posible el proceso conocido como firma digital. Una firma digital es equivalente a una firma manual, la cual proporciona la prueba que el que firma es el autor original del mensaje (autenticación). Si se desea firmar el mensaje que será enviado a un destinatario, el mensaje se cambia por medio de una función matemática (conocida como función hash) para lo cual hace un resumen del mensaje (código hash). Este resumen es único para cada mensaje y es equivalente a una huella digital. Luego este resumen o código hash se cifra con la clave privada y se adjunta al final del mensaje. Este código adjunto es conocido como firma digital. El destinatario puede verificar luego que el mensaje fue enviado por una persona que tiene una firma digital haciendo uso de la clave pública a través de una función hash similar. Si los dos códigos hash son similares entonces el que envió el correo firmado fue la persona correcta (no repudio) y no fue alterado (integridad) (ongei.gob.pe, 2002).

1.7.1 Función hash.

Antes de definir qué es una función hash o función resumen se hace necesario mencionar las funciones unidireccionales que son la base de las funciones hash. Para comprender qué es una función unidireccional basta con decir que para una función unidireccional se hace fácil calcular $f(x)$ pero resulta muy difícil calcular $f^{-1}(y)$. Dentro de estas funciones unidireccionales se encuentran las funciones unidireccionales con trampilla, estas tiene una información adicional que deben verificar. A esta función adicional que abarata los tiempos de computación se conoce como trampilla (Fuster, Hernández, Montoya, Muñoz, & Martín, 2012).

Una función resumen es una función unidireccional con trampilla que se le aplica a un mensaje de tamaño variable y proporciona un mensaje de tamaño fijo (Fuster, Hernández, Montoya, Muñoz, & Martín, 2012).

Teniendo Σ_{in} que representa una cadena de entrada y Σ_{out} que representa la cadena de salida. Cualquier función representada por la ecuación 1.5

$$h : \Sigma_{in}^{*} \rightarrow \Sigma_{out} \qquad (1.5)$$

Que puede ser computada eficientemente va a ser una función hash y genera valores hash de longitud n.

En esta definición el dominio de la función hash es Σ_{in}^{*} . En teoría la cadena de entrada puede ser de longitud infinita. En la práctica se asume una longitud máxima de la cadena de entrada n_{max} . En este caso la función hash es expresada como la ecuación 1.6.

$$h : \Sigma_{in}^{n_{max}} \rightarrow \Sigma_{out}^{n} \qquad (1.6)$$

Donde Σ_{in} y Σ_{out} son dos cadenas que típicamente son iguales.

En la figura 1.6 se representa el funcionamiento básico de una función hash.

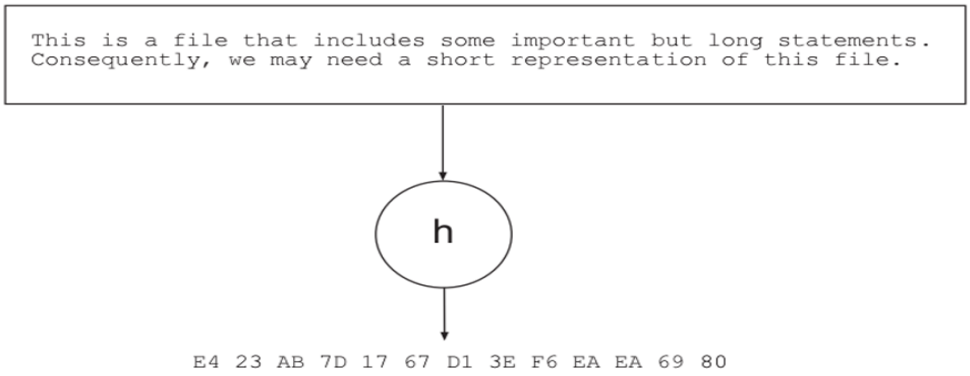

Figura 1. 6 Funcionamiento de una función hash
Descargada por el Autor

Las funciones hash deben tener las siguientes características (Fuster, Hernández, Montoya, Muñoz, & Martín, 2012):

- Dependencia de bits: el resumen de un mensaje o documento debe depender de todos los bits del mensaje de modo que si se cambia un único bit del mensaje su resumen debería cambiar por término medio en la mitad de sus bits.
- Resistencia a la preimagen: dado un resumen h debe ser computacionalmente obtener el mensaje M, es decir la función resumen debe ser difícil de invertir.
- Resistencia a la segunda preimagen: dado un mensaje cualquiera, M debe ser difícil encontrar otro mensaje diferente N cuyos resúmenes coincidan.
- Resistencia a colisiones: debe ser computacionalmente difícil encontrar una colisión, es decir, determinar dos mensajes distintos cualesquiera M y N cuyos resúmenes coincidan, es decir debe ser computacionalmente imposible encontrar dos mensajes diferentes cuyos resúmenes coincidan.

En el caso de no cumplir estas condiciones las funciones hash serían vulnerables.
Las funciones hash pueden ser atacadas por fuerza bruta, ataques a la preimagen y los ataques por colisión.

Función hash MD4 y MD5.

MD4 es la función precedente de MD5. MD4 proporciona un resumen de 128 bits para cualquier mensaje. Fue diseñada para que los ataques contra la misma precisaran de un esfuerzo computacional similar al de un ataque por fuerza bruta. Esta resistencia

significaba que encontrar dos mensajes distintos con el mismo valor resumen requiera de 2^{64} operaciones (ataque por colisión) y que encontrar un mensaje con un valor resumen predeterminado de antemano necesitará de alrededor de 2^{128} operaciones (ataques a la preimagen). Esta función ha sido rota desde hace varios años. MD5 al igual que MD4 proporciona como salida resúmenes de 128 bits. Esta función sigue siendo utilizada aunque se le han encontrado varias debilidades y su uso está desaconsejado (Fuster, Hernández, Montoya, Muñoz, & Martín, 2012).

Funciones SHA-0 y SHA-1.

La función SHA-0 se aplica a la versión original de la primera función SHA-1. Proporcionaba un resumen de 80 bits, esta fue retirada poco después de presentada porque se le descubrieron fallos significativos en su diseño (Fuster, Hernández, Montoya, Muñoz, & Martín, 2012).

La función SHA-1 proporciona un resumen de 80 bits y es la función resume más empleada en la actualidad debido a su empleo en los certificados digitales, aunque se le han encontrado algunas debilidades lo que la hace desaconsejable para aplicaciones de seguridad a medio o largo plazo (Fuster, Hernández, Montoya, Muñoz, & Martín, 2012).

SHA-2.

La familia SHA-2 contiene cuatro subalgoritmos SHA-224, SHA-256, SHA-384 y SHA-512 con resúmenes de 224, 256, 384 y 512 bits respectivamente. Aumentar la longitud de los resúmenes incrementa la seguridad de cada uno de ellos. Hasta el 2012 se empleaba con mayor frecuencia la función resumen SHA-1 debido a la incompatibilidad de SHA-2 con los protocolos existentes a pesar de que ofrece mayor seguridad (Fuster, Hernández, Montoya, Muñoz, & Martín, 2012).

1.8 Estándares de las Infraestructuras de clave pública

Los Estándares Criptográficos de Clave Pública fueron introducidos por la RSA Data Security para las entidades que desean una interfaz estándar con la criptografía de clave pública. Muchas organizaciones como *Apple, Microsoft, Digital, Lotus, Sun* y

Massachussets Institute of Technology han participado en su desarrollo pero solo la RSA *Data Security* toma la última decisión en su promulgación y revisión (Valdiviezo, 2013).

1.8.1 Estándares Criptográficos de Clave Pública (PKCS).

PKCS#1: es un estándar muy utilizado de la serie PKCS, los cuales son desarrollados y editados por *RSA Security* apoyado en desarrolladores de todo el mundo. Este estándar refiere un procedimiento para emplear el algoritmo RSA, para generar firmas digitales de mensajes sin codificar y cifrados, emplea la sintaxis precisada por la norma PKCS#7. Estas firmas se generan empleando la función hash al mensaje y cifrado de la huella digital derivada de la clave privada del firmante. Para encriptar mensajes en primer lugar se codifica con una clave simétrica la cual después es cifrada con una pública del destinatario del mensaje. PKCS#2 y PKCS#4 se han agregado a la PKCS#1 (Valdiviezo, 2013), (Delfs & Knebl, 2007).

PKCS#3 (Diffie-Hellman *Key-Agreement Standard*) refiere un procedimiento para realizar el intercambio de claves Diffie-Hellman (procert), (Valdiviezo, 2013).
PKCS#5 (*Password-Based Encryption Standard*) refiere un procedimiento para codificar mensajes con la clave secreta. Esto permite el envío cifrado de claves privadas entre dos computadoras como se refiere en el PKCS#8 (Valdiviezo, 2013).
PKCS#6 (*Extended-Certificate Syntax Standard*), refiere una sintaxis para certificados extendidos, es decir que permite extraer certificados X.509 de un superconjunto. También contienen propiedades como la dirección electrónica (Valdiviezo, 2013).
PKCS#7 (*Cryptographic Message Syntax Standard*) suministra una sintaxis general para la información que tenga una operación criptográfica asociada ya sea cifrado o firmado. Esta sintaxis es recursiva para que pueda incluir mensajes cifrados, también suministra un procedimiento para intercambiar certificados o listas de revocación de certificados, es decir que el PKCS#7 es compatible con varias diseños de gestión de claves basadas en certificados (Valdiviezo, 2013).
PKCS#8 (*Private-Key Information Syntax Standard*) muestra una sintaxis para los datos de la clave privada incluida en ellos, asi como un conjunto de propiedades y una sintaxis para las claves que se manejarán (Valdiviezo, 2013).

PKCS#9 (*Selected Attribute Types*) refiere varias propiedades para el empleo de los certificados extendidos, para los mensajes que son firmados digitalmente, para los datos de la clave privada y para los pedidos de firma de certificados (Valdiviezo, 2013).

PKCS#10 (*Certification Request Syntax Standard*) refiere la sintaxis para los pedidos de certificados, lo cual consiste en una denominación específica (*distinguished name)*, una clave pública y otras propiedades opcionales, todo esto firmado con la clave privada de quien hace el pedido. Este pedido se remite a una autoridad certificadora, la cual convierte ese pedido en un certificado X.509v3 o en uno extendido (Valdiviezo, 2013).

PKCS#11 (*Cryptographic Token Interface Standard*) puntualiza una interfaz de programación denominada *Cryptoki* para emplearla con unidades criptográficas de cualquier clase. *Cryptoki* tiene una orientación basada en objetos permitiendo que las aplicaciones ejecuten operaciones criptográficas sin saber la tecnología de los equipos (Valdiviezo, 2013).

PKCS#12 (*Personal Information Exchange Syntax Standard*) refiere la sintaxis para guardar en *software* las claves públicas del cliente, para resguardar sus claves privadas, los certificados y todo dato relacionado con la criptografía. Su propósito es el uso de un solo archivo de claves a las que se puede acceder desde cualquier aplicación (Valdiviezo, 2013).

PKCS#13 (*Elliptic Curve Cryptography Standard*) refiere un procedimiento de empleo de algoritmos de curva elíptica, la forma de producir y validar las medidas, las claves, el tipo de firma y cifrado, etc. Es similar a la PKCS#1 (Valdiviezo, 2013).

PKCS#15 (*Smart Card File Format*), nace para atender temas no incluidos en el PKCS#11. Pretende señalar la estructura de directorios y archivos de las tarjetas inteligentes (Valdiviezo, 2013).

1.9 Análisis de plataformas que permiten implementar una infraestructura de clave pública.

Existen varias plataformas que permiten implementar una infraestructura de certificación para garantizar la seguridad en las comunicaciones de una empresa.

1.9.1 OpenCA.

OpenCA es un software de código abierto (*opensource)* que implementa una autoridad de certificación robusta, utilizando los servicios provistos por otras aplicaciones de código abierto como OpenLDAP, OpenSSL, Apache y Apache mod_ssl.

OpenCA sigue los siguientes principios básicos:

- Adhesión a los estándares IETF.
- Evolución en base al *feedback* dado por los usuarios y desarrolladores.
- Disponibilidad del código manteniéndolo lo más "abierto" posible para que toda la comunidad colabore, tanto a través de su opinión como aportando posibles modificaciones al mismo.
- Interoperabilidad, ya sea por adherirse a los estándares así como para ajustarse a distintas plataformas y ambientes (Por ej: inclusión de Applets de JAVA para soportar Microsoft Internet Explorer, soporte para SCEP, entre otros).
- Uso de lenguajes de programación simples en la medida de lo posible, basándose en el principio de que la seguridad no está basada en la oscuridad, de modo tal que el código sea fácilmente legible (PERL fue elegido por su simplicidad y portabilidad).

OpenCA, por ser un software de código abierto, provee facilidades para modificar su funcionalidad de acuerdo a los requerimientos de cada infraestructura de clave pública.
Otro punto a tener en cuenta, es la posibilidad de configurar OpenCA para restringir el acceso a la interfaz de administración de cada módulo (AC y AR) de manera tal que sólo la persona que presenta un certificado con el rol de operador de dicho módulo pueda acceder al mismo y realizar únicamente las operaciones que le son permitidas (Díaz, y otros, 2006).

1.9.2 EJBCA.

EJBCA es un software de código abierto, escrito totalmente en Java. Permite implementar la infraestructura clásica de infraestructura de clave pública e incorpora

servicios avanzados como el sellado de tiempo y servidores de firmado (muy necesario para, por ejemplo, emitir facturas digitales desde múltiples puntos). Emplear EJBCA para implementar una infraestructura de clave pública permite emitir certificados para diferentes propósitos como (Paar & Pelzl, 2011):

- Autenticación.
- Firmas digitales.
- Seguridad en las comunicaciones con servidores SSL/TLS y clientes SSL/TLS.
- Tarjeta inteligente para el ingreso a Windows o Linux.
- Firmado y encriptación de correo electrónico encapsulado en MIME (SMIME).
- Uso de un solo certificado para garantizar la seguridad del acceso mediante contraseña a aplicaciones web.
- Creación de documentos firmados.
- Permite crear una infraestructura de clave pública móvil incluyendo iOS aportando seguridad a redes móviles como 3GPP/LTE/4G.
- Prevención de firmas falsas.

1.9.3 GnoMint.

GnoMint es un software de código abierto que permite gestionar y crear autoridades de certificación utilizados para cifrado y firmado de correos, acceso remoto VPN e identificación de páginas web seguras.

Pasos para crear un certificado usando GnoMint:

Una vez instalado y ejecutado el *software* aparece una ventana en la que aparecen las opciones que permiten crear un certificado dando click en la opción Certificate > Add > Self-signed CA.

Luego va a aparecer una nueva ventana pidiendo la información requerida por la CAs.
Una vez introducida la información necesaria aparece otra ventana pidiendo detalles sobre el certificado como:

- Tipo de clave privada: RSA o DSA.
- Longitud de la clave privada: 2048 es el valor por default
- Meses antes que el certificado expire: 240 es el valor por default, si se pone cero se entiende que el certificado no ha de expirar.

Luego de crear el certificado este va a ser registrado en la ventana principal.

GnoMint tiene varias versiones o revisiones. La revisión 1.2.0, por ejemplo, incluye una lista de certificados revocados (CRL) y permite la compilación en Windows (gnoMint, 2006).

La versión GnoMint 0.9.9 es capaz de importar CAs que han sido generados con el manejo de scripts incluidos en OpenSSL como CA.pl y openssl ca. Esta versión de GnoMint implementa un nuevo método de cifrado basado en AES que incluye protección de contraseñas y claves privadas al mismo tiempo que se garantiza la compatibilidad con los métodos de versiones anteriores (gnoMint, 2006).

1.9.4 OpenSSL.

Es un programa de código abierto que proporciona un entorno adecuado para cifrar los datos enviados a otra computadora dentro de una red y a su vez descifrarlos adecuadamente por el receptor, evitando así, el acceso a la información por intrusos con la utilización de *sniffers* (EcuRed).

El conjunto de herramientas OpenSSL es una característica de FreeBSD que ofrece una capa cifrada de transporte sobre la capa normal de comunicación, permitiendo la combinación con muchas aplicaciones y servicios de red (EcuRed).

El protocolo SSL (*Secure Sockets Layer*), permite un intercambio de información entre el servidor web y el navegador del usuario de forma segura. El objetivo de esta tecnología es permitir que solo el usuario autorizado pueda efectuar las operaciones. Mientras el protocolo HTTP utiliza un formato de dirección que empieza por http://, las direcciones en el protocolo SSL empiezan por https:// (EcuRed).

OpenSSL se emplea en la validación cifrada de clientes de correo, transacciones basadas en web para pagos con tarjetas de crédito y en muchos casos en sistemas que requieran seguridad para la información que se expondrá en la red (EcuRed).

Uno de los usos más comunes de OpenSSL es ofrecer certificados para usar con aplicaciones de software. Estos certificados aseguran que las credenciales de la compañía o individuo son válidas y no son fraudulentos. Si el certificado en cuestión no ha sido verificado por uno de las diversas "autoridades certificadoras", suele generarse una advertencia al respecto (EcuRed).

Ventajas de emplear el software OpenSSL**:**

- Seguridad Criptográfica: Establece una conexión segura entre dos partes (EcuRed).
- Interoperatividad: Intercambio en forma exitosa parámetros de cifrado sin tener conocimiento del código utilizado por el otro (EcuRed).
- Flexibilidad: Proporciona nuevos métodos de cifrado que evita la creación de un protocolo nuevo y la implementación de una nueva biblioteca de seguridad (EcuRed).
- Eficiencia: Incorpora ciertas facilidades que permiten mejorar el uso de la red (EcuRed).

1.9.5 Windows Server 2003.

Windows Server 2003 permite implementar una infraestructura de clave pública, instalando y configurando las CAs, permite la configuración de grupos y permisos de grupos, tiene la desventaja de ser un *software* propietario.

CAPÍTULO 2: PROPUESTA DE DISEÑO DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA PARA PYME.

2.1 Diseño de la infraestructura de clave pública

La infraestructura de clave pública se encarga de emitir certificados digitales para usuarios, *hosts* y servicios estableciendo una correspondencia entre la identidad del dueño del certificado con su clave pública. La elección entre una arquitectura con una única autoridad de certificación o jerárquica viene dada por las características de la comunidad donde será diseñada la infraestructura de clave pública, así como también los requerimientos que se hayan impuesto dentro de la organización donde se implementará (Valdiviezo, 2013).

2.1.1 Requerimientos iniciales

En el mundo existe una tendencia muy fuerte en los sectores en los que se intercambia información confidencial a subcontratar las infraestructuras PKI. Esta decisión prevalece por encima de la de gestionarlas internamente por la complejidad de los temas relacionados con el desarrollo de una PKI, la falta de especialistas en el tema y los tiempos de comercialización. Poner la seguridad criptográfica en manos de terceros es una falta irreparable para la seguridad de cualquier empresa con independencia del tamaño del proyecto. La decisión de desarrollo propio significa para Ecuador una tarea compleja donde se necesitan recursos y fuerza de trabajo altamente calificada pero es la decisión apropiada (Zanoletti, Jústiz, Díaz, & Nuñez, 2008). Por cuestiones fundamentalmente relacionadas con la criptografía como lo es la generación de las claves, y para poder garantizar la seguridad de la información es que se propone implementar una infraestructura de clave pública propia ya que se puede tener una mayor confianza en la fortaleza de las claves si estas han sido generadas internamente. De igual forma está el problema del almacenamiento seguro de la clave, si el proveedor guarda las claves que ha generado tiene la posibilidad de conseguir acceso a la información en cualquier momento (Zanoletti, Jústiz, Díaz, & Nuñez, 2008).

Por otra parte, con la compra a un tercero se corren riesgos como la entrada de código maligno en el programa, con el objetivo de inutilizar la aplicación en un momento

determinado, o la introducción de puertas traseras y debilidades en los algoritmos criptográficos, que permitan a un atacante ganar privilegios sobre el sistema y la información. Esto puede traer consecuencias graves, desde la afectación de los servicios que se estén brindando, hasta poner en riesgo la información de los usuarios (Zanoletti, Jústiz, Díaz, & Nuñez, 2008).

2.1.2 Descripción de la AC.

De acuerdo a las características de la empresa**,** y del estado actual de las infraestructuras de clave pública en el país, se decidió implementar una infraestructura de clave pública con una arquitectura jerárquica. Se va a configurar una autoridad de certificación raíz que va a encontrar *off-line* y una autoridad de certificación subordinada que va a formar parte de la red.

Este tipo de arquitectura permite generar autenticación a través de certificados digitales, brindando confiabilidad a los diferentes servicios de red; permite manejar políticas para crear, gestionar y revocar certificados digitales teniendo una idea básica para el manejo de los datos sensibles, los cuales deben ser protegidos mediante técnicas de encriptación (Valdiviezo, 2013).

La infraestructura de clave pública trabaja con el estándar X.509 para la implementación de los certificados digitales a través de la CA subordinada y dentro de una misma red, permitiendo el establecimiento seguro de la comunicación y el intercambio de información entre los usuarios que pertenecen al dominio de la empresa (Valdiviezo, 2013). Esta arquitectura permite la escalabilidad de la infraestructura de clave pública porque en la medida en que se implementen otras autoridades de certificación estas se van a poder añadir a la PKI. La arquitectura jerárquica va admitir la comunicación con otras infraestructuras de clave pública permitiendo así que cuando se implemente esta tecnología, de la que ya se han hecho varias investigaciones en el país, la PKI se comunique con estas otras infraestructuras.

2.2 Diagrama de la red.

2.2.1 Diagrama lógico de la red.

La red de la PYME seleccionada como caso de estudio, está estructurada en un Nodo Principal y tres sub-nodos; desde el punto de vista lógico presenta una topología de árbol-estrella. (Ver figura 2.1). Esta red cuenta con 6 servidores físicos, dos de ellos trabajan como servidores independientes y los otros 4 conforman un clúster ESX Server sobre el que corren 10 servidores virtuales.

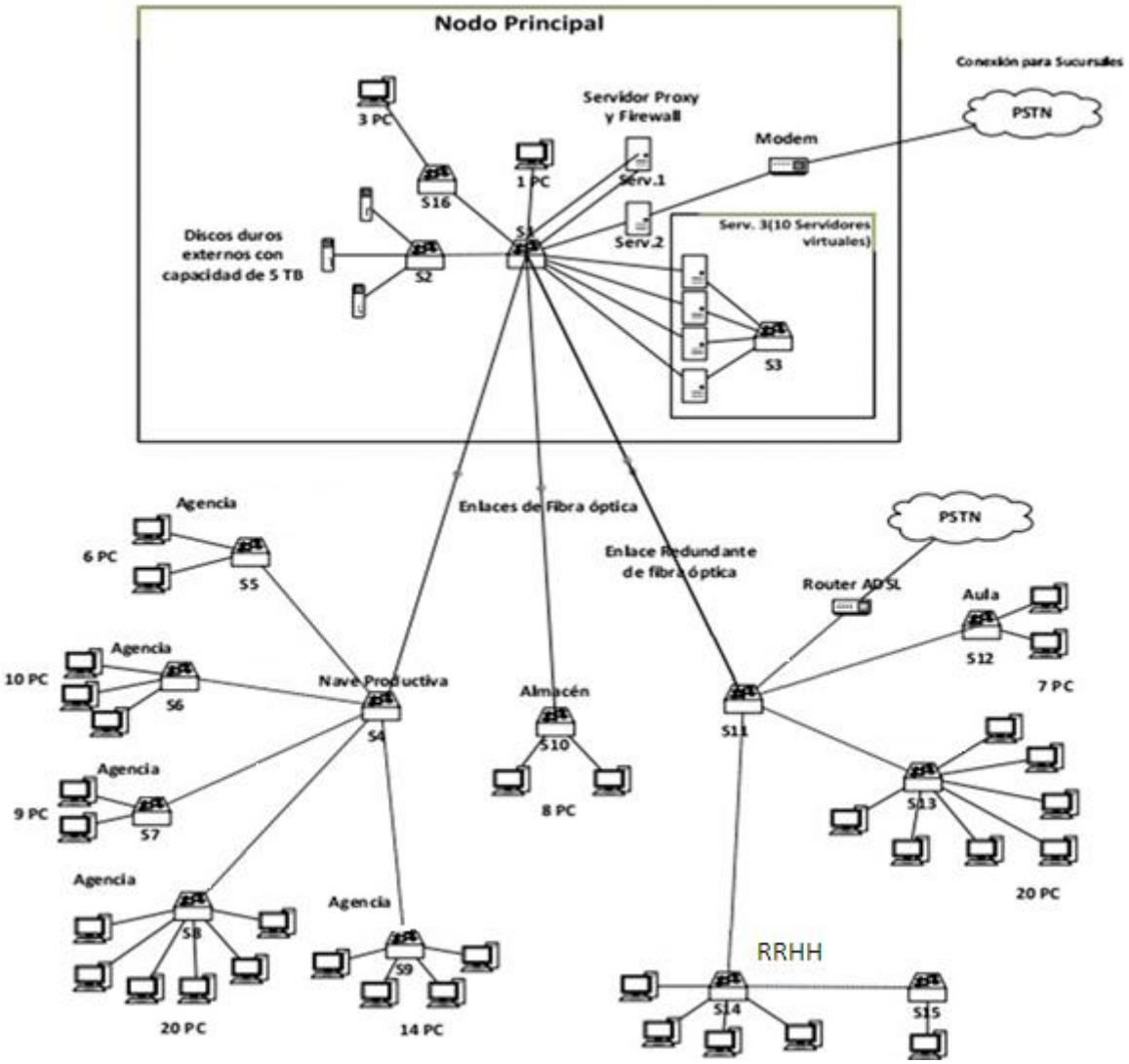

Figura 2. 1 Diagrama lógico de la red
Elaborada por el Autor

2.3 Propuestas de diseño lógico de infraestructura de clave pública en una PYME

Se propone configurar una autoridad de certificación raíz y ubicarla en el nodo principal, este servidor debe trabajar *off-line* y se recomienda que nunca haya estado conectado a Internet. A este servidor solo debe tener acceso el administrador de la red o de la infraestructura de clave pública y es de primordial importancia preservar su seguridad y controlar estrictamente el acceso a este debido a que si se compromete su seguridad toda la infraestructura estará comprometida.

La autoridad de certificación subordinada debe seguir normas similares de seguridad aunque en este caso sí trabajará conectada a la red, se debe restringir su acceso de modo que se pueda garantizar que su clave privada no será comprometida. Se propone ubicar la autoridad de registro en la oficina del administrador de la red. El esquema representado en la figura 2.2 muestra los cambios necesarios de la red actual de la empresa para implementar la infraestructura de clave pública.

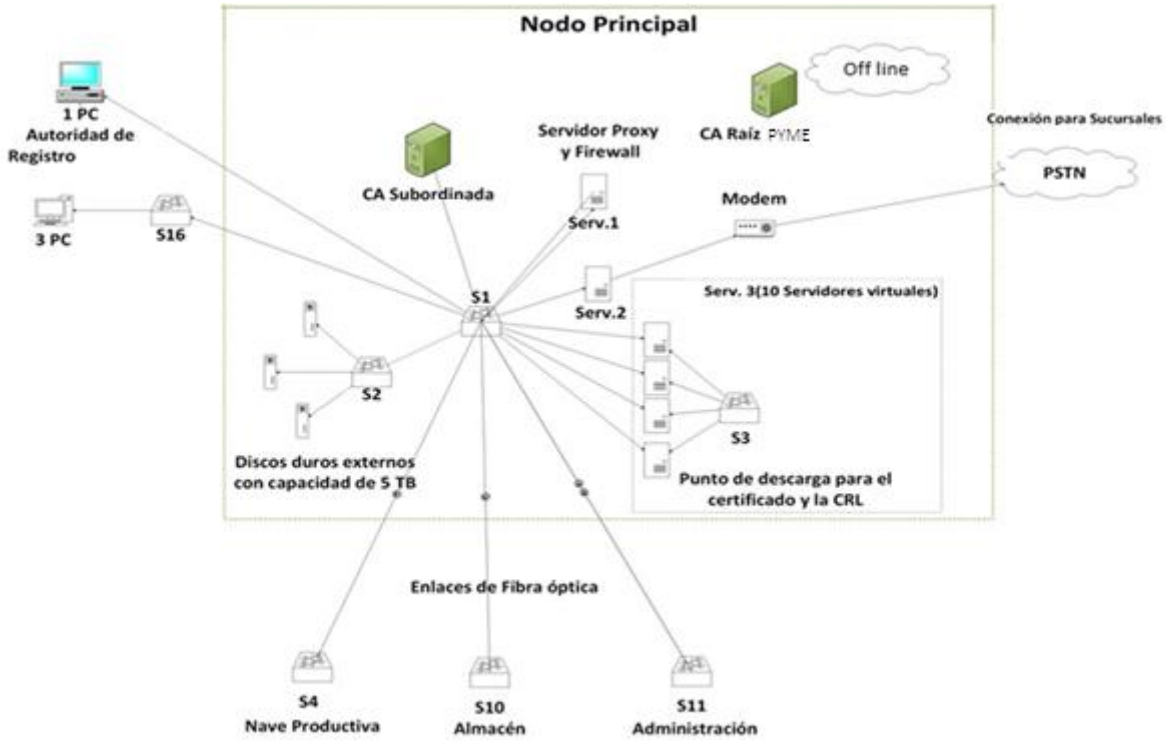

Figura 2. 2 Diagrama lógico propuesto para la infraestructura implementada.
Elaborada por el Autor

2.4 Propuestas de implementación de infraestructura de clave pública en una PYME

Se diseñaron dos propuestas para implementar una infraestructura de clave pública en la PYME; una de ellas se basa en el empleo del software libre realizando la configuración en el sistema operativo Ubuntu, basado en Debian. Para esta parte se empleó la herramienta OpenSSL para la emisión de certificados tanto para la autoridad de certificación raíz como para la autoridad de certificación subordinada. La otra propuesta se basa en el empleo de software propietario, realizando la configuraciones necesarias para implementar una infraestructura de clave pública sobre el sistema operativo Windows Server 2003.

2.4.1 Propuesta de infraestructura de clave pública con software libre

Linux es un sistema de libre distribución al encontrarse los ficheros y programas necesarios para su funcionamiento en servidores conectados a Internet. La tarea de reunir todos los ficheros y programas necesarios, configurarlos e instalarlos, puede ser complicada, por esto se dieron origen las distribuciones de Linux. Una distribución de GNU/Linux es una variante de ese sistema operativo que incorpora determinados paquetes de software para satisfacer las necesidades de un grupo específico de usuarios, dando origen a ediciones hogareñas, empresariales y para servidores. Pueden ser exclusivamente de software libre, o también incorporar aplicaciones o controladores propietarios (Valdiviezo, 2013).

Ubuntu está basado en Debian que es una distribución GNU/Linux y GNU/kFreeBSD. Es un sistema operativo completo, incluyendo el software y los sistemas para su instalación y gestión, todo ello basado en el núcleo Linux o FreeBSD y software libre (en especial del proyecto GNU).

Debian, ha tenido tanto éxito que, hoy en día, ha alcanzado un tamaño enorme. Las 11 arquitecturas que ofrece cubren 9 arquitecturas de hardware y 2 núcleos (Linux y FreeBSD). Por otra parte, con más de 14.500 paquetes fuente, el software disponible puede satisfacer casi cualquier necesidad de una empresa (Hertzog & Mas, 2013).

2.4.1.1 Configuración del servidor Apache

Apache es el servidor web más conocido y utilizado. De forma predeterminada, la instalación del paquete apache2 hace que también se instale la versión apache2-mpm-worker de Apache. El paquete apache2 es una coraza vacía que sólo sirve para asegurar que esté instalada alguna de las versiones de Apache (Barrios, 2014), (Hertzog & Mas, 2013).

Apache es un servidor modular y de mucha funcionalidad que está implementado por módulos externos que el programa principal carga durante su inicialización. La configuración predeterminada solo activa los módulos más comunes, pero activar nuevos módulos es simple como ejecutar *a2enmod módulo* (Hertzog & Mas, 2013); similarmente, se puede desactivar un módulo ejecutando *a2dismod módulo*. En realidad, estos programas sólo crean (o eliminan) enlaces simbólicos en /etc/apache2/mods-enabled/ que apuntan a los archivos en sí, almacenados en /etc/apache2/mods-available/ (Hertzog & Mas, 2013).

Con su configuración predeterminada, el servidor web escuchará en el puerto 80 (según se encuentra configurado en /etc/apache2/ports.conf) y servirá páginas del directorio /var/www/ según se encuentra configurado en /etc/apache2/sites-enabled/000-default) (Barrios, 2014), (Hertzog & Mas, 2013).

2.4.1.2 Configuración de Apache con soporte SSL/TLS.

Acerca de HTTPS

HTTPS es la versión segura del protocolo HTTP, inventada en 1996 por Netscape *Communications Corporation*. No es un protocolo separado de HTTP. Se trata de una combinación de este último con un mecanismo de transporte SSL o TLS, garantizando una protección razonable durante la comunicación cliente-servidor. Es ampliamente utilizado en la red mundial (www o *World Wide Web*) para comunicaciones como transacciones bancarias y pago de bienes y servicios (Barrios, 2014).

El servicio utiliza el puerto 443 por TCP para realizar las comunicaciones. El esquema URI (*Uniform Resource Identifier* o Identificador Uniforme de Recursos) es, comparando sintaxis, idéntico al de HTTP (http:), utilizándose como «https:»seguido del subconjunto denominado URL (*Uniform Resource Locator* o Localizador Uniforme de Recursos). Ejemplo: https://www.tesis.ec (Barrios, 2014)

Acerca de mod_ssl.

Mod_ssl es un módulo para el servidor HTTP Apache, el cual provee soporte para SSL versiones 2 y 3 y TLS versión 1. Es una contribución de Ralf S. Engeschall, derivado del trabajo de Ben Laurie (Barrios, Configuracion de Apache con soporte SSL/TLS, 2014). El paquete mod_ssl instala el archivo /etc/apache/conf.d/ssl.conf, que no es necesario modificar, puesto que se utilizarán archivos de inclusión, con extensión *.conf, dentro del directorio /etc/ apache/conf.d/, a fin de respetar la configuración predeterminada y poder contar con la misma, que es funcional, brindando un punto de retorno en el caso de que algo saliera mal (Barrios, 2014).

Con el siguiente comando se logra la instalación del paquete:

```
a2enmod ssl
```

Para habilitar SSL en el sitio**:**

```
a2ensite default-ssl
```

Se debe adecuar el sitio *default-ssl* para que tome los certificados creados y la conexión sea https

SSLCertificateFile /etc/apache2/**certificado.crt**
SSLCertificateKeyFile /etc/apache2/**clave.key**

2.4.1.3 Configuración de la infraestructura de clave pública.

Una vez que se ha accedido al sistema como el usuario *root* se crean los siguientes directorios:

```
mkdir /CA
mkdir /CA/clave
mkdir /CA/certificados
mkdir -m 0755 /CA/nuevoscertificados
mkdir -m 0755 /CA/crl                    (Linux)
```

- CA es el directorio de trabajo de la autoridad certificadora (Linux).
- certificados será el directorio donde se ubicarán los certificados (Linux).
- nuevos certificados es el directorio donde OpenSSL pone los certificados creados en formato PEM (sin encriptar) y en la forma [n° de serie].pem (por ejemplo: 15.pem) (Linux).
- crl es el directorio donde se coloca la lista de revocación de certificados (Linux).
- clave es el directorio donde se colocan las claves privadas (este directorio debe tener permisos extremadamente restrictivos, para que sólo sean leídos por el usuario *root*) (Linux).

Las extensiones de archivos que se generarán en estos directorios serán las siguientes (Linux):

- KEY: Claves privadas (deben tener permisos restrictivos) (Linux).
- CSR: Pedido de certificado (estos pedidos serán firmados por la CA para convertirse en certificados, luego pueden ser eliminados) (Linux).
- CRT: Certificado (puede ser distribuido públicamente) (Linux).
- PEM: Archivos que contienen tanto el certificado como la clave privada (deben tener permisos restrictivos) (Linux).
- CRL: Lista de revocación de certificados (puede ser públicamente distribuida) (Linux).

Para la configuración inicial de OpenSSL, se recomienda copiar el archivo de configuración por defecto de OpenSSL (openssl.cnf) al directorio /CA. En Ubuntu se encuentra en el directorio /etc/ssl/openssl.cnf (Linux):

```
cp /etc/ssl/openssl.cnf /CA
cp /etc/ssl/openssl.cnf /CA                    (Linux)
```

Luego se crean dos archivos que funcionan como bases de datos para OpenSSL (Linux):

```
touch /CA/index.txt
echo '01' > /CA/serial          (Linux)
```

Se debe crear una clave con algoritmo RSA de 2048 octetos y estructura x509, la cual se cifra utilizado Triple DES (*Data Encryption Standard*) permitiendo una inicialización normal con el servidor Apache, almacenado en formato PEM de modo que sea interpretable como texto ASCII. Se solicitará una clave de acceso para asignar a la firma digital, por lo que se recomienda utilizar una muy buena clave de acceso, la cual, mientras más complicada y difícil sea, mejor (Barrios, Configuracion de Apache con soporte SSL/TLS, 2014).

Con el siguiente comando se genera la clave privada. En la figura 2.3 se muestra lo que sucede al ejecutar el comando.

```
openssl genrsa -des3 -out clave/ca.key 2048
```

```
root@bambino:/CA# openssl genrsa -des3 -out clave/ca.key 2048
Generating RSA private key, 2048 bit long modulus
.....................+++
.....................................................+++
e is 65537 (0x10001)
Enter pass phrase for clave/ca.key:
Verifying - Enter pass phrase for clave/ca.key:
root@bambino:/CA#
```

Figura 2. 3 Generación de la clave privada
Descargada por el Autor

Si se utiliza este archivo (ca.key) para la configuración del anfitrión virtual, se requerirá de interacción del administrador cada vez que se tenga que iniciar, o reiniciar, el servicio apache, ingresando la clave de acceso de la firma digital. Este es el

procedimiento más seguro, sin embargo, debido a que resultaría poco práctico tener que ingresar una clave de acceso cada vez que se inicie el servicio Apache, resulta más conveniente generar una firma digital RSA, la cual permita iniciar normalmente y sin interacción alguna, al servicio Apache (Barrios, 2014), (PageGlimpse).

openssl rsa -in clave/ca.key -out clave/ca.pem

En la figura 2.4 se muestra las líneas de código generadas al ejecutar este comando.

```
root@bambino:/CA# openssl rsa -in clave/ca.key -out clave/ca.pem
Enter pass phrase for clave/ca.key:
writing RSA key
root@bambino:/CA#
```

Figura 2. 4 Generación de la clave privada RSA
Descargada por el Autor

A continuación, se genera el archivo CSR (*Certificate Signing Request*), el cual es el archivo de solicitud que se hace llegar a una RA (*Registration Authority* o Autoridad de Registro) quienes envían de vuelta un certificado firmado por dicha autoridad certificadora (PageGlimpse). (Ver figura 2.5)

openssl req -new -key clave/ca.key-out certificados/ca.csr

```
root@bambino:/CA# openssl req -new -key clave/ca.key -out certificados/ca.csr
Enter pass phrase for clave/ca.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ec
State or Province Name (full name) [Some-State]:Guayas
Locality Name (eg, city) []:SANTIAGO DE GYE
Organization Name (eg, company) [Internet Widgits Pty Ltd]:AUTORIDAD DE CERTIFI
ACION
Organizational Unit Name (eg, section) []:Pyme
Common Name (e.g. server FQDN or YOUR name) []:CA-Pyme
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
root@bambino:/CA#
```

Figura 2. 5 Certificado de solicitud
Descargada por el Autor

Luego de terminar la configuración inicial, se debe crear un certificado auto-firmado que será utilizado como el certificado del CA Pyme. Este será utilizado para firmar las solicitudes de certificados:

```
cd /CA
openssl x509 -req -days 730 -in certificados/ca.csr -signkey clave/ca.key –out certificados/ca.crt
```

La figura 2.6 muestra la información del certificado generado.

Figura 2. 6 Información del certificado generado
Descargada por el Autor

Se crearán dos archivos: certs/ca.crt, certificado de la CA públicamente disponible y con lectura para todos los usuarios; private/ca.key, clave privada del certificado de la CA, a pesar de que está protegida por una contraseña se debe restringir el acceso (Linux):

```
chmod 0400 /CA/private/ca.key        (Linux)
```

Una vez concluido los pasos anteriores se ha terminado de configurar la infraestructura de clave pública.

2.4.2 Propuesta con software propietario.

En este epígrafe se proporcionan instrucciones detalladas para generar una infraestructura de clave pública basada en Servicios de *Certificate Server de Microsoft Windows Server 2003*. El procedimiento incluye la instalación y configuración de las entidades emisoras de certificados (CA), la preparación del servicio de directorio *Active Directory* y de Servicios de *Internet Information Server* (IIS) de Microsoft y la configuración de la directiva de certificados de cliente.

2.4.2.1 Creación de los servidores.

En esta sección se describen las tareas básicas de preparación del hardware de servidor e instalación del sistema operativo. Se necesitan dos servidores: uno para la autoridad de certificación raíz y otro para la autoridad de certificación subordinada (TechNet, 2004).

Hardware del servidor de la autoridad de certificación raíz.

En la tabla 1.1 se muestra una especificación de hardware recomendada para la autoridad de certificación raíz, que se basa en la recomendaciones de hardware genéricas para Windows Server 2003 (Microsoft, 2004).

Tabla 2. 1 Especificación de software recomendada para el CA Raíz

CPU	Procesador a 733 MHz o superior
Memoria	256 MB
Interfaces de red	Ninguna (o deshabilitada)
Almacenamiento en disco	Controlador RAID (matriz redundante de discos independientes) IDE (electrónica integrada de dispositivos) o SCSI (interfaz estándar de equipos pequeños) 2 x 18 GB (SCSI) o 2 x 20 GB (IDE) configurados como volumen RAID 1 (unidad C) Medios de almacenamiento local extraíbles (CD-RW o cinta para copia de seguridad) Unidad de disco de 1,44 MB para la transferencia de datos

Fuente: (Microsoft, 2004)
Elaborada por el Autor

Gran parte de la garantía de seguridad de una autoridad de certificación depende de que no esté ni haya estado conectada a una red. Esto limita considerablemente la posibilidad

de que el equipo haya sufrido un ataque externo (ya que el atacante necesitaría algún tipo de acceso físico) (Microsoft, 2004).

Hardware del servidor de la autoridad de certificación subordinada.

Aunque existen requisitos de rendimiento para la autoridad de certificación, no son de gran importancia ya que, normalmente, la autoridad de certificación realizará pocas tareas en comparación con otros tipos de servidores. En este caso se puede aplicar el mismo criterio de calidad y confiabilidad que para seleccionar hardware para el servidor de autoridad de certificación raíz. Existen algunas diferencias pequeñas con la especificación de autoridad de certificación raíz en redes y almacenamiento, tal como se muestra en la tabla 1.2 (Microsoft, 2004).

Tabla 2. 2 Especificación de software recomendada para la CA subordinada

Elemento	Requisito
CPU	Procesador a 733 MHz o superior
Memoria	256 MB
Interfaces de red	2 tarjetas de interfaz de red (NIC) independientes, unidas para obtener mayor resistencia
Almacenamiento en disco	Controlador RAID IDE o SCSI 2 x 18 GB (SCSI) o 2 x 20-GB (IDE) configurados como volúmenes RAID 1 (unidades C y D) Medios de almacenamiento local extraíbles (CD-RW o cinta para copia

Fuente: (Microsoft, 2004)
Elaborada por el Autor

La especificación de servidor de esta tabla está ajustada a una población de 5.000 usuarios aproximadamente (Microsoft, 2004).

2.4.2.2 Configuración de la red (Microsoft, 2004).

La autoridad de certificación raíz no está conectada a la red (Microsoft, 2004). Se debe deshabilitar las interfaces de red en el sistema mediante **Conexiones de red** en **Panel de control** para impedir que se pueda tener acceso a la autoridad de certificación raíz a través de la red si se conecta a la misma por error (Microsoft, 2004).

La autoridad de certificación subordinada tiene una única interfaz de red (aunque se puede implementar uniendo dos tarjetas de red físicas para obtener una mayor resistencia). La interfaz de red se debe configurar con una dirección fija del Protocolo de Internet (IP) y otros parámetros de configuración de IP (puerta de enlace predeterminada, configuración de DNS, etc.), tal como corresponda a la red (Microsoft, 2004).

2.4.2.3 Instalación y configuración de Servicios de *Internet Information Server* (IIS)

IIS se utiliza para proporcionar puntos de descarga de CRL y certificados de autoridad de certificación para clientes que no utilicen Windows. Se recomienda no instalar IIS en la autoridad de certificación raíz. Aunque puede instalar IIS en la autoridad de certificación subordinada, un enfoque más seguro lo constituye el alojamiento de los puntos de descarga web para el certificado y la CRL de la autoridad de certificación en un servidor distinto de la propia autoridad de certificación. Es probable que exista un gran número de usuarios de certificados (internos y externos) que necesiten recuperar información de las listas CRL o la cadena de CA y no dispongan de permiso de acceso a la autoridad de certificación (Microsoft, 2004).

Instalación de Servicios de *Internet Information Server* en la CA subordinada PYME

IIS se instala con el administrador de componentes opcionales de Windows (al que se puede tener acceso mediante **Agregar o quitar componentes** del **Panel de control**). En la tabla 1.3 se enumeran los componentes que se deben instalar (Microsoft, 2004).

Tabla 2. 3 Componentes que deben instalarse

Componente	Estado de instalación
Servidor de aplicaciones	Seleccionado
Habilitar el acceso de red COM+	Seleccionado
Servicios de Internet Information Server	Seleccionado
Archivos comunes	Seleccionado
Administrador de servicios de *Internet Information Server*	Seleccionado
Servicio *World Wide Web*	Seleccionado

Fuente: (Microsoft, 2004)
Elaborada por el Autor

Para instalar IIS se ejecuta el comando (Microsoft, 2004)

```
sysocmgr /i:sysoc.inf /u:C:\MSSScripts\OC_AddIIS.txt    (TechNet, 2004)
```

Este comando indica al administrador de componentes adicionales que utilice las configuraciones de componentes especificada en el archivo de instalación desatendido C:\MSSScripts\OC_AddIIS.txt (TechNet, 2004):

```
[Components]
complusnetwork = On
iis_common = On
iis_asp = On
iis_inetmgr = On
iis_www = On                    (TechNet, 2004)
```

Para realizar la configuración de IIS para el acceso a la información de la autoridad de certificación (AIA) y la publicación de puntos de distribución de CRL (CDP) en la autoridad de certificación subordinada se debe crear un directorio virtual en IIS para utilizarlo como ubicación del protocolo de transferencia de hipertexto (HTTP) para los puntos de publicación de certificados y las CRL de la autoridad de certificación (denominados AIA y CDP, respectivamente) (Microsoft, 2004). Para crear un directorio virtual en IIS se deben seguir los pasos siguientes (Microsoft, 2004):

- Iniciar sesión en el servidor IIS (autoridad de certificación subordinada) con privilegios de administrador local.
- Crear la carpeta C:\CAWWWPub que contendrá certificados de autoridad de certificación y listas CRL (Microsoft, 2004).
- Establecer la seguridad en la carpeta con el explorador de Windows; en la tabla 2.4 se muestran los permisos que se deben aplicar. Los cuatro primeros ya deben aparecer (Microsoft, 2004).

Tabla 2. 4 Permisos que se deben aplicar a la carpeta CAWWWPub

Usuario/grupo	Permiso	Permitir o denegar
Administradores	control total	Permitir
Sistema	control total	Permitir
Propietarios del creador	Control total (sólo subcarpetas y archivos)	Permitir
Usuarios	Leer Listar el contenido de la carpeta	Permitir
IIS_WPG	Leer Listar el contenido de la carpeta	Permitir
Cuenta de invitado para Internet	Escritura	Denegar

Fuente: (Microsoft, 2004)
Elaborada por el Autor

- En la consola de administración de Servicios de *Internet Information Server* crear un nuevo directorio virtual en el siguiente sitio web predeterminado (Microsoft, 2004):
    - Al directorio virtual se le nombra infraestructura de clave pública, especificando C:\CAWWWPub como ruta de acceso.
- Se debe borrar la opción **Ejecutar secuencias de comandos (por ejemplo, ASP)** en los permisos de acceso al directorio virtual (Microsoft, 2004).

Comprobación del funcionamiento del directorio virtual de IIS.

- Se Inicia sesión en el servidor IIS (CA emisora) como miembro del grupo de administradores locales y se crea un archivo con un editor de texto como Bloc de notas (Microsoft, 2004). Se escribe algún texto reconocible. Por ejemplo: *Tesis Infraestructura de clave pública 2014.*
- Se debe guardar el archivo como test.htm en la carpeta que se creó para publicar la información de CDP y AIA en los pasos anteriores: C:\CAWWWPub (Microsoft, 2004).
- Si se abre cualquier explorador y se escribe la dirección URL http://10.30.6.101/pki/test.htm debe aparecer el texto *Tesis Infraestructura de clave pública 2014.* (Ver figura 2.7)

Figura 2. 7 Comprobación del funcionamiento del directorio virtual de IIS
Descargada por el Autor

2.4.2.4 Instalación y configuración de componentes de sistema operativo adicionales (Microsoft, 2004).

En esta sección se describe la instalación y configuración de los demás componentes que necesite el servidor (Microsoft, 2004). Se debe seguir estos procedimientos para los servidores de autoridad de certificación raíz y autoridad de certificación subordinada.

Preparación de *Active Directory* para la infraestructura de clave pública

Existen algunos requisitos fundamentales en la infraestructura de dominios de *Active Directory* para esta solución. Estos requisitos varían en función de si se instala la

solución en un entorno de *Active Directory* de *Windows 2000* o instalado inicialmente con *Active Directory* de *Windows Server 2003* (Microsoft, 2004).

Creación de un modelo de administración para la autoridad de certificación raíz y la autoridad de certificación subordinada.

Se realizó la configuración de un modelo de administración para la autoridad de certificación subordinada donde solo se utilizarán tres funciones: administrador de autoridad de certificación, auditor y operador de copia de seguridad. Estas funciones se muestran en la tabla 2.5 (Microsoft, 2004).

Tabla 2. 5 Funciones de administración de la PKI

Cuenta de usuario	Pertenencia a grupos de la cuenta de usuario
CAAdministrador	Administradores de infraestructura de clave pública de empresa Administradores de autoridad de certificación Administradores de certificados Administradores (administradores locales de la autoridad de certificación)
CAAuditor	Auditores de autoridad de certificación Administradores (administradores locales de la autoridad de certificación)
CARespaldo	Operadores de copia de seguridad de CA

Fuente: (Microsoft, 2004)
Elaborada por el Autor

Con esta disposición, la cuenta CAAdministrador podrá realizar todas las tareas administrativas en entidades emisoras de certificados de la empresa (incluida la aprobación y revocación de certificados) y tendrá el control administrativo de toda la información de configuración de infraestructura de clave pública de la empresa de *Active Directory* (Microsoft, 2004).

2.4.2.5 Instalación y configuración de la autoridad de certificación raíz.

Antes de configurar una autoridad de certificación raíz, se debe crear el archivo Capolicy.inf. Este archivo especifica las características del certificado de autoridad de certificación raíz, como la longitud de la clave, el período de validez del certificado, las ubicaciones de publicación de listas CRL y AIA, las directivas de certificados y la declaración de prácticas de certificados (CPS) (Microsoft, 2004).

La información de las CRL y AIA no se requiere para el certificado de autoridad de certificación en sí, de modo que los parámetros *CRLDistributionPoint* y *AuthorityInformationAccess* están definidos como Vacío en el archivo Capolicy.inf.

Creación del archivo CAPolicy.inf. (TechNet, 2004)
Escribir en un editor de texto, como Bloc de notas, el texto siguiente:

```
[Version]
Signature= "$Windows NT$"

[Certsrv_Server]
RenewalKeyLength=4096
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=8

[CRLDistributionPoint]
Empty=true

[AuthorityInformationAccess]
```

Empty=true (TechNet, 2004)

Como administrador guardar el archivo como C:\Windows\Capolicy.inf.

2.4.2.6 Instalación de componentes de software de servicios de *Certificate Server*

Iniciar sesión como miembro del grupo de administradores locales y en Panel de control, hacer clic en Agregar o quitar programas/Agregar o quitar componentes de Windows) (Microsoft, 2004).

- Seleccionar el componente **Servicios de *Certificate Server*** (Microsoft, 2004)**.**
- Seleccionar el tipo de autoridad de certificación como Autoridad de certificación raíz independiente y seleccionar la casilla de verificación. Utilizar la configuración personalizada mostrada en la figura 2.8 (Microsoft, 2004).

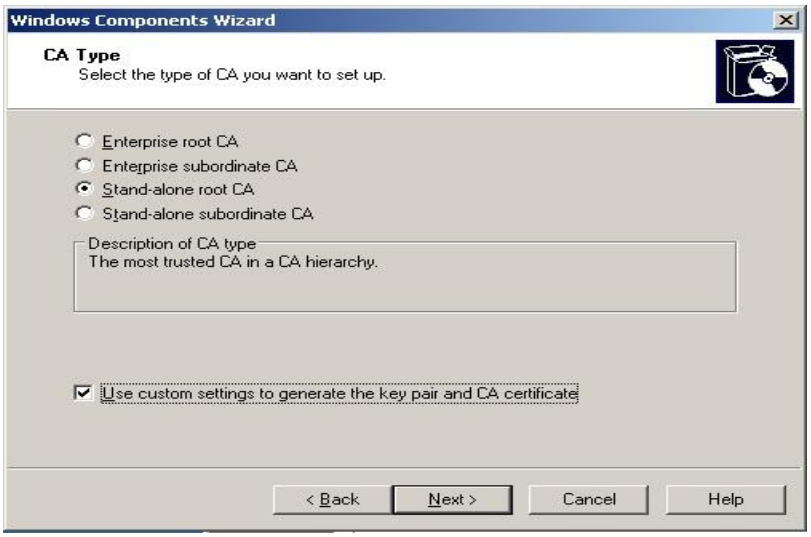

Figura 2. 8 Selección del tipo de CA
Descargada por el Autor

- En el cuadro de diálogo Pareja de claves pública y privada, dejar la configuración predeterminada, excepto para el valor de longitud de clave, que se debe establecer en 4096. El tipo de proveedor de servicios de cifrado debe ser *Microsoft Strong Cryptographic Provider*. (Ver figura 2.9) (Microsoft, 2004)

Figura 2. 9 Selección de CPS, del algoritmo de firma y longitud de la clave
Elaborada por el Autor

- La información de identificación de la autoridad de certificación de certificados se detalló como se indica a continuación (Ver figura 2.10):

  - Nombre común de autoridad de certificación: CA Raíz PYME.
  - Sufijo de nombre distintivo: DC=tesis2014, DC=ec (el nombre raíz de bosque de *Active Directory* de la organización) (Microsoft, 2004).
  - Período de validez: 8 años (Microsoft, 2004).

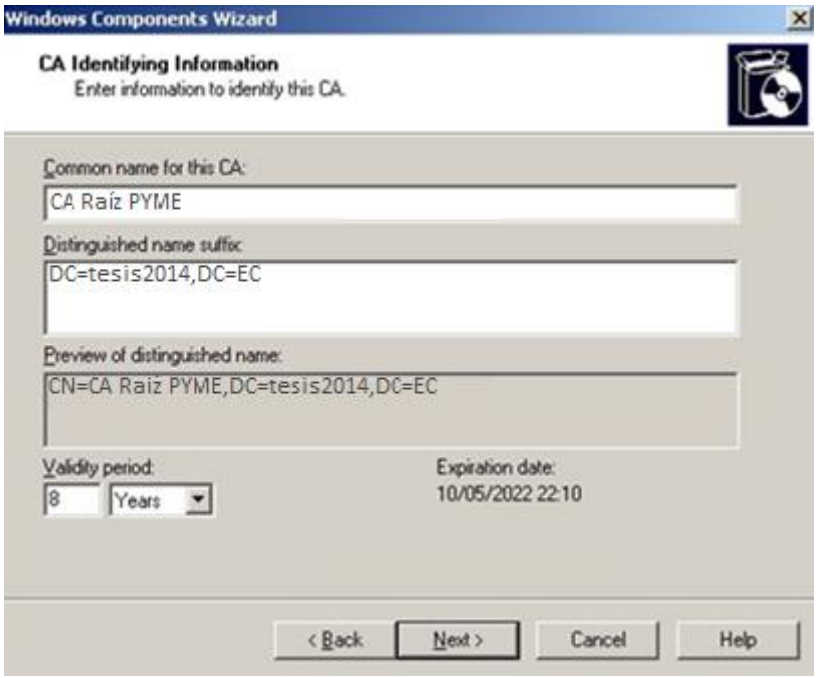

Figura 2. 10 Información de identificación de la CA
Descargada por el Autor

El CSP genera el par de claves, que se escribe en el almacén de clave de equipo local. Los valores predeterminados para la ubicación de la base de datos de certificados, los registros de base de datos y la carpeta de configuración se mantuvieron (Microsoft, 2004).

Comprobación de la instalación de la autoridad de certificación raíz.

Para comprobar que la instalación de la CA Raíz PYME ha sido correcta se siguen los siguientes pasos:

- Abrir la consola de administración Autoridad de Certificación (desde **Todos los programas**, **Herramientas administrativas**) y comprobar que se han iniciado los *Servicios de Certificate Server* y que puede ver las propiedades de la CA (Microsoft, 2004). (Ver figura 2.11)

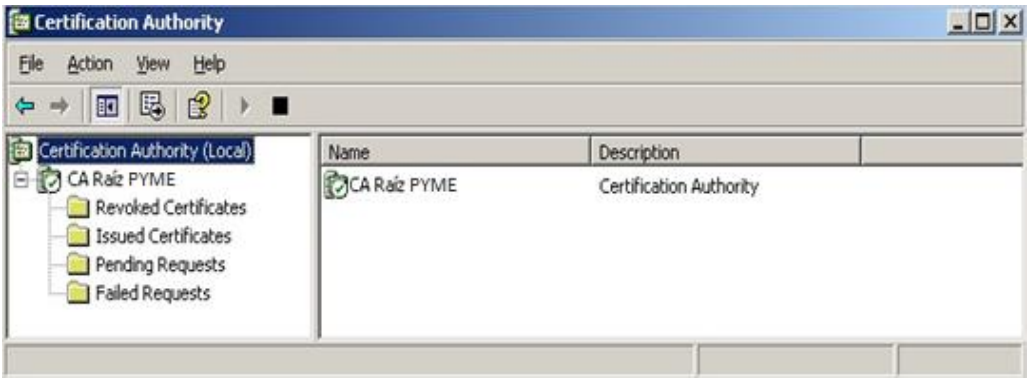

Figura 2. 11 Comprobación de la correcta instalación de la CA Raíz PYME
Descargada por el Autor

- En la ficha **General**, seleccionar el certificado de autoridad de certificación (**Certificado nº 0** en la lista) y, a continuación, hacer clic en **Ver certificado** (Microsoft, 2004)**.** (Ver figura 2.12)

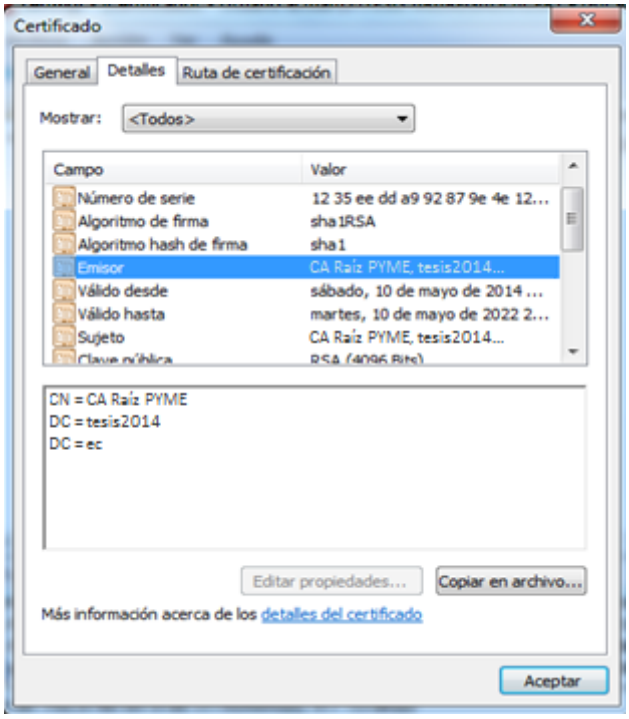

Figura 2. 12 Información del certificado generado
Descargada por el Autor

- Mediante la consulta de la ficha Detalles del certificado de la CA Raíz PYME se comprobó que los valores que se muestran coinciden con los especificados anteriormente.

2.4.2.7 Configuración de las propiedades de la CA Raíz PYME.

En el procedimiento de configuración de la CA Raíz PYME se aplican una serie de parámetros específicos del entorno. En la tabla 2.6 se muestran las propiedades de la CA Raíz PYME que se configuran.

Tabla 2. 6 Propiedades de la CA Raíz PYME

Propiedad de la CA	Descripción de la opción
Direcciones URL de punto de distribución de la CRL	Especifica las ubicaciones HTTP, LDAP y FILE desde las que se puede obtener una lista CRL actual. La ubicación FILE es una carpeta local que utiliza la autoridad de certificación para almacenar las listas CRL que emite. Los certificados que se emiten solo incluyen las ubicaciones HTTP y LDAP. La dirección URL de HTTP se muestra secuencialmente antes que LDAP, de modo que los clientes que utilicen certificados de la CA Raíz PYME no dependan de *Active Directory* para obtener listas CRL.
Direcciones URL de AIA	Ubicaciones donde se pueden obtener los certificados de la autoridad de certificación.
Período de validez	Período de validez máximo de los certificados emitidos (no es el mismo que el período de validez del certificado de autoridad de certificación, que se establece en CAPolicy.inf o mediante la CA Raíz PYME).
Período de la CRL	Frecuencia de publicación de la CRL.
Período de coincidencia de lista CRL	Período de coincidencia desde la emisión de una nueva CRL y la fecha de

	caducidad de la CRL anterior.
Período de diferencia entre listas CRL	Frecuencia de publicación de diferencia entre listas CRL (en la CA Raíz PYME la diferencia entre listas CRL está deshabilitada).
Auditoría de CA	Configuración de auditoría de CA. De forma predeterminada, toda la auditoría está habilitada.

Fuente: (Microsoft, 2004)
Elaborada por el Autor

Se debe copiar el certificado y la lista CRL de la CA Raíz para que se puedan publicar en *Active Directory* y en el servidor de publicación de certificados y las CRL de IIS. Luego se instala la autoridad de certificación subordinada, esto hará que todos los miembros del dominio (incluida la autoridad de certificación subordinada) importen el certificado de autoridad de certificación raíz a sus propios almacenes raíz y les permitirá comprobar el estado de revocación de los certificados emitidos por la autoridad de certificación raíz. (La CA subordinada debe poder comprobar el estado de revocación de su propio certificado antes de iniciar Servicios de *Certificate Server*) (Microsoft, 2004).

2.4.2.8 Instalación y configuración de la CA subordinada.

Durante el proceso de instalación, se produce un conjunto de interacciones complejas entre esta autoridad de certificación subordinada, la CA Raíz, Active Directory y el servidor Web. La figura 2.13 muestra interacciones principales entre sistemas distintos durante la instalación de la CA subordinada. Estas interacciones son (TechNet, 2004):

- Publicación de certificados y listas CRL de autoridad de certificación raíz en *Active Directory* (TechNet, 2004)
- Publicación de certificados y listas CRL de autoridad de certificación raíz en el servidor Web (TechNet, 2004)
- Instalación del software *Servicios de Certificate Server*, que genera una petición de certificados que debe trasladar a la autoridad de certificación raíz

en disco. En la autoridad de certificación raíz se emite el certificado para esa solicitud (TechNet, 2004).

- Instalación del certificado de la CA subordinada (TechNet, 2004).
- Publicación de certificados y listas CRL de CA subordinada en el servidor Web.

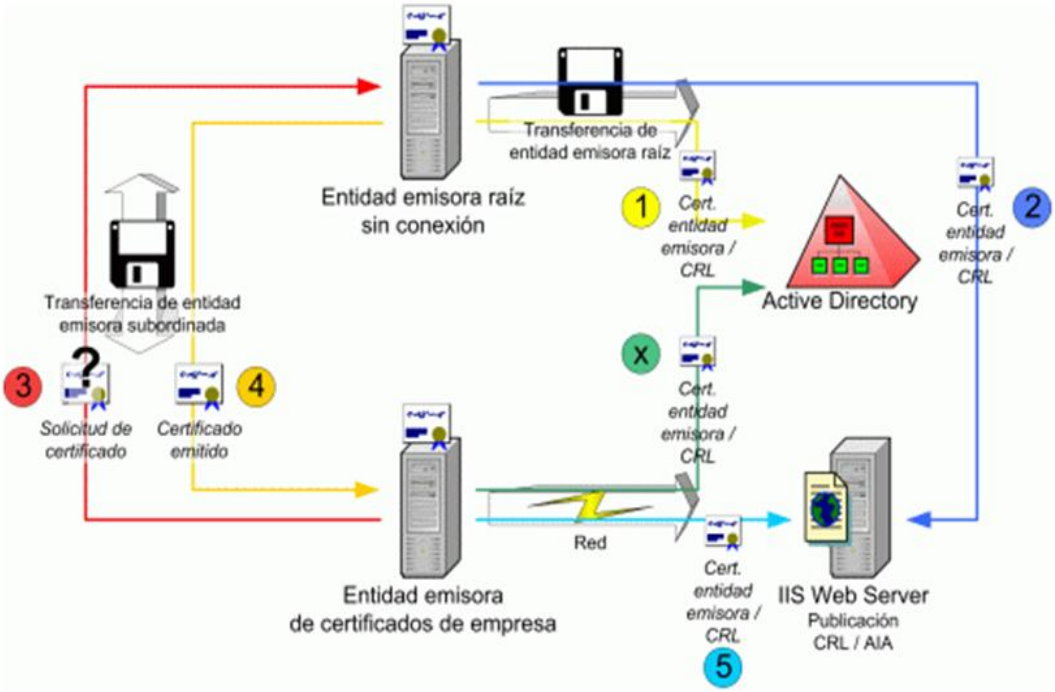

Figura 2. 13 Interacciones que ocurren durante la instalación de la CA subordinada
Fuente: (TechNet, 2004)

Para configurar la autoridad de certificación subordinada se sigue un protocolo semejante al de la configuración de la CA Raíz PYME.

Iniciar sesión como miembro del grupo de administradores locales y en Panel de control, hacer clic en Agregar o quitar programas/Agregar o quitar componentes de Windows (Microsoft, 2004).

- Seleccionar el componente **Servicios de *Certificate Server*** (Microsoft, 2004)**.**
- Seleccionar el tipo de autoridad de certificación como Autoridad de certificación subordinada de empresa y seleccionar la casilla de verificación. Utilizar la configuración personalizada mostrada en la figura 2.14.

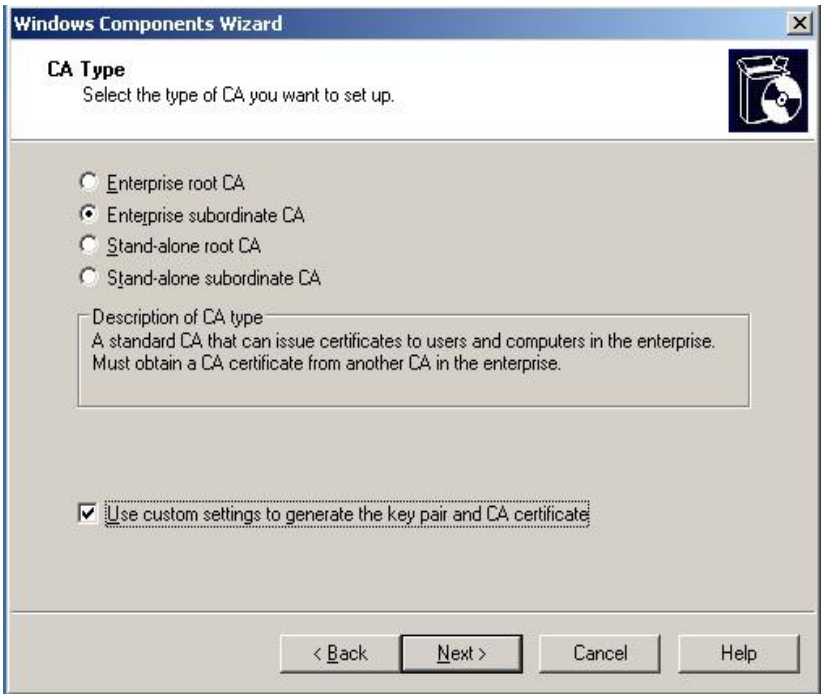

Figura 2. 14 Selección del tipo de CA
Descargada por el Autor

- En el cuadro de diálogo Pareja de claves pública y privada, dejar la configuración predeterminada, excepto para el valor de longitud de clave, que se debe establecer en 2048. El tipo de proveedor de servicios de cifrado debe ser *Microsoft Strong Cryptographic Provider* (Microsoft, 2004).
- La identificación de la autoridad de certificación se detalló como se indica a continuación (Ver figura 2.15):

  - Nombre común de autoridad de certificación: CA subordinada PYME.
  - Sufijo de nombre distintivo: DC=tesis2014, DC=ec (el nombre raíz de bosque de Active Directory de la organización) (Microsoft, 2004).

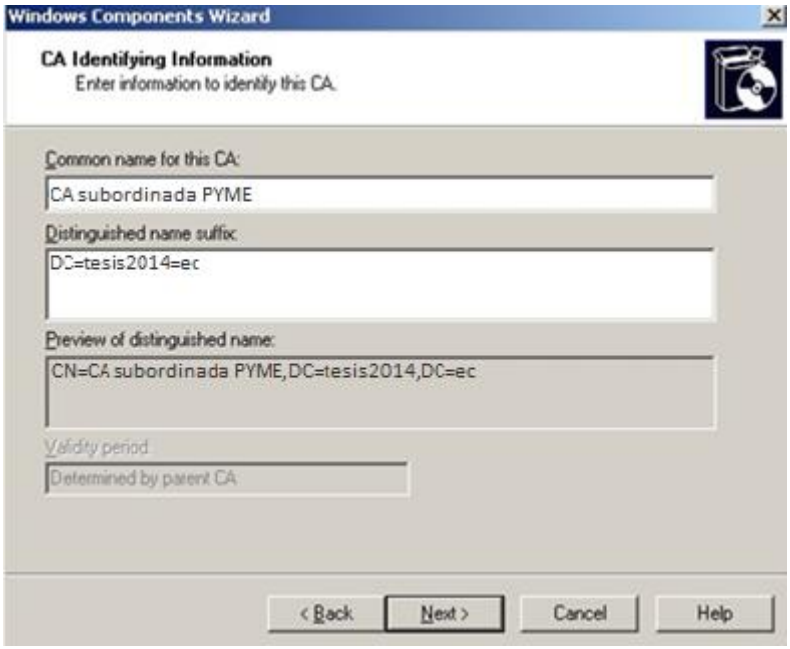

Figura 2. 15 Información de identificación de la CA
Descargada por el Autor

Durante la instalación y configuración de CA subordinada PYME se genera la petición de certificado a la CA Raíz PYME. Esta petición se guarda en un disco extraíble. (Ver figura 2.16)

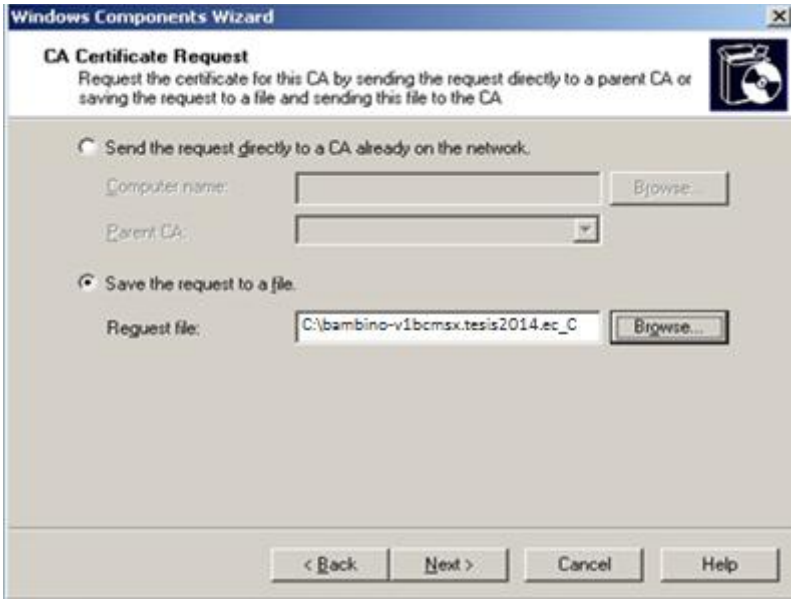

Figura 2. 16 Información de identificación de la CA
Descargada por el Autor

Luego aparece la opción de exportar el certificado y la clave privada. La figura 2.17 aparece el formato en que se va exportar el certificado.

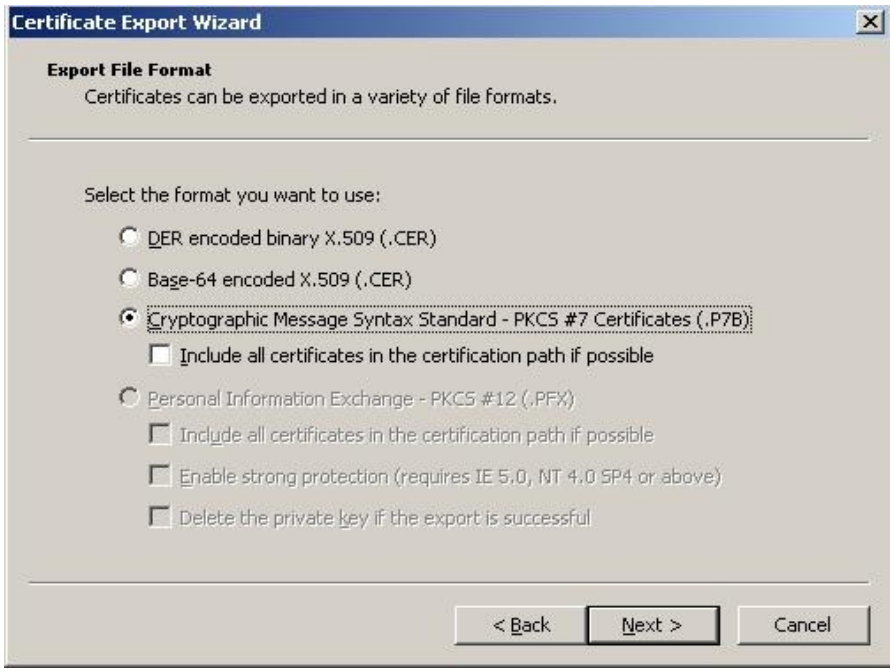

Figura 2. 17 Información de identificación de la CA
Descargada por el Autor

Comprobación de la instalación de la CA subordinada PYME.

Se siguen pasos similares para la comprobación de la instalación de la CA subordinada PYME. (Ver figura 2.18)

Figura 2. 18 Comprobación de la correcta instalación de la CA subordinada PYME
Descargada por el Autor

2.4.2.9 Envío de la petición de certificado a la autoridad de certificación raíz

La CA emisora debe enviar una petición a la CA Raíz PYME para que firme y emita un certificado para la CA subordinada PYME (Microsoft, 2004).

- Iniciar sesión en la autoridad de certificación raíz como miembro del grupo de administradores de certificados (Microsoft, 2004).
- En la consola de administración Autoridad de Certificación, en el menú Tareas de la autoridad de certificación, seleccionar Enviar solicitud nueva y, a continuación, enviar la petición transferida desde la CA emisora en un disco (Microsoft, 2004).
- El CA Raíz PYME requiere que se aprueben manualmente todas las solicitudes. Buscar la petición en el contenedor Peticiones pendientes de la MMC Autoridad de Certificación, comprobar que el campo Nombre común contiene el nombre de la CA subordinada y, a continuación, hacer clic con el botón secundario del mouse en la petición y en Emitir para aprobar la solicitud (Microsoft, 2004).
- Buscar el certificado recién emitido en el contenedor Certificados emitidos y abrirlo (Microsoft, 2004).
- Comprobar que los detalles de certificado sean correctos y, a continuación, hacer clic en Copiar al archivo para exportar el certificado a un archivo, guardar como archivo PKCS#**7** (Microsoft, 2004)

2.4.2.10 Instalación del certificado.

Ya puede instalarse la respuesta firmada (el paquete PKCS#7 que contiene el certificado) de la autoridad de certificación raíz en la CA emisora. Para publicar correctamente el certificado de autoridad de certificación en el almacén NTAuth de *Active Directory* (que identifica a la autoridad de certificación como autoridad de certificación de certificados de empresa), se debe instalar el certificado de autoridad de certificación mediante una cuenta que sea miembro tanto del grupo de administradores de infraestructura de clave pública de empresa como del grupo de administradores locales. El primer grupo tiene derechos para publicar el certificado en el directorio, mientras que el segundo tiene derechos para instalar el certificado de autoridad de

certificación en el servidor de autoridad de certificación (Microsoft, 2004). (Ver figura 2.19)

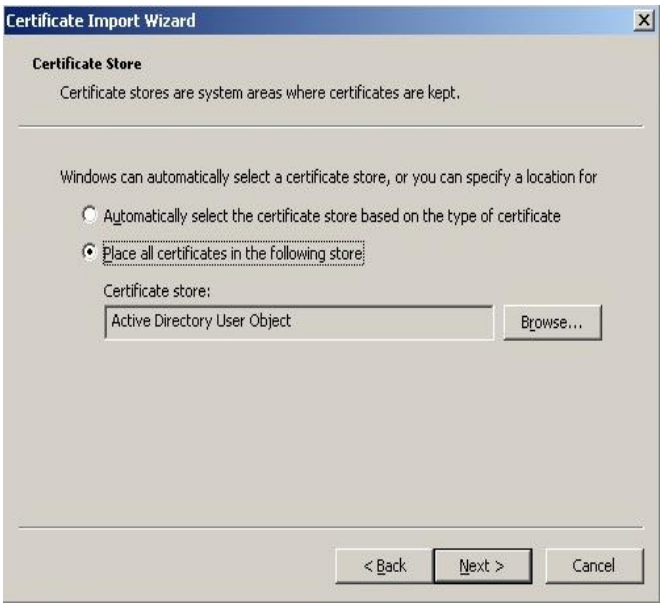

Figura 2. 19 Importación del certificado emitido por la CA Raíz PYME
Descargada por el Autor

2.5 Aplicaciones que permiten aprovechar las ventajas de infraestructura de clave pública

Existen varias aplicaciones que permiten aprovechar las ventajas de una infraestructura de clave pública.

- Web segura: en una intranet corporativa o en una extranet se pueden usar certificados para proporcionar seguridad fuerte mediante los protocolos SSL y TLS. Ambos protocolos proporcionan autenticación de cliente, autenticación de servidor y confidencialidad de datos (Valdiviezo, 2013).
- Correo seguro: el protocolo *Secure/Multipurpose Internet Mail Extensions* (S/MIME) también está basado en criptografía de clave pública y certificados. Este protocolo permite firmar y cifrar mensajes. Muchas aplicaciones de email proporcionan un sistema dual de claves para firmar y cifrar (Valdiviezo, 2013).
- Cifrado del sistema de ficheros: proporciona cifrado a nivel del sistema de ficheros. Como medida de seguridad, conviene que permita la recuperación de los datos por una persona adicional (Valdiviezo, 2013).

- Firma de código: protege contra descargas de código alterado (hackers) de sitios web (Valdiviezo, 2013).
- *Smartcard logon*: proporciona autenticación fuerte de dos factores (posesión de la *smartcard* y conocimiento del PIN (*Personal Identification Number*). A diferencia de las *passwords*, los PINs no se envían a través de la red, lo cual es una medida adicional de seguridad (Valdiviezo, 2013).
- *Virtual Private Network*: IPSec es un protocolo que funciona a nivel IP con certificados y se usa para autenticar los extremos de la comunicación (Valdiviezo, 2013).
- Actualmente cualquier aplicación puede aprovechar las ventajas que ofrece la implementación de PKI pues los fabricantes proporcionan APIs con las que se puede adaptar cualquier aplicación para que use la infraestructura de clave pública (Valdiviezo, 2013).

2.5.1 Implementación de una web segura.

Luego de la realización de la configuración de la infraestructura de clave pública, se realizó la certificación al acceso de una página web, empleando el protocolo SSL y el software OpenSSL, el cual viene incluido en el paquete de instalación del sistema operativo Ubuntu 12.04. Para realizar la certificación del sitio web se configuró un servidor Apache en la PC con sistema operativo Ubuntu y luego se configuró el servidor Apache con soporte para SSL. Para comprobar los resultados obtenidos se hicieron pruebas de acceso al sitio web desde otras PCs. Accediendo desde cualquier navegador hacia la página web se añade una excepción de seguridad. (Ver figura 2.20)

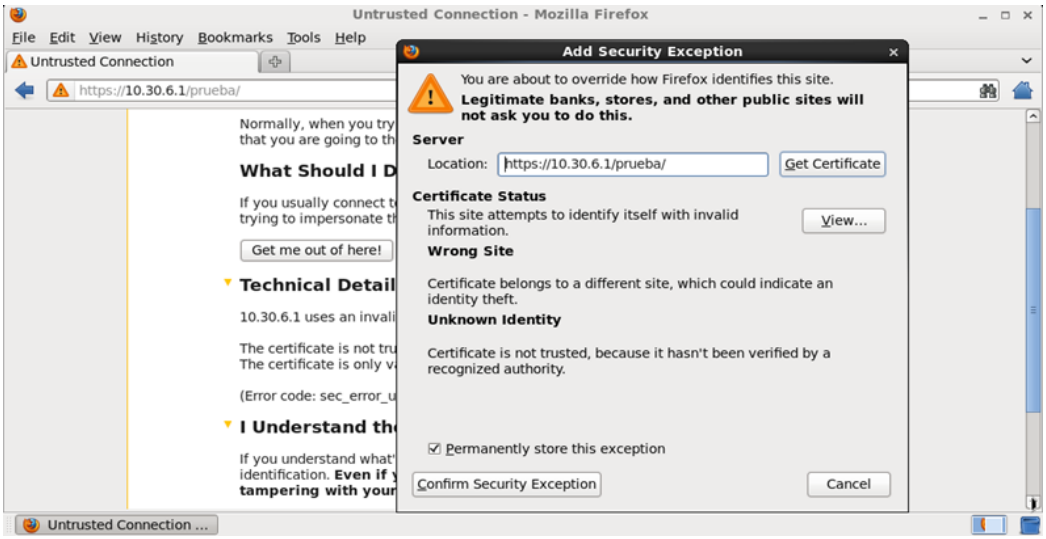

Figura 2. 20 Excepción de seguridad
Descargada por el Autor

En la figura 2.21 se muestra la información correspondiente a la página web.

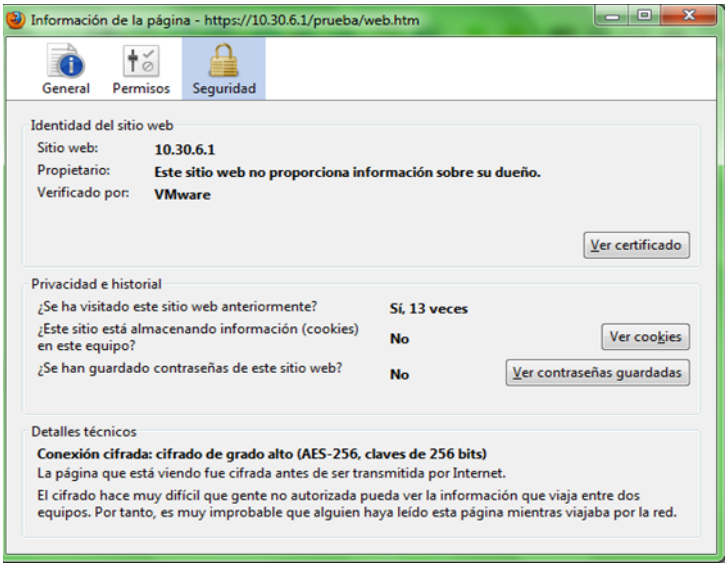

Figura 2. 21 Información correspondiente a la página web certificada
Descargada por el Autor

En la figura 2.22 se muestra la información del certificado generado.

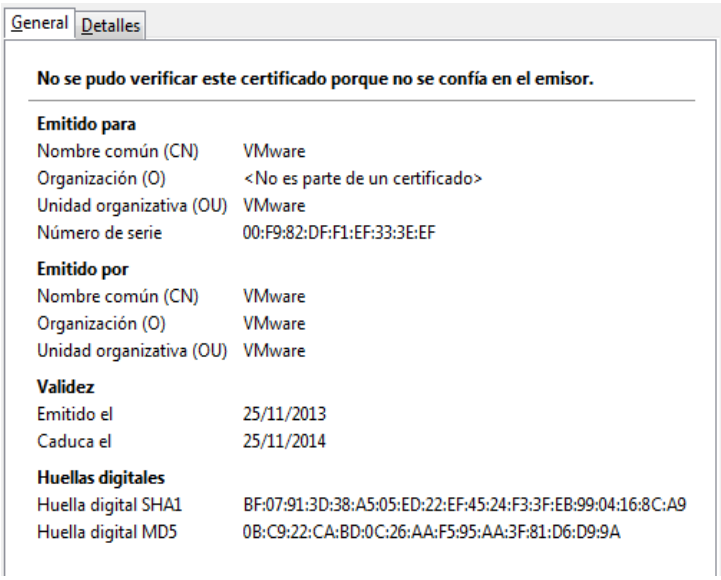

Figura 2. 22 Información correspondiente al certificado generado
Descargada por el Autor

CONCLUSIONES

- Con la finalidad de cumplir los objetivos específicos planteados para este trabajo de investigación se realizó un estudio del marco teórico general de los principales aspectos relacionados con la criptografía enfatizando en la rama de la criptografía asimétrica.
- Se efectuó una investigación profunda del funcionamiento de las Infraestructuras de Clave Pública.
- Se realizó un análisis comparativo de las diferentes herramientas que permiten la implementación de una infraestructura de clave pública.
- Se procedió a virtualizar un servidor Linux con distribución Ubuntu 12.04 y se realizaron las configuraciones necesarias para implementar una infraestructura de clave pública.
- También se virtualizó un servidor con Windows Server 2003 y configuración de la infraestructura de clave pública.
- Se procedió a seleccionar el método idóneo para implementar una infraestructura de clave pública en una PYME.
- De las diferentes alternativas de *software* se evaluaron dos soluciones: *Software* Libre y *Software* Propietario, validando cada una de ellas y eligiendo como la mejor opción el software libre OpenSSL por ser una de las alternativas que permite trabajar en comunidad, y tener a disposición todo el código fuente para evitar brechas de seguridad.
- Se escogió implementar una PKI con arquitectura jerárquica para darle escalabilidad a la infraestructura.
- De esta manera se consiguió cumplir el objetivo general planteado al implementar una Infraestructura de Clave Pública (PKI) en un ambiente virtualizado.

RECOMENDACIONES

- Se recomienda desarrollar la propuesta de infraestructura de clave pública para una PYME expuesta en este trabajo.
- Realizar las configuraciones pertinentes para implementar correo y FTP con PKI.
- Los fundamentos de la PKI justifican su empleo por instituciones que manejan información sensible en redes de comunicaciones, por el alto nivel de seguridad e integridad de la información que esta infraestructura provee.
- Implementar una infraestructura de clave pública para certificar e intercambiar información sensible por la red en una empresa es una vía compleja que exige mantener la seguridad en aquellos dispositivos en los que se almacenan las claves privadas pero al mismo tiempo es un método eficiente para garantizar la confidencialidad y la integridad de la información que viaja por la red.

BIBLIOGRAFIA

Alvarez, G. (Diciembre de 2010). *Sistemas de cifra con clave pública.* Obtenido de Intypedia: http://www.criptored.upm.es/intypedia/video.php?id=criptografia-asimetrica&lang=es

Barrios, J. (Junio de 2014). *Configuración de Servidores con GNU/Linux.* Obtenido de www.alcancelibre.org: http://www.alcancelibre.org/filemgmt/index.php?id=1

Blanco, E. (Mayo de 2014). *Diseño y desarrollo de una aplicación Android para el uso de identidades digitales, autenticación y firmas digitales en sistemas interactivos.* Obtenido de arantxa.ii.uam.es: http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20140519EvaMilagrosBlancoDelgado.pdf

Cánovas, O., Gómez-Skarmeta, A., López, G., & Martínez, G. (Enero de 2003). *UMU-PKIv6: Una infraestructura de certificación avanzada.* Obtenido de www.rediris.es: http://www.rediris.es/difusion/publicaciones/boletin/62-63/ponencia6.pdf

CryptoForge. (2013). *Seguridad de la información y algoritmos de encriptación.* Obtenido de www.cryptoforge.com.ar: http://www.cryptoforge.com.ar/encriptacion.htm

Delfs, H., & Knebl, H. (2007). *Introduction to Cryptography: Principles and Applications.* Berlin: Springer.

Díaz, F., Ambrosi, V., Luengo, M., Macía, N., Molinari, L., & Venosa, P. (Octubre de 2006). *Adaptando OpenCA para implementar una PKI para e-Science.* Obtenido de sedici.unlp.edu.ar: http://sedici.unlp.edu.ar/handle/10915/22017

Duran, R., Hernandez, L., & Muñoz, J. (2005). *El Criptosistema RSA.* Madrid: RA-MA EDITORIAL.

EJBCA. (Enero de 2014). *Open Source PKI Certificate Authority.* Obtenido de www.ejbca.org/: http://www.ejbca.org/

Ferguson, N., & Schneier, B. (2003). *Practical Cryptography.* Indianapolis: Wiley Publishing Inc.

Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography Engineering: Design Principles and Practical Applications.* Indianapolis: Wiley.

Fischer, S. (18 de Abril de 2008). *Analysis of Lightzeight Stream Ciphers.* Obtenido de infoscience.epfl.ch: http://infoscience.epfl.ch/record/115347/files/EPFL_TH4040.pdf

Fuster, A., Guia, D. d., Hernandez, L., & Montoya, F. (2004). *Técnicas criptográficas de protección de datos.* Madrid: RA-MA EDITORIAL.

Fuster, A., Hernández, L., Montoya, F., Muñoz, J., & Martín, J. (2012). *Criptografía, protección de datos y aplicaciones.* Obtenido de Ra-Ma. Instituto de Seguridad de la Información, Madrid: http://www.ra-ma.es/libros/CRIPTOGRAFIA-PROTECCION-DE-DATOS-Y-APLICACIONES/72641/978-84-9964-136-2

Gaines, H. (1989). *Cryptanalysis: A Study of Ciphers and Their Solution.* United States: Dover Publications.

ghacks.net. (30 de Julio de 2010). *Creating self-signed certificates with GnoMint.* Obtenido de www.ghacks.net: http://www.ghacks.net/2010/07/30/creating-self-signed-certificates-with-gnomint/

gnoMint. (15 de Septiembre de 2006). *gnoMint Certification Authority management made easy.* Obtenido de gnomint.sourceforge.net/: http://gnomint.sourceforge.net/

Hernandez, R. (Junio de 2009). *Certificados digitales.* Obtenido de drich1145.wordpress.com: https://drich1145.wordpress.com/certificados-digitales/

Hertzog, R., & Mas, R. (2013). *El libro del administrador de Debian.* Obtenido de debian-handbook.info: http://debian-handbook.info/browse/es-ES/stable/

Indra. (2005). *Infraestructura de clave pública (PKI).* Obtenido de www.incibe.es: https://www.incibe.es/extfrontinteco/es/pdf/Formacion_PKI.pdf

Koç, Ç. (2009). *Cryptographic Engineering.* Springer.

López, T. (2008). *Comunicación Personal: Infrestructura de Clave Pública.*

Lucena, M. (Marzo de 2002). *Criptografía y Seguridad en Computadores.* Obtenido de http://www.tierradelazaro.com/: http://www.tierradelazaro.com/public/libros/criptografia.pdf

Maiorano, A. (2010). *Criptrografia. tecnicas de desarrollo para profesionales.* Madrid: RA-MA EDITORIAL.

Menezes, A., vanOorshot, P., & Vanstone, S. (2011). *Handbook of Applied Cryptography.* CRC Press.

Montoya, F. (Octubre de 2010). *Sistemas de cifra con clave secreta.* Obtenido de Intypedia: http://www.criptored.upm.es/intypedia/video.php?id=criptografia-simetrica

ongei.gob.pe. (Diciembre de 2002). *Infraestructura de Llave Pública para el Estado Peruano (PKI) Framework.* Obtenido de www.ongei.gob.pe: http://www.ongei.gob.pe/publica/proyectos/4821.pdf

Oppliger, R. (2005). *Contemporary Cryptography* . Boston: Artech House Computer Security503.

Paar, C., & Pelzl, J. (2011). *Understanding Cryptography: A Textbook for Students and Practitioners.* Springer.

Ponce, V., Peñafiel, W., & Cobeña, C. (2005). *Implementación de un Web Site de Comercio Electrónico utilizando una infraestructura de red segura: Autoridad de Certificación, usando esquema PKI para generación de firmas digitales y certificados.* Obtenido de www.dspace.espol.edu.ec: https://www.dspace.espol.edu.ec/bitstream/123456789/3095/1/5612.pdf

procert. (s.f.). *Estandares aplicables en certificación electrónica.* Obtenido de www.procert.net.ve: http://www.procert.net.ve/documentos/estandar_certificacion.pdf

Ramos, M., & Lamadrid, A. (20 de Marzo de 2013). *Implementación de una infraestructura de clave pública (PKI). Caso de prueba en el Ministerio de Educación Superior.* Obtenido de www.inforedu.cu: http://www.inforedu.cu/documentos/Programa_Cientifico.pdf

Salomon, D. (2005). *Foundations of Computer Security.* London: Springer.

Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* Minneapolis: Wiley.

Smith, L. (1955). *Cryptography: The Science of Secret Writing.* United States: Dover Publications.

StDenis, T., & Johnson, S. (2006). *Cryptography for Developers.* Springer.

Talens-Oliag, S. (Noviembre de 2003). *Introducción a los certificados digitales.* Obtenido de www.uv.es: http://www.uv.es/sto/articulos/BEI-2003-11/certificados_digitales.pdf

Valdiviezo, T. (11 de Noviembre de 2013). *Análisis de la tecnología PKI y su aplicación en el aseguramiento de los servicios corporativos WWW, FTP y HTTP*. Obtenido de dspace.espoch.edu.ec: http://dspace.espoch.edu.ec/handle/123456789/2915

Vaudenay, S. (2006). *A Classical Introduction to Cryptography Applications for Communications Security.* Springer.

Zanoletti, G., Jústiz, D., Díaz, H., & Nuñez, Y. (2 de Diciembre de 2008). *Infraestructura de Clave Pública en Cuba. Sistema de Gestión de Certificados Digitales* . Obtenido de ccia.cujae.edu.cu. Convención Científica de Ingeniería y Arquitectura: http://ccia.cujae.edu.cu/index.php/siia/siia2008/paper/viewFile/1105/201

GLOSARIO DE TÉRMINOS

AES: Estándar Avanzado de Encriptación, del inglés Advanced Encryption Standard

API: Interfaz de Programación de Aplicaciones, del inglés Applications Programming Interface

CA: Autoridad de Certificación

CDP: Cisco Discovery Protocol

CPU: Unidad Central de Procesamiento

CRL: Lista de Certificados Revocados

DNS: Sistema de Nombre de Dominios, del inglés Domain Name System

DSA: Algoritmo de Firma Digital, del inglés Digital Signature Algorithm

ECC: Curvas Elípticas Criptográficas

GB: Giga byte

GPP: 3rd Generation Partnership Project

HTTP: Protocolo de Transferencia de Hipertexto, del inglés Hypertext Transfer Protocol

IDE: Dispositivos Electrónicos Integrados, del inglés Integrated Drive Electronics

IEC: Comisión Electrónica Internacional

IETF: Grupo Especial sobre Ingeniería de Internet, del inglés Internet Engineering Task Force

IIS: internet information server

iOS: Sistema Operative de iPod, touch iPad, iPhone.

IP: Protocolo de Internet

ISO: Organizacion Internacional para la Estandarización

ITU: Unión Internacional de Telecomunicaciones

LDAP: Lightweight Directory Access Protocol

LTE: Long Term Evolution

MB: Mega byte

NIC: Network Interface Card

PIN: Número de Identificación Personal

PKI: Infraestructura de Clave Pública

PKCS: Estándares de Criptografía de Clave Pública, del inglés Public Key Cryptography Standars

RA: Autoridad de Registro

RAID: Conjunto Redundante de Discos Baratos, del inglés Redundant Array of Inexpensive Disks

RSA: sistema criptográfico de clave pública proviene del nombre de sus creadores Rivest, Shamir y Adleman

SCSI: Interfaz de Sistemas de Computadoras Pequeñas, del inglés Small Computer System Interface

SHA: Algoritmo Resumen Seguro, del inglés Secure Hash Algorithm

S/MIME: Extensión de Correo de Internet de Propósitos Múltiples /Seguro, del inglés Secure/Multipurpose Internet Mail Extensions

SSL: Capa de Conexión Segura, del inglés Secure Sockets Layer

TLS: Seguridad de la Capa de Transporte, del inglés Transport Layer Security