REFERENCIA METODOLÓGICA PARA IMPLEMENTACIÓN DE SERVICIOS TELEMÁTICOS BASADOS EN IDENTIFICACIÓN DIGITAL

JOSÉ JULIÁN REINA MATERÓN

DIEGO MAURICIO PAZ CARRILLO

UNIVERSIDAD DEL CAUCA

FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

DEPARTAMENTO DE SISTEMAS

POPAYÁN - COLOMBIA

2006

REFERENCIA METODOLÓGICA PARA IMPLEMENTACIÓN DE SERVICIOS TELEMÁTICOS BASADOS EN IDENTIFICACIÓN DIGITAL

JOSÉ JULIÁN REINA MATERÓN

DIEGO MAURICIO PAZ CARRILLO

Documento Final de Trabajo de Grado para optar al título de:

Ingeniero en Electrónica y Telecomunicaciones

Director:

SILER AMADOR DONADO

Ingeniero de Sistemas

UNIVERSIDAD DEL CAUCA

FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

DEPARTAMENTO DE SISTEMAS

POPAYÁN - COLOMBIA

2006

... A ml Madre Amparo por enseñarme a luchar por lo que realmente se quiere a pesar de las dificultades y del sufrimiento que nos trae la vida

... A mi Padre José Otocar por su apoyo, por su paciencia y sabiduría

... A mi madrina Carmen por estar pendiente de mí, ser como una segunda madre y amiga

... A todas las personas y amigos que de alguna forma influenciaron en mí quien soy ahora

José Julián

... al poeta Víctor Daniel y a su musa de inspiración María Naín

... a mis hermanos Daniel Ricardo y Oscar Fernando

... a mis cuñadas

... al primer miembro de la segunda generación de la familia Paz Carrillo cuyo nombre no sabemos

Diego Mauricio

AGRADECIMIENTOS

Al ingeniero Carlos Enrique Serrano Castaño, por su apoyo y guía al principio y a lo largo del proyecto.

Al Grupo GNU/Linux de la Universidad del Cauca, por habernos permitido divulgar en sus espacios académicos parte de los avances del proyecto.

A la Red de Datos de la Universidad del Cauca, por habernos abierto las puertas para la realización de pruebas del prototipo del presente proyecto.

Al Grupo GNU/Linux de la Universidad Distrital, por habernos permitido divulgar los avances del proyecto en su evento Semana Linux de la Universidad Distrital.

A la Superintendencia de Industria y Comercio, quienes nos ayudaron con la información del estado del arte de la certificación digital en Colombia.

Al grupo de desarrollo de OpenCA, por habernos brindado la oportunidad de conocer el funcionamiento de una Entidad de Certificación gracias a las ventajas del software de código abierto.

Al grupo de desarrollo de RoundCube, por hacer un cliente de correo web tan usable y robusto.

A todas las personas que indirectamente colaboraron para que el presente proyecto se hiciera realidad.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

Las organizaciones están sufriendo un fuerte cambio en los diferentes procesos de comunicación electrónica. Los servicios telemáticos traidicionales están implantando mecanismos para garantizar la integridad, la aceptación, la confidencialidad y la autenticidad para el transporte de la información, por lo que no sólo basta que las comunicaciones sean eficientes, rápidas y confiables sino que se necesitan comunicaciones seguras donde cualquier mensaje de datos se encuentre firmado y avalado por un tercero de confianza. La sociedad de la información está exigiendo eliminar la suplantación de identidad y el anonimato, en el que se encuentra actualmente la mayoria de las redes.

La Referencia Metodológica para Implementación de Servicios Telemáticos basados en Identificación digital busca dar una aproximación global al problema de la ausencia de integración entre los Servicios Telemáticos basados en Identificación Digital y La Entidad de Certificación. La idea es ahincar esfuerzos para garantizar la identidad y la confidencialidad de los mensajes de datos, representados en los servicios telemáticos tradicionales.

Se espera que este esfuerzo sirva de guía para cualquier persona natural o jurídica que desee implementar una Entidad de Certificación o un Servicio de Identificación Digital, y se espera que su aplicación sea efectiva en los campos académicos, empresariales y gubernamentales colombianos.

PALABRAS CLAVES: Referencia Metodológica, PKI, Certificado Digital, Firma Digitales, Servicio Telemático basado en Identificación Digital.

ABSTRACT

Nowadays, communication between organizations are changing. Internet services are evolving in secure services. Trusted third-parties are required for achieving integrity, non-repudiation and confidenciality in any Digital Identification Based Telematic Service. Information society is asking for services that avoid identity suplantation and anonymity, the main feature of today's networks.

The "Referencia Metodológica para Implementación de Servicios Telemáticos basados en Identificación Digital" is a global solution for integrating Digital Identification Based Telematic Services and a Colombian Certification Entity. The project objective looks for a way of joining efforts for data identity and confidentiality achieving.

This project can be used as a guide for implementing either a Colombian Certification Entity or a Digital Identification Based Telematic Service in academy, enterprise and government.

KEYWORDS: Referencia Metodológica, Methodology, PKI, Digital Certificate. Digital Signature, Servicio Telemático basado en Identificación Digital, Digital Identification Based Telematic Service.

INTRODUCCIÓN

La seguridad es uno de los aspectos más importantes en la industria de las tecnologías de información. Debido al rápido crecimiento de la Internet y sus nuevas formas de realizar negocios, las organizaciones se encuentran experimentando presión al enfrentar los retos que la sociedad de la información impone y deben estar preparadas para realizar conexiones hacia el mundo externo con un mínimo de riesgos. Incluso dentro de éstas (las organizaciones), la información transportada, debe estar protegida de accesos no autorizados. Por consecuente, se requieren de métodos, tecnologías y metodologías que garanticen la integridad, confidencialidad y aceptación de la información.

Muchas tecnologías se encuentran disponibles en la actualidad para resolver parte de estos problemas, tal como la biometría, el ciframiento de la información o el uso de contraseñas y autenticación. La mayoría de estas soluciones son "islas" dentro del todo de un sistema de seguridad que quiera proveer servicios telemáticos de identificación digital, dejando en claro: “La seguridad debe estar diseñada e implementada desde una perspectiva de alto nivel”[1].

Entonces surge la pregunta. ¿Cómo se puede proveer confianza y confidencialidad en la internet desde una perspectiva de alto nivel? Para ésto, se requiere analizar las diferentes tecnologías vigentes en el mercado, y por ende al estudio y análisis de las Infraestructuras de llaves públicas (PKI)[2], la tecnología de seguridad más popular en la realización de transacciones de la Internet.

El proyecto "Referencia Metodológica para Implementación de Servicios Telemáticos basados en Identificación Digital" tuvo su origen al realizar un análisis del estado del arte de la certificación digital en Colombia y detectar una serie de falencias a nivel técnico y organizacional debido a la incapacidad para formular, desarrollar y evaluar un proyecto de implementación de servicios de identificación digital en el cual se logre integrar un entorno robusto de seguridad informática con la identificación de personas naturales o jurídicas por medio de servicios telemáticos en procesos de

1 JOHNER, Heinz; FUJIWARA, Seie y YEUNG, Amelia. Deploying a Public Key Infraestructure. Austin: IBM International Support Organization, 2000.

2 PKI es la infraestructura de seguridad utilizada para implementar servicios telemáticos basados en identificación digital

negocios tanto domésticos, como académicos o gubernamentales.

En el contexto de este trabajo se hablan de servicios telemáticos basados en identificación digital, servicios de identificación o servicios basados en certificados digitales, prácticamente se está hablando de lo mismo: un servicio software que es la punta del iceberg de una compleja infraestructura de seguridad hardware y software, cuyo objetivo es lograr la realización de algún tipo de transacción electrónica tratando de reducir al máximo la probabilidad de que ésta sea vulnerada.

Es así, como el presente proyecto de investigación busca estudiar el estado del arte sobre las distintas metodologías y tendencias filosóficas del conocimiento para plantear un referente que le pueda servir a cualquier persona interesada en que su PyME, o institución educativa pueda beneficiarse de las características de la tecnología de las infraestructuras de llaves públicas y los servicios que se pueden montar sobre éllas.

En su inicio, se recolectó información considerable, relacionada con los temas de criptografía, certificados digitales, normatividad relacionada con la identificación digital, estándares de seguridad y gestión de proyectos de desarrollo para analizarlos y poder darle al producto final la orientación idónea y así resolver el problema central de investigación, planteado en el anteproyecto.

Respecto a la metodología utilizada para realizar el presente proyecto de investigación, se utilizaron las corrientes filosóficas para generación y comprobación del conocimiento que son la base sobre la cual se fundamentan casi todas las corrientes metodológicas existentes hoy en día. Esta labor de análisis entre las filosofías del conocimiento, la ciencia y las metodologías de desarrollo de proyectos que prevalecen en la actualidad dió al proyecto la oportunidad de ser construido desde los cimientos, contrario a lo que hubiese sucedido si se utilizase alguna o algunas metodologías en particular como RUP (Rational Unified Process). Otro aspecto importante, es que en la presente referencia metodológica se ve reflejada una fuerte tendencia hacia la utilización de metodologías de desarrollo ágiles y flexibles, que se enfoquen en la explotación del personal como seres humanos y no como máquinas, donde la estrategia para dar un respuesta al problema de seguridad informática la formulará la persona que lea este documento a su libre voluntad y utilizando los elementos que del presente documento, considere necesarios.

En ese momento, se realizó la divulgación del conocimiento adquirido a través de conferencias en el espacio "Vive la vida Linux", organizado por el Grupo GNU/Linux de la Universidad del Cauca.

Dichas charlas estuvieron orientadas a que la comunidad académica se enterara acerca de la existencia de los diferentes tipos de criptografía, la existencia y uso de la firma digital, así como de los certificados digitales. Este tipo de eventos sirvieron como punto de partida para la posterior socialización de avances en el proyecto en eventos nacionales.

En la segunda parte del proyecto, se realizó el planteamiento inicial de una referencia metodológica dándole un enfoque dualista predictivo-adaptativo debido a su característica dualista hardware-software. Así fue como metodologías como ZOPP (Metodología para desarrollo de proyectos orientados a objetivos), XP (Programación extrema), Crystal, la Metodología para la Administración Total del Mejoramiento Continuo y el Modelo para Construcción de Soluciones fueron influenciando la filosofía del presente proyecto de investigación.

Otro punto clave en este punto fue la identificación total con los estándares abiertos y la filosofía del software libre. Las ventajas de trabajar en temas donde el conocimiento está al alcance de todos y donde no se da pie al ocultismo ni al oscurantismo garantiza en gran medida que el proyecto estuvo ideológica y tecnológicamente bien enfocado. Sin embargo, la referencia metodológica es independiente del proveedor del producto. Esto se hizo con el fin que pueda abarcar un campo de acción más amplio al que se había pensado inicialmente cuando se pensó únicamente en enfocarla hacia el software libre y/o de código abierto.

En la etapa final del proyecto se realizó la labor de validación de la referencia metodológica a través de un prototipo funcional en el cual se reunieron gran parte de los conceptos estipulados en la referencia metodológica inicial. Allí se hicieron pruebas con entidades de certificación de diferentes vendedores, se probaron mecanismos de autenticación, estrategias de seguridad perimetral, pruebas con algunos servicios de identificación digital tradicionales y algunos implementados por el equipo de trabajo. También en esta parte del proyecto se realizó la retroalimentación del proyecto, corrigiendo algunas percepciones iniciales del trabajo, eliminando actividades y agregando nuevas características.

Durante este periodo se realizó la divulgación de parte del conocimiento adquirido en el evento Cuarta Semana Linux de la Universidad Distrital a través de dos conferencias: una orientada a los ataques de denegación de servicio que puede sufrir una red de computadoras por medio de la utilización de *sniffers* y otra enfocada en la divulgación del conocimiento relacionado a mecanismos de autenticación y uso de tarjetas inteligentes en entornos abiertos.

Finalmente se realizaron las correcciones pertinentes a la referencia metodológica y la construcción del prototipo funcional completo, implementado con el servicio de correo electrónico seguro. Dicho prototipo fue construido utilizando la referencia metodológica y los documentos relacionados con la construcción de éste, se encuentran en los anexos del presente trabajo.

La bibliografía encontrada a través del presente proyecto de investigación es bastante heterogénea. Se podrán encontrar referenciados, desde libros de historia de las ciencias, hasta libros de gestión del conocimiento, pasando por los ya tradicionales estándares técnicos que son la base conceptual sobre la cual se fundamenta el presente proyecto de investigación. También vale la pena nombrar, la profunda influencia que tuvieron las leyes colombianas ya que fue sobre ellas, que se construyó la referencia metodológica. Las leyes dieron el marco de referencia sobre el cual el presente trabajo se debía mover; no se podían realizar tareas que no estuvieran contempladas por las leyes o que fueran en contravía de éllas.

El presente documento es el compendio de todas las experiencias laborales y académicas en torno a la temática de la seguridad informática y más precisamente los servicios de identificación digital. Fue un gran esfuerzo por sintetizar soluciones particulares en una gran solución general. Como se dijo en el anteproyecto, el objetivo no es solucionar todos los problemas relacionados con la certificación digital, sino, brindar un granito de arena en la identificación del problema, y tratar de dar una solución general a través de la presente referencia metodológica. Nosotros como equipo de trabajo, esperamos que el presente proyecto de investigación sea el punto de partida a que los bloques que forman este gran edificio de conocimiento den pie a otros proyectos de investigación de igual o mayor envergadura.

1. BASE CONCEPTUAL

1.1. INTRODUCCIÓN A LA CRIPTOGRAFÍA

PROPIEDADES DE UN SISTEMA DE SEGURIDAD

El requerimiento y principio básico para una solución que provea seguridad, deriva del siguiente concepto básico:

Los sistemas basados en computadoras son utilizados para procesar grandes cantidades de información de manera rápida, conveniente y confiable. La mayor parte de la información es importante para una persona en particular, o para una organización en general. Es por eso que los procesos basados en el transporte de información, se consideran críticos, ya que una persona, o una organización sufriría un daño invaluable si la información se pierde o llega de manera errónea a su destinatario[3]

Las características principales de un sistema de seguridad informática son[4]:

Autenticación

Autenticación es el proceso de verificar la validez de la existencia de un individuo dentro del sistema, e identificarlo. La autenticación no se encuentra limitada solo a seres humanos. Los servicios, aplicaciones y otras entidades pueden requerir de algún tipo de autenticación.

Autorización

Es también conocida como **Control de Acceso**. Es el proceso por medio del cual se asegura que cada usuario o entidad (servicio, aplicaciones) le sea permitido hacer solo lo que sea justo y necesario, sin arriesgar la seguridad del sistema.

Confidencialidad

La Información **sensible** no debe ser revelada a personas o entidades que no les corresponde. La Confidencialidad de los datos es también conocida como **privacidad** e involucra el concepto **cifrado de datos**.

---

3 SCHNEIER, Bruce. Applied Cryptography. Indianapolis: John Wiley & Sons, 1996.

4 NASH, Andrew y DUANE, William. PKI Infraestructura de Claves Públicas. Madrid: Mc. Graw Hill, 2003

Integridad

La integridad de la información se asegura que ésta no haya sido alterada o destruida por una persona o ente *no autorizado*.

Aceptación

Es también conocida como **No repudiación.** Es el proceso por medio del cual se asegura que no se niegue la autoría ni el acuse de recibo del mensaje por parte del emisor o el receptor. Este involucra el concepto de **Firma digital**.

TERMINOLOGIA

Emisor y Receptor

Supóngase que un emisor desea enviar un mensaje a un receptor. Además, este emisor desea enviar el mensaje de manera segura, es decir, que ningún tercero va a leer el mensaje.

Mensajes y Cifrado

El mensaje es un texto plano, el cual contiene la información a proteger. El proceso de convertir un mensaje en texto plano, a un mensaje que oculta la esencia de este, se le llama encripción. Al mensaje que ha sufrido el proceso de encripción se le llama Texto Cifrado. El proceso de volver un texto cifrado a su texto plano se le conoce como desencripción.

La ciencia de mantener a los mensajes seguros se le llama criptografía, y es practicado por los criptógrafos. Los criptoanalistas son los que practican el criptoanálisis, la ciencia de poder romper los textos cifrados. La rama de las matemáticas que encierra tanto a la criptografía, como al criptoanálisis, es la criptología y sus practicantes son los criptólogos. A partir de este momento al texto plano, se le denotara con la letra M, es decir, al mensaje que debe cifrarse. Este puede ser un flujo de bits, un texto plano, un mapa de bits, una voz digitalizada o cualquier información.

Al texto cifrado, lo denotaremos con la letra C. Este algunas veces puede tener el mismo tamaño de M, o en otras ocasiones no.

A la funcion de cifrado, la denotaremos con la letra E, es decir, es la funcion que opera a M, para obtener C. Es decir, en notación matemática:

$E(M) = C$

En el proceso contrario, el descifrado (el cual notaremos con la letra D) opera a C, para obtener M:

$D(C) = M$

De lo anterior se puede concluir la siguiente propiedad matemática acerca del cifrado y descifrado

de un texto plano:

D[E(M)] = M

Algoritmos y Llaves

Un algoritmo criptográfico, es una función matemática utilizada para cifrar y descifrar. Generalmente, hay dos funciones relacionadas, una para cifrar y otra para descifrar.

Si la seguridad de un algoritmo se basa en mantener el funcionamiento del algoritmo en secreto, es un algoritmo restringido (restricted algorithm). Los algoritmos restringidos han sido muy utilizados a través de la historia, pero hoy en día son incompatibles con los estándares establecidos. Los algoritmos restringidos no permiten ningún control de calidad o estandarización.

Es por eso, que este tipo de algoritmos son populares para aplicaciones que no necesitan mucha seguridad.

La criptografía moderna resuelve este problema, al utilizar una llave, la cual denotaremos con la letra K. Esta llave puede ser cualquier valor dentro de un rango. El rango de posibles valores de la llave es conocida como el espacio de llaves o keyspace. Tanto la encripción como la desencripción utilizan esta llave. Por ende, podemos decir:

Ek(M) = C

Dk(C) = M

El valor k denota la dependencia de la función de la llave.

Por ende, la propiedad 1 se podría reescribir así:

Dk[Ek(M)] = M

Algunos algoritmos utilizan diferentes llaves de cifrado y de descifrado. Así es que, para el ejemplo a continuación, la llave de cifrado la denotaremos como k1 y la llave de descifrado como k2. Entonces:

Ek1(M) = C

Dk2(C) = M

Dk2[Ek1(M)] = M

Por lo tanto toda la seguridad en estos algoritmos se encuentra basada en la llave, no en los detalles del algoritmo. Esto quiere decir que el algoritmo puede ser publicado y analizado. Se pueden crear productos que utilicen el algoritmo sin importar que un atacante conozca el funcionamiento del algoritmo, si este no conoce la llave de cifrado, no podrá leer el mensaje.

Un criptosistema es un algoritmo, más todos los posibles textos planos, más los textos cifrados y las llaves

ALGORITMOS SIMÉTRICOS

Existen dos tipos generales de algoritmos de cifrado, basados en llaves. Los algoritmos simétricos y los algoritmos de llave pública o asimétricos. Los algoritmos simétricos, o también conocidos como convencionales son algoritmos donde la llave de cifrado puede ser calculada de la llave de descifrado y viceversa. En la mayoría de los algoritmos simétricos la llave de cifrado y de descifrado son la misma. Estos algoritmos, también conocidos como algoritmos de llave privada, requieren de un acuerdo entre el emisor y el receptor acerca del valor de la llave, antes de realizar una comunicación segura. La seguridad de un algoritmo simétrico reside en la llave, divulgar la llave significa que cualquiera puede cifrar o descifrar el mensaje, lo cual significa que si la comunicación se quiere mantener en secreto, también se debe mantener en secreto la llave. La encripción y desencripción de un algoritmo simétrico es denotado de la siguiente forma:

$Ek(M) = C$

$Dk(C) = M$

Los algoritmos simétricos se encuentran divididos en dos categorías. Algunos operan los mensajes en texto plano bit a bit o byte a byte. Estos algoritmos son conocidos como algoritmos simétricos de flujo. Cuando los algoritmos operan por grupos de bits, a los cuales se les conoce como bloques, se les conoce como algoritmos simétricos de bloque.

Para los algoritmos de computación moderna, un bloque típico es de 128 bits, lo suficientemente grande para implicar un arduo trabajo de criptoanálisis y lo suficientemente pequeño para ser trabajable por el hardware disponible hoy en día en el mercado.

ALGORITMOS DE LLAVE PÚBLICA

Los algoritmos de llave pública, también conocidos como algoritmos asimétricos están diseñados de tal manera que la llave que es utilizada para cifrar es diferente de la llave utilizada para descifrar. Además, la llave de descifrado no puede ser calculada de la llave de cifrado. Los algoritmos son llamados de “llave pública” porque la llave de cifrado puede ser pública. Un completo extraño puede usar la llave de cifrado para cifrar el mensaje, pero sólo la persona adecuada puede descifrarlo con la llave de descifrado. En estos sistemas, a la llave de cifrado se le conoce como llave pública y a la llave de descifrado se le conoce como llave privada. Suponiendo que k1 es la llave pública y k2 es

la llave privada, entonces:

$Ek1(M) = C$

$Dk2(C) = M$

o también podríamos decir:

$Ek2(M) = C$

$Dk1(C) = M$

Lo cual significa que se puede cifrar un mensaje con la llave privada y se puede descifrar con la llave publica. Esto es muy útil cuando se va a trabajar con firmas digitales.

1.2. EL ESTÁNDAR PKIX

En criptografía, una infraestructura de clave pública (o, en inglés, PKI, Public Key Infrastructure) es una combinación de hardware y software, políticas y procedimientos que permiten asegurar la identidad de los participantes en un intercambio de datos usando criptografía pública.

El termino PKI se utiliza para referirse tanto a la autoridad de certificación y al resto de componentes, como para referirse, de manera más amplia y a veces confusa, al uso de algoritmos de clave pública en comunicación electrónicas. Este último significado es incorrecto, ya que no se requieren métodos específicos de PKI para usar algoritmos de clave pública.

Propósito y Funcionalidad

Una PKI permite a los usuarios autenticarse frente a otros usuarios y usar la información de los certificados de identidad (por ejemplo, las claves públicas de otros usuarios) para cifrar y descifrar mensajes. En general, una PKI consiste en un software para los clientes, un software de servidor (como una autoridad de certificación), hardware (por ejemplo, tarjetas inteligentes o smartcards) y unos procedimientos operacionales. Un usuario puede firmar digitalmente mensajes usando su clave privada, y otro usuario puede validar dicha firma (usando la clave pública del usuario contenida en el certificado que ha sido emitido por una autoridad de certificación de la PKI). Esto permite a dos (o más) entidades establecer una comunicación que garantiza la confidencialidad y la integridad del mensaje y la autenticación de los usuarios sin tener que intercambiar previamente ninguna información secreta.

Componentes

Los componentes habituales de una infraestructura de clave pública son:

* La autoridad de certificación (o, en inglés, CA, Certificate Authority): es la encargada de emitir y revocar certificados. Es la entidad de confianza que da legitimidad a la relación de una clave pública con la identidad de un usuario o servicio.

* La autoridad de registro (o, en inglés, RA, Registration Authority): es la responsable de verificar el enlace entre los certificados (concretamente, entre la clave pública del certificado) y la identidad

de sus titulares.

* Los repositorios: son las estructuras encargadas de almacenar la información relativa a la PKI. Los dos repositorios más importantes son el repositorio de certificados y el repositorio de listas de revocación de certificados. En una lista de revocación de certificados (o, en inglés, CRL, Certificate Revocation List) se incluyen todos aquellos certificados que algún motivo han dejado de ser válidos antes de la fecha establecida.

* La autoridad de validación (o, en inglés, VA, Validation Authority): es la encargada de comprobar la validez de los certificados digitales.

* La autoridad de sellado de tiempo (o, en inglés, TSA, TimeStamp Authority): es la encargada de firmar documentos con la finalidad de probar que existían antes de un determinado instante de tiempo.

* Los usuarios y entidades finales son aquellos que poseen un par de claves (pública y privada) y un certificado asociada a su clave pública. Utilizan un conjunto de aplicaciones que hacen uso de la tecnología PKI (para validar firmar digitales, cifrar documentos para otros usuarios, etc.)

La siguiente figura muestra la arquitectura general de una Infraestructura de Llaves Públicas, según el RFC 2459.

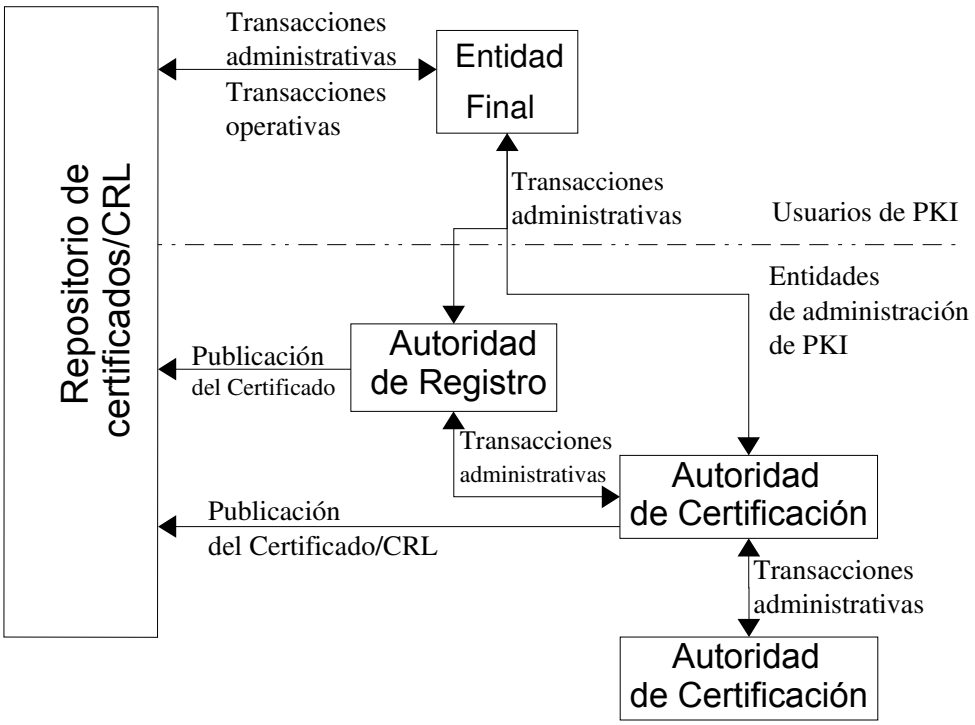


Figura 1. Arquitectura PKI

Algunas Implementaciones de PKI

Algunas de las principales Autoridades de Certificación, por ejemplo. VeriSign, no están en esta lista porque su software no está disponible para otros.

* Computer Associates eTrust PKI
* Entrust
* Microsoft
* Netscape CMS
* OpenCA
* RSA Security
* Safelayer

1.3. ASPECTOS LEGALES DE LA CERTIFICACIÓN DIGITAL EN COLOMBIA

Colombia es uno de los países pioneros en la emisión de leyes relacionadas con el comercio electrónico. En 1999 fue emitida la Ley 527 de 1999, que marcó el inicio de la legalidad de los mensajes de datos y fue la primera ley colombiana en nombrar los conceptos de certificados digitales, firma digital y entidad de certificación. Dicha ley surge como equivalente funcional de la Ley Modelo de Comercio Electrónico (LMCE) de la CNUDMI (Comisión de las Naciones Unidas para el Derecho Mercantil Internacional) de 1996.

Para realizar el análisis del estado del arte de la normatividad relacionada con identificación digital, entidades de certificación y firma digital, se ha preparado el siguiente gráfico:

<table>
<tr><td>Ley 527 de 1999</td><td>Decreto 1747 de 2000</td><td rowspan="2">Jurisprudencia</td><td rowspan="2">Circular Única de la Superintendencia de Industria y Comercio</td></tr>
<tr><td colspan="2">Ley Modelo de Comercio Electrónico CNUDMI</td></tr>
</table>

Figura 2. Arquitectura Legal de la Certificación Digital en Colombia

Ley 527 de 1999. (18 de Agosto). Ley que define y reglamenta el uso de los mensajes de datos, del comercio electrónico, de las firmas digitales y las entidades de certificación

Decreto 1747 de 2000. (11 de Septiembre). Decreto que reglamenta la Ley 527 de 1999, acerca de certificados y firmas digitales.

Jurisprudencia relacionada. En Colombia se han llevado a cabo una serie de demandas de inconstitucionalidad a la Ley 527 de 1999, entre las cuales se destacan:

- Demanda de inconstitucionalidad contra el artículo 6º de la Ley 527 de 1999. (Sentencia C-831-01, 8 de Agosto de 2001).

- Demanda de inconstitucionalidad contra los artículos 10º, 11º, 12º, 13º, 14º, 15º, 27º, 28º, 29º, 30º, 32º, 33º, 34º, 35º, 36º, 37º, 38º, 39º, 40º, 41º, 42º, 43º, 44º y 45º de la Ley 527 de 1999. (Sentencia C-662-02, 8 de Junio de 2000).

Las dos anteriores demandas fallaron a favor de la exequibilidad de los artículos relacionados.

Circular Única de la Superintendencia de Industria y Comercio. Según la Ley 527 de 1999, el organismo gubernamental encargado de registrar, regular y vigilar las entidades de certificación, es la Superintendencia de Industria y Comercio (http://www.sic.gov.co), quien en su circular única, en el Título V, Capítulo Octavo, da las pautas para registrar una Entidad de Certificación, ya sea ésta abierta o cerrada.

DIFERENCIA ENTRE ENTIDAD DE CERTIFICACIÓN Y AUTORIDAD DE CERTIFICACIÓN

La gran duda que surge a partir de los conceptos de Entidad de Certificación es ¿Qué relación existe entre la Entidad de Certificación nombrada por las normatividad legal colombiana y la Autoridad de Certificación nombrada en el estándar PKIX?

La respuesta es simple: cuando se habla de Entidad de Certificación, se está hablando de un todo, es decir, de todo el sistema de seguridad PKI, mientras que cuando se habla de Autoridad de Certificación, únicamente se está hablando de uno de los componentes de la arquitectura. Tal vez esa es la razón por la cual la ley no habla ni de Autoridades de Registro ni de Entidades Finales.

Un gráfico que nos ayuda a entender mejor la relación entre Entidad de Certificación y una Autoridad de Certificación, se puede ver a continuación:

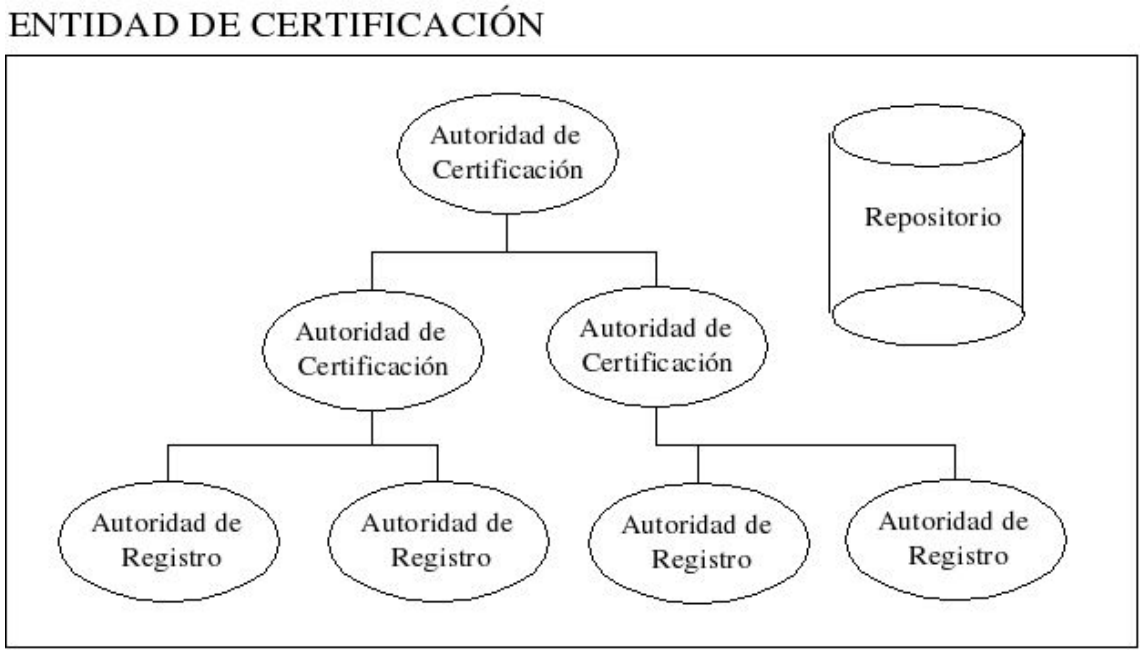


Figura 3. Figura que aclara la relación entre Entidad de Certificación y Autoridad de Certificación

2. PLANTEAMIENTO GENERAL DE LA REFERENCIA METODOLÓGICA

La ciencia saca sus conclusiones y conceptos del mundo, de acuerdo a la evidencia que se logra por medio de la experimentación, las deducciones lógicas y el pensamiento racional. Todo este conocimiento, obtenido mediante la observación y el razonamiento, sistemáticamente estructurado, tiene sus raíces en corrientes del conocimiento como el empirismo, el reduccionismo, el constructivismo social y la navaja de Occam.

a) Empirismo

Un concepto importante en la filosofía de la ciencia es el empirismo, o la dependencia de evidencia. El empirismo enfoca al conocimiento como una derivación de la experiencia en nuestras vidas. En este sentido, los enunciados científicos son sujetos a experiencias y observaciones. Las hipótesis científicas son desarrolladas y probadas a través de métodos empíricos que consisten de observaciones y experimentos, que al ser evaluadas, se convierten en la evidencia por medio de la cual la comunidad científica desarrolla sus teorías para tratar de explicar hechos relacionados con el mundo que nos rodea.

La observación es un elemento muy importante del empirismo, y se basa en el concepto de percepción como medio para llegar al conocimiento. Un concepto interesante en la observación es su tendencia al cambio, ya que al estar la observación estrechamente relacionada con el aprendizaje, y éste a su vez con el pensamiento, entonces en el momento que el pensamiento cambie, también lo va a ser la forma en que se observa. Esto trae una consecuencia interesante, y es que un mismo experimento puede arrojar los mismos resultados en dos distintas partes, pero socialmente puede arrojar observaciones diferentes.

b) Constructivismo Social

Otra raíz del conocimiento, es el *constructivismo social* [5], área de interés de historiadores, filósofos y sociólogos de la ciencia que piensan que las teorías científicas se encuentran demarcadas por su contexto social y político. Al *constructivismo social,* se le puede ver de cierta manera como una extensión del instrumentalismo, sólo que involucra a la ciencia con los aspectos sociales.

c) Reduccionismo

Otra corriente filosófica relacionada con la generación de ciencia, es el *reduccionismo*[6], que es la

5 PAUL, Ernest. Social Constructivism as a Philosophy of Mathematics. 1998

6 DAWKINS, Richard. Teleological Reductionism

actividad relacionada con dividir una observación, o una teoría en conceptos más simples, con el fin de poderla entender. Un ejemplo del reduccionismo, es la descripción del movimiento de un proyectil, ya que sería imposible describirlo sin separar la fuerza de la gravedad, del ángulo y velocidad inicial del proyectil. Únicamente, a través de este *análisis*, es que se puede formular dicha teoría.

d) La navaja de Occam

La **navaja de Occam**[7] (o **navaja de Ockham**, o **principio de economía**) hace referencia a un tipo de razonamiento basado en una premisa muy simple: *en igualdad de condiciones la solución más sencilla es probablemente la correcta*.

Es un principio atribuido al fraile franciscano inglés del siglo XIV Guillermo de Ockham que forma la base del reduccionismo metodológico. En su forma más simple, el principio de Occam indica que las explicaciones nunca deben multiplicar las causas sin necesidad. Cuando dos explicaciones se ofrecen para un fenómeno, la explicación completa más simple es preferible. Si un árbol achicharrado está caído en tierra, podría ser debido a la caída de un relámpago o debido a un programa secreto de armas del gobierno. La explicación más simple y suficiente es la lógica —más no necesariamente la verdadera— según el principio de Occam. En el caso de árbol, sería la caída del relámpago.

Por ejemplo, para explicar la caída de una manzana al suelo, podríamos plantear las siguientes explicaciones:

- Unos duendes traviesos invisibles e indetectables la han movido hasta el suelo, para fastidiarme.
- La madurez propia de la fruta ha debilitado la rama por la cual está unida al árbol y debido al peso excesivo de ésta, la gravedad ha propiciado su caída.
- Una tormenta a su paso tiró la manzana.

Todas estas alternativas explican igualmente el fenómeno desde el punto de vista lógico y experimental, pero el criterio de Occam nos obliga a escoger la segunda como verdadera, ya que las demás nos obligarían a asumir una serie de postulados mucho más complicados.

La teoría de *la navaja de Occam* se aplica a casos prácticos y específicos, englobándose dentro de los principios fundamentales de la filosofía de la escuela nominalista -fundada por el propio Ockham- que opera sobre conceptos individualizados y casos empíricos.

7 JEFFREYS, William. Sharpening Ockham's Razor on a Bayesian Strop

LA JUSTIFICACIÓN DE LOS ENUNCIADOS CIENTÍFICOS

Los enunciados más aceptados por la ciencia, son aquellos, cuya aplicabilidad es bastante amplia. Por ejemplo, la tercera ley de Newton plantea que para cada acción, existe una reacción igual a la acción. El anterior es un enunciado, ampliamente aceptado porque aplica para cada acción, en cualquier lugar, y en cualquier momento.

Pero es imposible para la ciencia probar la incidencia de cada acción, y encontrar una reacción. ¿Cómo es, entonces, que afirman que la tercera ley de Newton es cierta? La ciencia, por supuesto, ha probado muchas acciones, y probablemente en cada una de ellas hayan encontrado una reacción, pero, ¿Podrán asegurar que la próxima vez que se prueba la tercera ley de Newton, funcionará? Es por eso, que han surgido corrientes del conocimiento, como la inducción que buscan alternativas para corroborar el funcionamiento de las teorías científicas.

LA INDUCCION

El razonamiento inductivo sostiene que si una situación se mantiene en *todas* los casos observados, entonces la situación se mantiene para todos los casos. Entonces, luego de completar una serie de experimentos que soporten la tercera ley de Newton, entonces se sostiene que así se mantendrá para todos los casos.

La forma en que se explican las cosas por medio de la inducción es de cierta manera confusa, ya que no existe una conexión lógica entre la premisa y la conclusión. Un ejemplo importante de inducción es el por qué los cisnes son blancos. No importaba cuantas veces los científicos del siglo 17 observaron los cisnes, no existía un camino deductivo para concluir que los cisnes eran blancos.

CONCLUSIÓN

La razón por la cual se habla de algunas corrientes del conocimiento es porque fueron éstas, sobre las que se soportó la generación de la presente referencia metodológica y su validación.

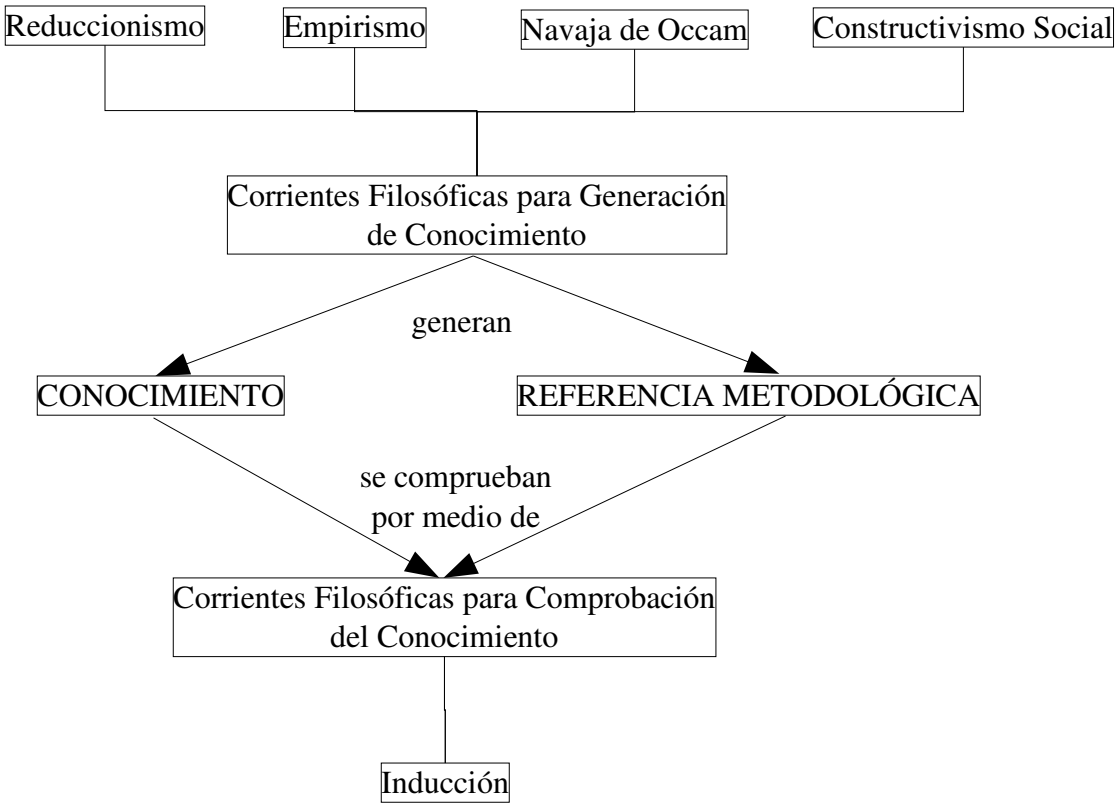


Figura 4. Filosofías de la Ciencia utilizadas para la Generación y Validación de la Referencia Metodológica

Como se puede observar en la figura anterior, se hace una analogía entre el conocimiento y la referencia metodológica ya que dentro del marco de referencia que se está trabajando significan lo mismo, es decir, para el equipo de trabajo la referencia metodológica es conocimiento, y como tal, puede llegar a ser generado a través de cualquier corriente filosófica para generación de conocimiento. Igual sucede con la validación, ¿Cómo validar que realmente la referencia metodológica funciona?, ¿Será que funcionará en todos los casos?

Es así, que luego de haber enunciado algunas corrientes filosóficas del conocimiento, la presente referencia metodológica define su posición siguiendo al *Reduccionismo,* al *Empirismo*, *al Constructivismo Social y La Navaja de Occam* para su generación, y a *La Inducción*, para su comprobación. ¿Por qué?

Esta referencia metodológica es fruto del trabajo de investigación y de pruebas realizadas sobre distintas alternativas para montar servicios de identificación digital. Todo ésto más la experiencia de administración de servidores de producción y gestión de proyectos software tradicionales, dieron la pauta para apostarle a una filosofía donde el conocimiento se basa en la experiencia. Además,

se desea dividir un proyecto en etapas, etapas que al sumarse podrían eventualmente producir un resultado positivo. Eso es una aplicación del *Reduccionismo,* nombrado anteriormente. El Constructivismo Social se puede ver en la Referencia Metodológica, en la contextualización social y política que se le ha dado. La Navaja de Occam se puede ver reflejada en la manera que se visualizó el problema.

En cuanto a la validación de la referencia metodológica, no se puede garantizar en ningún momento el éxito de su proceso y por eso la validación se realiza siguiendo la *Inducción* como filosofía. La mayoría de las aplicaciones que se encuentran trabajando en ambientes de producción hoy en día, tuvieron su inicio en la academia. De esta manera, se espera que la validación de la referencia metodológica en la Universidad del Cauca, no necesite de grandes alteraciones para llegar a funcionar en un entorno empresarial o gubernamental.

METODO Y METODOLOGIA

Una discusión muy particular siempre ha existido entre lo que es método y metodología, ya que son dos palabras que tienden a ser usadas para el mismo fin, aunque para algunos autores, es importante establecer una clara diferencia entre éllas.

Método, según el real diccionario de la lengua española[8] es el modo de decir o hacer con orden, mientras que metodología es la ciencia que estudia el método, es decir, los estudia en conjunto para resolver un problema de la ciencia en particular. Según Alexander Spirkin, en su libro "Dialectical Materialism", metodología es un sistema de principios y normas generales de organización y estructuración teórico-práctica de actividades.

En la ingeniería de software sucede lo mismo, una persona puede argumentar que un método es una receta, una serie de pasos para construir software, donde la metodología es un conjunto de recomendaciones para practicar, algunas veces acompañada de material educativo, plantillas, y herramientas de diagramación. En este sentido, un método, puede ser parte de una metodología. Incluso, algunos autores consideran que la metodología es un enfoque filosófico al todo del problema.

En este sentido, la ingeniería de software sería rica en métodos, pero escasa en metodologías. Se podría decir, que existirían dos grandes tipos de metodologías: la metodología de programación estructurada y la metodología de programación orientada a objetos.

Para este caso de estudio, se va a enfocar el concepto de metodología como el estudio de los

8 REAL ACADEMIA ESPAÑOLA. Diccionario de la Lengua Española. <http://www.rae.es>

métodos involucrados en la solución de un problema. Se va a buscar la agrupación de métodos, reglas y postulados para lograr el objetivo final: implementar un sistema capaz de prestar servicios telemáticos basados en identificación digital.

Así, entonces, se podría decir que la ingeniería de software posee muchas metodologías como Top-Down, Bottom-Up, RAD (Rapid Application Development), en cascada, basada en prototipos, entre muchas más[9].

Finalmente, surge la gran pregunta ¿Qué es una referencia metodológica y por qué este proyecto de investigación se enfoca en élla?.

Una Referencia Metodológica no es más que un referente hacia diversas metodologías, metodologías que buscan ordenar y guiar una serie de pasos para aumentar la probabilidad de éxito del proceso. Hay que aclarar que la presente referencia metodológica se encuentra enmarcada en el campo de las ciencias de la computación, y su objetivo es relacionar hacia una serie de metodologías para poder analizar e implementar servicios de identificación digital junto con la infraestructura de llaves públicas que la soporta.

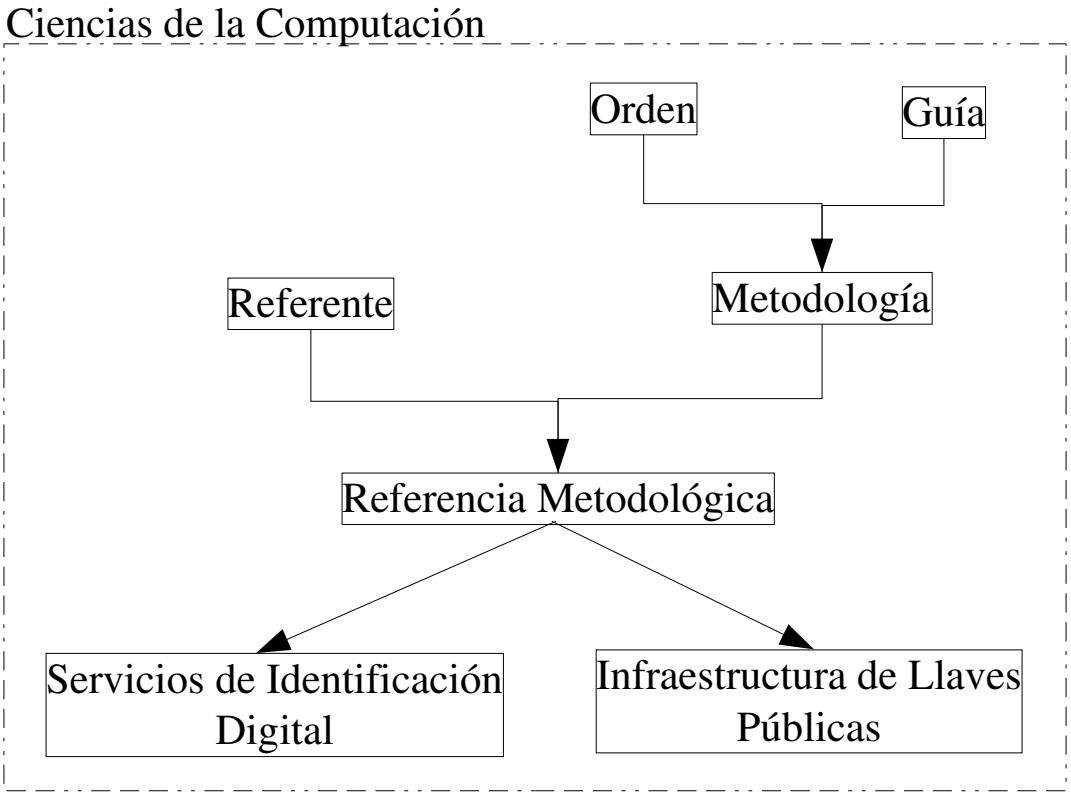


Figura 5. Concepto Referencia Metodológica

9 PRESSMAN, Roger. Ingeniería de Software: Un enfoque aplicado. 2002. p.13

LA REFERENCIA METODOLÓGICA PARA IMPLEMENTACIÓN DE SERVICIOS TELEMÁTICOS BASADOS EN IDENTIFICACIÓN DIGITAL

La Referencia Metodológica para Implementación de Servicios Telemáticos basados en Identificación Digital, es un esfuerzo para plantear una serie de buenas costumbres para implementar servicios de identificación digital desde la perspectiva de la seguridad informática, por medio de la formulación y ejecución de un proyecto de desarrollo. Entiéndase por proyecto de desarrollo a la asignación de una parte de los recursos de una comunidad humana, para producir de manera organizada bienes y/o servicios que atiendan necesidades y expectativas específicas de esa u otra comunidad.

Esta referencia metodológica se basa principalmente en el empirismo y la inducción. La metodología se encuentra planteada para que funcione en un entorno académico, empresarial y gubernamental, aunque sólo haya sido validada en un entorno académico y cerrado (Entiéndase por cerrado, a un sistema cerrado). Se desconoce su validez en un entorno abierto o cerrado, donde el fin sean las utilidades del negocio, no obstante, el diseño y el análisis realizado da para que en la teoría también funcione. Por eso es tan importante la adopción de la metodología por parte de la comunidad, ya que a medida que se valide, y se retroalimente, ésta podrá evolucionar, y perfeccionarse.

CARACTERÍSTICAS DE LA REFERENCIA METODOLÓGICA

1. ENFOQUE PREVENTIVO-ADAPTATIVO

Una de las razones por la cual el desarrollo de software puede orientarse a ser únicamente adaptativo[10], es mucho más sencillo de corregir. Quizás por esta mezcla Software/Hardware, en el contexto que se encuentra, se necesita de un plan de desarrollo del proyecto lo suficientemente preventivo, para poder evitar errores catastróficos de planeación, especialmente en lo concerniente al hardware, tal como las instalaciones físicas, los servidores necesitados, hardware de seguridad, etc.

Pero como la metodología puede incluir un fuerte proceso de desarrollo de software, en este caso de aplicación se va a enfocar desde el punto de vista adaptativo, es decir, que a medida que el software vaya evolucionando, y se encuentre sometido al cambio, éste se adaptará sin ningún problema.

2. ORIENTADO A LOS INDIVIDUOS

Uno de los enfoques de las metodologías tradicionales de desarrollo es llevar a cabo procesos en los cuales las personas son tratadas como piezas reemplazables. Es así, como se llega al punto que el rol es mucho más importante que los individuos mismos. Un analista, un administrador del proyecto, un desarrollador, un arquitecto software es mucho más importante que Juan Pérez, o un Fulano. Quizás una de las personas que más se ha opuesto a tratar a las personas como recursos ha sido Alistair Cockburn. En su artículo “Characterizing People as Non-Linear, First-Order Components in Software Development”[11], él propone que los procesos de desarrollo de software cuando requieren ser predictivos, necesitan de personal que se pueda predecir, pero los seres humanos son sistemas abiertos impredecibles. Más detalles acerca del comportamiento humano dentro de un equipo de trabajo ágil, se puede encontrar en los anexos en el artículo: "Los Procesos de Aprendizaje en las Metodologías Ágiles de Desarrollo".

3. UTILIZACIÓN DE LA MENOR DOCUMENTACIÓN POSIBLE

La documentación es algo importante en cualquier proceso de desarrollo, ya que es el soporte escrito que traza el proyecto, pero también se puede convertir en el principal obstáculo para el avance, si se excede su uso. La presente Referencia Metodológica “no” piensa ignorar la

10 FOWLER, Martin. The New Methodology <http://www.martinfowler.com/articles/newMethodology.html>

11 COCKBURN, Alistair. Characterizing People as Non-Linear, First Order Components in Software Development. <http://alistair.cockburn.us/crystal/articles/cpanfocisd/characterizingpeopleasnonlinear.html>

importancia de plasmar un impecable plan de desarrollo inicial de proyecto, ni tampoco va a desconocer la importancia de establecer rigurosas políticas de seguridad, ni la declaración de prácticas de certificación. Sin embargo, se aconseja, que la realización de la documentación posterior al plan de desarrollo inicial del proyecto sea lo más sencilla posible y no se exceda en detalles que enfrasquen la solución.

ETAPAS DE LA REFERENCIA METODOLÓGICA

La Referencia Metodológica plantea 3 etapas para cumplirse a cabalidad, etapas que describirán el grado de evolución del proyecto y subetapas que variarán dependiendo del caso de negocio planteado. Además, cada subetapa, constará de actividades que pueden ir desde la realización de un test de evaluación, hasta la generación de un documento de planeación, o la implementación de un servicio de la arquitectura.

Las 3 etapas planteadas, para la presente Referencia Metodológica son:

1. ETAPA DE PREPARACIÓN

Es donde se identifica la idea misma del proyecto y es en la cual se realiza el análisis de viabilidad de la construcción de la solución. En esta etapa se realiza el plan de desarrollo del proyecto como tal y donde se resuelven los siguientes interrogantes:

- ¿Qué se va a hacer?
- ¿Quién lo va a hacer?
- ¿Cómo se va a hacer?
- ¿Cuándo se va a hacer?
- ¿En donde se va a hacer?
- ¿Con qué recursos se va a hacer?

En la etapa de preparación se realiza el estudio de ingeniería del proyecto, es decir, se realiza el análisis de requerimientos y diseño de la arquitectura a implementar. También se definen las políticas de certificación y la declaración de prácticas de certificación.

La idea de esta primera fase es realizar todo lo concerniente a la planeación técnica, económica y legal del proyecto de implementación de servicios de identificación digital, junto a un análisis concienzudo de sus requerimientos lógicos y físicos. Esta etapa, es característica de las metodologías tradicionales, y por ende, busca ser lo más predictiva posible, no obstante, se le ha dado un enfoque más práctico y simple, sin descuidar los detalles importantes.

2. ETAPA DE IMPLEMENTACIÓN Y PUESTA EN MARCHA

La etapa de implementación y puesta en marcha es aquella donde se realiza la construcción de la infraestructura de seguridad que soportará los servicios de identificación digital, y además se implementarán los servicios mismos.

Esta etapa variará, dependiendo de las características de implementación planteadas durante la etapa de preparación del proyecto. Por ejemplo, si la ruta seguida para la implementación de la infraestructura de seguridad, se subcontrata, probablemente sea un camino a la implementación de los servicios basados en identificación digital, mientras que si se decide construir la infraestructura de seguridad, habrán que ser realizadas dos actividades: una para la construcción de la PKI, y otra para la construcción de los servicios basados en identificación digital.

Otra característica importante de esta etapa, es el entorno de trabajo, y cómo debe ser instalado de manera segura, es decir, si se va utilizar una solución basada en software privativo, o una solución basada en software libre y/o de código abierto.

Además en esta etapa se hará la construcción de las instalaciones de la planta encargada del servicio y su respectivo aseguramiento siguiendo los lineamientos planteados en la etapa de planeación y que se encuentran basados en el estándar ISO 17799[12].

3. ETAPA DE OPERACIÓN Y MANTENIMIENTO

Esta es la etapa final de la Referencia Metodológica y es donde se entra a operar el proyecto y se distingue por qué en ésta, se producen bienes o servicios.

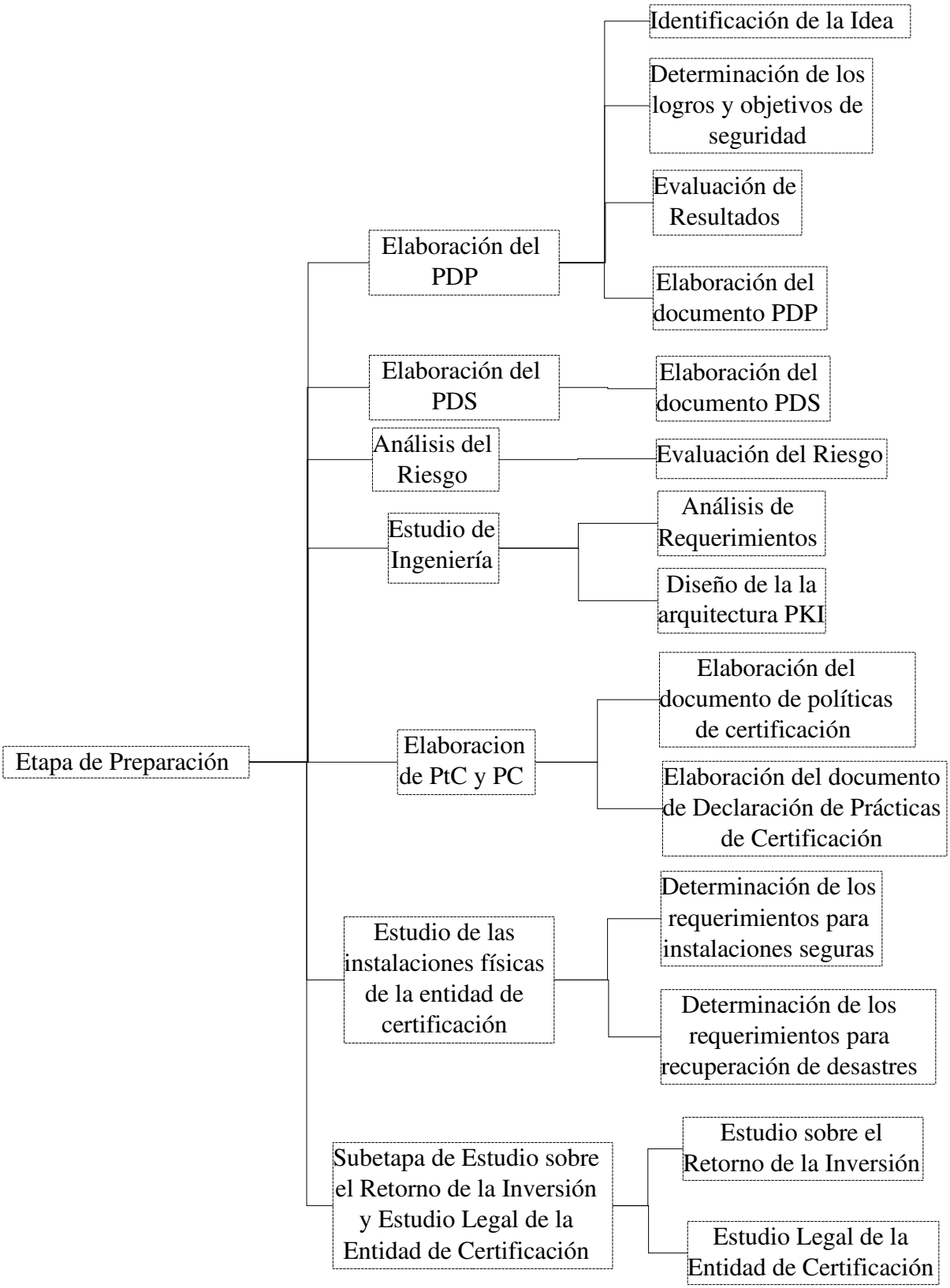
La etapa de operación y mantenimiento del proyecto se encuentra compuesta por dos subetapas, una para el correcto mantenimiento técnico de la infraestructura de seguridad y sus servicios, a la cual se le denomina “Evaluación periódica de la infraestructura y servicios de Internet”, y otra donde se plantea el mantenimiento organizacional de la Entidad de Certificación y sus servicios a través del concepto de “Administración Total del Mejoramiento Continuo”.

NOTA FINAL: La presente Referencia Metodológica asume dos premisas:

1. No se cuenta con una Entidad de Certificación
2. Se va a desarrollar el Servicio de Identificación Digital[13]

12 ISO. ISO 17799. Information technology. Code of Practice for Information Security Management.

13 Esta Referencia Metodológica se recomienda utilizar sí y sólo sí en un proyecto se cumplen las dos premisas


Etapa de Preparación
Elaboración del PDP
Identificación de la Idea
Determinación de los logros y objetivos de seguridad
Evaluación de Resultados
Elaboración del documento PDP
Elaboración del PDS
Elaboración del documento PDS
Análisis del Riesgo
Evaluación del Riesgo
Estudio de Ingeniería
Análisis de Requerimientos
Diseño de la la arquitectura PKI
Elaboracion de PtC y PC
Elaboración del documento de políticas de certificación
Elaboración del documento de Declaración de Prácticas de Certificación
Estudio de las instalaciones físicas de la entidad de certificación
Determinación de los requerimientos para instalaciones seguras
Determinación de los requerimientos para recuperación de desastres
Subetapa de Estudio sobre el Retorno de la Inversión y Estudio Legal de la Entidad de Certificación
Estudio sobre el Retorno de la Inversión
Estudio Legal de la Entidad de Certificación

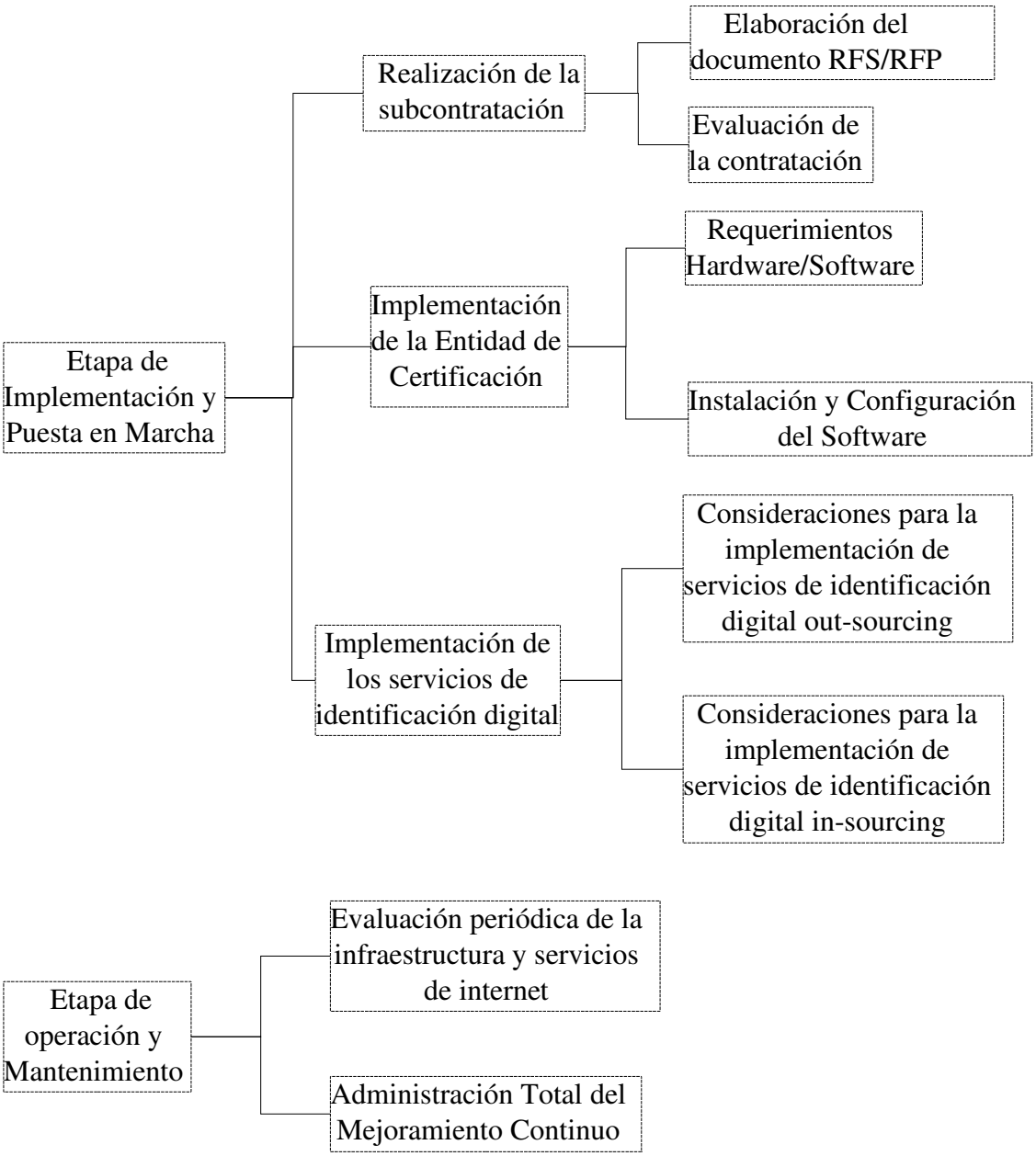


Figura 6. Esquema de la Referencia Metodológica

PDP: Plan de Desarrollo del Proyecto
PDS: Plan de Desarrollo del Servicio
PtC: Políticas de Certificación
DPC: Declaración de Prácticas de Certificación
RFS: Request for Strategy
RFP: Request for Proposal

3. ETAPA DE PREPARACIÓN

Predecir el futuro es una labor difícil de realizar en un proyecto para implementar servicios telemáticos basados en identificación digital, ya que los negocios y las tecnologías cambian tan rápidamente, que intentar realizar una tarea de adivinación resulta una labor casi imposible.

La razón por la cual se tiene que planear es para entender el "por qué" del proyecto.

Con base a ésto, entonces se podría decir que se planea porque:

- Se necesita asegurar que siempre se va a trabajar en los aspectos más importantes del proyecto
- Se necesita coordinar a los seres humanos que hacen parte del equipo de trabajo del proyecto
- Cuando ocurran eventos inesperados, entender la repercusión en los dos primeros

Lo primero es lo más razonable: no hay nada más frustrante que trabajar duro en una parte del proyecto que realmente no tiene preponderancia en la solución final, lo que conlleva a que sea parte residual del sistema.

La coordinación es una razón natural de la planeación, se tienen que coordinar a las personas (como seres humanos) que son parte de un equipo de desarrollo, y se debe buscar un trabajo de calidad, de manera individual así como grupal, es decir, que exista sinergia entre éllos.

El mundo real tiene la horrible costumbre de dañar planes. Es así, como la planeación tiene que pensarse en función de los eventos inesperados que pueden llegar a ocurrir así como la coordinación para poder afrontarlos.

Dentro de la etapa de preparación de la referencia metodológica planteda, se destacan las siguientes subetapas:

a) Subetapa de elaboración del plan de desarrollo del proyecto

Es donde se va a identificar la idea del negocio que se va a desarrollar y la determinación de sus logros y objetivos. Es el primer paso hacia un proyecto de implementación de servicios digitales exitoso y tiene una característica de planeación dual (Predictiva/Adaptativa), ya que se está trabajando con soluciones hardware y software.

b) Subetapa de elaboración del plan de desarrollo del servicio

Es donde se realiza la planeación del desarrollo de servicio de identificación digital. Allí se realiza el acercamiento con el cliente y se escriben los objetivos que se deben cumplir. Se realizan también allí, la planeación de las iteraciones y de las tareas para el desarrollo del software que va a prestar el servicio de identificación digital.

c) Subetapa de Análisis del Riesgo

Es donde se realizará una evaluación del sistema de seguridad que se desea implementar y sus posibles riesgos. A pesar que los riesgos son elementos que en ocasiones pueden llegar a ser impredecibles, existen algunos eventos comunes a los proyectos que pueden llegar a ser previstos y solucionados antes que ocurran.

d) Subetapa del Estudio de Ingeniería

Es donde se realiza el análisis de requisitos y el diseño de la arquitectura de seguridad. El objetivo es entrar en detalles acerca de las características técnicas que necesitan ser cubiertas por el sistema de seguridad final.

e) Subetapa de elaboración de las políticas de certificación y las prácticas de certificación

Esta subetapa pretende ayudar a la definición de las políticas de certificación y a las prácticas de certificación en el proceso de creación de la autoridad de certificación. El objetivo es proveer una lista de temas que necesitan ser comprendidos en una definición de políticas de certificación o en una declaración de prácticas de certificación.

f) Subetapa de estudio de las instalaciones físicas de la Entidad de Certificación

Se trata de realizar una aproximación a las características que debe tener las instalaciones donde se va a implantar el sistema de seguridad así como sus locaciones complementarias.

g) Subetapa de estudio del retorno sobre la inversión y estudio legal de la Entidad de Certificación

Es donde se realiza un estudio de la razón entre el valor total invertido en el proyecto, y sus

posibles ganancias. Este estudio puede ser útil para las organizaciones que busquen medir la viabilidad de sus proyectos para implementar servicios de identificación digital.

El estudio legal, brinda las pautas y trámites para legalizar la Entidad de Certificación.

3.1. SUBETAPA DE PLAN DE DESARROLLO DEL PROYECTO (PDP)

El inicio del proyecto es un paso trascendental que define en gran parte el éxito o fracaso de éste. Es por eso, que saber de manera clara qué se quiere y de qué manera se quiere hacer es una labor que implica tiempo y planeación.

Sin embargo, establecer el tiempo de desarrollo de un proyecto para implementar servicios telemáticos de identificación digital no es una tarea sencilla. Por un lado, las personas que se encuentran encargadas del proyecto desean tiempos considerables mientras que las personas externas a él, desean resultados visibles a corto plazo. Es así, como un proyecto coherente a las expectativas del cliente, debe basarse en un proceso confiable y sistemático que permita al cliente entender la razón de ser de los tiempos de entrega y así realizar un mejor planeamiento de los procesos de negocios dependiente de él.

De ahí la importancia de realizar una serie de actividades que permita a los miembros del equipo de planeación del proyecto, realizar un plan de desarrollo de proyecto, que sea coherente con su entorno socio-económico, y cuyo alcance sea real.

ACTIVIDAD No.1 : IDENTIFICACIÓN DE LA IDEA

Antes de comenzar la actividad, es bueno, saber qué es lo que se quiere hacer y sobre todo, qué servicios son los que se necesitan implementar en la organización, así que se va a conceptualizar lo que es un servicio de identificación digital:

Un **SERVICIO DE IDENTIFICACIÓN DIGITAL**, o **SERVICIO TELEMÁTICO BASADO EN IDENTIFICACIÓN DIGITAL**, es el equivalente no material de una **INFRAESTRUCTURA DE LLAVES PÚBLICAS (PKI)**, es decir, que es es ese bien intangible que ayuda a la realización de un **PROCESO DE NEGOCIO**.

Un **PROCESO DE NEGOCIO**[14], es toda aquella actividad del común, en la cual interviene una porción de la sociedad. Es así, como podemos hablar de Procesos de Negocio Académicos, o Procesos de Negocio Empresariales, o Procesos de Negocio Gubernamentales.

Continuando con los Servicios de Identificación Digital, se puede establecer una taxonomía de éllos, como la siguiente:

14 NASH, Andrew y DUANE, William. PKI Infraestructura de Claves Públicas. Madrid: Mc. Graw Hill, 2003. Capítulo 11

a) Mensajería Electrónica

- Correo Electrónico Seguro (Secure e-mail)
- Intercambio Electrónico de Datos Seguro (Secure EDI)
- Formularios Electrónicos Seguros

b) Redes

- Escritorio Seguro
- Intranets Seguras
- Extranets Seguras

c) Control de Acceso y Autenticación

- Control de Acceso a Entidades Finales
- Autenticación Robusta
- Autenticación Rápida

d) Servicios de Internet Seguro

- Acceso Remoto Seguro
- Aplicaciones Web Seguras
- IMAP/POP seguro

e) Otros

- Firmado de Objetos
- Estampillado Temporal de Eventos

La identificación de la idea, es un documento muy corto, en el cual se realiza una lluvia de ideas, acerca del proyecto a realizar y sobre todo, la necesidad a ser solventada.

Una vez identificada la idea, se debe proceder a evaluarla con base a las siguientes preguntas:

- ¿A quién va dirigido el proyecto?
- ¿La idea tendrá una amplia aceptación en la comunidad?
- ¿El monto de la inversión está dentro de las posibilidades de la organización?
- ¿Existe alguna experiencia anterior relacionada con el proyecto?
- ¿El o los servicios de identificación digital a implementar, cuentan con un mercado atractivo?
- ¿Se cuenta con una infraestructura de TI (Tecnologías de Información) básica para iniciar el proyecto?
- ¿Qué opciones existen para la infraestructura de llaves públicas que soporte el proyecto, conviene construirla, o subcontratarla?
- ¿Existe personal dentro de la organización capaz de llevar a cabo el proyecto, o hay que subcontratarlo?
- ¿La idea cuenta con apoyo institucional?
- ¿Existe una PKI en la organización?
- ¿Existen servicios de identificación digital ya implementados?

Todos estos factores deben ser concertados por el grupo inicial de trabajo, para establecer las características iniciales del proyecto y que marcarán el paso a medida que avance la iniciativa.

Hay que ser cuidadosos en no caer en "Modas", los servicios de identificación digital son un gran avance para una organización, pero no todas las organizaciones necesitan de éstos. Por ejemplo, no valdría la pena para una empresa que tiene un pequeño sistema de inventario, que apenas supera el millón de pesos, implementar un sistema de seguridad de orden tres (Saber algo, tener algo y ser alguien), para controlar el acceso a su pequeña base de datos.

Se debe prestar atención a la manera en que los servicios van a ser implementados, es decir, si se va a hacer de manera simultánea n servicios, o simplemente, se comienza con el de mayor importancia.

La decisión del público objetivo del proyecto, es una de las decisiones más trascendentales a tomar, y debe ser decidida de manera concienzuda, ya que es en ésta donde se va a reflejar, si se requiere de una Entidad de Certificación Abierta, o Cerrada; y ésta a su vez, determina la conveniencia de subcontratación o la construcción de ésta. (De ésto se hablará con más detalle en la siguiente actividad)

La aceptación de la comunidad, es un asunto que inicialmente es netamente especulativo, no obstante, un par de encuestas iniciales acerca de la aceptación del servicio, pueden llegar a ser de gran ayuda para intuir si la idea tiene acogida o no, y además para saber, si se cuenta con un mercado atractivo para el proceso de negocio a implementar.

ACTIVIDAD No. 2 : DETERMINACIÓN DE LOS LOGROS Y OBJETIVOS DE LA ENTIDAD DE CERTIFICACIÓN

En esta actividad se definirán las características esenciales de la entidad de certificación a ser implementada, las cuales tienen una gran importancia al momento de realizar los requisitos y el diseño de la arquitectura de seguridad.

Según la ley 527 de 1999, una entidad de certificación es aquella persona que, autorizada conforme a la ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.

Para la realización de esta actividad, se debe resolver un cuestionario sencillo que consta de los siguientes interrogantes:

a) ¿Entidad de Certificación Abierta o Cerrada?

Según el decreto 1747 de 2000, una entidad de certificación abierta es la que ofrece servicios propios de las entidades de certificación, tales que:

a) Su uso no se limita al intercambio de mensajes entre la entidad y el suscriptor, o

b) Recibe remuneración por éstos.

Así mismo, se define a una entidad de certificación cerrada como aquella que ofrece servicios propios de las entidades de certificación sólo para el intercambio de mensajes entre la entidad y el suscriptor, sin exigir remuneración por ello

Un aspecto inherente en los conceptos anteriores es que la entidad de certificación cerrada presta el servicio únicamente a sus suscriptores, es decir, a los usuarios de su organización, mientras que las entidades de certificación abiertas lo prestan a cualquier usuario de cualquier organización.

b) ¿Entidad de Certificación implementada por la organización y/o subcontratada?

Existen dos opciones para implantar una infraestructura de llaves públicas: la primera, que es utilizando los recursos propios de la organización, tales como personal, hardware, software, etc. y/o recurrir al alquiler de recursos externos para realizar algunas de las operaciones internas de ésta.

Por otro lado, la subcontratación implica que la organización permita a un tercero la implementación y operación de la infraestructura de llaves públicas.

Hasta este momento se tendrían cuatro opciones de entidad de certificación: una entidad certificación abierta implementada por la organización o subcontratada, o una entidad de certificación cerrada implementada por la organización o subcontratada.

Se puede dar el caso, que se den implementaciones híbridas de la infraestructura de llaves públicas. Por ejemplo, se puede subcontratar la implantación de ésta, pero el mantenimiento y la operación estaría a cargo de la organización. O también se podría pensar en que la entidad de certificación central puede ser administrada por un tercero, mientras que las entidades de registros están siendo administradas por la organización.

Los factores para determinar si se debe realizar la implementación de la infraestructura de llaves públicas a través de la misma organización o a través de un tercero son:

- Total de costos de implementación (Software, hardware, personal de mantenimiento, instalaciones, costos legales, etc)
- Grado de control que la organización considere necesario se debe tener sobre la operación de la PKI
- La percepción de confianza que los clientes van a tener de los servicios de identificación digital (por ejemplo, una infraestructura de llaves públicas implantada por una empresa especializada en servicios de seguridad va a dar mucho más confianza al cliente, que si fuese implementada por la

misma organización).
- Tiempo de respuesta asociado a las inquietudes relacionadas con los servicios de identificación digital y la difusión de información (Por ejemplo, cuánto tiempo se demora en brindarse la información acerca de una queja por X o Y razón)
- Nivel y disponibilidad de la atención al cliente
- Consideraciones de flexibilidad y escalabilidad
- Capacidad del tercero para afrontar las necesidades futuras de la organización
- Planeación y afrontamiento de desastres

c) ¿Entorno abierto y/o entorno privativo?

Este aspecto sólo aplica para el caso que se vaya a realizar la implementación de la entidad de certificación por parte de la organización. Un entorno privativo es aquel que se basa en la utilización de software privativo, es decir, software que prohíbe la modificación, la distribución y el acceso al código fuente de la aplicación.

Por el contrario, el entorno abierto permite manejar software de código abierto y que cumple ciertas características como libre distribución, acceso al código fuente, derivable e independiente de la tecnología [15].

Acerca de los factores determinantes para escoger si basar la solución software de la entidad de certificación en aplicación privativas y/o libres están:

- Costos de implementación (valor de licenciamiento del software privativo VS software de código abierto, Valor de mantenimiento del software privativo VS software de código abierto, etc.)
- Madurez y trayectoria del software (tiempo de desarrollo del software, trayectoria del fabricante del software, casos de éxito del software).
- Facilidad de gestión (facilidad para generar, revocar, editar y consultar certificados digitales)
- Algoritmos criptográficos implementados
- Valor agregado (servicios Web seguros, servicios de identificación digital "out of the box" como mensajería electrónica segura o gestión de host virtuales seguros)
- Soporte para autenticación de segundo y tercer orden (manejo de hardware de identificación biométrica y/o soporte para hardware de autenticación como tarjetas inteligentes o tokens usb).

Para el caso de estudio en cuestión, se va a realizar la implementación de los servicios de identificación digital (Mensajería Electrónica Segura) únicamente para los usuarios de la organización (Universidad del Cauca) y sin pedir remuneración por élla, por lo que aplicaría una

15 OPEN SOURCE INITIATIVE. Definición de Open Source. <http://www.opensource.org/docs/definition.php>

entidad de certificación cerrada. Como la Universidad del Cauca cuenta con las instalaciones y recursos adecuados para implementar la infraestructura de llaves públicas, se define que la entidad de certificación va a ser implementada. En cuanto al entorno, se escoge un entorno abierto por motivos de trayectoria, economía y calidad.

Un esquema de la decisión tomada por el caso de estudio, se muestra a continuación.

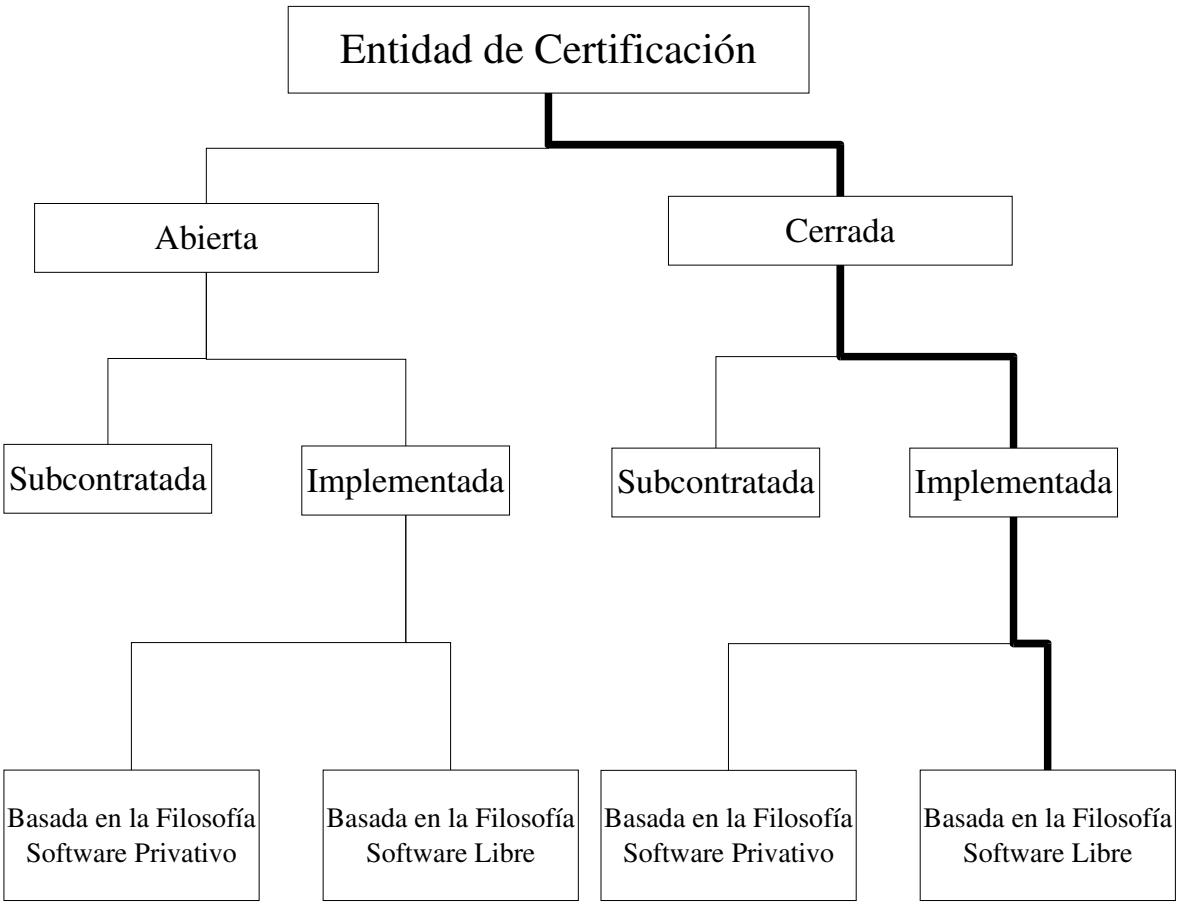


Figura 7. Árbol de Decisión para la Entidad de Certificación

ACTIVIDAD No. 3 : EVALUACIÓN DE RESULTADOS

La evaluación de resultados es una actividad importante, respecto al camino que se debe seguir en la referencia metodológica. Como se puede observar en el árbol de la figura anterior, existen seis caminos distintos para realizar la implementación de una entidad de certificación, por lo que la metodología debe adaptarse a cada una de las opciones.

Para facilitar la visualización de las etapas y actividades que son comprendidas por cada una de las posibilidades, se ha generado la siguiente tabla, con el fin de facilitar el trabajo:

Etapas y Actividades	***Entidad de Certificación Abierta***			***Entidad de Certificación Cerrada***		
	Implementada		Subcontratada	Implementada		Subcontratada
	E. Abierto	E. Privativo		E. Abierto	E. Privativo	
ETAPA DE PREPARACIÓN						
Subetapa de Elaboración del Plan de Desarrollo del Proyecto						
Identificación de la idea	X	X	X	X	X	X
Determinación de los logros y objetivos de seguridad	X	X	X	X	X	X
Evaluación de Resultados	X	X	X	X	X	X
Elaboración del documento PDP	X	X	X	X	X	X
Subetapa de Elaboración del Plan de Desarrollo del Servicio						
Elaboración del documento PDS	X	X	X	X	X	X
Subetapa de Análisis del Riesgo						
Evaluación del Riesgo	X	X	X	X	X	X
Subetapa de Estudio de Ingeniería						
Análisis de Requerimientos	X	X		X	X	
Diseño de la la arquitectura PKI	X	X		X	X	
Subetapa de Elaboración de PtC y PC						
Elaboración del documento de políticas de certificación	X	X	X	X	X	X
Elaboración del documento de Declaración de Prácticas de Certificación	X	X	X	X	X	X
Subetapa de estudio de las instalaciones físicas de la entidad de certificación						
Determinación de los requerimientos para instalaciones seguras	X	X		X	X	

Etapas y Actividades	***Entidad de Certificación Abierta***			***Entidad de Certificación Cerrada***		
	Implementada		Subcontratada	Implementada		Subcontratada
	E. Abierto	E. Privativo		E. Abierto	E. Privativo	
Determinación de los requerimientos para recuperación de desastres	X	X		X	X	
Subetapa de Estudio sobre el Retorno de la Inversión y Estudio Legal de la Entidad de Certificación						
Estudio sobre el Retorno de la Inversión	X	X	X	X	X	X
Estudio Legal de la Entidad de Certificación	X	X	X	X	X	X
ETAPA DE IMPLEMENTACIÓN Y PUESTA EN MARCHA						
Subetapa de realización de la subontratación						
Elaboración de los documentos RFS/RFP			X			X
Evaluación de la contratación			X			X
Subetapa de Implementación de la Entidad de Certificación						
Requerimientos Hardware/Software	X	X		X	X	
Instalación y Configuración del Software	X	X		X	X	
Subetapa de Implementación de los servicios de identificación digital						
Consideraciones para la implementación de servicios de identificación digital out-sourcing	X	X	X	X	X	X
Consideraciones para la implementación de servicios de identificación digital in-sourcing	X	X	X	X	X	X
ETAPA DE OPERACIÓN Y MANTENIMIENTO						
Evaluación periódica de la infraestructura y servicios de internet	X	X	X	X	X	X

Etapas ***y Actividades***	***Entidad de Certificación Abierta***			***Entidad de Certificación Cerrada***		
	Implementada		Subcontratada	Implementada		Subcontratada
	E. Abierto	E. Privativo		E. Abierto	E. Privativo	
Administración Total del Mejoramiento Continuo	X	X	X	X	X	X

Tabla 1. Matriz de Definición de las Subetapas a realizar durante el Proceso de Implementación del Servicio de Identificación Digital

* Significa que puede o no puede ser, dependiendo de las circunstancias

PtC: Políticas de Certificación

PC: Prácticas de Certificación

RFS: Request for Strategy

RFP: Request for Proposal

PDP: Plan de Desarrollo del Proyecto

PDS: Plan de Desarrollo del Servicio

ACTIVIDAD No. 4 : Elaboración del documento PDP (Plan de desarrollo del Proyecto)

El plan de desarrollo del proyecto es un documento donde se recopilan los datos que surgieron en las primeras actividades de la subetapa actual, para trazar la primera ruta que va a describir la solución más idónea al problema que se está tratando de resolver.

Los servicios telemáticos de identificación digital, tienen un objetivo común, el cual es el de la rentabilidad económica, el cual se hace más evidente en las entidades de certificación abiertas. A pesar que las entidades de certificación cerradas, no pueden (por ley) cobrar por la emisión, uso y gestión de los certificados, la implantación de estos mecanismos de seguridad, significan un mejoramiento en la seguridad de la comunicación interna y esto resulta de forma transparente en ahorro económico para la organización.

Es así, como directa o indirectamente, el proyecto se tiene que enfocar al ROI (Retorno de la inversión), un tema de preponderancia para determinar si se debe o no implementar la infraestructura de llaves públicas planteada para soportar la entidad de certificación. Acerca de este tema se hablará en la subetapa seis de la etapa de preparación, que se llama estudio de factibilidad.[16]

ESTUDIANDO EL ENTORNO

Lo primero que se debe hacer, antes de entrar de lleno a plantear la estrategia del plan de proyecto, es ubicarse dentro del entorno. Cualquier idea, proyecto o iniciativa se ejecuta bajo ciertas circunstancias socio-económicas, políticas, legales, tecnológicas y globales.

El sistema de identificación digital a ser implantado va a entrar en sinergia con el sistema socio-económico, político, legal y tecnológico de Colombia, por lo que se debe estudiar el estado del arte de estos aspectos.

Para el caso de estudio en cuestión, se pueden observar varios elementos importantes en cada uno de los entornos:

Socio-económico: Colombia desafortunadamente, es un país con una cultura muy baja relacionada con el tema del intercambio electrónico de datos enfocado al uso de los certificados digitales. Es escasa la gente que conoce el concepto de firma digital y sus aplicaciones, por lo que es un factor de sumo interés, al momento del estudio.

16 NASH, Andrew y DUANE, William. PKI Infraestructura de Claves Públicas. Madrid: Mc. Graw Hill, 2003.

Político: El panorama político de la certificación digital en Colombia tampoco es prometedor, como consecuencia del entorno socio-económico. El estado y sus representantes además del escaso conocimiento técnico del tema, al parecer no brindan el apoyo social adecuado para que la comunidad en general, se entere de la existencia de esta alternativa tecnológica para la realización de procesos de negocio domésticos, académicos, empresariales y gubernamentales[17].

Legal: Colombia ha sido uno de los pioneros en cuanto a emisión de leyes de comercio electrónico en Latinoamérica y muestra de éllo es la Ley 527 de 1999 y el Decreto 1747 de 2000, los cuales definen y reglamentan el uso de los mensajes de datos, del comercio electrónico, de las firmas digitales y las entidades de certificación.

Tecnológico: El número de usuarios de Internet en Colombia no es una de las cifras más alentadoras. En Diciembre de 2004, y según un estudio de la Comisión de Regulación de Telecomunicaciones CRT[18], hay aproximadamente 773,339 usuarios de internet, entre usuarios de xDSL, acceso conmutado y cable, 45,514 menos que en Junio de 2004, lo cual significa un estancamiento de uso. No obstante, se están llevando a cabo varias iniciativas para mejorar este aspecto como alianzas entre empresas de telecomunicaciones, reducción de las tarifas de internet por cable o internet por xDSL e implementación de servicios gubernamentales en línea.

En cuanto a la certificación digital en Colombia, se encuentran muy pocas entidades de certificación registradas ante la Superintendencia de Industria y Comercio (SIC). Sólo una entidad de certificación abierta (SOCIEDAD CAMERAL DE CERTIFICACIÓN DIGITAL CERTICAMARA S.A.) y cuatro entidades de certificación cerradas (AERONÁUTICA CIVIL, INSTITUTO COLOMBIANO DE CODIFICACIÓN Y AUTOMATIZACIÓN COMERCIAL IAC, BANCO DE LA REPUBLICA y A TODA HORA S.A).

DEFINIENDO LA IDEA GLOBAL

En la definición de la idea global del proyecto, se va a definir de manera general una hipótesis para la solución del problema que surge como consecuencia de una serie de necesidades.

Primero, hay que realizar una serie de premisas, con base a las necesidades planteadas en la actividad uno. Una buena alternativa es realizar esto por medio de una lista.

Segundo, hay que realizar el planteamiento de la pregunta central del problema, con base a las premisas anteriores. Esto significa que se deben tomar cada una de las necesidades y buscar una

17 FERNANDEZ, Fernando. Certificación digital en Colombia: Dificultades y Retos. <http://sitio.acis.org.co/Paginas/Publicaciones/columnista85.html>

18 CRT. Comisión Reguladora de Telecomunicaciones. <http://www.crt.gov.co>

pregunta cuya solución abarque la respuesta de al menos, los requisitos más importantes.

Tercero, es realizar un árbol de problemas, para buscar el problema central que se desea solucionar, tal y como lo sugiere ZOPP[19]. Un árbol de problemas es una herramienta para identificar los problemas centrales y sus principales causas, por medio del análisis de las causa-efecto.

Para realizar un árbol de problemas, se tienen que realizar los siguientes pasos[20]:

a) **Listar todos los problemas** que vengan a la cabeza. Los problemas deben ser identificados de manera cuidadosa: éstos deben ser problemas reales, no problemas hipotéticos, o que puedan llegar a suceder en el futuro.

b) Identificar el **problema central**; para esto se recurre al uso del ensayo y error, hasta cuando se considere por el equipo encargado de la planeación el verdadero problema central.

c) Determinar cuales de los problemas listados, son problemas **causa** y cuales son problemas **efecto**.

d) **Organizar jerárquicamente** los problemas causa y los problemas efecto, es decir, establecer cómo los problemas causa se relacionan con los problemas efecto y cómo el uno lleva al otro.

Para aclarar el concepto de la realización del árbol de problemas, se presenta el ejemplo de la siguiente figura con base al caso de estudio de la implementación del servicio de mensajería electrónica segura en la Universidad del Cauca.

Luego de realizar el árbol de problemas e identificar el problema central, se necesita realizar una concertación entre el equipo de trabajo para llegar a un consenso, acerca de la estrategia a tomar para solucionarlo. En esta labor es de gran utilidad las actividades dos y tres, ya que dieron en gran medida la visión de la solución que se desea implementar.

19 ZOPP. Ziel Orienterte Projekt Planung – (Planeación de Proyectos orientada a objetivos).

20 ZOPP. Problem Tree Analysis Tool <http://web.mit.edu/urbanupgrading/upgrading/issues-tools/tools/problem-tree.html>

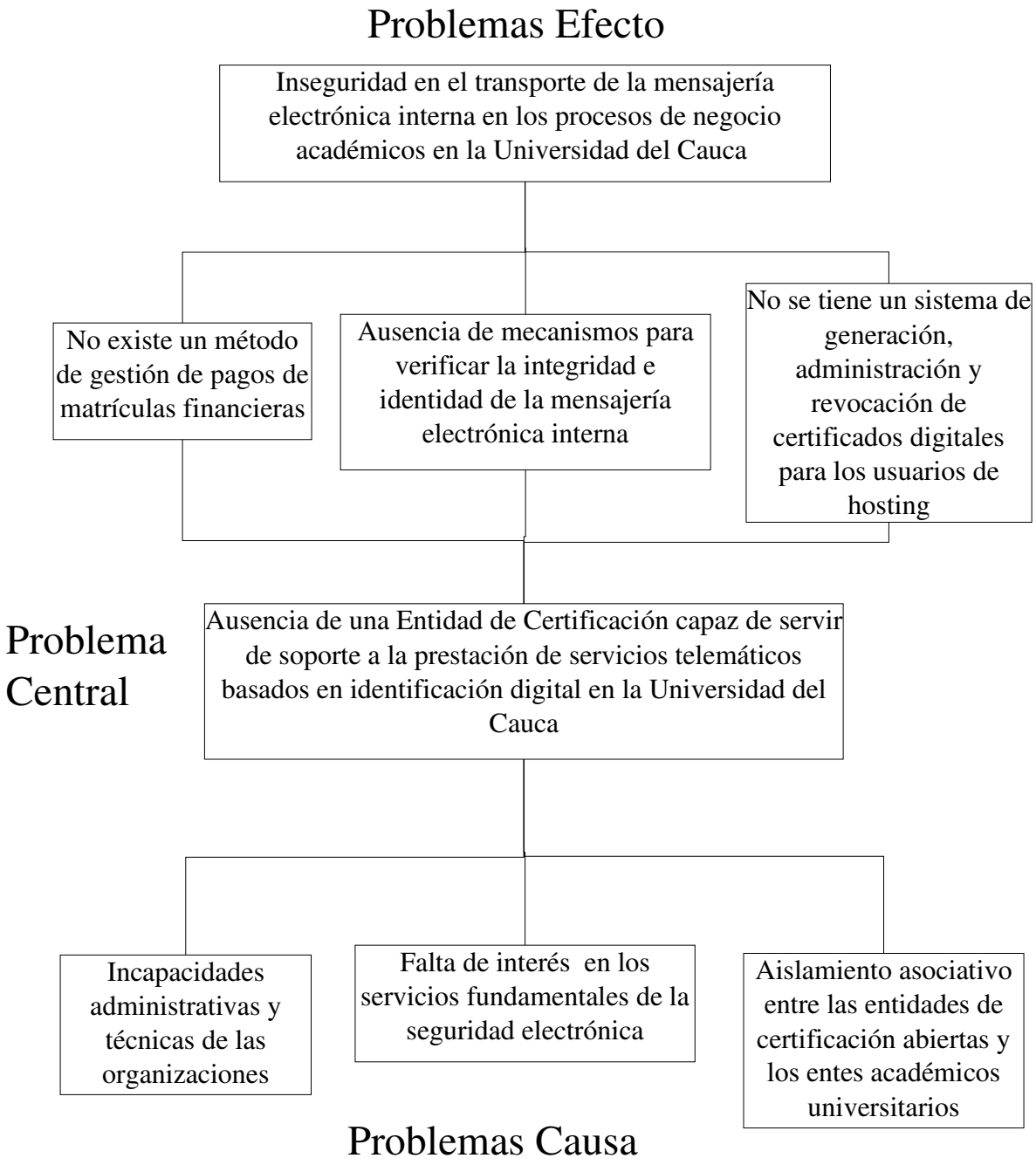


Figura 8. Ejemplo de un árbol de Problemas, donde se relacionan los problemas causa y los problemas efecto.

ESTABLECIENDO LOS OBJETIVOS

Una vez el problema a solucionar ha sido establecido, y la estrategia a seguir ha sido planteada, hay que establecer el objetivo general del proyecto. Resultará fácil encontrar el objetivo general, ya que simplemente es solucionar el problema central, planteado en el árbol de problemas, no obstante, se puede llegar a un objetivo general más filosófico, que acompañe a la solución técnica. Por ejemplo, en vez de decir que el objetivo general del proyecto es "Implementar X servicio de identificación digital", se podría llegar a algo más específico como "Fortalecer la confianza en las comunicaciones de Y organización por medio de la implementación de X servicio de identificación digital".

En cuanto a los objetivos específicos, son aquellos que en conjunto resultan en la consecución del objetivo general, es decir, son las tareas que se deben lograr a través del transcurso del proyecto para que al final se llegue a la meta esperada.

CARACTERIZANDO LOS SERVICIOS A SER IMPLEMENTADOS

En esta labor, se describirán los detalles iniciales del servicio (o los servicios) que va a ser implementado en el proyecto. Para éllo, se seguirán las siguientes pautas:

a) **Descripción del servicio**: es la visión inicial de la funcionalidad del servicio. Es el requerimiento inicial visto desde el cliente.

b) **Usuarios del servicio:** es la descripción de la demanda que se espera, debería tener el servicio. No se pretende establecer una demanda por medio de un estudio de mercadeo, sino establecer desde la perspectiva del cliente, cuales serían los posibles consumidores que se esperaría al menos debería tener el servicio de identificación digital.

c) **Estimación inicial de la inversión:** es el monto aproximado que la organización está dispuesta a invertir en el servicio de identificación digital.

d) **Análisis DOFA del servicio:** es la tarea que implica observar al servicio de identificación digital desde cuatro perspectivas: Fortalezas y Debilidades; Oportunidades y Amenazas.

ORGANIZANDO EL PROYECTO

Las personas dentro del equipo de trabajo del proyecto son las que determinan el éxito o fracaso del proyecto. Mientras mayor sea el número y la diversidad de personas, así mismo aumentará el

nivel de dificultad para controlar las tareas en el proyecto.

La organización de roles en los proyectos, es la tarea más difícil del líder del proyecto. Existen metodologías de desarrollo donde lo más importante es el rol y no las personas. Este tipo de división trae sus ventajas ya que ninguna persona dentro de un proyecto es indispensable; es así como las responsabilidades eran asignadas al Analista y no a Pepito Perez, o al Implementador, en vez de Fulano de Tal.

Algo que los líderes de proyectos como ese no tenían en cuenta, es que detrás de un rol, o un cargo dentro del proyecto, se encuentran seres humanos, que se caracterizan por ser altamente no lineales y variables[21] y descubren luego de cierto trabajo dos problemas:

1. Las personas en los proyectos no estuvieron interesadas en aprender acerca del sistema a crear.
2. Estuvieron totalmente dispuestos a ignorar al equipo líder y aún así realizaron su trabajo.

Es así, como se puede concluir que los seres humanos, así como los dispositivos activos tienen modos de éxito y modos de fallo. La siguiente son las principales características de las personas cuando trabajan en un proyecto.

1. Las personas son seres que se comunican, y que hacen su mejor esfuerzo cuando se encuentran "frente a frente" con su equipo de trabajo, con preguntas y respuestas en tiempo real.

2. Las personas tienen problemas cuando trabajan sobre el tiempo.

3. Las personas cambian de manera impredecible, cambia su estado de ánimo de día a día. También el lugar de trabajo es un factor de cambio de actitud.

4. Las personas normalmente quieren hacer bien las cosas, les gusta tomar la iniciativa y "hacer lo necesario" porque el proyecto tenga éxito.

En un proyecto para implementar servicios telemáticos de identificación digital, se necesitarían como mínimo, los siguientes roles:

EQUIPO LIDER

a) Director del Proyecto: Persona encargada de dirigir el proyecto en general. Es el encargado de

21 COCKBURN, Alistair. Characterizing People as Non-Linear, First Order Components in Software Development. <http://alistair.cockburn.us/crystal/articles/cpanfocisd/characterizingpeopleasnonlinear.html>

escoger la estrategia para lograr las metas y objetivos. También debe velar porque la comunicación, el tiempo y la incentivación del elemento más importante de la empresa: las personas.

b) Director de Seguridad: Persona encargada de verificar los procesos relacionados con el tema de la seguridad desde nivel técnico y organizacional. Debe tener la experiencia suficiente para evaluar idóneamente las actividades de implantación de la PKI y los servicios de identificación digital.

EQUIPO CENTRAL

a) Arquitecto PKI: Persona encargada de describir y diseñar la arquitectura de la Infraestructura de Llaves Públicas, así como la organización, procesos, funciones y gestión de la Entidad de Certificación.

b) Arquitecto Software: Persona encargada de establecer los requerimientos, analizarlos y diseñar la arquitectura de los servicios telemáticos de identificación digital que van a ser desarrollados.

EQUIPO DESARROLLADOR

a) Implementadores de Hardware de la PKI: Son las personas encargadas de construir la inraestructura locativa y de conectividad de la PKI, si es necesario.

b) Implementadores de Software de la PKI: Son las personas encargadas de instalar y configurar el software relacionado con la PKI y su gestión.

c) Implementadores de los Servicios de Identificación Digital: Son las personas encargadas de desarrollar o adaptar el software a los servicios de identificación digital requeridos.

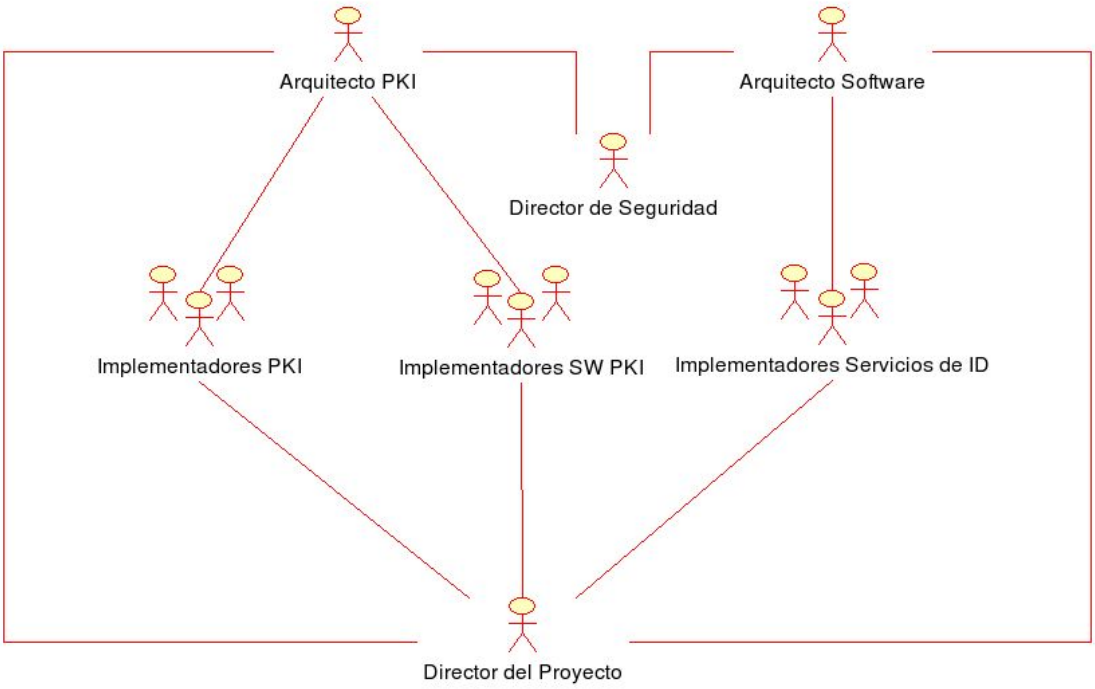


Figura 9. Estructura Organizacional Mínima de un Proyecto de Implementación de Servicios de Identificación Digital

PLANEACIÓN DEL PROYECTO

Un proyecto de implementación de servicios telemáticos de identificación digital es un proceso que usualmente dura entre 6 y 18 meses. Para realizar la correcta planeación de éste, se deben considerar tres puntos principales:

- Costos: Cuánto dinero será gastado y como presupuestarlo a través del tiempo.
- Tiempo: Cuánto tiempo durará la ejecución del proyecto (Tanto en sus fases, como en total)
- Alcance: Qué es lo que tiene que realizarse en cada de una de sus fases, y cuáles serán los indicadores de finalización.

Algo que se debe tener en cuenta al momento de realizar la planeación del proyecto, es que los planes de desarrollo emergen naturalmente y por ello, son continuamente modificados y refinados en términos de contenido, estructura y nivel de detalle. A medida que un requerimiento se refine, se entrarán en detalles, en los cuales las premisas son afirmadas o refutadas y sus resultados realimentarán el proyecto, en sus fases siguientes.

Así se puede concluir que el Plan de Desarrollo del Proyecto es un documento vivo, el cual se debe estar revisando y replanteando durante el ciclo de vida del proyecto.

PLANTILLA PARA EL PLAN DE DESARROLLO DEL PROYECTO

1. INTRODUCCIÓN
2. ENTORNO
2.1. ENTORNO SOCIAL Y CULTURAL
2.2. ENTORNO ECONÓMICO
2.3. ENTORNO TECNOLÓGICO
2.4. ENTORNO POLÍTICO Y LEGAL
2.5. ANÁLISIS GLOBAL DEL ENTORNO
3. DEFINICIÓN DE LA IDEA DEL PROYECTO
4. ANTECEDENTES
5. OBJETIVOS
5.1. OBJETIVO GENERAL
5.2. OBJETIVOS ESPECÍFICOS
6. CARACTERÍSTICAS DEL SERVICIO
6.1. DESCRIPCIÓN DEL SERVICIO
6.2. LOS USUARIOS DEL SERVICIO
6.3. ANÁLISIS DOFA DEL SERVICIO
7. ORGANIZACIÓN DEL PROYECTO
7.1 ESTRUCTURA ORGANIZACIONAL
7.2 ROLES Y RESPONSABILIDADES
8. PLANEACIÓN DEL PROYECTO
8.1 PLANEACIÓN DE LAS FASES
8.2 HITOS
8.3 RECURSOS DEL PROYECTO
9. CONCLUSIONES Y RECOMENDACIONES

3.2. SUBETAPA DE PLAN DE DESARROLLO DEL SERVICIO

La planeación del desarrollo de servicio de identificación digital es la parte más importante de esta referencia metodológica, ya que el objeto de estudio siempre ha sido éste (el servicio) y no la infraestructura de seguridad que se encuentra debajo.

Como se dijo en el planteamiento general de la metodología, se busca que el proceso de desarrollo de software cuente con las características de *adaptabilidad, agilidad y que sean orientadas a las personas,* lo cual se encuentra plasmado en el manifiesto[22] del desarrollo ágil de software.

Los cuatro (4) ítems a tener en cuenta durante la planeación del servicio, siguiendo la filosofía del desarrollo ágil de software son:

1. ¿Para qué planear?

Cualquier técnica para planeación de software debe tratar de crear *visibilidad*, es decir, que cada una de las personas involucradas en el proyecto puedan ver el progreso de éste. Para lo anterior se deben crear *hitos* claros, que no se estanquen y que representen claramente progreso. Los *hitos*, deben ser cosas que cualquier persona involucrada en el proyecto pueda entender, incluyendo al cliente. Algo que él pueda entender y confiar.

Los planes son utilizados para comprender el curso de los eventos alrededor del proyecto de software y sus consecuencias ante el cambio. Es por eso, que necesitamos diferentes planes, que deben ser simples y fáciles de actualizar. Los planes que son largos y complejos pueden llegar a no ser útiles porque son costosos y difíciles de mantener.

Los planes deben mantener un marco ético basado en la *honestidad y la responsabilidad*. La información utilizada para su planeación, debe ser real y en lo posible actualizada.

De acuerdo a lo anterior, se podría decir que se planea para controlar lo imprevisto, es decir, para controlar los miedos. Pero, ¿ cuál es el miedo que se debe minimizar?

Es así como hay que enfocarse en los dos (2) ejes principales del desarrollo ágil de software: el cliente y los desarrolladores (como seres humanos no lineales y de alto orden).

Entre los miedos comunes que pueden tener los clientes se tienen:[23]

22 BECK, Kent; BEEDLE, Mike; COCKBURN, Alistair y FOWLER, Martin. Manifesto for Agile Software Development. <http://agilemanifesto.org/>

23 FOWLER, Martin y BECK, Kent. Planning XP. 2000. p. 15

- No obtendrán lo que pidieron
- Se solicitarán cosas innecesarias
- Se pagará demasiado por algo pequeño
- Se perderá el control del proyecto debido a detalles técnicos que no interesan
- No verán nunca un plan que sea lo suficientemente claro para éllos

Entre los miedos comunes de los desarrolladores se tienen:

- Se les dirá que hagan más de lo que saben hacer
- Se les dirá que hagan cosas que no tienen sentido
- Que se les trate como máquinas desarrolladoras de software y no como personas
- Se están desactualizando técnicamente
- No se les diga claramente lo que tienen que hacer
- Tengan que sacrificar la calidad del producto debido a la fechas de entrega
- Tengan que resolver grandes problemas, sin poder discernir con otras personas acerca de él
- No se cuenta con el tiempo suficiente para lograr los objetivos

2. El arte de gestionar el proyecto de desarrollo del servicio

Gestionar un proyecto de desarrollo de software es muchas veces comparado con manejar un carro, ya que no consiste en poner el proyecto en el camino adecuado, sino en ir haciendo pequeños cambios y correcciones durante el transcurso de éste.

El desarrollo de software es un proceso. Éste puede ir o no ir mal. Para "mantenerlo andando", se debe estar continuamente dirigiendo, donde "dirigiendo" significa que se están haciendo evaluaciones constantes de la dirección que se está tomando, y la dirección hacia donde se quiere ir, haciendo pequeños y cuidadosos ajustes.

3. Las historias

La historia es la unidad funcional en un proyecto ágil de desarrollo de software basado en XP (Extreme Programming). El progreso de un proyecto se demuestra cuando se libera código probado e integrado que implementa una historia. Las historias deben ser entendibles para los clientes y desarrolladores, éstas se deben poder probar y evaluar por el cliente y deben ser lo suficientemente pequeñas para que los desarrolladores puedan construir una en lapsos muy cortos de tiempo.

Las características de las buenas historias son:

- *Las historias deben ser entendibles por el cliente*. No es una muy buena idea hacer los requisitos tan complejos ya que se requeriría tiempo de estudio en Ingeniería de Requerimientos para poderlos entender. El lenguaje para construir una historia debe ser español básico, utilizando las expresiones verbales más simples y naturales.

Ejemplo: *"El sistema debe chequear la sintaxis de la oración que es entrada en el campo de texto Subject".*

- *Mientras más cortas sean las historias, es mucho mejor*. La historia representa un concepto y no una especificación detallada. Una historia no es más sino un acuerdo entre el cliente y el desarrollador acerca de una característica del software.

- *Cada historia debe proveer algo de valor para el cliente.* Si el cliente no está obteniendo algo de la actividad que se está realizando. ¿Por qué debería pagar por eso? Cualquier infraestructura técnica debe ser construida en conjunto con las historias y debe ser construida para soportar las historias.

- *Los desarrolladores no deben construir las historias.* Cualquier idea o característica que un desarrollador pueda considerar, no deberá aparecer en una historia, a menos que el cliente la apruebe.

- *Las historias no deben ser difíciles de implementar.* La idea es que se puedan construir varias historias en una iteración.

- *Las historias deben ser creadas entre el cliente y los desarrolladores.* El cliente debe escribir la historia, y el desarrollador debe estimarla. Las dos partes deben colaborar y comunicarse para lograr esto.

- *Las historias deben ser independientes entre si.* A pesar que intentar realizar esto es algo casi imposible en un proyecto de desarrollo de software, pero se debe tratar que cada modulo funcional posea bajo acoplamiento y alta cohesión con los demás.

- *Las historias deben poderse probar.* Cuando se trabaja en un proyecto de planeación de servicios software, un punto de gran importancia es saber que sus componentes funcionan correctamente y que se pueden probar y depurar cada uno por separado.

4. Ordenando las historias

Uno de los aspectos claves de la planeación es decidir en qué orden se deben realizar las cosas. Y la cuestión es que en ésto, no se puede predecir si la decisión tomada fue la correcta o la errónea.

La noción de orden es un punto clave de la planeación. En grandes proyectos de ingeniería, se utilizan análisis de dependencia y diagramas de PERT[24]. La dependencia entre tareas es el factor dominante para la toma de decisiones en la organización de los elementos. Para ésto, se debe escribir una lista de tareas y establecer las dependencias entre éllas. Observando estas tareas y la duración de cada una de las actividades que conlleva, se pueden llegar a comprender los aspectos clave para establecer la ruta de trabajo óptima para el proyecto.

Otro factor de gran importancia, al momento de ordenar las historias, es su valor de negocio, es decir, la importancia que ésta tiene para el cliente. Uno de los errores que se podrían llegar a cometer en el momento de la organización de las tareas, es dejar las más valiosas para el cliente para el final, ya que en el momento que éste desapruebe o rechace alguna de estas tareas "valiosas", provocaría un trastorno, en el curso normal del proyecto o incluso podría implicar perdidas económicas abismales por la no tenida en cuenta de éste (el cliente).

5. Realización del primer plan

El primer plan es el más difícil y el menos certero del proyecto y tiene dos incertidumbres en particular: la velocidad de realización y el tamaño de las historias. A continuación se listarán algunos criterios para la realización de éste:

- La velocidad de desarrollo es posible medirla, pero una buena aproximación no puede ser inducida sin antes haber realizado un par de iteraciones dentro del proyecto. Antes de cualquier medida, lo mejor es suponer con base a la velocidad de desarrollo de las primeras historias.

- Calcular el tiempo de realización de una historia puede ser difícil al principio. El procedimiento que mejor da resultados es hacer que el equipo de trabajo comience con las historias con las cuales se sienta mejor. Una vez se sepa, cuánto se pueden llegar a demorar con una historia sencilla, se podrá calcular cuánto se podrán demorar con el resto de las historias.

- Acerca del tiempo que debe durar cada iteración, se aconseja que no sean tan extensas, como se acostumbra (seis meses o más) sino que por lo contrario, éstas sean cortas. (entre una y tres

24 PERT. Program evaluation and review technique.

semanas).[25]

6. Planeación de las iteraciones

Cada iteración está planeada para separar las historias de cada iteración en tareas. Las tareas se usan para planificar el tiempo de los programadores, haciéndolos trabajar en las tareas que ellos quieran, para así poder estimarlas y balancearlas, si es necesario.

El plan final debe estar sincronizado al ritmo del negocio, ya que éste debe darle al personal encargado del negocio una visión de historias que puedan ser contadas como una buena historia en el mercado. El plan de iteración es sincronizado al ritmo de la programación. Así, entonces podemos decir que dos semanas es suficiente para:

- Desarrollar alguna nueva funcionalidad
- Hacer alguna refactorización importante
- Desarrollar alguna infraestructura
- Realizar algunas pruebas

A diferencia del *Plan Final*, el Plan de Iteración está muy involucrado con los desarrolladores. Ellos deciden qué cosas se van a hacer y cómo se van a hacer. El cliente también está involucrado y por eso se deben realizar reporte de mitad de iteración para el cliente vea qué está sucediendo con el proyecto.

Una de los principios importantes de esta metodología es que las fechas no se pueden correr, se puede llegar a reducir el alcance, pero las fechas de entrega se deben mantener fijas. Esto es algo normal de cualquier proyecto de desarrollo: querer correr las fechas de entrega de cualquier elemento (sea iteración o historia) con el ánimo de agregarle alguna funcionalidad adicional.

7. Administrando el equipo de desarrollo

Uno de los aspectos de interés dentro de esta metodología es su capacidad para reaccionar al cambio, pero ¿Cómo se debe reaccionar ante el ingreso de nuevos integrantes al equipo de trabajo?

Es bueno darle a los integrantes nuevos del equipo de trabajo una o dos iteraciones para que se comiencen a acostumbrar al ritmo de trabajo. Así ellos podrán:

25 EXTREME PROGRAMMING GROUP. Extreme Programming practices and principles. <http://www.egroups.com/group/extremeprogramming>

- Relacionarse con compañeros de trabajos más experimentados
- Leer código y casos de pruebas
- Hablar con los clientes

Durante este tipo de orientación, no es obligatorio realizar una disminución en la velocidad de trabajo del equipo completo. El tiempo empleado para resolver una duda a un nuevo integrante no debería ser lo suficientemente crítico para tener que bajarle el ritmo de trabajo al proyecto.

8. Adaptación: La esencia de las metodologías ágiles

No todos los proyectos basados en metodologías ágiles deben actuar exactamente iguales. Una vez que se sepa cómo se debe comportar un proceso de desarrollo ágil básico, se le agregará o quitará dependiendo de los gustos y necesidades para ajustarse más precisamente la situación.

Hasta el momento, se ha sido un poco prescriptivos: iteraciones de dos semanas, historias pequeñas y métodos para ordenar las historias han sido, entre otros, patrones básicos que simplemente tratan de ilustrar una de muchas formas de realizar un proceso de desarrollo del servicio ágil.

Pero no hay que olvidar que en las manos del director del proyecto se encuentra definir si los tiempos son verdaderamente adecuados. Por ejemplo, si se ve que una iteración, se alcanzó a realizar en un tiempo más pequeño de lo previsto, es la misión de éste prever que la siguiente iteración se podría modificar a un lapso de tiempo más corto.

También hay que aclarar que en las manos del director del proyecto está encontrar la "combinación mágica" que va a dar el resultado perfecto y que esta combinación depende de la forma de interpretar verdaderamente el problema y las posibles formas de solución de ésta. Los criterios y métodos planteados a lo largo de esta subetapa sólo sugieren un par de buenas costumbres de planeación; ya es misión del director del proyecto profundizarlas y explotarlas al máximo para su propósito.

3.3. SUBETAPA DE ANÁLISIS DE RIESGO

Análisis es una evaluación crítica que implica la reducción de un objeto de estudio en sus partes constitutivas, su descripción y su relación con el todo [26]. El análisis de riesgo busca destacar los hechos esenciales de los secundarios (abstracción), haciendo relaciones y distinciones, encontrando lo que es determinante. Se hace referencia a los riesgos de seguridad computacional que pueden surgir del uso de la tecnología de la información.

Evaluación del Riesgo

La Evaluación de Riesgo es un proceso de análisis e interpretación. Puede ser orientada en áreas distintas como: controles técnicos y operacionales para ser diseñados en una nueva aplicación, en el uso de las telecomunicaciones, o en toda la Organización.

El primer paso es identificar el sistema a considerar (su ámbito, y sus límites con otros sistemas), la parte del sistema que será analizada y el método analítico para evaluar los riesgos.

La evaluación debe enfocarse primariamente en ciertas áreas con un riesgo de seguridad desconocido y en áreas conocidas por su alto riesgo.

Los Factores que influencian los límites de la evaluación son: la fase del ciclo de vida en que se encuentre el sistema (el nivel de detalle debe ser diferente para un nuevo sistema en desarrollo que para un sistema ya existente), la importancia relativa del sistema (entre más esencial sea el sistema, la evaluación debe ser más exhaustiva), y la magnitud y tipos de cambios realizados en el sistema desde la última evaluación de riesgos.

La metodología para evaluar los riesgos puede ser formal o informal, detallada o simplificada, de alto o bajo nivel, cuantitativa o cualitativa, o una combinación de todos éstos. No existe el mejor método para todos los ambientes y todos los usuarios.

La forma como se defina el ámbito, los límites y la metodología afectará enormemente en términos de: la cantidad de esfuerzo gastado, y la utilidad que se pueda obtener de los resultados de la evaluación. Estos factores deben seleccionarse de tal forma que produzcan resultados claros, específicos y útiles para el sistema y su organización.

La evaluación de riesgos produce un beneficio muy importante: un conocimiento más profundo

26 WIKIPEDIA. Analysis. <http://en.wikipedia.org/wiki/Analysis>

sobre los Sistemas y la Organización.

En la práctica se debe comprender e integrar la noción de Incertidumbre: no es posible obtener siempre información completa sobre todos los sistemas, datos, modelos, vulnerabilidades y amenazas. La información no siempre estará disponible. La incertidumbre siempre está presente y se debe tomar en cuenta en todas las fases de evaluación de riesgos.

A pesar de ésto, el análisis con todas sus etapas provee una herramienta muy poderosa para evaluar riesgos asociados con sistemas computacionales y organizacionales. La incertidumbre no debe invalidar la evaluación ni los resultados, así como los datos y los modelos corren el riesgo de ser imperfectos, son un acercamiento necesario y suficiente para el propósito del análisis de riesgos.

El siguiente diagrama muestra la interrelación entre las etapas de evaluación de riesgos considerando siempre la incertidumbre:

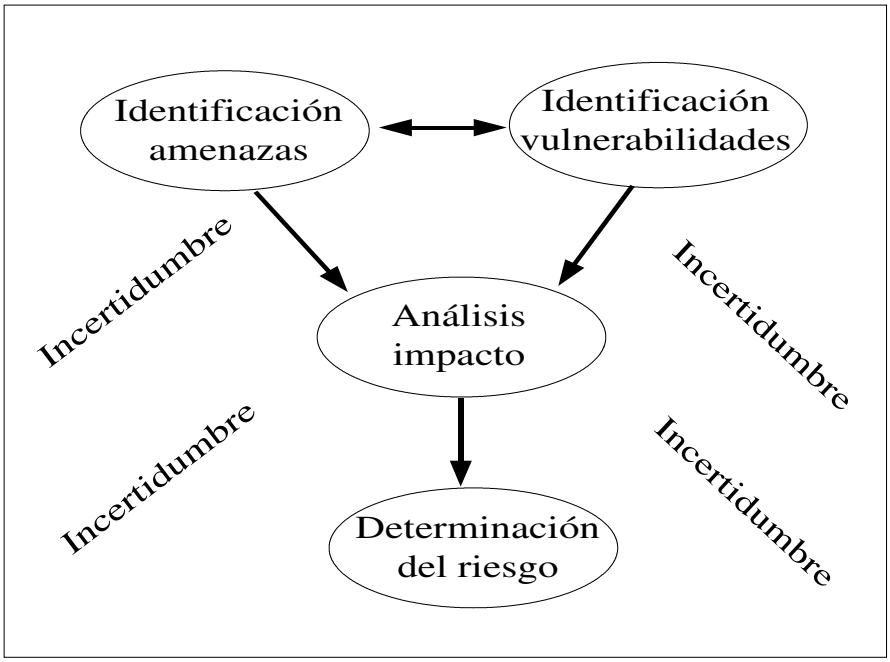


Figura 10. Interrelación de las Etapas de Evaluación de Riesgos

Identificación de las Amenazas

Una amenaza es una entidad o evento con el potencial para perjudicar un sistema. Amenazas típicas son errores, fraude, empleados disgustados, fuego, inundaciones, virus, y hackers.

Las amenazas deben ser identificadas y analizadas para determinar la probabilidad de su ocurrencia y su potencial para dañar los activos de la organización.

Además de analizar las amenazas más importantes, se deben investigar áreas poco estudiadas, nuevas o no documentadas. Si algún activo de la Organización ha sido bien asegurado y tiene un buen control de acceso, se requerirá menos esfuerzo para identificar amenazas a éste que en el caso de software o procedimientos de almacenamiento no probados.

Es fundamental concentrarse en aquellas amenazas con mayor probabilidad de ocurrencia y que puedan afectar activos importantes. En muchos casos, determinar qué amenazas son más realistas no es posible incluso después de haber realizado el proceso de identificación.

La probabilidad de ocurrencia es una estimación de la frecuencia o capacidad para que suceda una amenaza. Se debe considerar la presencia, tenacidad y fortaleza de las amenazas así como la efectividad de los correctivos.

En general, la información que existe sobre muchas amenazas es insuficiente, particularmente con las de origen humano, por lo tanto la experiencia en esta área es muy útil.

La regla general es: “entre mayor sea la probabilidad de ocurrencia de una amenaza, mayor es el riesgo”[27] .

Identificación de las Vulnerabilidades

Una vulnerabilidad es una condición o debilidad en los procedimientos de seguridad, controles técnicos, controles físicos, u otros controles que puedan ser aprovechados por una amenaza.

Normalmente las vulnerabilidades se analizan en términos de falencias existentes en las protecciones y correctivos de los sistemas.

Las vulnerabilidades contribuyen al riesgo, pueden permitir que una amenaza perjudique al sistema.

27 NIST. An Introduction to Computer Security. p. 61

También se presentan casos en que la ocurrencia de una vulnerabilidad induce la amenaza, por ejemplo algún empleado se ve tentado a alterar información cuando se encuentra un computador con una sesión abierta.

Análisis del Impacto

El análisis del impacto busca estimar el grado de perjuicio o pérdida que podría ocurrir. El impacto se refiere a todo el perjuicio agregado que ocurre no sólo al corto plazo, sino también al largo plazo.

Mientras los impactos a corto o mediano plazo a menudo resultan en revelación, modificación, destrucción o denegación de servicio, las consecuencias más significativas son los efectos de largo plazo, como pérdida del negocio, incapacidad para realizar la misión del sistema, pérdida de reputación, violación de la privacidad, lesiones o pérdida de la vida. Entre más severo sea el impacto de una amenaza, mayor es el riesgo al sistema, y por lo tanto a la organización.

Determinación del Riesgo

La evaluación del riesgo se usa para soportar dos funciones relacionadas: la aceptación del riesgo y la selección de controles o correctivos efectivos. Para cumplir con estas funciones, la evaluación de riesgos debe producir resultados muy claros y útiles que reflejen lo verdaderamente importante para la Organización. Para determinar los riesgos se debe limitar su interpretación hacia los riesgos más significativos, y así lograr que el proceso se enfoque a reducir el esfuerzo total mientras se consiguen resultados útiles.

Los resultados de este proceso pueden ser representados de forma cualitativa y/o cuantitativa. Las medidas cuantitativas pueden ser expresadas por ejemplo en términos de la reducción de pérdidas monetarias esperadas[28]. Las medidas cualitativas son descriptivas y pueden ser expresadas en términos como: alto, medio o bajo.

Si los riesgos son determinados e interpretados de forma consistente en la Organización, los resultados pueden utilizarse para priorizar la seguridad de los sistemas.

28 NIST. An Introduction to Computer Security. p. 63

3.4. SUBETAPA DE ESTUDIO DE INGENIERÍA

El estudio de ingeniería es la subetapa en la cual, se estudian los detalles técnicos de la Infraestructura de Llaves Públicas desde la perspectiva de hardware y software.

ACTIVIDAD 1: ANÁLISIS DE REQUERIMIENTOS

Basándose en la información que ha sido recopilada y en el Plan de Desarrollo del Proyecto y el Análisis de Riesgos, más las necesidades que van surgiendo, la primera actividad a realizar es encontrar los requerimientos en las siguientes áreas:

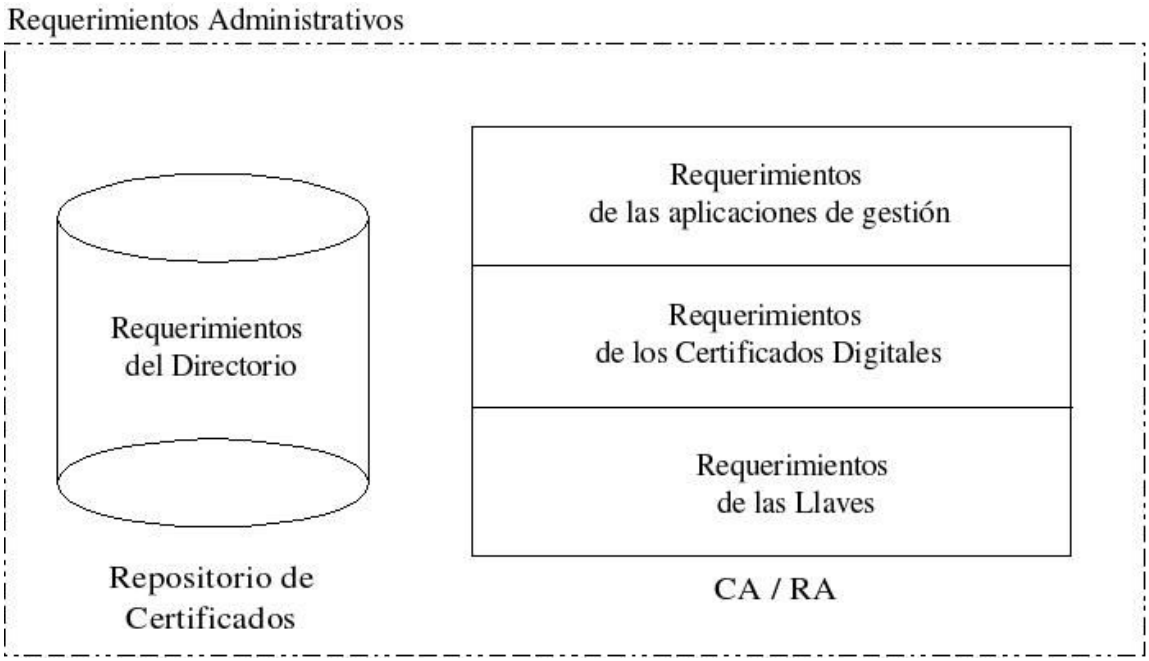


Figura 11. Requerimientos de una Entidad de Certificación

a) REQUERIMIENTOS GENERALES

La organización necesita determinar si alguno o todos los requerimientos listados a continuación deben ser tenidos en cuenta al momento de la realización del documento:

1. La Entidad de Certificación debe ser construida en un ambiente 24x7, donde los servicios se encuentran disponibles a todo momento.

2. El tiempo en que la solución PKI va a ser construida debe ser definida y comunicada a los miembros de la organización.

3. Todos los productos comprados y sus componentes (Hardware y Software) deben tener una garantía mínima de un año, después de la implementación.

4. La solución debe proveer servicio técnico al cliente 24x7 (24 horas, los 7 días de la semana). El fabricante debe responder a la llamada en un lapso máximo de 2 horas, y solucionar el problema en un tiempo menor de 12 horas.

5. El mantenimiento preventivo debe ser programado según la conveniencia del cliente.

6. La solución propuesta debe incluir herramientas para integrarse con productos complementarios dentro de la PKI, según las necesidades del cliente.

7. La solución propuesta debe permitir a la organización emitir y revocar llaves mapeadas en objetos X.500[29]

8. La capacidad de gestión de certificados debe mantener y distribuir certificados X.509 para asegurar las comunicaciones entre cualquier entidad que soporte la PKI.

9. La solución propuesta debe asegurarse que los passwords no vayan a ser transmitidos en "texto plano" a través de la red o que vayan a ser almacenados sin ningún tipo de seguridad.

10. La arquitectura debe basarse en estándares y soportar al menos: X509v3, LDAP, PKCS #11 y S/MIME

b) REQUERIMIENTOS ADMINISTRATIVOS

1. La solución PKI debe proveer la personalización de las funciones administrativas de la Entidad de Certificación

2. La solución debe incluir un plan de recuperación de llaves y que no comprometa la organización legalmente.

3. La solución debe proveer mecanismos para la separación administrativa de funciones para garantizar la seguridad de los datos más importantes.

4. Se deben prestar servicios de estampillado del tiempo en la PKI para garantizar la validez

29 X.500 es la especificación del protocolo para acceder a un directorio organizacional.

temporal de las transacciones

5. La solución debe dar la posibilidad de ver el estado las transacciones por medio de herramientas de generación de reportes.

6. El producto debe tener un sistema espejo donde se pueda administrar la Entidad de Certificación.

c) REQUERIMIENTOS DE LAS APLICACIONES

1. La solución debe dar la posibilidad de extender su dominio de confianza a través de otras autoridades de certificación de manera jerárquica o distribuida.

2. La solución debe dar la posibilidad de instalar múltiples Autoridades de Registro para ejecutar funciones administrativas en la PKI.

3. La solución debe tener mecanismos de generación de reportes para los usuarios finales y para los administradores.

4. La solución debe tener soporte para VPNs.

5. La solución debe dar la posibilidad de escoger entre varios tipos de certificados en la misma infraestructura y que puedan ser enviados a diferentes usuarios con diferentes perfiles.

6. La solución debe estar provista de confidencialidad, integridad, aceptación, identificación, autenticación y autorización.

7. La solución debe tener soporte para usb tokens, tarjetas inteligentes, dispositivos biométricos y otros dispositivos de autenticación.

8. La solución debe tener soporte para correo seguro, S/MIME y otras aplicaciones de comercio electrónico y en múltiples plataformas.

d) REQUERIMIENTOS DE LOS CERTIFICADOS PKI

1. La solución debe brindar una interfaz de usuario amigable e intuitiva para gestionar los certificados digitales.

2. La solución debe ser escalable

3. La solución debe tener la posibilidad de emitir certificados internamente, y externamente a otras entidades y clientes.

4. La solución debe tener soporte para el uso de extensiones personalizadas y que puedan ser incluidas en los certificados emitidos por la Entidad de Certificación.

5. La solución debe contar con la posibilidad de consulta de certificados digitales de los usuarios.

6. La solución debe ser capaz de gestionar la revocación de certificados en una organización de mediano personal (10000 usuarios).

e) REQUERIMIENTOS DE LAS LLAVES

1. La solución debe contar con la funcionalidad de recuperación de llaves, tanto a nivel de usuario como a nivel de administración.

2. La solución debe contar con un historial de cambios realizados a las llaves, tales como cambios de nombre, cambios de departamento y cualquier cambio físico que surja como consecuencia de los anteriores.

3. La solución debe almacenar con seguridad la llave privada de firmado de la Autoridad de Certificación raíz y sus subordinados.

f) REQUERIMIENTOS DEL DIRECTORIO

1. La solución debe emitir certificados a cualquier aplicación basada X.509 tales como aplicaciones web y VPNs.

2. La solución debe ser capaz de integrarse con otros directorios existentes y de otros fabricantes y poder compartir sus nombres y atributos.

TEMAS Y PREGUNTAS A TENER EN CUENTA DURANTE LA ACTIVIDAD DEL ANÁLISIS DE REQUERIMIENTOS

1. Determinación de los lenguajes y plataformas sobre los cuales se va a soportar la infraestructura

de seguridad.

2. Definición de los detalles del plan de recuperación la Autoridad de Certificación.

3. Administración distribuida de los certificados digitales, los registros y la revocación.

4. Evaluación del proceso de recuperación de 1000 correos electrónicos seguros debido a una pérdida de password. ¿Cómo puede ser afrontado este problema, de la forma más sencilla posible ?

5. Búsqueda de alguna calificación o estudio de "benchmarking" de confianza acerca de hardware de seguridad enfocado a los servicios de identificación digital.

6. Realización del estudio sobre cuál escritorio es más seguro (si se escoge el uso de una GUI). Buscar el Sistema Operativo más adecuado para soportar las aplicaciones de seguridad.

7. Entendimiento del proceso de revocación de certificados. ¿ La solución soporta una revocación de certificados en tiempo real?

8. Definición de la consulta de certificados revocados offline

9. ¿ Cómo es el proceso para que los certificados digitales sean visibles por cualquier persona?

10. Análisis del número de pasos que se tienen que llevar a cabo para solicitar un certificado digital.

11. Análisis de los detalles relevantes de las llaves y sus posibles limitaciones.

12. Observación de cómo el sistema actúa frente a un cambio de nombre en el certificado y ver si aún continúa el historial del usuario.

13. Análisis del proceso de desciframiento de los datos cuando es cifrado por otro usuario. Realizar ésto tanto online, como offline.

14. Analizar las opciones privativas y libres para implementación del servicio de directorio.

15. Determinación de los algoritmos criptográficos a ser utilizados.

16. Análisis de la necesidad de hardware adicional como generador de números aleatorios y acelerador criptográfico en la solución a implementar.

PLANTILLA PARA REALIZACIÓN DEL DOCUMENTO DE REQUERIMIENTOS

1. INTRODUCCIÓN
2. REQUERIMIENTOS GENERALES
3. REQUERIMIENTOS ADMINISTRATIVOS
4. REQUERIMIENTOS DE LAS APLICACIONES DE GESTIÓN
5. REQUERIMIENTOS DE LOS CERTIFICADOS PKI
6. REQUERIMIENTOS DE LAS LLAVES
7. REQUERIMIENTOS DEL DIRECTORIO
8. OTROS REQUERIMIENTOS
9. CONCLUSIONES Y RECOMENDACIONES

ACTIVIDAD 2: DISEÑO DE LA ARQUITECTURA PKI

El documento de diseño de la arquitectura PKI es el escrito donde se definirá el sistema que dará soporte a los procesos relacionados con certificados digitales y los servicios de identificación digital.

Dejando a un lado los servicios de identificación digital y enfocándose en la arquitectura de seguridad, siempre son necesarios algunos elementos PKI básicos, como una Autoridad de Certificación (CA), una Autoridad de Registro (RA) y un repositorio de certificados. Éstos pueden estar combinados en un sólo servidor, o soportados en varios.

Un tema importante a tener en cuenta al momento de realizar la arquitectura de la PKI, es tener en cuenta la infraestructura de red con la que se cuenta (en caso que se tenga). La arquitectura CA (Autoridad de Certificación) es una consideración primaria, la arquitectura más simple es la que tiene la CA raíz y expide directamente todos los certificados.

Figura 12. Arquitectura PKI Plana

Esta arquitectura tiene entre sus ventajas, que implica menos costos en hardware y software; además su gestión es más sencilla. No obstante, hacer que la PKI sea accesible por los usuarios, es una cuestión que arriesga la seguridad del sistema. Por esta razón, se puede pensar en una CA jerárquica para evitar este tipo problemas, ya que la CA raíz sólo expide certificados a sus CA subsidiarias y después puede quedar fuera de línea.

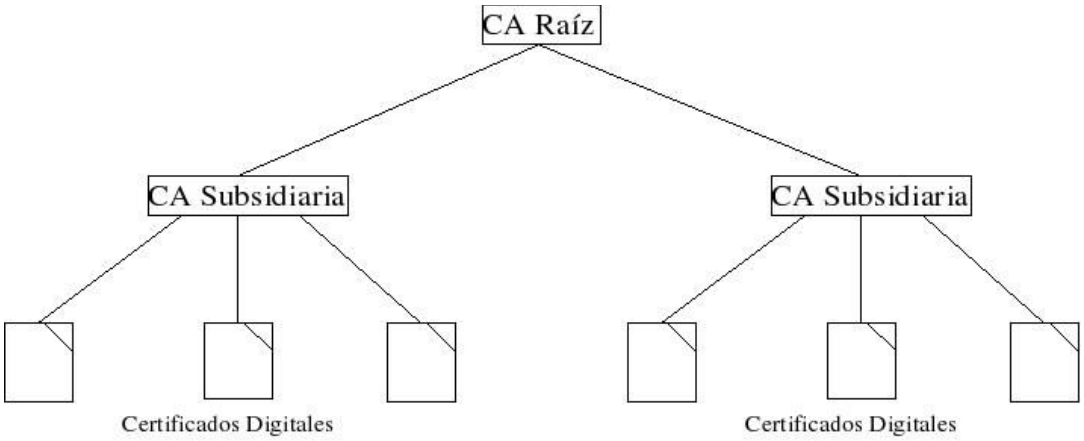


Figura 13. Arquitectura PKI Jerárquica

Otro tema de la arquitectura es determinar si se separa la función de registro de la CA. A menudo, la seguridad es un factor guía, dado que tener solicitantes de certificados interactuando directamente con la CA abre una ruta hacia intentos de intromisión. Si estos intentos tienen éxito, el nivel de confianza que se puede tener en la CA se puede derrumbar y la administración se enfrentaría a problemas como la reexpedición de todos los certificados.

Los servidores RA también pueden ayudar a reducir el tráfico hacia la CA. Además se puede instalar la CA en una instalación segura y alejada de los servidores RA.

Las preguntas que a este punto se tienen que plantear son las siguientes:

1. ¿Cuántos niveles debe tener la jerarquía CA?
2. ¿Habrá algún usuario externo al certificado?
3. ¿Serán elementos consolidados o separados, los que realicen las funciones de la CA, como la RA y el repositorio de certificados?. Si son separados, ¿cuántos serán necesarios de cada uno? ¿En dónde estarán localizados?

MANEJO DE LOS USUARIOS

Los usuarios, son un elemento importante al momento de pensar en la arquitectura de la PKI, ya que para éllos se busca la seguridad de los datos. Sin embargo, existen usuarios difíciles, quienes hay que tener en cuenta al momento de la realización de la arquitectura como aquellos que tienden a olvidar sus contraseñas. Además, obligar a una presencia física ante una autoridad de registro puede llegar a ser un problema, si se está hablando de grandes poblaciones (más de 10000 personas). Otro problema es la separación geográfica de los usuarios, ya que se impone un obstáculo para la generación y renovación de los certificados.

Es por eso, que se deben tener en cuenta las siguientes preguntas, en el momento del diseño de la arquitectura PKI

1. ¿Cuántos usuarios recibirán certificados? ¿Cuántos de estos usuarios son internos a la empresa? ¿Cuántos externos?

2. ¿Cuántos tipos de usuarios existen y cuáles son? ¿Alguna de éstas categorías de usuarios requerirá diferentes formas de identificación antes que se les pueda expedir un certificado?

3. ¿Dónde se encuentran localizados los usuarios? ¿Se encuentran dentro de un lugar o dispersos en una región?

CONTENIDO DEL CERTIFICADO

La interoperabilidad es una característica fundamental de cualquier sistema PKI y por ende el diseño de los perfiles de certificados.

Un perfil de certificado define la manera como se deben codificar elementos específicos del certificado. Si una CA afirma que expide certificados que siguen un perfil específico, las

aplicaciones que usen PKI tienen una buena idea sobre la manera de decodificar los certificados de esa CA.

Sin embargo, adoptar un perfil puede no ofrecer suficiente definición para el certificado. Perfiles como PKIX definen campos básicos que deben aparecer en los certificados, pero todavía suministran opciones de codificación para algunos campos.

Publicar certificados en una estructura de directorio existente puede ser un aspecto por considerar si el *nombre distinguido* (DN) del directorio no corresponde con el DN de la Autoridad de Certificación (CA). En casos como éste, habría que realizar una adaptación software del gestor de certificados y el directorio organizacional, esto se puede hacer de dos formas: una es modificando el código fuente, en caso que sea software libre u otra es solicitando a la empresa que desarrolla el software que realice los cambios.

En este punto, vale la pena resaltar las siguientes preguntas:

1. ¿Son aplicables los perfiles de certificados a la PKI que se está diseñando? ¿Qué tan bien se alinean con las otras necesidades de las aplicaciones PKI?

2. ¿Qué algoritmos de cifrado y longitudes de clave se usarán en los certificados?

3. ¿Se usarán certificados para firmar y cifrar? ó ¿Se expedirán certificados para firmar separados?

4. ¿Qué campos de certificados se necesitarán para las aplicaciones PKI? ¿Para soportar los socios? ¿Qué extensiones adicionales se usarán?

DISEÑO DE LA BASE DE DATOS

La mayoría de las grandes organizaciones están migrando los repositorios de usuarios a directorios organizacionales, tales como LDAP (Lightweight Directory Access Protocol). Es por eso que se deben evaluar estos elementos al momento del diseño de la arquitectura PKI.

De ahí la importancia de definir si los datos de usuarios y sus certificados irán en un directorio o en una base de datos, ya que habría que establecer estrategias para cumplir con el estándar. Usualmente es supone que los certificados se publican en directorios LDAP, debido a que es la forma más común para realizar esa labor. Otro punto de suma importancia es definir si los certificados se agregarán junto a la entrada de los usuarios o se hará en una nueva parte del

directorio.

Los certificados revocados y los que se hayan vencido son otro aspecto de la base de datos. Los primeros deben estar almacenados de modo que se puedan seguir verificando las firmas en documentos antiguos. Sin embargo, estos certificados consumirán espacio de almacenamiento, por lo que se deberá decidir cuánto tiempo durarán los certificados revocados almacenados antes de declararse "fuera de uso".

Otro aspecto importante es saber gestionar los certificados de los usuarios cuando éste posee más de uno. Es por eso, que se debe pensar en soluciones como *tipos de objeto* identificadores para el certificado en uso y otro, para los certificados revocados.

En caso, que se desee integrar el uso de los certificados digitales con algún mecanismo de autenticación, se debe considerar la integración de los certificados y las cuentas de usuario, de modo que este último recibe un certificado, cuando se le expida una cuenta corporativa.

Las preguntas que se deben realizar respecto al diseño de la base de datos que va a soportar la PKI, son las siguientes:

1. ¿Se utilizarán las bases de datos corporativas existentes para dinamizar la inscripción de certificados?

2. ¿El esquema predeterminado de publicación del directorio de la CA, cómo se sincronizará con el esquema de directorio existente? ¿Se puede ajustar el producto CA para corresponder con su esquema? ¿Se requerirá personalización?

3. ¿Se dejarán en la base de datos los certificados revocados y los que han expirado?

4. ¿Se integrará un repositorio de certificados con la administración de la cuenta de usuario?

SEGURIDAD PERIMETRAL

La seguridad perimetral es un aspecto complementario pero de suma importancia al momento de diseño de la arquitectura PKI ya que es la encargada de garantizar el debido aislamiento entre los elementos de la red que se deseen deber estarlo, tales como la CA Raíz y el Servidor de Directorio. Es por eso, que se deben tener en cuenta la inclusión de Firewalls y Detectores de Intrusos dentro de la arquitectura PKI.

Un firewall es un elemento de red cuya función es prevenir comunicaciones inseguras, de acuerdo a unas políticas establecidas. Un firewall tiene la tarea básica de controlar el tráfico entre distintas zonas de confianza. Las típicas zonas de confianza son la Internet (Zona con NO confianza) y una red interna (Zona con ALTA confianza). El objetivo final es dar conectividad controlada entre zonas con diferentes niveles de confianza bajo la regla por defecto del menor privilegio posible. Existen distintos tipos de firewalls, tales como los firewall de nivel de red y los firewall de nivel de aplicación, entre otros.

Los sistemas de detección de intrusos (IDS) son elementos de red que son utilizados para detectar accesos no autorizados a los servidores de producción de una organización, es decir, a la Autoridad de Certificación y a las Autoridades de Registro de la arquitectura PKI. Los IDS son necesarios para detectar tráfico de red malicioso y ciertos tipos de ataques como los orientados a las aplicaciones, al host, escala de privilegios, inicio de sesión no autorizado, acceso a los archivos sensibles y malware (virus, troyanos y gusanos).

Todo esto ayuda a la creación de zonas desmilitarizadas (DMZ) dentro de la arquitectura, que son áreas de la red de datos que se encuentran ubicadas entre la red interna de la organización y una red externa, que es usualmente la internet.

PLANTILLA PARA LA ARQUITECTURA DE LA PKI

1. INTRODUCCIÓN
2. DESCRIPCIÓN DE LA ARQUITECTURA
3. DESCRIPCIÓN DEL PROCESO DE CERTIFICACIÓN
4. FUNCIONES ORGANIZACIONALES DE LA ENTIDAD DE CERTIFICACIÓN
5. CONCLUSIONES Y RECOMENDACIONES

3.5. SUBETAPA DE ELABORACIÓN DE LAS POLÍTICAS DE CERTIFICACIÓN Y DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

ACTIVIDAD 1: ELABORACIÓN DE LAS POLÍTICAS DE CERTIFICACIÓN

El estándar X.509 define las políticas de certificación como "un conjunto de reglas que indican la aplicabilidad de un certificado a una comunidad en particular y/o a una aplicación con ciertos requerimientos de seguridad". La versión 3, de un certificado X.509 puede tener una indicación de políticas de certificación, la cual puede ser utilizada por un usuario para decidir si confiar o no del certificado. Una política de certificación, es representado dentro del certificado digital por medio de un identificador de objeto (OID).

Las políticas de certificación se soportan en tres campos, dentro del certificado digital: extensión de políticas de certificación, extensión de mapeo de las políticas y extensión de políticas de restricción.

EXTENSIÓN DE POLÍTICAS DE CERTIFICACIÓN

La extensión de políticas de certificación tiene dos variantes: una marcada como crítica y otra como no crítica.

Las políticas de certificados marcadas como "no críticas", listan las políticas que la Autoridad de Certificación declara que son aplicables, sin embargo, el uso del certificado no se encuentra restringido a los propósitos indicados en las políticas aplicables.

Si las políticas de certificación se marcan "críticas", actúa como las enunciadas en el párrafo anterior, pero con un rol adicional, que es indicar que el uso del certificado se encuentra restringido a una de las políticas identificadas. Por ejemplo, la autoridad de certificación decide que el certificado sólo debe ser utilizado de acuerdo a los términos listados en las políticas de certificación. Ésto se realiza con el fin de proteger a la Autoridad de Certificación contra el daño ocasionado por un usuario de confianza que utiliza un certificado de manera inapropiada de acuerdo a lo estipulado en las políticas de certificación.

EXTENSIÓN DE MAPEO DE LAS POLÍTICAS

La extensión de mapeo de políticas sólo es utilizada por las Autoridades de Certificación, para indicar que ciertas políticas de su dominio pueden ser consideradas equivalentes a otras políticas que se encuentran en el dominio del objeto de certificación.

Por ejemplo, la organización A va a establecer una relación de confianza con la organización B, a

través de un acuerdo de certificación cruzada con el propósito de proteger el EDI (Intercambio Electrónico de Datos). Sin embargo, A tiene una política de protección a las transacciones financieras llamada A-e-commerce. Así mismo B tiene una llamada B-e-commerce. A simple vista se puede ver que la generación de certificados entre ambos dominios no proveerá la interoperabilidad necesaria ya que ambas tienen sus propias políticas para protección de transacciones. Una solución a este problema es reconfigurar las aplicaciones financieras para que soporten ambas políticas. Y la otra es, utilizar el mapeo de políticas, que simplemente diría que la política A-e-commerce es equivalente en el Dominio A, a la política B-e-commerce del dominio B.

EXTENSIÓN DE POLÍTICAS DE RESTRICCIÓN

La extensión de las políticas de restricción soporta dos características opcionales. La primera, es la capacidad de la Autoridad de Certificación para requerir que las indicaciones de una política de certificado se encuentre explícitamente en todos los certificados subordinados de la ruta de certificación. Los certificados que se encuentren al principio de la ruta serán considerados por el usuario como parte del dominio de confianza.

La otra opción es la capacidad de la Autoridad de Certificación para deshabilitar las políticas de mapeo para las autoridades de certificación subordinadas en una ruta de certificación. Ésto es útil cuando la certificación sale del dominio de confianza. Por ejemplo, A confía en B y B confía en C, pero A no está obligado a confiar en C.

ACTIVIDAD 2: ELABORACIÓN DE LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

El término "Declaración de Prácticas de Certificación" es definido por la ABA[30] como aquella "declaración de práctica" que utiliza que una Autoridad de Certificación para emitir certificados.

La *Declaración de Prácticas de Certificación* se puede tomar como la información en la cual la Autoridad de Certificación describe sus sistemas de confianza y las prácticas que utiliza en sus operaciones y emisión de certificados, o puede ser un estatuto o regulación aplicable a la Autoridad de Certificación cubriendo un tema similar. Puede ser también un contrato entre la Autoridad de Certificación y el suscriptor. Una *Declaración de Prácticas de Certificación* puede ser comprendida por múltiples documentos entre los cuales se puede encontrar un documento legal, un contrato privado y/o una declaración.

Existen ciertas vías para implementar de manera legal la *declaración de prácticas de certificación*, las cuales permiten establecer relaciones particulares entre la CA y el suscriptor. Muchas veces

30 ABA. American Bar Association. <http://en.wikipedia.org/wiki/American_Bar_Association>

cuando existe una relación preestablecida de confianza entre elementos de una PKI, el documento de *declaración de prácticas de certificación* es el documento que simplemente se utiliza para darle efecto legal a esa relación.

Algo importante respecto a la *declaración de prácticas de certificación* es hacerle entender al suscriptor el compromiso de aceptarlas, ya que el respectivo entendimiento de los términos aumentaría el nivel de responsabilidad del usuario respecto a los certificados digitales.

DIFERENCIA ENTRE LAS PC Y LA DPC

La *Declaración de Prácticas de Certificación* es un documento detallado acerca de la Entidad de Certificación y sus prácticas, que necesitan ser entendidas por el suscriptor y consultada por terceros (ya sean de confianza o no). Usualmente este documento es mucho más detallado que la definición de las políticas de certificación. Por ende, las DPC son mucho más comprensibles y robustas, y además brindan información útil como los servicios ofrecidos por la CA y el ciclo de vida del certificado digital en la organización.

Aunque el documento de *declaración de prácticas de certificación* es indispensable para entender el funcionamiento de la Autoridad de Certificación, no garantiza la interoperabilidad entre éllas. Es por eso que existen las Políticas de Certificación, que son la solución técnica a ese tipo de circunstancias.

La principales diferencias entre la *declaración de prácticas de certificación* y las *políticas de certificación* son las siguientes:

- La mayoría de las organizaciones que operan una Entidad de Certificación documentan sus prácticas en una *declaración de prácticas de certificación*. La DPC es uno de los medios que tiene la organización para protegerse legalmente y posicionar las relaciones de negocio con sus suscriptores y otras entidades.
- En el otro lado se tiene las *políticas de certificación*, que son aplicables a más de una organización. Es posible ver que si una política es lo suficientemente buena, será aplicada de manera masiva por muchas Entidades de Certificación, mientras que eso no se puede hacer con *la declaración de prácticas de certificación*. Es así, como se pueden ver políticas de certificación aplicadas a una empresa, mientras que declaración de prácticas de certificación aplicada a una sola.

PLANTILLA PARA LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

1. Introducción
2. Términos generales
3. Identificación y Autenticación
4. Requerimientos Operacionales
5. Control de Seguridad Física, Procedimental y de Personal
6. Control de Seguridad Técnica
7. Perfiles de Certificados y CRLs
8. Administración de especificaciones.

3.6. SUBETAPA DE ESTUDIO DE LAS INSTALACIONES FÍSICAS

Las instalaciones Físicas de la Entidad de Certificación deben estar ubicadas en áreas protegidas y resguardadas por un perímetro de seguridad definido, con vallas de seguridad y controles de acceso apropiados. Deben estar físicamente protegidas contra accesos no autorizados, daños e intrusiones. Se deben tener mecanismos para recuperación de desastres y planes de contingencia.

Requerimientos para Instalaciones Seguras

Perímetro Físico de Seguridad

La protección física puede llevarse a cabo mediante la creación de diversas barreras físicas alrededor de las sedes de la organización y de las instalaciones de la Entidad de Certificación. Cada barrera establece un perímetro de seguridad, cada uno de los cuales incrementa la protección total provista.

Las organizaciones deben utilizar perímetros de seguridad para proteger las áreas que contienen instalaciones físicas de la Entidad de Certificación. Un perímetro de seguridad es algo delimitado por una barrera, por ej. una pared, una puerta de acceso controlado por tarjeta o un escritorio u oficina de recepción atendidos por personas. El emplazamiento y la fortaleza de cada barrera dependerán de los resultados de una evaluación de riesgos.

Se deben considerar e implementar los siguientes lineamientos y controles, según corresponda:

a) El perímetro de seguridad debe estar claramente definido.

b) El perímetro de un edificio o área que contenga las Instalaciones de la Entidad de Certificación debe ser físicamente sólido (por ej. no deben existir claros [o aberturas] o áreas donde pueda producirse fácilmente una irrupción). Las paredes externas del área deben ser de construcción sólida y todas las puertas que comunican con el exterior deben ser adecuadamente protegidas contra accesos no autorizados, por ej., mediante mecanismos de control, vallas, alarmas, cerraduras, etc.

c) Debe existir un área de recepción atendida por personal u otros medios de control de acceso físico al área o edificio. El acceso a las distintas áreas y edificios debe estar restringido exclusivamente al personal autorizado.

d) Las barreras físicas deben, si es necesario, extenderse desde el piso hasta el techo, a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo, la ocasionada por incendio e inundación.

e) Todas las puertas de incendio de un perímetro de seguridad deben tener alarma y cerrarse automáticamente.

Controles Físicos de Acceso

Las áreas protegidas deben ser resguardadas por adecuados controles de acceso que permitan garantizar que sólo se permite el acceso de personal autorizado. Deben tenerse en cuenta los siguientes controles:

a) Los visitantes de áreas protegidas deben ser supervisados o inspeccionados y la fecha y horario de su ingreso y egreso deben ser registrados. Sólo se debe permitir el acceso a los mismos con propósitos específicos y autorizados, instruyéndose en dicho momento al visitante sobre los requerimientos de seguridad del área y los procedimientos de emergencia.

b) El acceso a la información sensible, y a las instalaciones de la Entidad de Certificación, debe ser controlado y limitado exclusivamente a las personas autorizadas. Se deben utilizar controles de autenticación, por ej. tarjeta y número de identificación personal (PIN), para autorizar y validar todos los accesos. Debe mantenerse una pista protegida que permita auditar todos los accesos.

c) Se debe requerir que todo el personal exhiba alguna forma de identificación visible y se lo debe alentar a cuestionar la presencia de desconocidos no escoltados y a cualquier persona que no exhiba una identificación visible.

d) Se deben revisar y actualizar periódicamente los derechos de acceso a las áreas protegidas.

Protección de las Instalaciones Físicas de la Entidad de Certificación

El área protegida debe estar cerrada con llave, o dentro de un perímetro de seguridad física, el cual puede estar bloqueado y contener cajas fuertes o gabinetes con cerraduras.

Para la selección y el diseño de un área protegida debe tenerse en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También deben tomarse en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad. Asimismo, se deberán considerar las amenazas a la seguridad que representan los edificios y zonas aledañas, por ej. filtración de agua desde otras áreas.

Se deben considerar los siguientes controles:

a) Las instalaciones deben ubicarse en lugares a los cuales no pueda acceder el público.

b) Los edificios deben ser discretos y ofrecer un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores, que identifiquen la presencia de actividades de procesamiento por parte de la Entidad de Certificación.

c) Las puertas y ventanas deben estar bloqueadas cuando no hay vigilancia y debe considerarse la posibilidad de agregar protección externa a las ventanas, en particular las que se encuentran al nivel del suelo.

d) Se deben implementar adecuados sistemas de detección de intrusos. Los mismos deben ser instalados según estándares profesionales y probados periódicamente. Estos sistemas comprenderán todas las puertas exteriores y ventanas accesibles. Las áreas vacías deben tener alarmas activadas en todo momento. También deben protegerse otras áreas, como la sala de cómputos o las salas de comunicaciones.

e) Las instalaciones físicas de la Entidad de Certificación administradas por la organización deben estar físicamente separadas de aquellas administradas por terceros.

f) Las guías telefónicas y listados de teléfonos internos que identifican las ubicaciones de las instalaciones de la Entidad de Certificación no deben ser fácilmente accesibles al público.

g) Los materiales peligrosos o combustibles deben ser almacenados en lugares seguros a una distancia prudencial del área protegida. Los suministros a granel, como los útiles de escritorio, no deben ser almacenados en el área protegida hasta que sean requeridos.

h) El equipamiento de sistemas de soporte UPC (Usage Parameter Control) de reposición de información perdida ("fallback") y los medios informáticos de resguardo deben estar situados a una distancia prudencial para evitar daños ocasionados por eventuales desastres en el sitio principal.

Desarrollo de Tareas en Áreas Protegidas

Para incrementar la seguridad de un área protegida pueden requerirse controles y lineamientos adicionales.

Esto incluye controles para el personal o terceras partes que trabajan en el área protegida,

así como para las actividades de terceros que tengan lugar allá. Se deberán tener en cuenta los siguientes puntos:

a) El personal sólo debe tener conocimiento de la existencia de un área protegida, o de las actividades que se llevan a cabo dentro de la misma, según el criterio de necesidad de conocer.

b) Se debe evitar el trabajo no controlado en las áreas protegidas tanto por razones de seguridad como para evitar la posibilidad de que se lleven a cabo actividades maliciosas.

c) Las áreas protegidas desocupadas deben ser físicamente bloqueadas y periódicamente inspeccionadas.

d) El personal del servicio de soporte externo debe tener acceso limitado a las áreas

protegidas. Este acceso debe ser otorgado solamente cuando sea necesario y debe ser autorizado y monitoreado. Pueden requerirse barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, y que están ubicadas dentro del mismo perímetro de seguridad.

e) A menos que se autorice expresamente, no debe permitirse el ingreso de equipos fotográficos, de vídeo, audio u otro tipo de equipamiento que registre información.

Aislamiento de las Áreas de Entrega y Carga

Las áreas de entrega y carga deben ser controladas y, si es posible, estar aisladas de las instalaciones físicas de la Entidad de Certificación, a fin de impedir accesos no autorizados. Los requerimientos de seguridad de dichas áreas deben ser determinados mediante una evaluación de riesgos. Se deben tener en cuenta los siguientes lineamientos:

a) El acceso a las áreas de depósito, desde el exterior de la sede de la organización, debe estar limitado a personal que sea previamente identificado y autorizado.

b) El área de depósito debe ser diseñada de manera tal que los suministros puedan ser descargados sin que el personal que realiza la entrega acceda a otros sectores del edificio.

c) Todas las puertas exteriores de un área de depósito deben ser aseguradas cuando se abre la puerta interna.

d) El material entrante debe ser inspeccionado para descartar peligros potenciales antes de ser trasladado desde el área de depósito hasta el lugar de uso.

e) El material entrante debe ser registrado, si corresponde, al ingresar al sitio pertinente.

Seguridad del Equipamiento

El equipamiento debe estar físicamente protegido de las amenazas a la seguridad y los peligros del entorno. Es necesaria la protección del equipamiento (incluyendo el que se utiliza en forma externa) para reducir el riesgo de acceso no autorizado a los datos y para prevenir pérdidas o daños. Esto también debe tener en cuenta la ubicación y disposición del equipamiento. Pueden requerirse controles especiales para prevenir peligros o accesos no autorizados, y para proteger instalaciones de soporte, como la infraestructura de cableado y suministro de energía eléctrica.

Ubicación y Protección del Equipamiento

El equipamiento debe ser ubicado o protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado. Se deben tener en cuenta los siguientes puntos:

a) El equipamiento debe ser ubicado en un sitio que permita minimizar el acceso innecesario a las áreas de trabajo.

b) Las instalaciones de la Entidad de Certificación, que manejan datos sensibles, deben ubicarse en un sitio que permita reducir el riesgo de falta de supervisión de las mismas durante su uso.

c) Se deben adoptar controles para minimizar el riesgo de amenazas potenciales, por ej. robo, incendio, explosivos, humo, agua o falta de suministro, polvo, vibraciones, efectos químicos, interferencia en el suministro de energía eléctrica, radiación electromagnética.

d) La organización debe analizar su política respecto de comer, beber y fumar cerca de las instalaciones de la Entidad de Certificación.

e) Se deben monitorear las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de la Entidad de Certificación.

f) Se debe considerar el impacto de un eventual desastre que tenga lugar en zonas próximas a la sede de la organización, por ej. un incendio en un edificio cercano, la filtración de agua desde el cielo raso o en pisos por debajo del nivel del suelo o una explosión en la calle.

Suministros de Energía

El equipamiento debe estar protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. Se debe contar con un adecuado suministro de energía que esté de acuerdo con las especificaciones del fabricante o proveedor de los equipos. Entre las alternativas para asegurar la continuidad del suministro de energía podemos enumerar las siguientes:

a) múltiples bocas de suministro para evitar un único punto de falla en el suministro de energía.

b) suministro de energía ininterrumpible (UPS)

c) generador de respaldo.

Se recomienda una UPS para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas de la organización. Los planes de contingencia deben contemplar las acciones que han de emprenderse ante una falla de la UPS. Los equipos de UPS deben inspeccionarse periódicamente para asegurar que tienen la capacidad requerida y se deben probar de conformidad con las recomendaciones del fabricante o proveedor.

Se debe tener en cuenta el empleo de un generador de respaldo si el procesamiento ha de continuar en caso de una falla prolongada en el suministro de energía. De instalarse, los generadores deben ser probados periódicamente de acuerdo con las instrucciones del fabricante o proveedor. Se debe disponer de un adecuado suministro de combustible para garantizar que el generador pueda funcionar por un período prolongado.

Asimismo, los interruptores de emergencia deben ubicarse cerca de las salidas de emergencia de las salas donde se encuentra el equipamiento, a fin de facilitar un corte rápido de la energía en caso de producirse una situación crítica. Se debe proveer de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía. Se debe implementar protección contra rayos en todos los edificios y se deben adaptar filtros de protección contra rayos en todas las líneas de comunicaciones externas.

Seguridad del Cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información debe ser protegido contra interceptación o daño. Se deben tener en cuenta los siguientes controles:

a) Las líneas de energía eléctrica y telecomunicaciones que se conectan con las instalaciones de la Entidad de Certificación deben ser subterráneas, siempre que sea posible, o sujetas a una adecuada protección alternativa.

b) El cableado de red debe estar protegido contra interceptación no autorizada o daño, por ejemplo mediante el uso de conductos o evitando trayectos que atraviesen áreas públicas.

c) Los cables de energía deben estar separados de los cables de comunicaciones para evitar interferencias.

d) Entre los controles adicionales a considerar para los sistemas sensibles o críticos se encuentran los siguientes:

- instalación de conductos blindados y recintos o cajas con cerradura en los puntos terminales y de inspección.
- uso de rutas o medios de transmisión alternativos
- uso de cableado de fibra óptica
- iniciar barridos para eliminar dispositivos no autorizados conectados a los cables.

Mantenimiento de Equipos

El equipamiento debe mantenerse en forma adecuada para asegurar que su disponibilidad e integridad sean permanentes. Se deben considerar los siguientes lineamientos:

a) El equipamiento debe mantenerse de acuerdo con los intervalos servicio y especificaciones recomendados por el proveedor.

b) Sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.

c) Se deben mantener registros de todas las fallas supuestas o reales y de todo el

mantenimiento preventivo y correctivo.

d) Deben implementarse controles cuando se retiran equipos de la sede de la organización para su mantenimiento. Se debe cumplir con todos los requisitos impuestos por las pólizas de seguro.

Baja Segura o Reutilización de Equipamiento.

La información puede verse comprometida por una desafectación descuidada o una reutilización del equipamiento. Los medios de almacenamiento conteniendo material sensitivo, deben ser físicamente destruidos o sobrescritos en forma segura en vez de utilizar las funciones de borrado estándar.

Todos los elementos del equipamiento que contengan dispositivos de almacenamiento, por ej. discos rígidos no removibles, deben ser controlados para asegurar que todos los datos sensitivos y el software bajo licencia, han sido eliminados o sobrescritos antes de su baja. Puede ser necesario realizar un análisis de riesgo a fin de determinar si medios de almacenamiento dañados, conteniendo datos sensitivos, deben ser destruidos, reparados o desechados.

Requerimientos para Recuperación de Desastres

Las contingencias desde la Seguridad Computacional hacen referencia a un evento con el potencial para interrumpir las operaciones computacionales, y por lo tanto las funciones críticas del negocio para la Entidad de Certificación. Este tipo de eventos pueden darse por fallas eléctricas, problemas de hardware, fuego, tormentas. Si el evento es demasiado destructivo se le llama **Desastre**.

Para disminuir el daño que las contingencias y los desastres causan, las organizaciones pueden anticiparse para controlar el evento, a ésto se le llama **planeación de contingencias**, o **recuperación de desastres**, o **continuidad del negocio**. Va más allá que una planeación porque busca mantener las funciones críticas de la organización en operación en caso de la interrupción.

Proceso de Planeación de Contingencias y los requerimientos para recuperación de desastres se pueden enumerar en seis pasos:

1. **Identificar las funciones críticas del negocio**, de la Entidad de Certificación y establecer prioridades sobre éstas.
2. **Identificar los recursos que soportan esas funciones críticas**, además del marco de tiempo en que se usen, y el efecto de la falta de disponibilidad del recurso. Los tipos de recursos que soportan funciones críticas son: recursos humanos, datos y aplicaciones automatizadas, servicios basados en procesamiento computacional (servicios de comunicación, servicios de información y servicios que provee la Entidad de Certificación), infraestructura física, registros y documentación.
3. **Anticipar las contingencias o desastres potenciales**. Mediante la creación de

escenarios que ayuden a la organización a desarrollar un plan dirigido a un rango de aspectos que pueden salir mal. Los escenarios pueden contener contingencias menores y mayores. Es necesario la creatividad y la investigación para encontrar contingencias poco obvias.

4. **Seleccionar estrategias para las contingencias**. Es necesario considerar los controles que ya existan para prevenir y disminuir las contingencias, se debe coordinar prevención y recuperación. Una estrategia de este tipo normalmente consiste de tres partes: **respuesta a la emergencia** (acciones iniciales para proteger vidas y limitar el daño), **recuperación** (pasos para mantener el soporte de las funciones críticas) y **retorno a operación**. La selección de la estrategia debe ser basada en consideraciones prácticas como viabilidad y costo. Se puede usar la evaluación de riesgos para ayudar a estimar el costo de las opciones para una estrategia óptima, esta evaluación debe realizarse en áreas donde no hay claridad sobre la mejor estrategia a utilizar. Al desarrollar las estrategias se deben soportar los recursos identificados que soportan las funciones críticas.

5. **Implementar las estrategias para las contingencias**. En este paso se deben realizar preparaciones apropiadas, documentar las estrategias, y entrenar a los empleados. Preparación incluye designar personal responsable de tareas específicas para los casos de contingencias, mantener la documentación actualizada de políticas y procedimientos de la Organización y revisión de las tareas para las contingencias. El caso de las copias de seguridad (backups) para los datos y las aplicaciones es una parte crítica de cualquier plan de recuperación de desastres, por ejemplo las copias de seguridad se pueden usar para recuperar archivos después de que un virus los ha corrupto, o después de que un huracán destruya todo el centro de procesamiento de datos (Entidad de Certificación). Hay Organizaciones que implementan un sólo plan de contingencia general para toda la Organización y otras que usan varios planes de contingencia, incluso algunas tienen un plan diferente para cada recurso computacional. Saber cuántos planes de contingencia se deben implementar depende de las circunstancias únicas de cada Organización. Se puede designar a un coordinador especial para preparar los planes en cooperación con otros administradores funcionales y de recursos computacionales o se puede poner la responsabilidad directamente en los administradores de éstos recursos. Los planes documentados, almacenados de forma segura y actualizados continuamente son de crítica importancia durante la ocurrencia de estos eventos, con procedimientos claros de tal forma que cualquier persona pueda ejecutar el plan con un mínimo conocimiento. Todo el personal debe ser entrenado para casos de contingencias y desastres, los nuevos empleados deben ser entrenados apenas se unen a la Organización.

6. **Prueba y revisión de la estrategia**. Los planes deben ser probados periódicamente porque siempre habrán fallas en la estrategia y en su implementación. Además, el plan se

irá desactualizando a medida que pase el tiempo. La frecuencia de las pruebas dependerá de la Organización y sus sistemas. Hay varios tipos de pruebas como la revisión, análisis y simulación de desastres. Una **revisión** puede ser una prueba sencilla para probar que tan acertada es la documentación del plan de contingencia y determinar si los archivos pueden ser restaurados o si los empleados conocen los procedimientos de emergencia. El **análisis** puede realizarse sobre todo el plan o porciones, es benéfico que el análisis sea realizado por una persona que no haya desarrollado la estrategia pero que tenga buen conocimiento de las funciones críticas de la Organización. La **simulación de desastres** son pruebas que proveen información de mucha importancia con respecto a las fallas de los planes de contingencia y proveen una práctica real para una emergencia. Entre más críticos sean las funciones y los recursos tomados en cuenta para el plan de contingencia, se vuelve más benéfico realizar la simulación de desastres. Los resultados de las pruebas deben ser usadas para mejorar los planes, actualizar los procedimientos y la documentación.

3.7. SUBETAPA DE ESTUDIO DEL RETORNO SOBRE LA INVERSIÓN Y ESTUDIO LEGAL

ACTIVIDAD No. 1: Estudio del Retorno sobre la Inversión

Dentro de la etapa de planeación de la Entidad de Certificación, existe un aspecto a tener en cuenta que poco tiene que ver con la tecnología: el ROI (Retorno sobre la Inversión del acrónimo inglés Return over Investment), un estudio que sirve para determinar la viabilidad económica de la implantación del sistema de seguridad sobre el cual se van a soportar los servicios de identificación digital.

A pesar que no existe una herramienta para cuantificar el éxito o fracaso de una inversión de capital en un negocio de manera absoluta, se podría pensar que un estudio de ROI podría ser algo inútil e inoficioso en el proceso de implantación de una Infraestructura de Llaves Públicas, sin embargo, una cuantificación, así sea aproximada del factor *inversión* y el factor *retorno*, puede ser un instrumento de gran ayuda al momento de observar la viabilidad del proyecto.

Para medir el ROI de una Entidad de Certificación, se deben tener en cuenta 2 factores: la I o *inversión* y la R o el *retorno*:

1. Medición de la I (Inversión) en el Proyecto

El tema central del estudio de la I en un ROI, consiste en la determinación del *Costo Total de la Propiedad* (TCO - Total Cost of Ownership), el cual permite capturar los diferentes elementos de costos que se relacionan con la implantación de la PKI. El TCO se enfoca en cuatro aspectos: productos/tecnologías, planta/instalaciones, personal y procesos.

<u>Productos/Tecnologías</u>

En esta categoría se deben tener en cuenta todos los elementos tecnológicos de la arquitectura PKI y sus diferentes opciones, tales como formas de pago, formas de adquisición, administración y licenciamiento. Durante la estimación de éstos costos, se podrá llegar a la conclusión que existe una relación entre el costo de productos/tecnología y el número de usuarios de la Entidad de Certificación.

<u>Planta (Instalaciones)</u>

En esta categoría se deben tener en cuenta todas las instalaciones que se requieren para operar los componentes de la PKI, más el costo de la recuperación de éstas, en caso de un desastre.

Procesos

En esta categoría se deben tener en cuenta todas las personas que hacen parte de la estructura organizacional de la Entidad de Certificación, ya sean éstos parte del personal interno, o externo de la organización.

Procesos

El proceso de implantación de una PKI, implica muchas etapas (Etapa de Preparación, etapa de implantación y puesta en marcha, etapa de operación y mantenimiento). Es así, como en esta categoría se capturan los costos relacionados con las actividades realizadas a través de cada una de las etapas del proyecto.

2. Medición de la R (Retorno) en el Proyecto.

El aspecto económico más importante de un negocio es el retorno de capital, tanto a corto, como a largo plazo. La cuantificación de estos costos, enmarcado en un referente específico es a lo que se le conoce como *medición de los rendimientos financieros*.

A nivel general, existe un método simple para realizar este proceso, el cual consta de los siguientes pasos:

a) Análisis de los Servicios de Identificación Digital
b) Establecimiento y aplicación de la medida de la "R"
c) Análisis de resultados a nivel presente y futuro

Como se había visto en la subetapa 1, en la actividad de *identificación de la idea*, existe una taxonomía para clasificar los servicios telemáticos basados en identificación digital. Durante el transcurso de dicha actividad, se realizó el análisis de las necesidades de la comunidad que se iba a beneficiar de esos servicios, por lo que realizar éste de nuevo, sería redundar. Sin embargo, se podría pensar en que tan viable son económicamente estos servicios escogidos para ser implementados, así como en la posibilidad de agregar a futuro nuevos servicios económicamente rentables.

En el proceso de establecimiento de la medida "R", hay que tener en cuenta 3 aspectos: ingresos, costos y cumplimiento.

Los ingresos, son la cuantificación de cualquier cantidad de corrientes de ingresos incrementales para las aplicaciones PKI. La cuantificación del porcentaje de ingresos por transacciones en línea y el porcentaje de aumento de clientes son ejemplos de este tipo.

Los costos, y los mecanismos para su reducción son temas importantes al momento de aumentar los rendimientos financieros de la PKI, a pesar que su realización es más por táctica que por estrategia. Ejemplos de ésto son los ahorros en los costos de la PKI y su evaluación.

El cumplimiento es el aspecto más importante para el cliente, junto con el costo del servicio. Éste se encuentra estrechamente relacionado con la calidad y por ende, es indispensable cumplirlo, si se desea competente en el mercado. Al momento de estudiar este tema, se deben tener en cuenta el cumplimiento de las regulaciones y normatividades, el cumplimiento con los socios del proyecto y sobre todo, el cumplimiento con los clientes.

ACTIVIDAD No. 2: Estudio legal de la Entidad de Certificación

Como se vió en la base conceptual, en Colombia existen una ley encargada de regular lo concerniente a la emisión de certificados digitales, el comercio electrónico y el intercambio electrónico de datos (Ley 527 de 1999), además de un decreto (Decreto 1747 de 2000), en el cual se complementan los aspectos relacionados a funcionalidad y requerimientos relacionados con la entidad de certificación. Es así como de éste podemos extraer dos artículos de suma importancia para los intereses de planeación de la implementación de la entidad de certificación tales como:

ENTIDADES DE CERTIFICACIÓN CERRADA

Artículo 3°*. Acreditación de requisitos de las entidades de certificación cerradas. Quienes pretendan realizar las actividades propias de las entidades de certificación cerradas deberán acreditar ante la Superintendencia de Industria y Comercio que:*

1. Los administradores y representantes legales no están incursos en las causales de inhabilidad previstas en el literal c) del artículo 29 de la Ley 527 de 1999, y

2. Están en capacidad de cumplir los estándares mínimos que fije la Superintendencia de Industria y Comercio de acuerdo a los servicios ofrecidos.

Esto quiere decir que cualquier persona jurídica pública o privada que quiera establecer una entidad de certificación cerrada no debe estar representada legalmente por personas que hayan sido condenadas a pena privativa de libertad, excepto por delitos políticos o culposos; o que hayan sido suspendidas en el ejercicio de su profesión por falta grave a la ética o hayan sido excluidas de

aquélla.

En el literal 2, de este artículo, se referencia a la Superintendencia de Industria y Comercio, entidad encargada, según el artículo 41 de la Ley 527 de 1999 a ser el ente encargado de autorizar, velar y en general gestionar los temas relacionados con las entidades de certificación en Colombia. Es así como se debe remitir a la Circular Única expedida por dicho estamento, específicamente al *Título V*, *Capítulo Octavo*, denominado "Entidades de Certificación Ley 527 de 1999", donde se establece que la persona que solicite autorización como entidad de certificación cerrada, deberá diligenciar la solicitud de autorización para entidad de certificación formato 3020-F08 anexo 3.9, adjuntando un certificado de existencia y representación legal o copia de las normas que le otorgan la calidad de representante legal de una entidad pública, de notario o cónsul.

Entre los detalles importantes a tener en cuenta al momento de llenar dicha solicitud se encuentran los servicios que prestará la entidad de certificación (Servicios Telemáticos basados en Identificación Digital), la dirección de la Entidad de Certificación, una breve descripción de los servicios y finalmente una descripción y diseño de la arquitectura de la Infraestructura de Llaves Públicas.

ENTIDADES DE CERTIFICACIÓN ABIERTA

***Artículo 5°**. Acreditación de requisitos de las entidades de certificación abiertas. Quienes pretendan realizar las actividades propias de las entidades de certificación abiertas deberán particularizarlas y acreditar ante la Superintendencia de Industria y Comercio:*

1. Personería jurídica o condición de notario o cónsul.

Cuando se trate de una entidad extranjera, se deberá acreditar el cumplimiento de los requisitos contemplados en el libro segundo, título VIII del Código de Comercio para las sociedades extranjeras que pretendan ejecutar negocios permanentes en territorio colombiano. Igualmente deberá observarse lo establecido en el artículo 48 del Código de Procedimiento Civil.

2. Que los administradores y representantes legales no están incursos en las causales de inhabilidad previstas en el literal c) del artículo 29 de la Ley 527 de 1999.

3. Declaración de Prácticas de Certificación (DPC) satisfactoria, de acuerdo con los requisitos establecidos por la Superintendencia de Industria y Comercio.

4. Patrimonio mínimo de 400 salarios mínimos mensuales legales vigentes al momento de la autorización.

5. Constitución de las garantías previstas en este decreto.

6. Infraestructura y recursos por lo menos en la forma exigida en el artículo 9° de este decreto.

7. Informe inicial de auditoría satisfactorio a juicio de la misma Superintendencia.

8. Un mecanismo de ejecución inmediata para revocar los certificados digitales expedidos a los suscriptores, a petición de estos o cuando se tenga indicios de que ha ocurrido alguno de los eventos previstos en el artículo 37 de la Ley 527 de 1999.

Parágrafo 1°. La Superintendencia de Industria y Comercio tendrá la facultad de solicitar ampliación o aclaración sobre los puntos que estime conveniente.

Parágrafo 2°. Si se solicita autorización para certificaciones recíprocas, se deberán acreditar adicionalmente la entidad reconocida, los certificados reconocidos y el tipo de certificados al cual se remite, la vigencia y los términos del reconocimiento.

Abrir una Entidad de Certificación Abierta, como se puede ver, implica unos requerimientos extras según la ley, tales como la creación de la *Declaración de Prácticas de Certificación* (Subetapa anterior) y ante todo, un respaldo patrimonial representado en en 400 salarios mínimos. Además de eso, se tienen que cumplir unas características técnicas, que son las que se han venido contemplando a lo largo de este escrito.

Además, la Superintendencia de Industria y Comercio realizará una auditoría a los elementos anteriormente nombrados, lanzando un juicio acerca del cumplimiento o no de éstos.

En cuanto a la circular única de dicho estamento, los requerimientos para lograr la autorización legal de una Entidad de Certificación Abierta son:

a) Llenar la solicitud de autorización para Entidad de Certificación formato 3020-F08 anexo 3.9
b) Formato 3020-F09 información de administradores o representantes legales anexo 3.10 diligenciado por el representante legal encargado de la Entidad de Certificación acompañado de:
- Certificado judicial vigente o documento equivalente proveniente del país o países donde hayan residido por cada uno de los administradores y representantes legales
- Una certificación de representante legal que diligenció el formato 3020-F09, en el cual haga constar que de acuerdo a la información suministrada y disponible, ninguno de los administradores y representantes legales de la Entidad se encuentra incurso en alguna de las inhabilidades estipuladas en el literal c del artículo 29 de la ley 527 de 1999.
c) Copia del acto que le otorga la personería jurídica y de las normas que le otorgan la calidad de representante legal de una entidad pública de notario o cónsul, o certificado de existencia y representación legal. Cuando se trate de persona extranjera , se deberá acreditar el cumplimiento de lo señalado en el libro II título VII del código de comercio y en el artículo 48 del código de procedimiento civil, según lo dispuesto en el número 1 del artículo 5 del decreto 1747 de 2000.

d) Informe de auditoría en los términos del numeral 8.3.2 del título V de la circular única de la Superintendencia de Industria y Comercio, en el cual se declara la conformidad de cada una de las condiciones previstas en el artículo 29 de la ley 527 de 1999, el decreto 1747 de 2000 y el título V de dicha circular.

e) Estados financieros presentados conforme a la ley y con una antigüedad no superior a seis meses (6) según lo dispuesto en el numeral 1 del artículo 7 del decreto 1747 de 2000.

f) Copia del documento que acredite que se han constituido las garantías de acuerdo a lo dispuesto en el artículo 8 del decreto 1747 de 2000.

g) Descripción detallada de la infraestructura, procedimientos y recursos, según lo previsto en el artículo 9 del decreto 1747 de 2000. El cumplimiento de los requisitos deberá acreditarse según los previsto en el capítulo cuarto del título V, de la circular única de la Superintendencia de Industria y Comercio.

h) Declaración de prácticas de certificación DPC.

4. ETAPA DE IMPLEMENTACIÓN Y PUESTA EN MARCHA

4.1. SUBETAPA DE REALIZACIÓN DE LA CONTRATACIÓN

Realización de la Subcontratación

En Colombia existen dos posibilidades al realizar una contratación:

-Contratación con una Entidad Estatal: Según la Ley 80 de 1993, en Colombia, la contratación con Entidades Estatales se debe efectuar siempre a través de licitaciones o concursos públicos, este es un procedimiento mediante el cual la entidad estatal formula públicamente una convocatoria para que, en igualdad de oportunidades, los interesados presenten sus ofertas y seleccione entre ellas la más favorable. La selección de contratistas se hace de forma objetiva, los factores de escogencia se basan en cumplimiento, experiencia, organización, equipos, plazo, precio y la ponderación precisa, detallada y concreta de los mismos contenida en un análisis previo a la subscripción del contrato.

-Contratación directa y Privada: Se deben elaborar los documentos RFS (Request for Strategy) y RFP (Request for Proposal). Estos documentos proveen una marco de referencia para la Organización que desea contratar soluciones de PKI.

Elaboración de los Documentos RFS y RFP

A continuación se expresan algunos lineamientos para elaborar los documentos RFS y RFP necesarios para obtener información sobre los prestadores de soluciones de PKI, evaluarlos y seleccionar los potenciales para desplegar la infraestructura del negocio.

Lineamientos para Elaborar un documento RFS (Request for Strategy)

El primer paso para la implementación de una PKI implica obtener más información sobre la tecnología de PKI, sus productos y soluciones. En este momento se debe considerar la realización de un documento RFS. El propósito de crear este documento consiste en permitir a los prestadores de soluciones de PKI dar información sobre sus productos y soluciones relacionados con sus PKI, la siguiente es una plantilla para el documento de RFS:

1. Preguntas sobre la solicitud de información
2. Términos y condiciones
3. Omisiones
4. Introducción

5. Antecedentes
6. Ámbito Propuesto de Desarrollo
7. Costo del Desarrollo
8. Presentación de Materiales

La organización ganará información muy valiosa de los productos, servicios, procesos, costos, opciones, alternativas, y consideraciones disponibles. El documento de RFP se puede desarrollar como resultado de los documentos de RFS y de evaluación de la PKI.

Lineamientos para Elaborar un Documento RFP

El documento RFP es el método típico utilizado para asistir en la evaluación de prestadores de soluciones de PKI potenciales que se puedan seleccionar para desplegar la infraestructura del negocio.

El RFP permite a los proveedores de soluciones de PKI responder a preguntas específicas que son de interés clave para el negocio. Usualmente se les pide responder en las áreas de Tecnología, Producto, y Organización del prestador de soluciones PKI.

Capacidad del Proveedor de Soluciones de PKI

PKI es una inversión a largo plazo. La historia del prestador de soluciones de PKI con el producto, la tecnología y la habilidad para soportar y mejorarlo son consideraciones importantes. Además su capacidad para asistir a los clientes con el despliegue de PKI determinará la habilidad para desplegar el producto en su propio ambiente. Los puntos que deben ser tomados en cuenta en esta área del RFP deben incluir lo siguiente:

- Finanzas del prestador de servicios de PKI: Ganancias y porcentaje del negocio de PKI.
- Enfocarse en el negocio del prestador de servicios de PKI: e-security, PKI y otras áreas.
- Versión de PKI actual: Cuánto tiempo ha estado en funcionamiento; cuales fueron las nuevas características introducidas; cuando será el próximo lanzamiento esperado y cuáles son las posibles mejoras al producto.
- Registro del producto: El producto ha ganado premios en la industria; donde se ha instalado el producto; cual ha sido la escala del despliegue del producto.
- Soporte del prestador de servicios de PKI: Número de empleados; número de consultantes técnicos experimentados con el producto de PKI que puedan asistir con el despliegue del producto; ¿Qué opciones de soporte son disponibles para los compradores?
- Referencias del prestador de servicios de PKI: de los clientes que ya tienen instalado el producto de PKI.

- Lenguaje: ¿Puede el proveedor de soluciones de PKI soportar múltiples lenguajes?
- Conocimiento básico: ¿Puede el proveedor de soluciones de PKI soportar un conocimiento básico en Internet que puede ser de acceso seguro para los compradores?
- Herramientas de trabajo: ¿Puede la solución de PKI incluir herramientas para el desarrollador de aplicaciones? ¿Estas herramientas ofrecen funciones de criptografía y administración de llaves para la integración dentro de las aplicaciones? ¿La solución soporta herramientas multiplataforma?
- Precio: ¿Cómo se le ha puesto precio al producto de PKI? ¿La solución de PKI incluye una fecha de expiración definida para los certificados sobre los cuales se requiera una tarifa de renovación? ¿El proveedor ofrece soporte o contratos de mantenimiento? ¿Cual es el costo por ese soporte y mantenimiento?

Capacidad de Investigación y desarrollo del Prestador de Soluciones de PKI

El objetivo es comprender el esfuerzo del proveedor para introducir características al producto, así como determinar la calidad del producto y el régimen de pruebas en el ambiente del prestador del soluciones de PKI. Las preguntas recomendadas deben incluir:

- Inversión: investigación y desarrollo en términos del número de empleados y capital.
- Características del producto: historia del producto; número de versiones liberadas y la frecuencia.

Tecnología de la Autoridad de Certificación

El núcleo de la solución de PKI es el producto de la Autoridad de Certificación del prestador de soluciones de PKI. Este es el componente que es responsable de sacar, administrar y validar certificados digitales. El tipo de cuestionamientos que deben realizarse son:

- Suspensión del Certificado: ¿La solución de PKI soporta la suspensión de certificados?
- Autoridad de Certificación subordinada: ¿Puede la CA funcionar como una subordinada dentro de una jerarquía de mayor nivel?
- Llaves Privadas: ¿Soporta soluciones basadas en hardware para el uso seguro del firmado de la llave de firmado de la CA?
- Capacidades de la CA: para alta disponibilidad; redundancia.
- Soporte DSA: ¿Soporta DSA para firmado digital? ¿Se soporta el almacenamiento de llaves de DSA en dispositivos hardware?
- Usuarios Móviles: ¿Hay credenciales para los usuarios móviles?

- Comunicaciones Seguras: ¿Se soportan entre el cliente y el RA; entre RA y CA; y entre el CA y los agentes administradores?
- API: ¿Pueden las soluciones de PKI ser modificadas?
- Estampa del Tiempo: ¿Se soporta?
- Copias de seguridad de la CA: ¿La gestión de llaves y servicios de administración se encuentran disponibles durante el proceso de las copias de seguridad (backup)?

Tecnología de la Autoridad de Registro

La RA (Autoridad de Registro) es un componente opcional de una PKI. Las cuestiones que se deben incluir en el RFP son:

- ¿La solución de PKI soporta la RA?
- Comunicaciones seguras: ¿La comunicación es segura entre la CA y la RA?
- Soporte de Registro: ¿La solución de PKI soporta disponibilidad de registro 24 X 7?
- ¿La solución de PKI soporta Múltiples RA?
- Administración: ¿Pueden los administradores acceder de forma segura a la RA usando navegadores web?

Tecnología de Servicios de Directorio

Se incluyen las siguientes cuestiones:

- ¿La solución de PKI incluye un directorio?
- Capacidad de restauración: ¿Puede la CA restaurar todos los certificados activos al directorio?
- Acceso al directorio: ¿Es basado en estándares?
- LDAP: ¿Soporta el uso del directorio LDAP? ¿Soporta X.500? ¿Se soporta la comunicación entre múltiples servidores LDAP para balanceo de carga, redundancia y escalabilidad?
- ¿Se soporta el formato de nombre distinguido (distinguished name)?

Tecnología de Administración

Se incluyen las siguientes cuestiones en esta área:

- ¿Puede ser configurada la interfaz administrativa con un API?
- ¿Se soporta la Revocación por Volumen?
- Automatización: ¿Puede el proceso de inicialización y registro de usuarios ser

automatizado?

- ¿Pueden las funciones administrativas ser delegadas, de tal forma que los administradores puedan solamente administrar usuarios de su división?
- Intervención del Rastro: describe cualquier capacidad de intervención y reporte soportados por la solución de PKI

Tecnología de Certificados

Los certificados son un componente fundamental de una PKI. Para el RFP se debe tener en cuenta lo siguiente:

- Tipos de Certificados: ¿Qué tipo de certificados pueden ser expedidos por la Autoridad de Certificación (SSL, S/MIME, VPN, SET) ?
- X509: ¿Se expiden los certificados conforme con el formato X509? ¿Qué versión de X509 se soporta?
- Tiempo de vida del certificado: ¿Se puede determinar?
- Actualización del certificado: ¿Es posible actualizar automáticamente los certificados?
- Certificado Raíz: ¿Puede la solución de PKI soportar la capacidad de que una CA se autocertifique, genere un par de llaves, cree y firme un certificado Raiz para su propia operación?
- Certificados Múltiples: Puede la solución de PKI soportar múltiples certificados por usuario (¿Un certificado para firmar y otro para cifrar por ejemplo?)
- Atributos para los certificados: ¿Puede la solución soportar atributos para los certificados?
- Extensiones Personalizadas: ¿La solución soporta extensiones personalizadas para el certificado, qué tipos?

Tecnología de Administración de las Llaves y el Certificado

Típicamente las soluciones de PKI soportan la capacidad para expedir certificados digitales y múltiples llaves utilizadas para firmar y para cifrar. En el RFP se debe incluir:

- Llaves: ¿La solución de PKI soporta la generación de múltiples llaves?
- Copia de seguridad de las llaves: La solución soporta copias de seguridad de las llaves
- ¿La solución soporta distribución inmediata de las llaves de la CA de tal forma que no haya necesidad de distribuirlas manualmente?
- ¿Expiración de la llave: pueden las llaves de firmado y de cifrado expirar en tiempos diferentes?

- ¿La solución soporta actualización de llaves automáticamente?
- ¿Puede la llave de firmado de la CA ser almacenada en software o hardware para una recuperación futura?
- ¿Puede la llave privada estar bien protegida en una estación cliente?

Tecnología de Revocación de Certificados

La PKI debe asegurar la validez de los certificados. La revocación de certificados es un servicio muy importante para la PKI. Además no se debe degradar su desempeño si el número de usuarios aumenta.

Lo siguiente se debe tomar en cuenta en el RFP:

- ¿Soporta la Revocación de Certificados? ¿Qué métodos se soportan? ¿soporta una revisión en línea?
- ¿Qué tan rápido se propaga la notificación de un certificado comprometido a través del sistema o red? ¿La notificación se envía inmediatamente después de la revocación?
- ¿Se puede personalizar la publicación de CRL's?
- ¿Se soporta la Revocación en Volumen?
- ¿Es la Revocación de Certificados escalable para millones de usuarios?

Recuperación de Llaves

La capacidad de recuperación de llaves se requiere para los negocios que operan en un ambiente altamente regulado y son sujetos a inspecciones periódicas de sus transacciones. En algunos casos se requiere al acceso a datos cifrados y archivos por individuos diferentes al usuario original de los datos.

El RFP debe tomar en cuenta:

- La solución soporta capacidad de recuperación de llaves?
- La solución soporta la recuperación de llaves privadas de los usuarios?
- Si las llaves de un usuario se pierden o se corrompen, qué tanto debe comprometerse el usuario para recuperar sus llaves?
- Cómo se mantiene el servicio de no repudio mientras se provee el servicio de recuperación de llaves?
- La solución soporta un registro seguro de todos los intentos de acceder las llaves privadas?

Interoperabilidad y PKI

Entre más aplicaciones y usuarios utilicen PKI, se requiere interoperabilidad. Se debe incluir en

esta área:

- ¿Qué estándares soporta el producto? ¿Soporta PKCS #7?, ¿PKCS #10? ¿Soporta MD-5, ¿SHA-1? ¿Curva Elíptica (PKCS #13)? ¿DES y 3DES? ¿Diffie-Helman (PKCS #3)? ¿SSL? ¿TLS?
- ¿El prestador de soluciones de PKI realiza pruebas de interoperabilidad?
- ¿El producto soporta soluciones VPN, soporta Ipsec?
- ¿El producto soporta diferentes navegadores como Internet Explorer, Mozilla, etc?
- ¿La solución reconoce y puede trabajar con productos y certificados de otros prestadores de soluciones de PKI?
- ¿Soporta el estándar PKIX para certificados cruzados? ¿Soporta tiempos de vida flexibles en certificados cruzados?

Seguridad

Para la seguridad se debe incluir:

- ¿El producto ofrece protección de llaves por Hardware?
- ¿Soporta tarjetas inteligentes para el almacenamiento de certificados digitales?
- ¿Soporta un límite de tiempo que caracterice el acceso seguro?
- ¿Soporta el ciframiento y desciframiento de archivos y directorios en el escritorio del usuario? ¿Se realiza de forma automática?
- ¿Puede la solución asegurar el uso de contraseñas fuertes para proteger las llaves privadas en el navegador y prevenir el mal uso?

Elaboración del Documento de Evaluación para una PKI Organizacional

El documento de evaluación de una PKI resume todos los requerimientos que se esperan de una PKI para su organización basados en entrevistas realizadas, requerimientos del negocio para aplicaciones y servicios emergentes, requerimientos de seguridad, y los estándares industriales de PKI.

El documento provee información que será útil en el desarrollo de una arquitectura PKI. El público intencionado para este documento incluye personal técnico y administradores del negocio que asistirán, planearán e implementarán una PKI.

Las entrevistas, reuniones, investigaciones, y análisis requerido para crear el documento de

evaluación de la PKI es un ejercicio de dos semanas. Las entrevistas y reuniones resultan en necesidades, requerimientos, e ideas para posibles usos de la PKI dentro de la Organización.

Plantilla del documento de Evaluación

El documento de Evaluación de la PKI debe incluir las siguientes secciones:

- Sección I: Resumen Ejecutivo

  -Se describe el propósito de una evaluación de la solución de PKI. Se debe dar un resumen de la información de las otras secciones del documento.

- Sección II: Descripción General

  -Describe los objetivos específicos del documento de evaluación de PKI y los detalles del audiencia objetivo para el cual se realiza el documento. Por ejemplo: El documento se desarrolla para el uso de personal técnico y administradores de la Organización y busca ayudar en la instalación e implementación de una PKI en el negocio.

- Sección III: Descripción de la tecnología PKI

  -Introduce PKI a un nivel ejecutivo, explica por qué PKI es importante, incluye terminología de PKI, protocolos relacionados, componentes, funciones básicas, características de PKI, servicios de seguridad, y aplicaciones de PKI.

- Sección IV: Planes del Negocio para la PKI

  -Responsabilidades, funciones, servicios y modelos de proveedores de PKI. Se identifica el ámbito de la PKI dentro de la Organización, sus aplicaciones, la línea de tiempo de implementación y los modelos de PKI. Se identifican las áreas donde PKI puede hacer una diferencia en la operación, servicios y seguridad de la Organización.

- Sección V: Aplicaciones disponibles para la PKI

  -Se resumen las aplicaciones PKI de interés para la Organización. Posibles aplicaciones de la tecnología PKI son: control de acceso, correo electrónico seguro, SSL, VPN seguras, firmas digitales, ciframiento de archivos, transferencia de documentos, SET (transacciones electrónicas seguras), etc.

- Sección VI: Requerimientos de las Unidades del Negocio

  Se determinan los requerimientos para una PKI según entrevistas y discusiones con las diferentes unidades de la Organización. Se provee información en las siguientes áreas: Posibles aplicaciones disponibles en PKI, número de certificados, Jerarquía de confianza, autoridad de certificación raíz, período de certificación y renovación, revocación de certificados, certificados de ciframiento, requerimientos de ancho de banda, reportes, facturas, atención al cliente, copias de seguridad y recuperación.

- Sección VII: Tipos de Certificados y Contenido

  Se evalúan los diferentes tipos de certificados que puede necesitar la Organización. Estos tipos de certificados incluyen: certificados SSL para navegadores, certificados para servidor Web, para correo electrónico seguro, certificados Ipsec para acceso remoto, certificados WAP y certificados de ciframiento.

- Sección VIII: Procesos de Registro

  Se evalúan los requerimientos de la Organización para el registro, incluyendo: niveles de autenticación requeridos, autenticación manual, métodos de autenticación automatizados, criterio de autenticación, responsabilidad de las funciones de la autoridad de registro, biometría y sensibilidad de los datos.

- Sección IX: Instalaciones para el hosting de la Autoridad de Certificación

  Se evalúan los requerimientos para la seguridad física de la Autoridad de Certificación, tomando en cuenta: seguridad física de los sistemas, procedimientos que deben seguirse para acceder a las instalaciones físicas, y requerimientos para el personal de la Organización.

Evaluación de la Contratación

Se refiere a la evaluación de la propuesta para implementar soluciones de PKI en la Organización. Se deben tomar en cuenta puntos claves que hacen de una propuesta una buena oferta como los siguientes:

-Si la contratación es con una Entidad Estatal, la propuesta debe cumplir con la ley 80 de 1993 y se debe cumplir con los criterios especificados por la Ley para poder evaluar y contratar.

-Si la contratación es directa o privada, se debe verificar que la propuesta cumpla con los requerimientos del negocio para aplicaciones y servicios, requerimientos de seguridad, y los estándares industriales de PKI. Del documento RFS se debe obtener la mejor información sobre los productos, servicios, procesos, costos, opciones, alternativas, y consideraciones disponibles. El documento RFP es el factor más importante al momento de evaluar una propuesta, aquí se definen características claves para seleccionar al prestador de soluciones de PKI, se consideran en la evaluación las siguientes características: Capacidad del proveedor de soluciones de PKI, Capacidad de investigación y desarrollo, Tecnología de la Autoridad de Certificación, Tecnología de la Autoridad de Registro, Tecnología de Servicios de Directorio, Tecnología de Administración, Tecnología de Certificados, Tecnología de Revocación de Certificados, Recuperación de Llaves, Interoperabilidad y Seguridad.

4.2. SUBETAPA DE IMPLEMENTACIÓN DE LA ENTIDAD DE CERTIFICACIÓN

La implementación de la entidad de certificación es la actividad en la cual, se realiza la instalación y configuración de cada uno de los componentes PKI, especificados durante la *Etapa de Preparación.*

A pesar que el software encargado de la administración de la Entidad de Certificación en general, puede ser desarrollado por la organización, no es algo aconsejable si se trata de una empresa sin una alta trayectoria en el campo del desarrollo de software de seguridad ya que los procesos enmarcados dentro de este software requieren de un alto grado de rendimiento y calidad. Así es, como el concepto de *implementación*, empleado en la implementación de la Entidad de Certificación, significa *Instalación y Configuración*, y no *Codificación,* como se podría llegar a percibir.

Una visión general de la arquitectura del software a implementar, se puede ver en la siguiente figura:

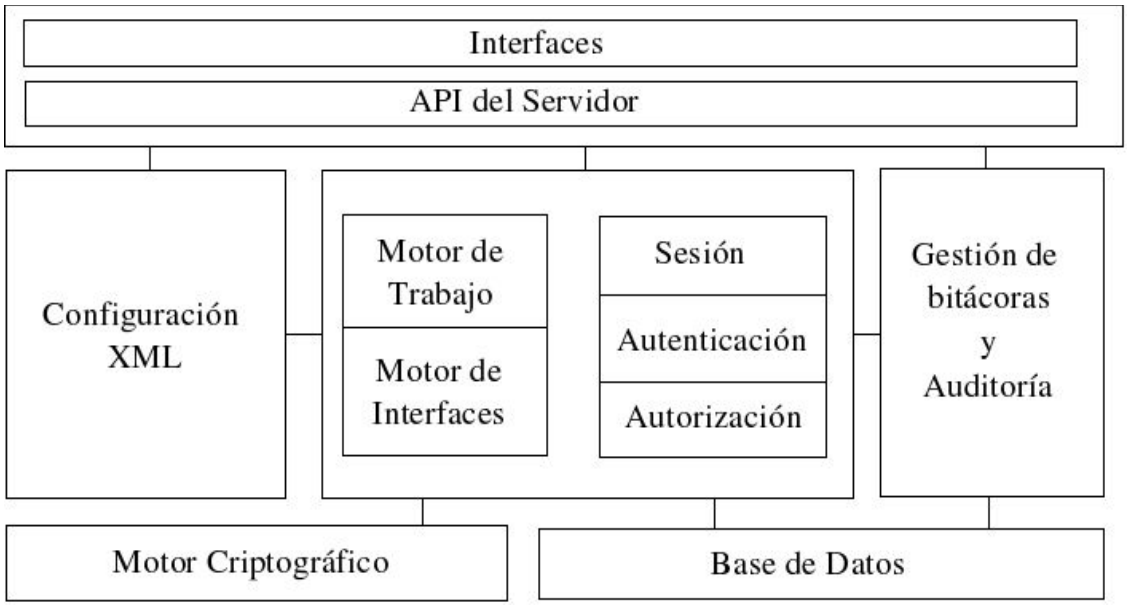


Figura 14. Arquitectura del Software de Gestión de una Entidad de Certificación

Como se puede observar a primera instancia, no se realiza una distinción explícita entre una Autoridad de Certificación y una Autoridad de Registro, ya que la diferenciación entre éstas se realizará por medio de la configuración XML.

Los usuarios y aplicaciones que accedan a los servicios de una PKI, lo deben de hacer por medio

una *interfaz*. Entre las interfaces comunes se encuentran las *interfaces web*, o las clásicas *líneas de comando*. Los componentes internos de la PKI utilizarán para su comunicación SCEP (Simple Certificate Enrollment Protocol)[31] u OSCP (Online Status Certificate Protocol)[32].

Dentro de esta arquitectura funcional, las diferentes interfaces utilizan la *API del Servidor* para poder comunicarse con el *Sistema Central PKI*, que es el corazón funcional de la Autoridad de Certificación/Entidad de Registro.

El *Sistema Central* se deberá comunicar con una *Configuración XML*, que consiste en un conjunto de archivos de configuración, donde se guardarán los distintos valores de configuración de la Autoridad de Certificación o de la Autoridad de Registro, tales como los parámetros de la base de datos, el control de acceso, etc.

Todos los eventos que sucedan en el software de la Autoridad de Certificación o la Autoridad de Registro, deben ser sujetos a una extensa auditoría por medio de un módulo totalmente independiente. El sistema debe estar en la capacidad de enviar los registros a un archivo plano, o a un archivo tipo "syslog" de Unix, o a una base de datos.

El motor criptográfico corresponde a la implementación de los distintos algoritmos en cifrado que va a utilizar el *Sistema Central,* para realizar sus procesos de emisión, eliminación, edición y firma de certificados digitales. Entre los motores criptográficos más reconocidos, se encuentra OpenSSL[33].

La base de datos es el lugar donde se van a almacenar los datos relacionados con los certificados digitales y sus respectivos usuarios. Cada fabricante de software de Administración de Entidades de Certificación, dará la libertad o no de elegir entre distintas bases de datos comerciales en el mercado, así como su respectiva configuración (Standalone o distribuida).

En resumen, las características principales del software que va a administrar la entidad de certificación (Autoridades de Certificación y Autoridades de Registro), debe tener las siguientes características:

- Interfaz de Usuario amigable
- Interfaz LDAP
- Interfaz con las Autoridades de Registro
- Interfaz con las Autoridades de Certificación
- SCEP (Simple Certificate Enrollment Protocol)

31 SCEP. Simple Certificate Enrollment Protocol. <http://www.ietf.org/internet-drafts/draft-nourse-scep-12.txt>

32 OSCP. Online Status Certificate Protocol. <http://www.ietf.org/rfc/rfc3125.txt>

33 CHANDRA, Pravir; MESSLER, Matt y VIEGA, John. Network Security with OpenSSL. 2002. p. 8

- OSCP (Online Status Certificate Protocol)
- Filtrado de IP para las diferentes interfaces
- Autenticación basada en *frases de paso.*
- Autenticación basada en certificados (Incluyendo tarjetas inteligentes).
- Control de acceso basado en reglas.
- Sujetos de certificados flexibles
- Sujetos de certificados extensibles
- Revocación basada en PIN.
- Revocación basada en la firma digital
- Emisión de CRLs (Listas de Revocación de Certificados)
- Alertas de expiración de certificados

PASOS BÁSICOS PARA LA IMPLEMENTACIÓN DE UNA AUTORIDAD DE CERTIFICACIÓN O DE UNA AUTORIDAD DE REGISTRO

1. REQUERIMIENTOS HARDWARE / SOFTWARE

Algunos productos software para gestión de CA/RA no son completamente monolíticas, es decir, dependen de aplicaciones adicionales, para poder funcionar. Entre las aplicaciones que normalmente se pueden llegar a necesitar, se encuentran:

- **Servidor Web:** es la aplicación encargada de servir de interfaz, para que los usuarios y administradores accedan a la gestión de sus perfiles y certificados.

- **Módulo interfaz Web-SSL:** es el encargado de realizar la comunicación de las peticiones seguras entre el usuario y el servidor web, utilizando el *motor criptográfico*.

- **Motor criptográfico:** es el conjunto de aplicaciones y librerías encargadas de proveer la funcionalidad criptográfica al software que lo necesite.

- **Servidor de Directorio:** es la aplicación encargada de almacenar y gestionar los datos relacionados a los usuarios de la organización. Usualmente en estos directorios, se almacenan los certificados digitales.

- **Plataforma de Desarrollo de Software:** es el conjunto de aplicaciones y librerías que van a soportar el código de la aplicación de gestión, ya se encuentre éste en código fuente, en cuyo caso

será interpretado (Scripting) o en código objeto, donde será ejecutado.

Como se puede observar, las anteriores características pueden o no instalarse de manera automática, dependiendo del software a instalar, sin embargo, es recomendable conocer estos componentes para conocer el funcionamiento de las aplicaciones.

En cuanto a la parte hardware, es bueno contar con un equipos de buenas características y en lo posible ensamblados para alto rendimiento.

2 INSTALACIÓN Y CONFIGURACIÓN DEL SOFTWARE

En cualquier Software de Gestión de CA/RA se van a encontrar las siguientes opciones básicas a configurar durante o después de la instalación de las aplicaciones.

2.1 CONTROL DE ACCESO

El *Control de Acceso*, es el espacio donde se realiza la configuración relacionada, con los permisos, las especificaciones del canal y el manejo de sesiones. Usualmente este consta de un conjunto de archivos, que son por lo común archivos XML, que pueden ser configurados manualmente o a través de un aplicativo de usuario.

Usualmente el *Control de Acceso* se encuentra dividido en *Verificación del Canal, Inicio de Sesión, Gestión de Sesiones y Listas de Control de Acceso (ACL).* Una visión general de estos pasos, se puede ver en la siguiente ilustración:

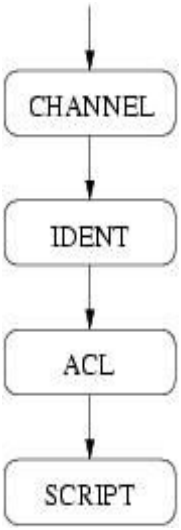


Figura 15. Manejo del Control de Acceso en el Software de Gestión de una Entidad de Certificación

Verificación del Canal

La configuración del canal verifica los parámetros de la conexión de entrada para detectar servicios mal configurados o clientes obsoletos. Normalmente, los valores de éstos se traducen en expresiones regulares para la realización de su trabajo.

Así es, como se debe de poder contar con la flexibilidad para configurar el protocolo de transmisión de datos, dependiendo de los requerimientos del sistema. Por ejemplo, se debe tener la posibilidad de escoger si se va a usar una conexión segura (SSL) o una insegura (HTTP). También, se debe tener la posibilidad de definir el algoritmo de cifrado que se va a utilizar durante la conexión. (El algoritmo de cifrado tanto simétrico como asimétrico).

Inicio de Sesión

Existen múltiples formas de iniciar sesión en las diferentes aplicaciones del administrador de la CA/RA, de los cuales los más comunes son:

a) *Ninguno:* Se debe tener la posibilidad de que no exista ningún tipo de autenticación, es decir, cualquier persona puede pasar los canales de verificación para utilizar la interfaz. Ésto no hace más sino desactivar el Control de Acceso y es útil para pruebas de funcionamiento y para depurar errores.

b) *Password:* Este método se utiliza para autenticar a los usuarios y administradores por medio de un *Nombre de Usuario (Login) y una Contraseña (Password).* Esta autenticación se debe poder hacer por medio de una Base de Datos local, o una externa. También debe tener la posibilidad de poder cambiar los algoritmos de cifrado y su fortaleza en bits.

c) *Certificado:* Este es quizá el método de autenticación más avanzada. El usuario debe firmar su Identificador de Sesión, y el servidor se encarga de verificar la firma. La llave privada del certificado, puede estar almacenada en un archivo local del cliente o en un dispositivo de autenticación, tal como una tarjeta inteligente.

Gestión de Sesiones

La gestión de sesiones es hoy un proceso de configuración relativamente simple porque sólo existe un método para manejarlas (A través de *cookies*) en el cliente. La otra variable importante a definir es el tiempo de vida de la sesión después de la última acción, la cual debe encontrarse aceptada por el rango definido previamente por la aplicación.

Listas de Control de Acceso

En las listas de control de acceso, se encuentran las reglas que van a seguir los diferentes usuarios dentro del sistema. Cada regla va estar compuesta por una bandera de aceptación o denegación de la regla, seguido por el usuario al cual se le aplica. También cada regla debe definir las acciones que puede realizar cada usuario dentro del sistema.

2.2 CONFIGURACIÓN DE LAS EXTENSIONES DE LOS CERTIFICADOS

El motor criptográfico es el componente del sistema encargado de brindar la funcionalidad relacionada con el ciframiento simétrico y asimétrico de los datos y por ende, es el encargado de crear los certificados digitales y firmarlos. Así es, como la aplicación de gestión de la CA/RA, debe tener la posibilidad de poder personalizar las extensiones de los certificados a emitir.

Las extensiones definidas por los certificados X.509 v3 proveen métodos para asociar atributos adicionales con usuarios o llaves públicas y para gestionar una jerarquía de certificados. El formato X.509 v3 también permite la creación de extensiones privadas para transportar información única de la organización dentro de sus componentes PKI. Cada extensión en un certificado esta diseñado para ser crítica o no crítica. A continuación, se van a listar las extensiones recomendadas para ser utilizadas en los certificados dentro de la Internet y el administrador del sistema debe elegir, cuales de éllas serán las más idóneas para ser utilizadas dentro de la organización.

I. Extensiones Estándar

a) Authority Key Identifier: Esta extensión provee un medio para identificar la llave pública correspondiente a la llave privada utilizada para firmar un certificado. Esta extensión es utilizada cuando el usuario posee muchos pares de llaves, o tiene diferentes llaves para firmar.

b) Subject Key Identifier: Esta extensión provee un medio para identificar los certificados que cotienen una llave pública en particular.

c) Key Usage: Este certificado define el propósito (Ciframiento, Firma, Firma de Certificados) de la llave contenida en el certificado.

d) Private Key Usage Period: Esta extensión, se sugiere, no debe ser utilizada en una PKI de Internet. Las CAs que se rijan de acuerdo a este perfil no deben generar certificados que incluyan una extensión crítica del periodo de uso de la llave privada. Esta extensión permite al emisor del certificado especificar un periodo de validez diferente para la llave privada, como para el certificado.

e) Certificate Policies: Esta extensión contiene una secuencia de una o más términos de información de políticas, cada una de éllas formada por un *Identificador de Objeto (OID)* y unos calificadores opcionales.

f) Policy Mappings: Esta extensión es utilizada en los certificados de la CA. Lista una o más pares de OIDs; cada para incluye un *issuerDomainPolicy* y un *subjectDomainPolicy*. Cada par debe considerar el *issuerDomainPolicy* equivalente para cada *subjectDomainPolicy* dentro de la CA.

g) Subject Alternative Name: Esta extensión permite que identidades adicionales puedan ser enlazadas al sujeto (subject) del certificado. Entre las opciones definidas se encuentran la dirección de correo electrónico, un nombre de DNS, una dirección IP, o un identificador de recurso uniforme (URI).

h) Issuer Alternative Names: Así como la anterior, esta extensión es utilizada para asociar identidades de la Internet al emisor de un certificado.

i) Subject Directory Attributes: Esta extensión es utilizada para transportar los atributos de identificación del sujeto.

j) Basic Constraints: Esta extensión identifica si el sujeto del certificado en una CA y la máxima profundidad de la ruta de certificación válida que se incluye en el certificado.

k) Name Constraints: Esta extensión, que sólo debe ser usada en los certificados de la CA, indica un espacio de nombres en el cual todos los nombres de los sujetos en los certificados posteriores dentro de la ruta de certificación deben ser localizados.

l) Policy Constraints: Esta extensión obliga a la validación de la ruta de certificación de dos maneras. Puede ser utilizado para prohibir el mapeo de políticas o requerir que cada certificado en la ruta contenta un identificador de política aceptable.

m) Extended Key Usage: Esta extensión indica uno o más propósitos para el cual, la llave pública certificada podrá ser usada, como agregado o reemplazo del propósito indicado en la *key usage extension.* Usualmente, esta extensión aparece en sólo en los certificados de las entidades finales.

n) CRL Distribution Points: Esta extensión identifica cómo la información de la CRL debe ser obtenida.

o) Inhibit Any-Policy: Esta extensión indica que el OID especial *anyPolicy*, con el valor { 2 5 29 32

32 0 }, no es considerado una pareja explícita para otras políticas de certificado.

p) Freshest CRL: Esta extensión, identifica como la información delta CRL es obtenida.

II. Extensiones Privadas para Internet

a) Authority Information Access: Esta extensión indica como acceder a la información y los servicios de una CA para el emisor de los certificados. La información y los servicios podrán incluir validación on-line y datos de las políticas de la CA. Esta extensión puede ser incluida en los certificados de las entidades finales o en las CAs.

b) Subject Information Access: Esta extensión indica como se debe acceder a la información y los servicios para el sujeto de los certificados. Cuando el sujeto es una CA, la información y los servicios podrán incluir validación del certificado y datos de políticas de CA.

2.3 CONFIGURACIÓN DE LAS PETICIONES DE FIRMA DE CERTIFICADO (CSR)

Una *Petición de Firma de Certificado* (CSR - Certificate Signing Request) es un mensaje enviado desde un aplicante a certificado hacia una Autoridad de Certificación para aspirar a que ésta lo firme y así poder tener un Certificado de Identificación Digital. Antes de crear una CSR, el aplicante genera un par de llaves, manteniendo la llave privada en secreto. La CSR contiene información identificando al aplicante (Tal como el nombre del directorio, en caso que sea un certificado X.509) y la llave pública escogida por el aplicante.

La definición del formato en que se deben realizar las CSRs se encuentra estandarizado en el PKCS #10[34] y por el RFC 2986.

I. Definición de los Atributos Adicionales

Uno de los aspectos de consideración al momento de diseñar el CSR, es saber que información se debe solicitar de los usuarios. En ocasiones puede resultar necesario almacenar dentro del certificado información delicada como la dirección de correo electrónico, o la dirección del hogar del usuario o su teléfono. Esta información puede ser almacenada dentro del certificado pero no se

34 PKCS. Public Key Cryptography Standards. <http://www.rsasecurity.com/rsalabs/node.asp?id=2124>

debe mostrar, es decir, que en la práctica, no se guarda en el certificado que se expide para el público.

II. Peticiones PKCS #10

Los primeros certificados digitales que fueron utilizados en los servidores basados en Software Libre fueron autogenerados, es decir, el administrador generaba su par de llaves para el protocolo que deseaba asegurar (HTTP, IMAP, POP, LDAP, SMTP, etc.) y luego firmaba su certificado con la llave privada que había generado. Esto daba como resultado, la no interacción con una Entidad de Certificación que garantice la seguridad de la información.

Así es, como el administrador de la Entidad emisora PKCS #10, debe definir los datos que deben ser dados por el cliente que desee que su CSR sea firmada por la Entidad de Certificación.

2.4 CONFIGURACIÓN DEL SUJETO (SUBJECT) DE LA CA/RA

La configuración del *subject* de la Autoridad de Certificación o de Registro, se resume simplemente a la definición del Nombre Distinguido (DN - Distinguished Name) bajo el cual se van a emitir los certificados digitales.

El *Nombre Distinguido* (DN) es una secuencia de *Nombres Distinguidos Relativos* (RDN), conectados por comas.

Un RDN es un atributo con un valor asociado de la forma **attribute=***valor*; normalmente expresado en el formato de cadenas UTF-8. Los tipos de atributos típicos utilizados por los RDN son los siguientes:

Identificador	*Tipo de Atributo X.500*
DC	domainComponent
CN	commonName
OU	organizationalUnitName
O	organizationName
STREET	streetAddress
L	localityName
ST	stateOrProvinceName
C	countryName
UID	userid

Los siguientes son ejemplos de nombres distinguidos:

CN=Pepito Perez, OU=Ventas, DC=Organizacion,DC=com

CN=Fulanito, OU=Admin, DC=Organizacion,DC=com

2.5 CONFIGURACIÓN LDAP

La mayoría del software de administración de entidades de certificación provee una interfaz LDAP para administrar de manera centralizada los repositorios de certificados. Dependiendo de la aplicación, este proveerá el mecanismo para acceder a este repositorio, ya sea por cliente web, o algún otro cliente en particular.

También es importante conocer si el software de administración viene con un servidor de directorio o necesita que se instale éste por aparte.

En caso que la instalación del directorio se tenga que realizar por separado, hay que asegurarse que cuente con los siguientes esquemas:

- *Core schema (RFC 2251 - RFC 2256)*
- *Cosine and Internet X.500 schema (RFC 1274)*
- *InetOrgPerson schema (RFC 2798)*

También es indispensable asegurarse que el *Nombre Distinguido (DN)* del directorio concuerde con el del Motor Criptográfico emisor de los certificados digitales.

También puede ser necesario, la configuración de los parámetros del servidor de directorio, tales como *la Dirección IP, el Puerto del Servidor (LDAP/386 o LDAPS/636), la Base del DN, el Usuario Administrador, el Password del Usuario Administrador, la Versión de LDAP (Por defecto 3), entre otros.*

4.3. SUBETAPA DE IMPLEMENTACIÓN DE LOS SERVICIOS DE IDENTIFICACIÓN DIGITAL

La implementación de los servicios de identificación digital se puede realizar de dos maneras: una en la cual se haga por medio de un tercero, que tome las historias escritas en la subetapa del plan de desarrollo del servicio y las implemente, devolviendo un software "out of the box" y que no más sea instalarlo y configurarlo sobre la infraestructura de llaves públicas (Out-source developing).

Otra forma es realizar la implementación con recursos propios de la organización. Este método puede ser conveniente en caso que el servicio a implementar sea sencillo y no necesite de mayores complicaciones (In-source developing).

A continuación, se van a listar algunos criterios a tener en cuenta durante el proceso de implementación de los servicios telemáticos de identificación digital, tanto cuando se hace "out-sourcing" como "in-sourcing".

CONSIDERACIONES PARA LA IMPLEMENTACIÓN DE SERVICIOS DE IDENTIFICACIÓN DIGITAL OUT-SOURCING

Instalación de la Base de Datos

El primer paso, antes de instalar la base de datos en el servidor donde se va a establecer el servicio de identificación digital es ver que se estén cumpliendo con los requerimientos técnicos de la base de datos. Algunas de éllas, pueden requerir especificaciones hardware bastante complejas así como un sistema operativo determinado. Existen otras cuyos requerimientos pueden llegar a ser un poco más flexibles.

La automatización de la instalación es otro concepto importante. Existen bases de datos cuyos métodos de instalación son muy poco complicados y no requieren de gran interacción con el usuario, sin embargo, se podría llegar en algún caso a requerir de una base de datos de código abierto en donde se aconsejaría durante el proceso de instalación, la realización del código fuente de esta. También estas bases de datos de código abierto pueden ser encontradas en forma binaria, en cuyo caso habría que confiar en la "no alteración del código fuente", por lo que sólo se deben instalar bases de datos de fuentes muy confiables tales como los paquetes oficiales de las distribuciones del sistema operativo.

Hay que cuidar, cualquiera que sea el tipo de instalación, de contar con los requisitos software necesarios tales como librerías, plataformas de desarrollo, etc.

En caso de ser la instalación, una actualización de alguna versión de base de datos anterior, se

recomienda la lectura del manual, ya que esta varía dependiendo de la base de datos y su sistema operativo.

Configuración de la Base de Datos

Los pasos básicos para la configuración de una base de datos son:

1. Configuración del Administrador de Bitácoras.
2. Configuración de la localización de los archivos de la base de datos.
3. Configuración de red (Dirección IP, Número de puerto, Número máximo de conexiones, Habilitación de conexiones tcp o únicamente locales, Tiempo de sesión).
4. Configuración de los usuarios de la base de datos.
5. Configuración del consumo de recursos de máquina (RAM, Disco Duro, SWAP, Recursos del Kernel).

Instalación y Configuración de los Servicios de Identificación digital

Usualmente la instalación de software cuya funcionalidad es algún servicio de identificación digital debe ser lo más sencilla e intuitiva posible.

El alcance y la profundidad en su configuración dependen en gran medida de la calidad del desarrollo de software.

Por ejemplo, supongamos que queremos utilizar algún tipo de mensajería segura utilizando SMIME[35], el software encargado de realizar esta labor debe darnos a configurar los parámetros básicos tales como la dirección del directorio LDAP donde se encuentran los certificados y el servidor de correo que va a enviar los mensajes.

CONSIDERACIONES PARA LA IMPLEMENTACIÓN DE SERVICIOS DE IDENTIFICACIÓN DIGITAL IN-SOURCING

En esta parte de la subetapa, se van a enumerar algunos errores de implementación de código fuente comunes que se deben evitar en cualquier proyecto de desarrollo y que representan la principal causa de errores futuros, así como "bugs", desbordamientos de buffer o simplemente comportamientos inesperados de la aplicación.[36]

35 SMIME. Secure / Multipurpose Internet Mail Extensions. <http://www.ietf.org/html.charters/smime-charter.html>

36 FOWLER, Martin; BECK, Kent; BRANT, John; OPDYKE William y ROBERTS, Don. Refactoring: Improving the Design of Existing Code. 1999. p. 63

Error típico No. 1: Código duplicado. El número uno de los errores a evitar durante la implementación de los servicios de identificación digital es el código duplicado. Si se logran identificar durante esta etapa, o en alguna de las iteraciones de construcción del software estructuras que se repiten, hay que buscar la forma de unificarlos.

Error típico No. 2: Métodos muy grandes. Los programas que mejor trabajan y más durán son aquellos cuyos métodos son los más pequeños. Aquellos métodos que son demasiado grandes, son más difíciles de entender y por ende difíciles de corregir.

Error típico No. 3: Clases muy grandes. Este error sucede cuando una clase trata de hacer demasiado en un programa. Usualmente estas clases muestran demasiadas instancias. Cuando una clase tiene demasiadas instancias, muy probablemente haya código duplicado cerca.

Error típico No. 4: Listas de parámetros muy grandes. Es una muy buena costumbre aprovechar la potencia de los objetos para no pasar todo los parámetros al método sino únicamente lo necesario para él. En los programas orientados a objetos las listas de parámetros tienden a ser mucho más pequeñas que en los programas tradicionales.

Error típico No. 5: Cambios divergentes. Este error ocurre cuando una clase tiene que ser frecuentemente cambiada en diferentes formas y por diferentes por razones. Por ejemplo, hay veces que se necesitan cambiar ciertos métodos en una clase cada vez que se agrega una base de datos al sistema, en este caso se está cayendo en el error de cambios divergentes.

Error típico No. 6: Cirugía a los escopetazos. Este error es similar al anterior pero con sus respectivas diferencias. En éste, cada vez que se realiza un cambio en una clase, afecta a clases secundarias provocando la corrección de éstas últimas. Lo anterior puede llegar a provocar fallas ya que se puede llegar a omitir una que otra corrección repercutiendo en comportamientos inesperados del sistema.

Error típico No. 7: Envidia de características. Este error ocurre cuando un método dentro de una clase, parece más interesado por los métodos de otra clase, que en los métodos que se encuentran en la suya. Ésto suele suceder cuando hay un método que realiza cierta cantidad considerable de accesos a los métodos de otra clase, simplemente para calcular algún valor.

5. ETAPA DE OPERACIÓN Y MANTENIMIENTO

5.1. EVALUACIÓN PERIÓDICA DE LA INFRAESTRUCTURA Y SERVICIOS DE RED

La Infraestructura y los Servicios de Internet abarca un gran rango de actividades electrónicas y en red, incluyendo servicios de información, productos, hardware y software y recursos de telecomunicaciones que los usuarios y proveedores reciben de la red. Así como una inversión a largo plazo, la red debe ser tan escalable como se requiera; por lo tanto basándose en tecnologías escalables y robustas. El desempeño de la Infraestructura y los Servicios de Internet responde a una pregunta: ¿Qué tan bien está su red haciendo lo que debería hacer?

Se debe proveer una estrategia que cumpla con las necesidades del negocio, maximice el desempeño de la red, reduzca los costos de las tecnologías de la Información (IT), mejore la estabilidad, escalabilidad y seguridad de la red, actualice políticas de uso para los servicios, la seguridad y la administración.

La Organización debe planear la evaluación periódica y generar servicios adicionales para evaluar su Infraestructura y Servicios de Internet, y crear estrategias con los siguientes lineamientos:

- Realizar un plan de proyecto detallado.
- Examinar y documentar el entorno de red actual incluyendo inventario de hardware de red, software y aplicaciones, configuración de enrutadores, switches, cableado de red, utilización de protocolos y utilización de memoria.
- Evaluar el desempeño actual de la red, incluyendo patrones de tráfico, optimización de ancho de banda, y conectividad a internet, vulnerabilidades de red, políticas de seguridad y procedimientos de copias de seguridad (backup).
- Realizar un reporte detallado de los resultados.
- Identificar las oportunidades de consolidación de la red, simplificación y reducción de costos.
- Evaluar la adición de nueva infraestructura de red y nuevos Servicios de Identificación Digital según los objetivos a largo y corto plazo de la Organización.
- Planear y diseñar redes y servicios según las recomendaciones que se obtengan.
- Revisión de los planes de proyecto.
- Ejecutar el plan de proyecto.
- Desarrollar seguimientos periódicos, basados en información adicional del desempeño y el

mantenimiento.

La evaluación trae beneficios como: mejoramiento de la capacidad de la red, desempeño, tolerancia a fallos y disponibilidad, monitoreo de los servicios de identificación digital y las actividades de red como parte de las medidas de seguridad, asistencia en una mejor planeación para el desarrollo futuro de la red, generación de advertencias tempranas para evitar las crisis y mejores definiciones de sistemas, tráfico y configuraciones.

5.2. ADMINISTRACIÓN TOTAL DEL MEJORAMIENTO CONTINUO PARA LA ORGANIZACIÓN ENCARGADA DE GESTIONAR LA ENTIDAD DE CERTIFICACIÓN

La sociedad de hoy ha sido testigo de los primeros y turbulentos años de una revolución tan preponderante, como cualquier otra en la historia de la humanidad. Han surgido nuevos medios para la comunicación que han sobrepasado a cualquiera de sus predecesores (teléfono, televisión). El surgimiento de la Internet ha posibilitado el nacimiento de una economía basada en la interconexión de la inteligencia humana. Así es, como se llega al concepto de *Economía Digital,* una nueva forma de mirar la adquisición de capital, en la cual la riqueza llega gracias a la aplicación del conocimiento y la inteligencia a estos nuevos servicios de interconexión humana, cambiando a los participantes, las reglas y los requisitos para la supervivencia y el éxito.

Es así, como la supervivencia y la rentabilidad en un mercado tan hostil y cambiante no solo depende de la calidad del servicio prestado. También depende de la manera como se utilicen todos los recursos para mejorar la calidad de los productos y la productividad de las operaciones y de cómo estas se integran correctamente a las tecnologías con el propósito de generar el mejoramiento de la organización. *Calidad, Productividad, Tecnología y Costos* deben equilibrarse para asegurar que se satisfagan todas las necesidades y expectativas de los integrantes internos y externos a la organización.

De esta manera es como la Administración Total del Mejoramiento Continuo (ATMC) proporciona un escenario para que los emprendedores de los servicios de IT (Tecnologías de Información) tengan una oportunidad de ganar ante la dura competencia, o peor aún, ante la ausencia de élla y desinterés por sus servicios.

Es por esto, que esta referencia metodológica *recomienda* que se tome en serio este punto, para que de esta manera se logren los 12 objetivos que garanticen el éxito de los servicios telemáticos de identificación digital al momento de ser inmersos al mercado:[37]

1. Incremento de la dedicación al mejoramiento
2. Incremento de la inversión del propietario
3. Incremento de la atención por parte de la gerencia
4. Mejoramiento del proceso
5. Incremento de la satisfacción al empleado
6. Incremento de la confiabilidad, tanto para sus empleados, como para sus clientes
7. Incremento de la cooperación de los empleados, dentro de la organización
8. Producción de mejores productos y servicios

37 HARRINGTON, James H. Administración Total del Mejoramiento Continuo. 1997. p. XX

9. Disminución de las quejas, por parte del cliente
10. Incremento de la lealtad del cliente
11. Incremento de las utilidades
12. Incremento de los rendimientos del dueño de la Organización

LA ESENCIA DE LA ADMINISTRACIÓN TOTAL DEL MEJORAMIENTO CONTINUO

El dilema de la gerencia en cualquier organización consiste en el hecho que los recursos con los que cuenta son bastante limitados, y por ende, cualquier esfuerzo de mejoramiento se puede encaminar a parte de la solución, y no a la solución completa como tal. Cinco metodologías se reconocen generalmente dentro de este grupo de "soluciones parciales", entre las cuales se tienen:
- Administración total de costos
- Administración total de la productividad
- Administración de la calidad total
- Administración total de recursos
- Administración total de la tecnología

Es por eso, que con el propósito de mejorar las muchas facetas del mejoramiento se ha desarrollado una metodología llamada "Administración Total del Mejoramiento Continuo" (ATMC), representada en la pirámide de 5 niveles mostrada a continuación[38]:

Figura 16. Pirámide de la Administración Total del Mejoramiento Continuo

38 HARRINGTON, James H. Administración Total del Mejoramiento Continuo. 1997. p. 20

Nivel 1: Dirección. En este nivel, los *Bloques de Construcción (BC)* desarrollan la estrategia que establecerá la dirección futura del proceso de mejoramiento y concentrarán la energía de la organización en relaciones de negocios clave.

Nivel 2: Conceptos básicos. En este nivel, los BC introducen en la organización las metodologías básicas de mejoramiento y las integran a las actividades normales de los negocios.

Nivel 3: Procesos de despacho. En este nivel, los BC se concentran en los procesos que dirigen las industrias de productos y servicios, haciendo la organización más efectiva, eficiente y adaptable, a medida que se reducen costos, tiempo de ciclo y variación.

Nivel 4: Impacto Organizacional. En este nivel, los BC desarrollan nuevas mediciones y estructuras organizacionales.

Nivel 5: Retribución y reconocimiento. En este nivel, el BC se concentra en el desarrollo de un sistema de retribución y reconocimiento que proporcione retribuciones financieras y no financieras. Este sistemas esta diseñado para reforzar la importancia de otras tareas dentro de la pirámide.

Ahora puede surgir la pregunta ¿Por qué se escogió una pirámide para representar el ATMC?. La respuesta es sencilla: se seleccionó con el fin de representar fortaleza y longeividad ya que una pirámide es sinónima de estas dos.

A continuación, se va a entrar en detalles, de cada unos de los *Bloques de Construcción (BC)*, que se forman dentro de la pirámide.

NIVEL 1: DIRECCIÓN

BC1: Liderazgo de la alta gerencia. La alta gerencia debe hacer algo más que apoyar el concepto ATMC. Debe formar parte del proceso, participar en su diseño, asignar recursos y libremente dedicar su tiempo al personal. El comienzo de cualquier proceso de mejoramiento es la alta gerencia.

BC2: Planes de negocios. Todos los empleados necesitan comprender la razón de ser de la organización, cuáles son sus reglas de comportamiento y hacia dónde se dirige ésta. Estas directrices deben comunicarse con claridad dentro de la organización para definir lo que es realmente un plan de negocios: el establecimiento de la dirección de la empresa, los productos y servicios que se van a proporcionar, qué mercados se van a atender y qué metas se van a alcanzar en el futuro.

BC3: Plan de cambio ambiental. El único aspecto sobre el cual la gerencia tiene control, es el ambiente dentro de la organización. Si se desea mejorar, se debe cambiar el ambiente interno para generar los resultados deseados.

BC4: Enfoque en el cliente externo. Las organizaciones se forman para servir a los clientes. Satisfacer al cliente, debe ser la única razón por la cual se encuentra una organización de IT en el mercado. De esta manera, el éxito de la organización reside en gran parte de la excelente comprensión y estrecha relación de trabajo con el cliente/consumidor externo.

BC5: Sistemas de administración de calidad. Este bloque de construcción se utiliza para establecer sistemas de administración de calidad, que se encuentran a la par con las buenas prácticas de negocios. Este nivel básico de sistemas operativos mínimos, es necesario antes que se puedan implementar en forma efectiva métodos más sofisticados de mejoramiento. Estos sistemas de administración de la calidad deben ajustarse a los criterios de las series ISO-9000.

NIVEL 2: CONCEPTOS BÁSICOS

BC6: Participación de la gerencia. Este bloque de construcción está diseñado para hacer que todos los niveles de la gerencia participen activamente en el esfuerzo de mejoramiento. Hacer que la gerencia se sienta confortable en un papel de liderazgo, es esencial para el logro del éxito de todo el proceso.

BC7: Formación de equipos. La utilización de la gerencia y de equipos de empleados para solucionar los problemas de la organización e involucrarse en su proceso de cambio, constituyen un aspecto clave en el competitivo ambiente de negocios de la actualidad. Este bloque de construcción desarrolla conceptos de equipo como parte del proceso administrativo y prepara a los empleados con el finque participen en un ambiente de equipo.

BC8: Excelencia individual. La gerencia debe proporcionar el ambiente, al igual que las herramientas, que permitan y estimulen a los empleados para que alcancenla excelencia y se enorgullezcan de su trabajo, retribuyéndolos luego, con base a sus logros.

BC9: Relaciones con el proveedor. Las organizaciones ganadores tienen proveedores ganadores. El destino de las dos empresas inevitablemente se encuentra ligado. Una vez que el proceso de mejoramiento comienza a afianzarse dentro de una organización, es el momento de comenzar a trabajar con los proveedores. El objetivo de esta asociacion consiste en ayudarles a mejorar el desempeño de su producción e incrementar las utilidades, mientras se reducen los costos de los productos y/o servicios para ésta.

NIVEL 3: LOS PROCESOS DE DESPACHO

BC10: Cambio radical de procesos. Este bloque de construcción utiliza equipos interfuncionales de mejoramiento de procesos (EMP), con el propósito de dar un salto cuántico radical en los procesos decisivos de negocios. Éste se concentra en hacer más eficientes, efectivas y adaptables, aquellas partes importantes de la organización.

BC11: Excelencia del proceso de producto. Este bloque de construcción se concentra en la manera de diseñar y mantener los procesos de despacho de productos, de tal forma que satisfagan consistentemente a los clientes externos y/o internos.

BC12: Excelencia en los procesos de servicios. Los procesos de distribución para los productos y servicios son muy distintos. Estas diferencias hacen necesario aplicar diversos métodos de mejoramiento y métodos comunes, de distintas maneras, en la distribución del servicio.

NIVEL 4: IMPACTO ORGANIZACIONAL

BC13: Proceso de medición. Este bloque de construcción destaca la importancia de un plan general de mediciones en todos los procesos de mejoramiento. Ayuda a que la organización desarrolle un sistema equilibrado al respecto, que demuestre cómo se pueden apartar o complementar entre sí las mediciones interactiva, como calidad, productividad y utilidades.

BC14: Estructura organizacional. A medida que se empiezan a transformar los sistemas de concepción funcional y de mediciones hacia una visión de desarrollo de la organización, la burocracia es eliminada de los procesos y las decisiones se toman a niveles muy inferiores. En este nuevo ambiente, a los empleados se les da "*empowerment*" para que ejecuten sus labores y respondan por sus acciones.

NIVEL 5: RETRIBUCIONES Y RECONOCIMIENTO

BC15: Retribuciones y reconocimiento. Este proceso debe diseñarse para halar en conjunto toda la pirámide. Necesita reforzar el comportamiento deseado de todos. Igualmente, es imprescindible que se comprenda muy bien para que todos escuchen la palabra "Gracias" en forma diferente. Si la organización desea que todos asuman un rol activo en el proceso de mejoramiento, debe estar en capacidad de agradecer a cada individuo, en una forma que sea significativa para éste. Existen momentos para retribuir el esfuerzo en forma de mención meritoria y otros en forma de retribución económica.

Finalmente, se puede ver un resumen de la pirámide y sus bloques de construcción, en la ilustración siguiente:

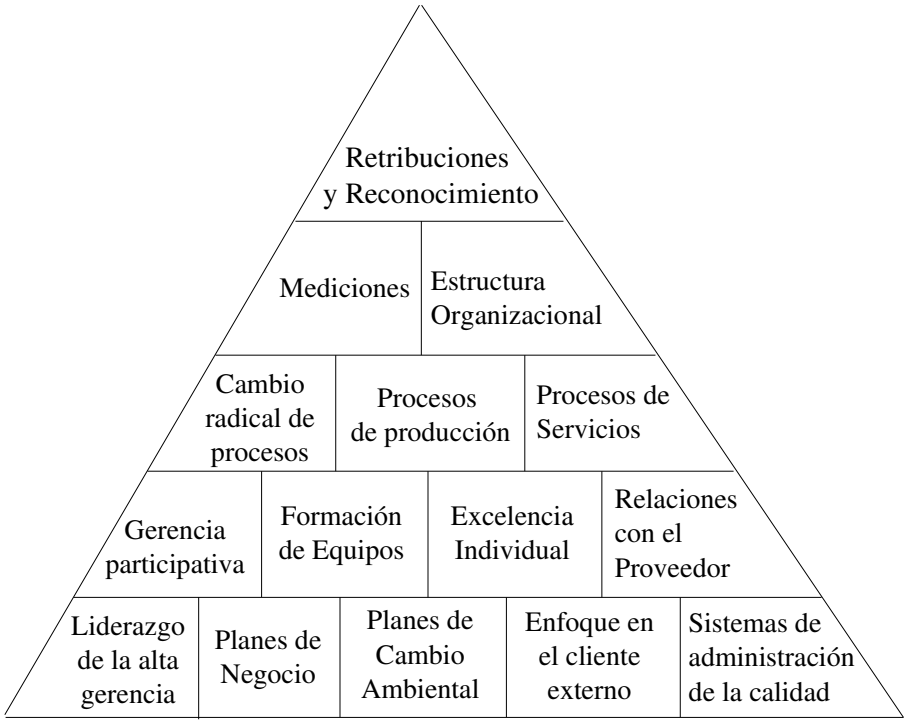


Figura 17. Tareas que hacen parte de la Administración Total del Mejoramiento Continuo

6. CONCLUSIONES

1. Organización en la Elaboración del Plan de Desarrollo del Proyecto (PDP): la clave del éxito

En las primera actividades del proyecto es donde se identificó realmente lo que se desea realizar y más o menos cómo se vería el producto final ya funcionando. El hecho de seguir un proceso en el cual la definición de nuestros objetivos se forman conforme hacemos lluvias de ideas se llama organización. Si debido al afán de implantación se comienzan a menospreciar estos pequeños pero sencillos pasos, se van a comenzar a tener resultados inesperados y sobre todo, pérdidas en los recursos (Tanto de tiempo como económicos).

A pesar que la referencia metodología iza la bandera de la "flexibilidad" y la "adaptabilidad", esto no significa que se tenga que ser desordenados y poco organizados al momento de definir lo que se quiere hacer. El afán no lleva sino al cansancio y es bueno dedicar fuertes sesiones de tiempo a esta primera labor.

2. La importancia Flexibilidad Elaboración del Plan de Desarrollo del Servicio

Cuando se habló de un servicio de identificación digital, a lo largo de la referencia metodológica, se estaba hablando a la vez del desarrollo software de éste, ya que en su esencia un servicio de identificación es eso: software. A pesar que existen cantidades abismales de metodologías para desarrollar software, el presente proyecto de investigación se sintió identificado con las metodologías de desarrollo ágiles.

De ahí la importancia de ser flexibles al momento de pensar en la solución para de el servicio de identificación. La flexibilidad consiste en ser ágiles, en pensar en liberar cada una de las historias a desarrollar. Flexibilidad consiste en hacer que el equipo de trabajo sea realmente un equipo, que las personas luchen en pro del proyecto y sobre todo, que éllos encuentren la libertad para poder explotar su potencial al máximo.

En cuanto a la implementación del servicio telemático, fue "ideal" poner metas cortas, ya que se cumplieron rápido, y al cumplirse rápido así mismo fue su corrección. No hay que temer a liberar código fuente; existen millones de personas en el mundo dispuesta a ayudarnos si lo que se está haciendo les parece interesante: ese es el ideal del software libre.

3. La importancia de conocer el alcance de la infraestructura en el estudio de ingeniería

Cuando se realizó el estudio de ingeniería de la entidad de certificación a construir en la Universidad del Cauca, se tuvo que ser coherentes con los recursos y con la infraestructura de red existente: no se puede pensar en la gran infraestructura dotada de los mecanismos y arquitecturas nombradas. Se fue más sencillo, y se pensó en una arquitectura sencilla, que es suficiente para cubrir la demanda aparente de los servicios de identificación digital. Sin embargo, se diseñó pensando en el futuro, ya que si algún día se quisiera ampliar, no habrían problemas, todo está dentro del estándar.

De ahí la importancia de no sobredimensionarse al momento de realizar los requerimientos de una infraestructura de llaves públicas. No hay que caer en el error de crear los requerimientos para la gran infraestructura, cuando los recursos y las necesidades de la empresa no lo ameritan. Hay que tener cuidado en revisar muy bien lo que se quiere y las necesidades a cubrir del documento del plan de desarrollo del proyecto.

4. La importancia de asesorarse en la creación de la declaración de prácticas de certificación

Pensar que la construcción de una entidad de certificación corresponde únicamente a ingenieros es un error. Y más si se tratan de creación de políticas y claúsulas institucionales. Los abogados son mejor para eso que los ingenieros. De ahí, la importancia que un abogado siga el proceso de creación de Declaración de Prácticas de Certificación. El único ser capaz de aterrizar los conceptos técnicos de los ingenieros y desarrolladores a conceptos que pueden ser eventualmente para algún lío jurídico o para brindar soporte legal a los procesos de identificación digital.

5. Hay muchas formas de hacer negocio con una PKI

No siempre hay que pensar en dinero cuando se habla de infraestructura de llaves públicas. Si bien las PKI fueron pensadas para la realización segura de transacciones que manejan procesos de negocio financieros, los procesos de negocio académicos merecen de la mismas bondades a pesar que su fin no sea el dinero.

6. La validez legal de los certificados digitales es un tema crítico

Registrar la entidad de certificación ante el ente gubernamental encargado de su registro y regulación es algo supremamente importante. Tan importante como si se omitiera este detalle, no

habría soporte legal que respaldase las transacciones que se realizan y por ende ante algún eventual problema, no habría ningún soporte legal respaldando las firmas que la entidad de certificación hubiese generado.

7. Las ventajas del Software Libre

Durante la etapa de implementación del software de la entidad de certificación se conocieron las bondades del software libre. Fácil de instalar, buena documentación, realmente se sabe lo que se está haciendo y sobre todo, se conoce qué realmente se está instalando. Todo esto es supremamente útil al momento de solucionar alguna falla posterior o para mejorar la calidad del servicio prestado.

8. La importancia de los pequeños detalles (Cliente)

Algo para recalcar en la implementación de los servicios de identificación digital son los pequeños detalles. Al cliente le interesan los pequeños detalles: que el botón se encuentre fácil de acceder y que el proceso para utilizar el servicio sea lo más intuitivo posible. Esos son los pequeños detalles que para el cliente son importante y son muchas veces ignorados en el desarrollo del servicio.

9. Porque el fin de la construcción de la PKI es el principio de la gestión de élla

La gestión es el factor más importante para que un proyecto continúe. Cuando se finaliza con la construcción de los servicios y la entidad de certificación, comienza el gran reto para la gestión y es no dejar que todo ese esfuerzo invertido sea en vano. Por eso la importancia de marcar un plan de administración para que la organización crezca y a mediano plazo la infraestructura al igual que los servicios de identificación digital a prestar.

7. RECOMENDACIONES

1. La Referencia Metodológica debe verse como una guía flexible y abierta para la implementación de servicios basados en identificación digital y no como una metodologÍa predictiva que se deba seguir a través de pasos rígidos.
2. En caso que la Organización cuente con una Entidad de Certificación instalada y no desee instalar servicio de identificación digital alguno, no es aconsejable la utilización de la presente Referencia Metodológica
3. No es necesario seguir fielmente las diferentes plantillas de documentos encontradas en la referencia. La estructura de los documentos puede reacomodarse según necesidades específicas.
4. Se debe tener precaución al momento de realizar la elección del hardware para la Entidad de Certificación. Se deben buscar referencias y documentos donde se comprueben la compatibilidad entre éste y el sistema operativo donde se va a poner en funcionamiento. Es preciso indagar con el proveedor y en las listas de discusión especializadas en el tema, antes de tomar cualquier decisión.
5. Al comienzo de todo proyecto para implementación de servicios de identificación digital se debe realizar una cuidadosa planeación. Dedicar el tiempo suficiente para entender lo que se quiere hacer en el plan de desarrollo del proyecto es algo vital para aumentar la probabilidad de éxito del proyecto.

BIBLIOGRAFÍA

ADAMS, Carlisle y LLOYD Steve. Understanding PKI: Concepts, Standars and Deployment Considerations. Boston: Addison Wesley, 2002. 352p.

CARTER, Gerald. LDAP System Administration. Sebastopol: O'reilly, 2003. 308p.

CHANDRA, Pravir; MESSLER, Matt y VIEGA, John. Network Security with OpenSSL. Sebastopol: O'reilly, 2002. 384p.

CISCO SYSTEMS. Academia de Networking de Cisco Systems. Guia del Primer año. Madrid: Pearson, 2004. 1008p.

DORASWAMY, Naganand. IPSec: The New Security Standard for the Internet, Intranets and Virtual Private Networks. New Jersey: Prentice Hall, 2003.

GLASS, Robert. Facts and Fallacies of Software Engineering. Boston: Addison Wesley, 2002. 224p.

GUSTAFSON, David. Theory and Problems of Software Engineering. Nueva York: Mc. Graw Hill, 2002. 236p.

FOWLER, Martin y BECK, Kent. Planning Extreme Programming. Boston: Addison Wesley, 2000. 160p.

FOWLER, Martin; BECK, Kent; BRANT, John; OPDYKE William y ROBERTS, Don. Refactoring: Improving the Design of Existing Code. Boston: Addison Wesley, 1999. 464p.

HARRINGTON, James H. Administración Total del Mejoramiento Continuo. Santa fe de Bogota: Mc. Graw Hill, 1997. 506p.

HEERKENS, Gary. Project Management. Nueva York: Mc. Graw Hill, 2002. 256p.

HERMAN, Roger. ¡Turbulencia! Retos y oportunidades en el mundo del trabajo. Santa fe de Bogota: Mc. Graw Hill, 1997. 216p.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Compendio: Tesis y otros trabajos de grado. Bogotá: ICONTEC, 2004.

ISO. ISO/IEC 17799: Information technology - Code of practice for information security management. Geneva: ISO, 2000. 84p.

JOHANSEN, Oscar. Introducción a la Teoría General de Sistemas. Mexico DF: Editorial Limusa, 1989. 167p.

JOHNER, Heinz; FUJIWARA, Seie y YEUNG, Amelia. Deploying a Public Key Infraestructure. Austin: IBM International Support Organization, 2000. 254p.

KOTLER, Philip. A framework for Marketing Management. New Jersey: Prentice Hall, 2001. 456p.

KUCZMARSKI, Thomas. Innovación: Estrategias de liderazgo para mercados de alta competencia. Santa fe de Bogota: Mc. Graw Hill, 1997. 213p.

MARCHAL, Benoit. XML con ejemplos. Mexico DF: Prentice Hall, 2001. 520p.

MCNAB, Chris. Network Security Assessment. Sebastopol: O'reilly, 2004. 396p.

MENDEZ LOZANO, Rafael Armando. Formulación y Evaluación de Proyectos. Neiva: Quebecor Impreandes, 2000. 265p.

NASH, Andrew y DUANE, William. PKI Infraestructura de Claves Públicas. Madrid: Mc. Graw Hill, 2003. 544p.

PIPER, Fred y MURPHY, Sean. Cryptography: A very Short Introduction. Oxford: Oxford University Press, 2002. 142p.

PRESSMAN, Roger. Ingeniería del Software. Un Enfoque Práctico. Madrid: Mc. Graw Hill, 2002. 601p.

RAINA, Kapil. PKI Security Solutions for the Enterprise: Solving HIPAA, E-Paper Act, and Other Compliance Issues. Indianapolis: John Wiley & Sons, 2003. 334p.

RANKL, Wolfgang y EFFING, Wolfgang. Smart Card Handbook. Londres: John Wiley & Sons, 2003.

1123p.

SCHNEIER, Bruce. Applied Cryptography. Indianapolis: John Wiley & Sons, 1996. 784p.

SCOTT, Charlie; WOLFE, Paul y ERWIN, Mike. Virtual Private Networks, Second Edition. Sebastopol: O'reilly, 1999. 225p.

SERRANO, Carlos. Modelo Integral para el Desarrollo Armónico del Ser. Popayán: Universidad del Cauca, 2003.

SERRANO, Carlos. Modelo Integral para el Profesional en Ingeniería. Popayán: Universidad del Cauca, 2002.

SILBERSCHATZ, Abraham; KORTH, Henry y SUDARSHAN, S. Fundamentos de Bases de Datos. Madrid: Mc. Graw Hill, 2002. 787p.

STONEBURNER, Gary; GOGUEN, Alice y FERINGA, Alexis. Risk Management Guide for Information Technology Systems. Washington: NIST-National Institute of Standards and Technology, 2001. 55p.

THOMAS, Stephen. SSL & TLS Essentials. Securing the Web. Indianapolis: John Wiley & Sons, 2000. 212p.