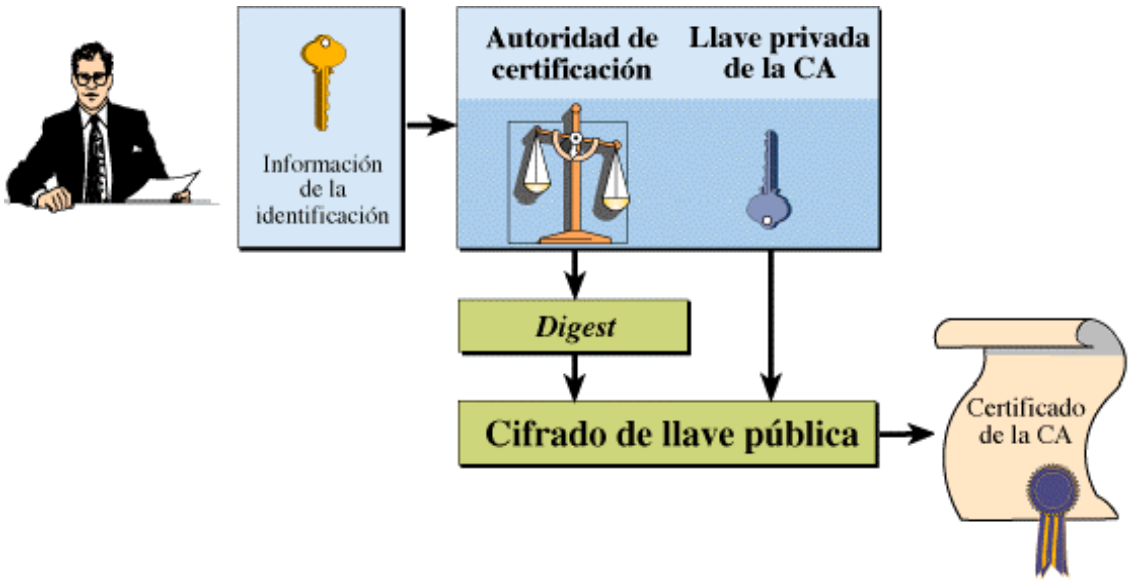
C A P Í T U L O VII

AUTORIDADES DE CERTIFICACIÓN



7.1 INTRODUCCIÓN

En un sistema criptográfico de clave pública cada usuario tiene que hacer accesible su clave pública a todos los demás, por ejemplo, introduciéndola en una base de datos de libre acceso. Esto plantea el problema de que un intruso introduzca o modifique la clave pública de otro usuario y se haga pasar por él. Por tal razón, cuando se recibe una clave pública ¿cómo saber que la identidad del propietario de esta clave no es falsa? Si una persona se hace pasar por otra y envía claves públicas a los receptores, este podrá:

- Firmar digitalmente un mensaje en nombre de otro.
- Realizar transmisiones confidenciales mediante claves de sesión donde el interlocutor piensa que se comunica con otra persona.

Este problema es conocido como *Suplantación de Personalidad*. Para evitar este problema, las claves públicas deben ser Certificadas. Es decir, la clave pública de cada usuario esta firmada por cierta Autoridad Certificadora con un sistema de firma digital de clave pública.

Cuando se desea establecer un protocolo criptográfico con alguien, se obtiene su clave pública certificada y se verifica la firma de la CA. Para ello se requiere la clave pública de la CA que puede, a su vez, estar certificada por una autoridad de nivel superior. Todo el sistema funciona sobre una estructura jerárquica de autoridades certificadoras.

Las claves públicas de las CAs de nivel más alto deben ser conocidas por todos los usuarios sin que sea posible el engaño. Ello se puede conseguir, por ejemplo, haciendo que estas claves formen parte del software de comunicaciones, como: Netscape Communicator o Internet Explorer.

7.2 ORGANISMOS DE CONTROL

La acreditación, control y sanción de los Proveedores de Servicios de Certificación (PSC) será ejercido por la Superintendencia de Telecomunicaciones y por la Superintendencia de Bancos, para el caso de los PSC relacionados con el Sistema Financiero Nacional [LIB 007] y en especial tendrá las siguientes funciones [WWW 017]:

1. Autorizar conforme a la reglamentación expedida por el Gobierno Nacional la operación de entidades de certificación en el territorio nacional.
2. Velar por el adecuado funcionamiento y la eficiente prestación del servicio por parte de las CAs y el cabal cumplimiento de las disposiciones legales y reglamentarias de la actividad.
3. Efectuar las auditorías a las entidades certificadoras.
4. Definir reglamentariamente los requerimientos técnicos que califiquen la idoneidad de las actividades desarrolladas por las CAs.
5. Evaluar las actividades desarrolladas por las CAs autorizadas conforme a los requerimientos definidos en los reglamentos técnicos.
6. Revocar o suspender la autorización para operar como entidad de certificación.
7. Requerir en cualquier momento a las CAs para que suministren información relacionada con los certificados, las firmas digitales emitidas y los documentos en soporte informático que custodien o administren.
8. Imponer sanciones a las CAs por el no cumplimiento o cumplimiento parcial de las obligaciones derivadas de la prestación del servicio.
9. Ordenar la revocación o suspensión de certificados cuando la CA los emita sin el cumplimiento de las formalidades legales.

10. Designar los repositorios y entidades de certificación en los eventos previstos en la Ley.
11. Proponer al Gobierno Nacional la implementación de políticas en relación con la regulación de las actividades de las CAs y la adopción de los avances tecnológicos para la generación de firmas digitales, la emisión de certificados, la conservación y archivo de documentos en soporte electrónico.
12. Aprobar los reglamentos internos de la prestación del servicio, así como sus reformas.
13. Emitir certificados en relación con las firmas digitales de las CAs.
14. Velar por el cumplimiento de las disposiciones constitucionales y legales sobre la promoción de la competencia y prácticas comerciales restrictivas en los mercados atendidos por las entidades de certificación.

7.3 AUTORIDADES DE CERTIFICACIÓN (CA)

Una CA es una institución o empresa comercial que atestigua por la identidad de individuos, organizaciones u otro Certificador de nivel jerárquico inferior. Son entidades públicas o privadas cuya función es ofrecer confianza en los certificados que firman. Generan claves públicas y certificados para usuarios bajo demanda, además de dar a conocer sus claves públicas para las comprobaciones. Los usuarios se deben identificar personalmente para pedir un certificado a una CA. Es un sistema parecido a la cédula de identidad, donde el estado, como entidad de confianza, genera un documento que los bancos y las empresas consideran fiable.

Para descentralizar la gestión de CAs está previsto crear una estructura jerárquica a nivel mundial. Las CAs locales son certificadas por otras de nivel

superior hasta llegar a la principal que es de confianza en todo el mundo. Así se consigue que la confianza sea mundial, para la red Internet sin fronteras, y que la gestión pueda ser local, para los procesos judiciales y facilitar el proceso de identificación personal *(ver figura 7.1)*.

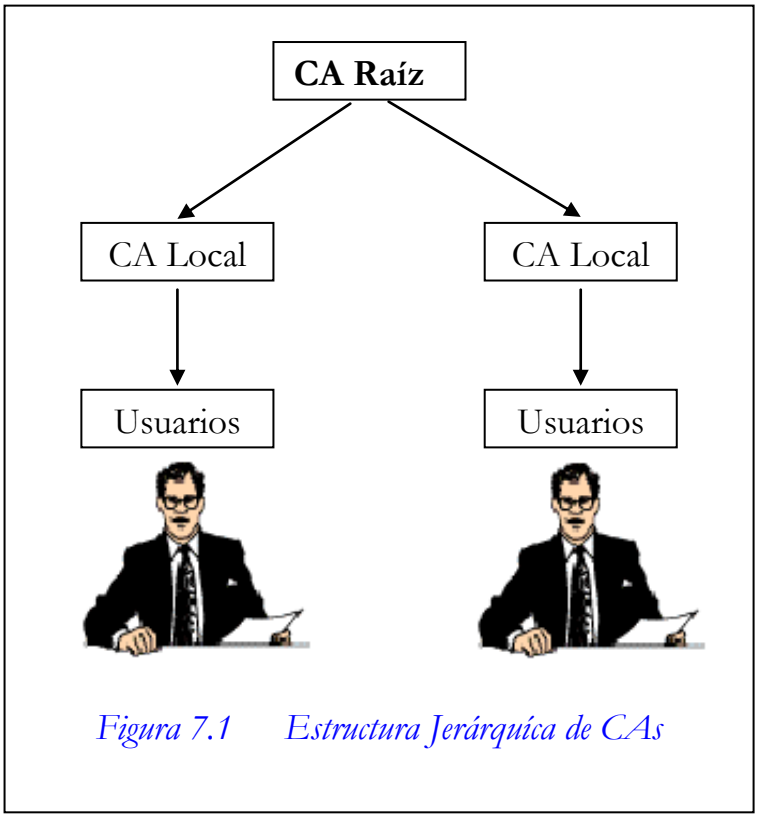


Figura 7.1 Estructura Jerárquica de CAs

Con el tiempo, durante el ejercicio de sus funciones, una autoridad de certificación puede verse fácilmente desbordada si cubre un área geográfica muy extensa o muy poblada, por lo que a menudo delega la labor de verificar la identidad de los solicitantes a las llamadas *Autoridades de Registro* (AR). Las AR pueden abrir multitud de oficinas regionales dispersas por un gran territorio, llegando hasta los usuarios en los sitios más remotos, mientras que la CA se limitaría así a certificar a todos los usuarios aceptados por las AR

dependientes de ella. Gracias a esta descentralización se agiliza el proceso de certificación y se aumenta la eficacia en la gestión de solicitudes.

Actualmente la CA más conocida es la empresa privada americana VeriSing (www.verisign.com), además de Entrust y las empresas de tarjetas de crédito como: Visa, Mastercard y American Express.

7.3.1 VERISIGN (www.verisign.com)

VeriSign es una de las empresas líder en el mercado en servicios de seguridad para el comercio electrónico y las comunicaciones. Es el proveedor tecnológico que permite a las empresas u organizaciones emitir certificados digitales para identificar a sus empleados, proveedores, socios comerciales, etc.

Ahora su compañía puede incorporar autenticación, privacidad y firma digital, basadas en certificados, para ser utilizados en sus sistemas de correo, aplicaciones sobre Web, VPN, ERP, etc.

VeriSign ha creado un conjunto de productos y servicios que permiten a su empresa integrar de manera rápida y segura sus actuales aplicaciones con la tecnología de certificados.

7.3.2 ENTRUST (http://www.entrust.com/)

Entrust, una de las empresas líder en soluciones de Infraestructura de Clave Pública o PKI, tiene como objetivo asegurar la privacidad y la autenticidad de los datos de las empresas. Entrust ofrece soluciones de seguridad para e-business para los mercados de business-to-business (B2B), business-to-consumer (B2C) y empresarial. Su tecnología basada en infraestructuras de

Claves públicas combina las capacidades de encriptación y firma digital. La familia de software de Entrust ofrece una solución de seguridad completa, a través de plataformas múltiples para sobremesas, redes corporativas, Intranet e Internet.

Los productos de Entrust son utilizados por los sectores financieros, administrativos e industrias de alta tecnología y han sido seleccionados como tecnología de seguridad, por compañías como IBM, Tandem y Hewlett Packard. Entrust también es uno de los desarrolladores líderes en cifrado de claves públicas, arquitecturas de seguridad, y estándares internacionales.

Entre los Productos y Servicios para Soluciones de Seguridad más comunes en los diferentes proveedores tenemos los siguientes:

- ✓ **Web .-** Seguridad en transacciones a través de la red local e Internet.
- ✓ **Wireless.-** Protección en transacciones móviles.
- ✓ **Escritorio.-** Seguridad en los datos y la información.
- ✓ **E-Mail.-** Seguridad, comunicación global, rapidez.
- ✓ **PKI.-** La plataforma de seguridad para e-business.
- ✓ **VPN.-** Seguridad en redes y accesos remotos.
- ✓ **ERP.-** Asegura sus aplicaciones de negocios.
- ✓ **Desarrollo.-** Herramientas para asegurar sus aplicaciones.

7.4 REQUISITOS PARA LA FORMACIÓN DE UNA CA

Se contempla que cualquier entidad u organización pública o privada se constituya en Proveedor de Servicios de Certificación (PSC), fomentando así la libre competencia también en este mercado. Ahora bien, para que una persona jurídica se constituya en la figura de autoridad de certificación es necesario que cumpla una serie de requisitos establecidos por el Gobierno Nacional, con base en las siguientes condiciones [WWW 017]:

1. Ser persona jurídica.
2. Poseer una serie de garantías técnicas que demuestren la fiabilidad necesaria de sus servicios, la rapidez y la seguridad en la prestación de los mismos, el empleo de personal calificado y con la experiencia necesaria para dicha prestación, la utilización de sistemas y productos fiables protegidos contra toda alteración, la toma de medidas contra la falsificación de certificados y el uso de sistemas fiables para almacenarlos.
3. Los representantes legales, administradores y personal operativo no podrán ser personas que hayan sido condenados a pena privativa de la libertad, o que hayan sido suspendidas en el ejercicio de su profesión por faltas grave contra la ética.
4. Por otro lado, se definen las garantías económicas de los prestadores de servicios de certificación, a los que se les exige un seguro de responsabilidad civil para cubrir posibles perjuicios, en los cuales se demuestre su responsabilidad, bien por negligencia o por algún fallo técnico o de seguridad en sus equipos.
5. Obtener de la Superintendencia de Telecomunicaciones la correspondiente autorización para operar como entidad de certificación, siempre y cuando cumpla con todos los requerimientos técnicos establecidos por el Gobierno Nacional.

7.5 DEBERES Y OBLIGACIONES DE LA CA

Las Entidades de certificación tendrán, entre otros, los siguientes deberes y obligaciones [WWW 017]:

1. Emitir certificados conforme a lo solicitado o acordado por el suscriptor[33].
2. Implementar los sistemas de seguridad para garantizar la emisión y creación de firmas digitales, la conservación y archivo de certificados y documentos en soporte de mensaje de datos[34].
3. Garantizar la protección y debido uso de la información suministrada por el suscriptor.
4. Garantizar la prestación permanente del servicio de entidad de certificación.
5. Atender oportunamente las solicitudes y reclamaciones hechas por los suscriptores.
6. Efectuar los avisos y publicaciones conforme a lo ordenado en la Ley.
7. Conservar registrada toda la información y documentación relativa a un certificado reconocido durante quince años, con el fin de garantizar que los certificados puedan ser aportados como prueba en los procesos judiciales que pudieran surgir en relación con el uso de la firma digital.
8. Suministrar la información que le requieran las entidades administrativas competentes o judiciales en relación con las firmas digitales y certificados emitidos y en general sobre cualquier documento electrónico que se encuentre bajo su custodia y administración.
9. Actualizar permanentemente los medios técnicos conforme a las especificaciones adoptadas por el Gobierno Nacional mediante reglamento.

[33] Persona que contrata con una entidad de certificación la expedición de un certificado, para que sea nombrada o identificada en él.
[34] Información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares.

10. Permitir y facilitar la realización de las auditorías por parte de la Superintendencia de Telecomunicaciones.
11. Publicar en un repositorio un listado de los certificados suspendidos o revocados.
12. Publicar en un repositorio su práctica de autoridad de certificación.
13. Elaborar los reglamentos que definen las relaciones con el suscriptor y la forma de prestación del servicio.

7.6 AUDITORÍAS A LAS ENTIDADES DE CERTIFICACIÓN

La Superintendencia de Telecomunicaciones realizará por lo menos una vez al año una visita de auditoría a cada CA autorizada para operar, con el objeto de evaluar el cumplimiento y desempeño de sus operaciones dentro de los parámetros fijados en la Ley [WWW 017].

Como resultado de las visitas de auditoría, la Superintendencia evaluará el desempeño de cada una de las CAs, formulando las recomendaciones e imponiendo las medidas pertinentes que deben ser atendidas por las entidades vigiladas para efectos de normalizar y optimizar la prestación del servicio de conformidad con las exigencias legales y reglamentarias.

Si como resultado de la auditoría se establece que la CA no ha cumplido con los requerimientos legales y reglamentarios en el desempeño de sus operaciones, la Superintendencia podrá imponer cualquiera de las sanciones previstas en la Ley.

7.7 MANIFESTACIÓN DE PRÁCTICA DE LA CA

Cada CA autorizada publicará, en un repositorio de la Superintendencia de Telecomunicaciones o en el que ésta designe, una manifestación de práctica de entidad de certificación que contenga la siguiente información [WWW 017]:

1. El nombre, la dirección y el número telefónico de la CA.
2. La clave pública actual de la CA.
3. El resultado de la evaluación obtenida por la CA en la última auditoría realizada por la Superintendencia.
4. Si la autorización para operar como Entidad de certificación ha sido revocada o suspendida (la clave pública de la CA) se incluirá un registro que deberá contener la fecha de la revocación o suspensión y los motivos de la misma.
5. Los límites impuestos a la CA en la autorización para operar.
6. Cualquier evento que sustancialmente afecte la capacidad de la CA para operar.
7. Cualquier información que se requiera mediante reglamento.

7.8 CESE DE ACTIVIDADES POR PARTE DE LA CA

Las CAs autorizadas pueden cesar en el ejercicio de actividades, siempre y cuando haya recibido autorización por parte de la Superintendencia de Telecomunicaciones [WWW 017].

Una vez que la Superintendencia autorice la cesación de actividades, la CA que cesará de operar, deberá enviar a cada suscriptor un aviso con no menos de noventa (90) días de anterioridad a la fecha de la cesación efectiva de

actividades, en el cual solicitará autorización para revocar o publicar en otro repositorio de otra CA, los certificados que aún se encuentran pendientes de expiración.

Pasados sesenta (60) días sin obtenerse respuesta por parte del suscriptor, la CA podrá revocar los certificados no expirados u ordenar su publicación en un repositorio de otra CA; en ambos casos, dando aviso de ello al suscriptor.

7.9 SANCIONES IMPUESTAS A LA CA

La Superintendencia de Telecomunicaciones de acuerdo con el debido proceso y el derecho de defensa, podrá imponer según la naturaleza y la gravedad de la falta, las siguientes sanciones a las CAs que incumplan o violen las normas a las cuales debe sujetarse su actividad [WWW 017]:

1. Amonestación.
2. Multas. El monto de la multa se graduará atendiendo al impacto de la infracción sobre la calidad del servicio ofrecido, y al factor de reincidencia.
3. Suspender de inmediato todas o algunas de las actividades de la entidad infractora.
4. Separar a los administradores o empleados responsables, de los cargos que ocupan en la CA sancionada. También se les prohibirá a los infractores trabajar en empresas similares por un periodo de diez (10) años.
5. Prohibir a la CA infractora prestar directa o indirectamente los servicios de entidad de certificación por el término de diez (10) años.
6. Revocación definitiva de la autorización para operar como entidad de certificación, cuando la aplicación de las sanciones anteriormente enumeradas, no haya sido efectiva.

7.10 CERTIFICADOS DIGITALES X.509 V3

Los certificados X.509 V3 es un formato estándar para la certificación de claves públicas recomendado por la ISO (International Standards Organization). El certificado es esencialmente una clave pública y un identificador, firmados digitalmente por una Autoridad de Certificación. Su utilidad es demostrar que una clave pública pertenece a un usuario concreto.

El estándar X.509 sólo define la sintaxis de los certificados, por lo que no está atado a ningún algoritmo en particular, y contempla los siguientes campos [WWW 006]:

- **Versión.-** La versión del protocolo X.509.
- **Número de serie.-** Identificador único del certificado, asignado por la CA.
- **Identificador del algoritmo empleado para la firma digital.**
- **Nombre de la CA.**
- **Periodo de validez.-** La fecha de inicio y la fecha final.
- **Nombre del Usuario.**
- **Clave pública del Usuario.**
- **Identificador único de CA.-** Cada CA tiene un número de identificación único en el mundo.
- **Identificador único del Usuario.-** Los usuarios tienen un identificador único en la CA para todos sus certificados.
- **Extensiones.-** Posibles extensiones de información, como E-mail, etc.
- **Firma Digital del CA-** El CA firma con su clave privada todos los campos anteriores.

Estos certificados se estructuran de forma jerárquica, de tal forma que nosotros podemos verificar la autenticidad de un certificado comprobando la firma de la autoridad que lo emitió, que a su vez tendrá a otro certificado expedido por otra autoridad de rango superior. De esta forma vamos subiendo en la jerarquía hasta llegar al nivel más alto, que deberá estar ocupado por un certificador que goce de la confianza de toda la comunidad, *(ver figura 7.2)*.

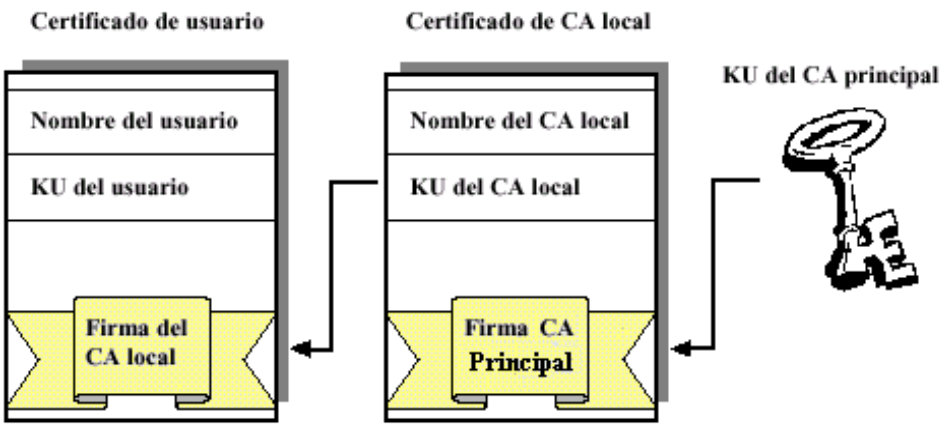


Figura 7.2 Estructura Jerárquica de Certificados

El mecanismo que debe emplearse para conseguir un certificado X.509 es enviar nuestra clave pública (nunca la clave privada) a la autoridad de certificación, después de habernos identificado positivamente frente a ella.

Existen autoridades de certificación que, frente a una solicitud, generan el par de claves (pública y privada) y lo envían al usuario. Hemos de hacer notar que en este caso, si bien tendremos un certificado válido, nuestro certificador podría descifrar todos nuestros mensajes.

Actualmente todas las claves públicas se envían en certificados excepto las primeras de confianza que sirven para firmarlos. Aceptar o rechazar una clave pública depende de la firma que la avala en el certificado. Todos los programas navegadores y de correo actuales están preparados para recibir certificados, comprobarlos y dar un mensaje al usuario de auténtico o no.

Los certificados permitirán a sus titulares realizar una gran cantidad de acciones a través de la Internet, como por ejemplo [WWW 020]:

- Acceder por medio de su navegador a sitios web restringidos, a los cuales les deberá presentar previamente el certificado, cuyos datos serán verificados y en función de los mismos se le permitirá o denegará el acceso.
- Enviar y recibir correo electrónico cifrado y firmado.
- Ingresar en Intranets corporativas, e incluso a los edificios o instalaciones de la empresa, donde se le pedirá que presente su certificado, posiblemente almacenado en una tarjeta inteligente.
- Firmar software para su uso en Internet, como applets de Java o controles ActiveX de Microsoft, de manera que puedan realizar acciones en el navegador del usuario que de otro modo le serían negadas.
- Firmar cualquier tipo de documento digital, para uso privado o público.
- Realizar transacciones comerciales seguras con identificación de las partes, como en SSL, donde se autentica al servidor web, y especialmente en SET (Transacciones Electrónicas Seguras), donde se autentican tanto el comerciante como el cliente.

7.11 SUSPENSIÓN Y REVOCACIÓN DE CERTIFICADOS

El suscriptor de una firma digital certificada, puede solicitar a la entidad de certificación que expidió un certificado, la suspensión[35] o la revocación[36] del mismo. La revocación o suspensión del certificado se hace efectiva a partir del momento en que se registra por parte de la CA. Este registro debe hacerse en forma inmediata, una vez recibida la solicitud de suspensión o revocación.

Una Entidad de certificación revocará un certificado emitido por las siguientes razones [WWW 017]:

1. A petición del suscriptor o un tercero en su nombre y representación.
2. Por muerte del suscriptor.
3. Por disolución del suscriptor en el caso de las personas jurídicas.
4. Por la confirmación de que alguna información o hecho contenido en el certificado es falso.
5. La clave privada de la CA o su sistema de seguridad ha sido comprometido de manera que afecte la confiabilidad del certificado.
6. Por el cese de actividades de la entidad de certificación.
7. Por orden judicial o de entidad administrativa competente.
8. Violación a las políticas de la AC por parte del suscriptor.
9. Expiración del certificado.

El suscriptor de una firma digital certificada está obligado a solicitar la revocación del certificado correspondiente en los siguientes casos [WWW 017]:

[35] Interrumpir temporalmente el periodo operacional de un certificado.
[36] Finalizar definitivamente el periodo de validez de un certificado.

1. Por pérdida de la clave privada.
2. La clave privada ha sido expuesta o corre peligro de que se le dé un uso indebido.

Si el suscriptor no solicita la revocación del certificado en el evento de presentarse las anteriores situaciones, será responsable por las pérdidas o perjuicios en los cuales incurran terceros de buena fe exentos de culpa que confiaron en el contenido del certificado.

Una vez registrada la suspensión o revocación de un certificado, la CA debe publicar, en forma inmediata, un aviso de suspensión o revocación en todos los repositorios en los cuales la CA publicó el certificado.

7.12 DEBERES DE LOS SUSCRIPTORES

Los suscriptores tendrán los siguientes deberes [WWW 017]:

1. Recibir las claves por parte de la CA o generar las claves utilizando un sistema de seguridad exigido por la CA.
2. Suministrar información completa, precisa y verídica a la CA.
3. Aceptar los certificados emitidos por la CA, demostrando aprobación de sus contenidos mediante el envío de éstos a una o más personas o solicitando la publicación de éstos en repositorios.
4. Mantener el control de la clave privada y reservarla del conocimiento de terceras personas.
5. Efectuar oportunamente las correspondientes solicitudes de suspensión o revocación.

7.13 RESPONSABILIDAD DE LOS SUSCRIPTORES

Los suscriptores serán responsables por la falsedad o error en la información suministrada a la CA. También serán responsables en los casos en los cuales no de oportuno aviso de revocación o suspensión de certificados en los casos indicados anteriormente.