REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA ELÉCTRICA

PROPUESTA DE LA INFRAESTRUCTURA DE CLAVE PÚBLICA (ICP) PARA LA ADMINISTRACIÓN PÚBLICA NACIONAL (APN) Y LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (DPC) PARA LA AUTORIDAD DE CERTIFICACIÓN RAÍZ DE VENEZUELA

Trabajo presentado para optar a la Especialización en Comunicaciones y Redes de Comunicaciones de Datos.

AUTOR: Lic. María Del C. Liendo López

CARACAS, NOVIEMBRE 2.006

TRABAJO ESPECIAL DE GRADO

PROPUESTA DE LA INFRAESTRUCTURA DE CLAVE PÚBLICA (ICP) PARA LA ADMINISTRACIÓN PÚBLICA NACIONAL (APN) Y LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (DPC) PARA LA AUTORIDAD DE CERTIFICACIÓN RAÍZ DE VENEZUELA

TUTOR Académico: Prof.: Vincenzo Mendillo

Presentado ante la ilustre
Universidad Central de
Venezuela para optar al Título
De Especialista en Comunicaciones y Redes de Comunicación de Datos
Por la Lic. María Del C. Liendo López

CARACAS, NOVIEMBRE 2.006

DEDICATORIA

A todas aquellas persona
que me ayudaron de una u otra manera en
especial a mis padres que siempre me apoyaron y me
dieron fuerza para salir de todas las
adversidades, a mis hermanos
que sea un ejemplo para ellos este esfuerzo
de constancia y voluntad
para mi querido futuro esposo por impulsar que termine este proyecto
y además a todas esas fuerzas del universo
que no son palpables pero que
se encuentran en mi corazón.

AGRADECIMIENTOS

En primer lugar doy un agradecimiento especial a Dios, que me guía, me protege y me da fuerza en todos los momentos de mi vida. No encuentro palabras de agradecimiento para estas grandes personas que son tan importantes para mi, que ni con unas simples gracias le puedo agradecer el hecho de estar aquí, lo que les puede decir los amo, a mi madre Bárbara por su ternura, a mi padre Oswaldo por su sabiduría, a mis hermanos Oswaldo y Deysis por su apoyo y a mi querido futuro esposo Arturo.

Le agradezco de corazón al profesor Mendillo por la confianza, paciencia depositada y por abrirme el camino para conocer a las personas que trabajan en SUSCERTE, que Dios lo bendiga.

A la Señora Gipsy por atenderme, escucharme, apoyarme y regalarme el bello tesoro de la amistad al igual que Jenifer del postgrado que Dios las bendiga.

También le agradezco en especial al Ingeniero Jorge Uyá por abrirme las puertas de la Superintendencia de Servicios de Certificación Electrónica, atenderme, enseñarme y darme la oportunidad de compartir con ese bello grupo de trabajo, que Dios los bendiga desde el Superintendente Rafael hasta el presente Omar Montilla, Sra. Dora, Nurys, Jacqueline, Nelly, Sergio, Esther, Ildelen, Rosita, Sara, Lesbia, Nelly, Jessica, Félix, Milagros, Maria Rosa, Andry, Armando, María Mercedes.

A Todos mis amigos (José Antonio, Héctor, Roberto, Marly, Profesora Gertrudis López, Milagros Salazar, Sr. Luis, Reyli, Robert, Ana Rosa, Ana Belén, Neudith, ect.) y demás personas que de una u otra manera me dieron ese empujón para seguir en este proyecto, gracias, esto no solamente queda en puras palabras sino que sale del corazón.

INDICE GENERAL

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA ELÉCTRICA

PROPUESTA DE LA INFRAESTRUCTURA DE CLAVE PÚBLICA (ICP) PARA LA ADMINISTRACIÓN PÚBLICA NACIONAL (APN) Y LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (DPC) PARA LA AUTORIDAD DE CERTIFICACIÓN RAÍZ DE VENEZUELA

Autor: Lic. María Del Carmen Liendo López

Tutor: Prof. Vincenzo Mendillo

Septiembre 2006

RESUMEN

El objetivo principal de este trabajo es diseñar la Infraestructura de Clave Pública (ICP) del Proveedor de Servicios de Certificación (PSC) de carácter público para suministrar los servicios de certificación electrónica a la Administración Pública Nacional (APN) y elaborar la primera versión de la Declaración de Práctica de Certificación de la Autoridad de Certificación (AC) Raíz Nacional.

Para lograr este objetivo se realizaron diferentes actividades. Primero la investigación de los estudios previos realizados por la Superintendencia de Certificación Electrónica (SUSCERTE) y las necesidades actuales para la puesta en marcha de la certificación electrónica nacional. En el levantamiento de información también se consideró la base legal y en paralelo el tema de Infraestructura de Clave Pública (ICP) y todos los agentes que forman parte de esta nueva tecnología que fortalece la seguridad. Con lo anterior se obtuvo la base para proceder con la propuesta de Infraestructura de Clave Pública en la Administración Pública Nacional y la construcción de la primera versión de la Declaración de Prácticas de Certificación (DPC) para la Autoridad de Certificación Raíz o ancla de confianza de toda la certificación electrónica del país.

El diseño efectuado en este trabajo sentará las bases para su posterior implementación usando tecnología de clave pública bajo software libre para la gestión de certificados del Proveedor de Servicios de Certificación (PSC) de carácter público. Además se elabora la primera versión de la DPC de la AC Raíz permitirá darla a conocer permaneciendo en un repositorio con acceso público.

INTRODUCCIÓN

Actualmente en el país, al igual que en el resto del mundo, cada vez en forma exponencial aumentan las personas que se conectan a Internet, porque se ha creado una conectividad mundial que une millones de redes, grandes y pequeñas, y cientos de millones de computadores individuales y, cada vez más otros dispositivos, como los teléfonos móviles. Entre las razones de usar Internet se encuentra consultar el estado de las transferencias bancarias, correo electrónico, comunicaciones en línea, solicitud de servicios (pasaporte, financiamientos, declaración de impuesto sobre la renta, consultas de leyes, avances tecnológicos, proyectos, programas de estudio, pagos de servicios, información del país, talleres, eventos, entre otros..).

Ante el constante aumento del intercambio de información en línea, la seguridad se ha convertido en una prioridad para muchos usuarios de Internet, con importancia crítica, hasta el punto de que constituye un requisito previo para el crecimiento del comercio electrónico y el funcionamiento de la economía en su conjunto. La combinación de varios factores es la razón que la seguridad de la información y de las comunicaciones se encuentre en la actualidad a la cabeza de las prioridades del país, porque tradicionalmente la seguridad de las informaciones públicas se basaba en el sentido común, pero actualmente la utilización de nuevas tecnologías presenta nuevos riesgos y obliga a profundizar en cuestiones de seguridad.

Se hace, por lo tanto, necesario trasladar también los sistemas de seguridad al contexto donde los usuarios necesitan sentir confianza y aceptación en sus actividades en Internet, ya que el principal problema reside en que no existe contacto directo entre las partes implicadas. Entonces se necesita un documento electrónico que ofrezca las

mismas funcionalidades que los documentos físicos con el agregado de ofrecer garantías aún sin presencia física en el mundo electrónico.

Todo apunta a brindar seguridad en los medios electrónicos. El estándar ISO/IEC 17799:2000 la define como la preservación de la:

1. **Confidencialidad:** Asegura que la información sólo está accesible para los usuarios autorizados.

2. **Integridad:** Garantiza la completitud y exactitud de la información y sus métodos de procesamiento.

3. **Disponibilidad:** Asegura que sólo los usuarios autorizados tienen acceso a la información y sus activos asociados cuando es requerido.

En el ámbito internacional, para cumplir con la definición de seguridad anterior, se han experimentado cambios radicales en la incorporación de tecnologías y normativas legales que otorgan garantía a los documentos electrónicos para que los servicios que estén vinculados a la tecnología lo sean de forma segura y gocen de confianza, basados en la ley.

Una de las posibles soluciones al problema de la seguridad y privacidad de las transacciones electrónicas son los mecanismos criptográficos, siendo los dos elementos fundamentales el certificado electrónico y la firma electrónica, a fin de resguardar la privacidad y seguridad en la transmisión.

En Venezuela el problema de la seguridad hace que la Administración Pública Nacional (APN) base el sistema de seguridad electrónica en la identificación a través de un marco legal constituido por el Decreto con rango y fuerza de Ley 1.204 sobre Mensajes de Datos y Firmas Electrónicas (LSMDFE) creado en el año 2.001, que otorga y reconoce eficiencia y valor jurídico a la firma electrónica, al mensaje de datos y a toda información inteligible en formato electrónico. Es así como se crea la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) como ente regulador de la certificación electrónica del país, posteriormente en el año 2.004 se crea y publica el Reglamento Parcial del Decreto rango y fuerza de LSMDFE que regula la acreditación de los Proveedores de Servicios de Certificación (PSC) ante SUSCERTE.

Es entonces SUSCERTE el encargado del diseño de la Infraestructura de Clave Pública (ICP) en ingles es Public Key Infraestructura (PKI) de Venezuela, que consiste en un sistema informático y un conjunto de reglas, políticas y normas para una comunicación y transacciones seguras entre organizaciones o individuos, para aportar a los procedimientos electrónicos las cualidades de confidencialidad, integridad y disponibilidad y no repudio que éstos requieren y ofrecer las garantías adecuadas en Internet.

Es así que el gobierno a través de SUSCERTE responde al problema de seguridad en las transacciones de Internet con la certificación electrónica utilizando una ICP Nacional bajo el modelo jerárquico subordinado como el adoptado en Brasil y Argentina, donde están representados los diferentes sectores: público, privado, finanzas y educación, entre otros, del país. El modelo parte de una raíz encargada de generar y administrar los certificados electrónicos a los PSC de los sectores público y privado.

De esta forma SUSCERTE, como ente regulador para desempeño de su gestión en función de excelencia, debe establecer y describir los procedimientos del ancla o raíz de confianza de la ICP Nacional necesarios para proteger, gestionar y dar inicio a las operaciones de certificación electrónica en el país. Además de impulsar y apoyar a la creación del PSC de carácter público que prestará en la APN los servicios de certificación electrónica cumpliendo con la LSMDFE.

El presente trabajo de grado consiste en el análisis y diseño de un sistema certificación electrónica confiable para Venezuela capaz de llevar el control de la gestión de los certificados electrónicos emitidos por la raíz a las autoridades de certificación de los proveedores de servicios de certificación electrónica a entidades finales y así difundir a la comunidad en general confianza en los servicios electrónicos.

La estructura de este trabajo de grado se esquematiza en cinco capítulos:

CAPITULO I: Se describe el contexto del problema y su formulación. Objetivos generales y específicos de la investigación. Se destaca la importancia del trabajo a través de la justificación y por último los alcances y limites del trabajo presentad.

CAPITULO II: Se presenta lo que se ha considerado esencial conocer sobre la seguridad electrónica, mecanismos criptográficos, Infraestructura de Clave Pública, modelos de confianza, dispositivos criptográficos seguros y la organización de SUSCERTE.

CAPITULO III: Se expone el método de investigación, con el tipo y diseño de la investigación para luego escoger el instrumento para hacer el análisis a los datos

recolectados con la finalidad de cumplir con los objetivos del presente trabajo de grado.

CAPITULO IV: Se expone el diseño de la Infraestructura de Clave Pública Nacional en general y se especifica la infraestructura del Proveedor de Servicio de Certificación de carácter público para la Administración Pública Nacional (APN).

CAPITULO V: Se define la Declaración de Prácticas de Certificación de la Autoridad de Certificación Raíz de Venezuela.

PROBLEMA DE INVESTIGACIÓN

En este capítulo se describe el propósito de la investigación, la utilidad de la misma y las metas a cumplir en este trabajo de grado.

.

CONTEXTO DEL PROBLEMA DE INVESTIGACIÓN

En Venezuela, al igual que el resto del mundo, se está trabajando en la certificación electrónica, creándose la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE). En el artículo Nº 20 del Capítulo V de la Superintendencia de Servicios de Certificación Electrónica se define como un servicio autónomo dependiente del Ministerio de Ciencia y Tecnología mediante el decreto con fuerza de Ley 1.204 "Ley sobre Mensaje de Datos y Firma Electrónica" (LSMDFE), publicado en Gaceta Oficial de la República Bolivariana de Venezuela Nº 37.148 del 28 de febrero de 2001, y en el artículo 21 del mismo capítulo se define que SUSCERTE tiene por objeto acreditar, supervisar y controlar a los Proveedores de Servicios de Certificación (PSC) electrónica públicos y privados del país.

Una vez formada la base legal, la Superintendencia define el modelo a implantar para la Infraestructura de Clave Pública (ICP) Nacional, obteniendo el modelo jerárquico subordinado. Este parte de una Raíz o ancla del cual se deriva toda la confianza hacia todos los proveedores acreditados. Además es el responsable de llevar el control y la administración de la Raíz como ente regulador de los servicios de certificación electrónica para garantizar que se cumplan los estándares y lineamientos internacionales de seguridad.

SUSCERTE, como custodio de la Raíz, debe garantizar el resguardo de tal forma que se encuentre segura y se realice la generación, administración de los certificados electrónicos a los proveedores acreditados. Así estos proveedores podrán prestar el servicio de certificación electrónica a los usuarios registrados, emitiendo y gestionando los certificados electrónicos, siempre y cuando estos sean validados por el ente regulador para tener plena validez jurídica en Venezuela.

Para dar cumplimiento a lo expresado en la LSMDFE, en SUSCERTE se plantearon encuestas para determinar cómo será la operación de la Raíz Nacional y se concluyó que no existe el documento con el alcance, responsabilidades, obligaciones, procedimiento de solicitud, vigencia, revocación, renovación, de la gestión de los certificados electrónicos emitidos a los proveedores acreditados. Entonces se decidió que es importante elaborar el documento de la Declaración de Prácticas de Certificación de la Autoridad de Certificación (AC) Raíz para que sean de conocimiento público las características, operación, distribución, controles físicas, auditoria, políticas y ciclo de vida de los certificados electrónicos emitidos y gestionados por la AC Raíz Nacional y así generar confianza.

Otro punto destacado en la encuesta fue la necesidad de hacer cumplir con la disposición final tercera de la LSMDFE, donde se indica que es obligatorio que se cree un PSC de carácter público que preste los servicios de certificación electrónica a la Administración Pública Nacional (APN). Para ello se planteó partir con un diseño o modelo del primer PSC acreditado para satisfacer las necesidades del sector público y así avanzar hacia un gobierno electrónico más seguro.

Finalmente se quiere formar el Sistema Nacional de Certificación Electrónica, para que en el país se use la firma electrónica, los certificados electrónicos en las aplicaciones para dar respuesta rápida a sus trámites y confianza a los ciudadanos que son cada vez más, los que usan los medios electrónicos en su vida diaria. Y establecer alianzas con otros países para intercambiar documentos, procesos administrativos, comercio electrónico a través de Internet teniendo la certeza de quien dice ser es realmente la persona. Con esto SUSCERTE impulsará en Venezuela el uso de los certificados electrónicos y las firmas electrónicas en el sector público y privado.

FORMULACIÓN DEL PROBLEMA DE INVESTIGACIÓN

Para satisfacer la labor de SUSCERTE con el país, en el área de seguridad electrónica, se ha planteado resolver el siguiente problema de investigación:

¿Cuál es la estrategia basada en el marco regulatorio venezolano y en la tecnología de Infraestructura de Clave Pública (ICP) para que la Administración Pública Nacional (APN) comience a prestar los servicios de certificación electrónica usando la firma electrónica y los certificados electrónicos? Y ¿Cuáles son los procedimientos que el ancla o raíz de confianza de la ICP Nacional operada por SUSCERTE requiere para la gestión y emisión de certificados electrónicos a los Proveedores de Servicio de Certificación (PSC) del sector público y privado del país?

OBJETIVO GENERAL DE LA INVESTIGACIÓN

El objetivo general que se pretende alcanzar es:

Impulsar el uso de los certificados electrónicos y la firma electrónica a través de la Infraestructura de Clave Pública Nacional cuyo modelo de arquitectura es la jerárquica subordinada que parte de una única Raíz, administrada por SUSCERTE para la gestión y emisión de los certificados electrónicos a los Proveedores de Servicios de Certificación del sector público y privado.

OBJETIVOS ESPECÍFICOS DE LA INVESTIGACIÓN

Para cumplir con el objetivo anteriormente planteado, se deben lograr los siguientes objetivos específicos:

- Analizar los modelos de ICP de otros países, en especial los de la administración pública.
- Evaluar las Declaraciones de Prácticas de Certificación definidas en otros países para la Autoridad de Certificación (AC) Raíz.
- Conocer y cumplir con el Decreto LSMDFE, el Reglamento Parcial del Decreto LSMDFE y las normas que establezca SUSCERTE.
- Definir la estrategia de infraestructura necesaria de clave pública nacional.
- Definir la Declaración de Prácticas de Certificación (DPC) de la AC Raíz de Venezuela, siguiendo la estructura definida por SUSCERTE.

JUSTIFICACIÓN E IMPORTANCIA

Esta tesis se justifica por las siguientes razones:

1. Se podrá cumplir con el marco legal y las normativas en materia de firmas electrónicas y certificados electrónicos vigentes en el país.

2. Es una excelente oportunidad para contribuir a la seguridad de información a través del uso de la Firma Electrónica y Certificados Electrónicos en las aplicaciones de la Administración Pública Nacional (APN).

3. Se diseña una arquitectura de clave pública para ser utilizada por todos los Proveedores de Servicios de Certificación Electrónica del sector público y privado.

4. Se podrá sustituir el proceso de firma manuscrita en las operaciones efectuadas a través de Internet, por la Firma Electrónica con validez jurídica.

5. Permite garantizar que la persona que firma electrónicamente sólo puede ser realizada por el autor de la firma y no pueda negar que ha estampado su firma en el documento.

6. La Norma ISO 17799 hace hincapié en el uso de mecanismos criptográficos que contribuyen al control por riesgos internos en la seguridad de la información en las empresas y organizaciones.

7. La promoción de talleres, congresos y eventos o de cualquier actividad realizada por SUSCERTE para impulsar el uso de la Firma Electrónica y Certificados Electrónicos.

8. Proporciona la Declaración de Prácticas de Certificación (DPC) de la raíz de la certificación electrónica de Venezuela.

9. Ofrece una estrategia para el Desarrollo e Implementación de la ICP bajo Software Libre en la Administración Pública, cumpliendo el Decreto 3.390.

10. Brinda a los usuarios finales los certificados electrónicos de una manera rápida, confiable, cómoda y eficiente.

11. Permite participar y apoyar a la Asociación Latinoamericana de Integración (ALADI) en el proyecto de la digitalización de Certificación de Origen para el comercio electrónico en la región latinoamericana.

ALCANCES Y LÍMITES DE LA INVESTIGACIÓN

En cuanto al alcance de esta tesis se tiene que:

Se basa en el modelo de la ICP de Venezuela para la APN, donde se esquematiza la cadena de confianza que parte desde la AC Raíz, punto inicial de la ICP de Venezuela. La misma estará instalada en el Centro de Cómputo de Datos de SUSCERTE ubicada en el Sótano 3 de la Torre del Ministerio de Ciencia y Tecnología (MCT).

Se utiliza la primera versión de la Declaración de las Prácticas de Certificación (DPC) de la AC Raíz para iniciar la operación de certificación electrónica en Venezuela basada en un esquema realizado en SUSCERTE por una tesis anterior, siguiendo el Decreto con rango y fuerza de LSMDFE, su Reglamento, los estándares y lineamientos de seguridad de SUSCERTE.

En cuanto a los límites de esta tesis tenemos:

La realización de la prueba piloto, con organismos de la Administración Pública Nacional (APN) a través de los certificados electrónicos y firmas electrónicas

incorporadas en sus aplicaciones básicas, como es el caso del correo electrónico seguro con la finalidad de masificar los mismos y dar la confianza necesaria en sus operaciones electrónicas, cumpliendo con los estándares internacionales aprobados para lograr la interoperabilidad y garantizar la protección a la privacidad de los datos e información de los usuarios del Estado.

MARCO TEÓRICO

El presente capítulo expone trabajos previos de Infraestructura de Clave Pública realizados en SUSCERTE, la base legal, la base teórica con definiciones de una visión general de la seguridad, de Infraestructura de Clave Pública (ICP), los modelos de arquitectura, los dispositivos criptográficos seguros y los fundamentos referenciales de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).

ANTECEDENTES DE LA INVESTIGACIÓN

Los estudios previos que guardan relación con el problema planteado en el presente trabajo son:

Falcón, Marifrancy. (2005). Tesis **"Modelos de Declaración de Prácticas de Certificación y Políticas de certificados, que los proveedores de servicios de certificación consignen ante la superintendencia de servicios de certificación electrónica (SUSCERTE) como requisito parcial para la acreditación"**.

RESUMEN

"La finalidad de este trabajo de investigación es hacer un Modelo de Declaración de Prácticas de Certificación y Política de Certificados, que los Proveedores de Servicios de Certificación Consignen ante la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) como requisito parcial para su Acreditación. Esta investigación es de tipo cualitativo ya que permite describir de una manera sistemática y factible los aspectos tratados en dicha investigación. Para el desarrollo de este trabajo, se recopiló información teórica de libros, Internet y trabajos que sirvieron de Marco Referencial. Además de analizar diversas leyes entre ellas se encuentra la Ley Sobre Mensaje de Datos y Firmas Electrónicas que es la base fundamental para la realización de esta investigación. Esta Propuesta describe los pasos que deben cumplir los Proveedores de Servicios de Certificación a la hora de optar por su acreditación. Como conclusión de esta investigación se puede demostrar la importancia que tiene para la Superintendencia de Servicios de Certificación

Electrónica la realización de esta propuesta ya que facilita las herramientas para el fin propuesto".

Esta tesis aporta el modelo de la estructura de Declaración de Prácticas de Certificación para el presente documento. Es el esquema para ajustar el proceso de operación de la Autoridad de Certificación Raíz para la publicación de la responsabilidades, alcance, controles físicos, auditoria, y solicitud, generación, revocación, validez de los certificados electrónicos.

Segovia, Nurys y Díaz, Lucelys. (2004). Tesis **"Estudio para la propuesta de la autoridad de certificación raíz (root) de las acreditaciones a otorgar por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE)"**.

RESUMEN

"La Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) tiene como objeto promover el uso de certificados electrónicos en Venezuela. SUSCERTE, como parte de su trabajo, debe contar con una Autoridad de Certificación Raíz (Root), la cual permitirá la generación de un certificado raíz que será posteriormente utilizado por los Proveedores de Servicios de Certificación Electrónica (PSECs) y así tengan ese grado de confianza e integridad y el no repudio a la hora que ellos ofrezcan el servicio como proveedores. Actualmente en Venezuela no se cuenta con ninguna Infraestructura de Clave Pública (Public Key Infrastructure, PKI) óptima. Solo existen instalaciones aisladas que no cuentan con ninguna certificación raíz con niveles de seguridad necesaria; algunas de estas instalaciones utilizan una Autoridad de Certificación Raíz que se encuentra fuera del país. Por las razones antes mencionadas

es de vital importancia para SUSCERTE la creación de una Autoridad de Certificación Raíz (Root), ya que mediante ésta se podrá garantizar la confiabilidad, seguridad, disponibilidad y fiabilidad de los servicios prestados que estén subordinadas a la Raíz y sentar las bases para que Venezuela pueda contar con una Infraestructura de Clave Pública (PKI) controlada que ayudará al incremento del uso de Comercio Electrónico y Gobierno Electrónico".

Esta tesis aporta el modelo jerárquico subordinado base del Sistema Nacional de Certificación Electrónica de Venezuela. La Infraestructura de Clave Pública tiene una única raíz y de allí se desprende toda la confianza en el sistema, es decir todo aquel proveedor que se encuentre subordinado a la raíz estará en la cadena de confianza así todos los que son parte del sistema garantizan seguridad y validez. La raíz o ancla de confianza esta bajo el control de SUSCERTE para proporcionar seguridad en la emisión de los certificados electrónicos a los proveedores que se acrediten y también la superintendencia es responsable de elaborar la normativa que los proveedores deben cumplir para garantizar el cumplimiento de los estándares y lineamientos de certificación electrónica.

BASES LEGALES

Para la fecha existen sólo diecisiete países en el mundo con un marco legal establecido por sus respectivos gobiernos en el desarrollo de certificación electrónica, es decir apenas está comenzando a establecerse las reglas para que en el mundo entero los trámites electrónicos tengan la misma validez jurídica que los documentos en físico.

La situación de Venezuela al igual que en Europa, Brasil, Argentina, donde hay la legislación sobre la materia, se restringe quien puede convertirse en prestador de servicios de certificación electrónica a diferencia, de otros países como los Estados Unidos donde reina mayor libertad de mercado, porque las reglas no son siempre claras.

Según Pagés, el rol fundamental, en esta etapa embrionaria de las Tecnologías de Información y comunicación (TIC) en Venezuela, consiste en promover y profundizar las políticas públicas y la base legal para incentivar la creación de la infraestructura física, facilitar el uso y el acceso a la red de las nuevas tecnologías para toda la población.

En el siguiente punto se hace referencia no sólo a la normativa legal de los mensajes de datos y firmas electrónicos, sino a toda la legislación en TIC vigente en Venezuela que hace hincapié a los documentos electrónicos.

1. Artículos 108 y 110 de la Constitución Nacional.
2. Ley sobre Mensajes de Datos y Firmas Electrónicas.
3. Reglamento Parcial del Decreto Ley Sobre Mensajes de Datos y Firmas Electrónicas.
4. Ley Orgánica de Ciencia, Tecnología e Innovación.
5. Decreto 825.

6. Ley Orgánica de la Administración Pública.

7. Ley de Licitaciones.

8. Ley Especial sobre Delitos Informáticos.

9. Ley de Registro Público y del Notariado.

10. Ley de Protección al Consumidor y al Usuario

11. Código Orgánico Tributario.

12. Ley Orgánica de Telecomunicaciones

1. **Artículos 108 y 110 de la Constitución Nacional**: La carta magna de Venezuela reconoce el interés público de la ciencia, la tecnología, el conocimiento, la innovación y sus aplicaciones y los servicios de información necesarios por ser instrumentos fundamentales para el desarrollo económico, social y político del país, así como para la seguridad y soberanía nacional. Igualmente establece que el Estado garantizará servicios públicos de radio, televisión y redes de bibliotecas y de informática, con el fin de permitir el acceso universal a la información. Los centros educativos deben incorporar el conocimiento y aplicación de las nuevas tecnologías, de sus innovaciones, según los requisitos que establezca la ley.

2. **Ley sobre Mensajes de Datos y Firmas Electrónicas:** Este Decreto-Ley. Tiene por objeto reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y a los Certificados Electrónicos. Homologa los efectos de la firma autógrafa a la firma electrónica, establece los requisitos mínimos que confieran seguridad e integridad a

los mensajes de datos y a la firma electrónica, establece los requisitos mínimos que debe tener un Certificado Electrónico, crea un Registro de Proveedores de Servicios de Certificación, crea la Superintendencia de Servicios de Certificación Electrónica para registrar y supervisar a los Proveedores de Servicios de Certificación. Con estos elementos principales y otros que se establecen en este proyecto de ley, se brinda seguridad y certeza jurídica a los actos y negocios electrónicos, mientras se perfeccionan y estandarizan los usos, costumbres y modos de relacionarse y comerciar por este medio a nivel mundial.

3. **Reglamento Parcial del Decreto Ley Sobre mensajes de Datos y Firmas Electrónicas:** Este reglamento tiene por objeto fijar la normativa que regula la acreditación de los Proveedores de Servicios de Certificación ante la Superintendencia de Servicios de Certificación Electrónica además de la creación del Registro de Auditores, así como los estándares, planes y procedimientos de seguridad, de conformidad con el Decreto Ley.

4. **Ley Orgánica de Ciencia, Tecnología e Innovación:** Este Decreto-Ley tiene por objeto fijar los principios orientadores que en materia de ciencia, tecnología e innovación, establece la Constitución de la República Bolivariana de Venezuela, organizar el Sistema Nacional de Ciencia, Tecnología e Innovación, definir los lineamientos que orientarán las políticas y estrategias para la actividad científica, tecnológica y de innovación, con la implantación de mecanismos institucionales y operativos para la promoción, estímulo y fomento de la investigación científica, la apropiación social del conocimiento y la transferencia e innovación tecnológica, a fin de fomentar la capacidad para la generación, uso y circulación del conocimiento y de impulsar el desarrollo nacional. En materia específica de Tecnologías de Información y Comunicación se puede resaltar lo establecido en el artículo 22: “El Ministerio de Ciencia y Tecnología coordinará las actividades del Estado que, en el área de tecnologías de información, fueren programadas, asumirá competencias que en

materia de informática, ejercía la Oficina Central de Estadística e Informática, así como las siguientes:

- Actuar como organismo rector del Ejecutivo Nacional en materia de tecnologías de información.
- Establecer políticas en torno a la generación de contenidos en la red, de los órganos y entes del Estado.
- Establecer políticas orientadas a resguardar la inviolabilidad del carácter privado y confidencial de los datos electrónicos obtenidos en el ejercicio de las funciones de los organismos públicos.
- Fomentar y desarrollar acciones conducentes a la adaptación y asimilación de las tecnologías de información por la sociedad.

5. Decreto 825: Declara el acceso y el uso de Internet como política prioritaria para el desarrollo cultural, económico, social y político de la República Bolivariana de Venezuela, reforzando lo previamente establecido en el Plan Nacional de Telecomunicaciones sobre el desarrollo de una Sociedad de la Información. Igualmente, el Decreto dispone las directrices que deberán seguir los órganos de la Administración Pública Nacional para la inserción de esta tecnología de información en todos los ámbitos de la nación. En este sentido, se establece: Incorporar en el desarrollo de sus actividades, objetivos relacionados con el uso de Internet, la utilización de Internet para funcionamiento operativo de los organismos públicos tanto interna como externamente, hacer uso preferente de Internet en sus relaciones con los particulares, para la prestación de servicios comunitarios entre los que se mencionan, a título enunciativo, las bolsas de trabajo, los buzones de denuncia, planes comunitarios con los centros de salud, educación, información, entre otros, así como cualquier otro servicio que ofrezca facilidades y soluciones a las necesidades de la población. Ordena que en un plazo no mayor de tres años, el 50% de los programas

educativos de educación básica y diversificada deberán estar disponibles en formatos de Internet, de manera tal que permitan el aprovechamiento de las facilidades interactivas, todo ello previa coordinación del Ministerio de Educación, Cultura y Deportes.

6. **Ley Orgánica de la Administración Pública:** En los artículos 12 y 148 se recogen exitosamente algunos de los postulados previamente establecidos en el Decreto 825 elevándolos a rango de precepto orgánico. En éstos establece lo siguiente: Los órganos y entes de la Administración Pública deberán utilizar las nuevas tecnologías tales como los medios electrónicos, informáticos y telemáticos, para su organización, funcionamiento y relación con las personas. Cada órgano y ente de la Administración Pública deberá establecer y mantener una página en Internet, que contendrá, entre otra información que se considere relevante, los datos correspondientes a su misión, organización, procedimientos, normativa que lo regula, servicios que presta, documentos de interés para las personas, así como un mecanismo de comunicación electrónica con dichos órganos y entes disponibles para todas las personas vía Internet. También establece que los órganos y entes de la Administración Pública podrán incorporar tecnologías y emplear cualquier medio electrónico, informático, óptico o telemático para el cumplimiento de sus fines. Los documentos reproducidos por los citados medios gozarán de la misma validez y eficacia del documento original, siempre que se cumplan los requisitos exigidos por ley y se garantice la autenticidad, integridad e inalterabilidad de la información.

7. **Ley de Licitaciones:** Establece un capítulo completo para permitir que en los procedimientos regulados por dicha ley se puedan utilizar los medios electrónicos. El objetivo del Decreto-Ley es promover la actualización tecnológica en los procesos de contratación y procura del Estado y demás entes sometidos a la Ley. Con estos preceptos se incluyen en dichos procesos todos los beneficios de los adelantos tecnológicos que permiten, además de cumplir con los principios establecidos en la Ley, el ser más ágiles, eficientes y económicos. Permite igualmente, mediante la

aceptación del uso de estas herramientas, llevar un control automatizado que al mismo tiempo podrían generar los indicadores y estadísticas que sean necesarias. Este Decreto-Ley también incorpora una definición de "medios electrónicos" e incorpora el principio de "no exclusión o discriminación de base tecnológica". El fin último es que los procedimientos de selección del contratista y de contratación se realicen en un ambiente totalmente electrónico.

8. Ley Especial sobre Delitos Informáticos: Tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en dicha ley. Esta ley tipifica los delitos y establece penas con sus circunstancias agravantes y atenuantes y también penas accesorias, entre las clases de delitos que establece se encuentran:

- Contra los sistemas que utilizan tecnologías de información.
- Contra la propiedad.
- Contra la privacidad de las personas y de las comunicaciones.
- Contra los niños y adolescentes.
- Contra el orden económico.

9. Ley de Registro Público y del Notariado: El propósito de este Decreto-Ley ha sido la adaptación del ordenamiento jurídico a los cambios actuales, entre los que se encuentran la nuevas tecnologías informáticas para llegar a una automatización del sistema registral y notarial, así como unificar en un mismo texto normativo las disposiciones que regulen la actuación de los Registros Civiles y Subalternos, de los Registros Mercantiles y de las Notarías Públicas. Se considera de interés público el uso de medios tecnológicos en la función registral y notarial para que los trámites de

recepción, inscripción y publicidad de los documentos sean practicados con celeridad, sin menoscabo de la seguridad jurídica. La Ley establece que los asientos registrales y la información registral emanada de los soportes electrónicos del sistema registral venezolano surtirán todos los efectos jurídicos que corresponden a los documentos públicos. Entre los principales postulados referidos a las TIC, tenemos que todos los soportes físicos del sistema registral y notarial actual se digitalizarán y se transferirán progresivamente a las bases de datos correspondientes. El proceso registral y notarial podrá ser llevado a cabo íntegramente a partir de un documento electrónico y se establece que la firma electrónica de los Registradores y Notarios tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa.

10. Ley de Protección al Consumidor y al Usuario: Tiene por objeto la defensa, protección y salvaguarda de los derechos e intereses de los consumidores y usuarios, su organización, educación, información y orientación, así como establecer los ilícitos administrativos y penales y los procedimientos para el resarcimiento de los daños sufridos por causa de los proveedores de bienes y servicios y para la aplicación de las sanciones a quienes violenten los derechos de los consumidores y usuarios. En materia de TIC, establece un Capítulo (V) completo referido al Comercio Electrónico, incluyendo una definición de éste. Establece los deberes del proveedor de bienes y servicios dedicados al comercio electrónico, entre los que se cuenta el de aportar información confiable, desarrollar e implantar procedimientos fáciles y efectivos que permitan al consumidor o usuario escoger entre recibir o no mensajes comerciales electrónicos no solicitados, adoptar especial cuidado en la publicidad dirigida a niños, ancianos, enfermos de gravedad, entre otros, el deber de informar sobre el proveedor, garantizar la utilización de los medios necesarios que permitan la privacidad de los consumidores y usuarios, ofrecer la posibilidad de escoger la información que no podrá ser suministrada a terceras personas, ofrecer la posibilidad de cancelar o corregir cualquier error en la orden de compra, antes de concluirla, proporcionar mecanismos fáciles y seguros de pago, así como información acerca de su nivel de

seguridad y especificar las garantías. Atribuye al INDECU la obligación de educar a los consumidores a cerca del comercio electrónico y fomentar su participación en él.

11. Código orgánico Tributario: Permite la utilización intensiva de medios electrónicos y permite la declaración y pago de tributos a través de Internet. Los artículos más relevantes en cuanto a TIC se refiere, son: el artículo 125, que establece que la Administración Tributaria podrá "utilizar medios electrónicos o magnéticos para recibir, notificar e intercambiar documentos, declaraciones, pagos o actos administrativos y en general cualquier información. A tal efecto se tendrá como válida en los procesos administrativos, contenciosos o ejecutivos, la certificación que de tales documentos, declaraciones, pagos o actos administrativos realice la Administración Tributaria, siempre que demuestre que la recepción, notificación o intercambio de los mismos se ha efectuado a través de medios electrónicos o magnéticos". El artículo 138, establece que cuando la Administración Tributaria "reciba por medios electrónicos declaraciones, comprobantes de pago, consultas tributarias, recursos u otros trámites habilitados para esa tecnología, emitirá un certificado electrónico que especifique la documentación enviada y la fecha de recepción, la cual será considerada como fecha de inicio del procedimiento de que se trate. En todo caso, se prescindirá de la firma autógrafa del contribuyente o responsable (…) La Administración Tributaria establecerá los medios y procedimientos de autenticación electrónica de los contribuyentes o responsables. El artículo 162, numeral 3 del Código Orgánico Tributario, establece: "Las notificaciones se practicarán, sin orden de prelación, en alguna de estas formas (…). Por correspondencia postal efectuada mediante correo público o privado, por sistemas de comunicación telegráficos, facsimilares, electrónicos y similares siempre que se deje constancia en el expediente de su recepción. Cuando la notificación se realice mediante sistemas facsimilares o electrónicos, la Administración Tributaria convendrá con el contribuyente o responsable la definición del domicilio facsimilar o electrónico".

12. Ley Orgánica de Telecomunicaciones: En materia específica de TIC podemos destacar algunos postulados de esta Ley; la promoción a la investigación, el desarrollo y la transferencia tecnológica en materia de telecomunicaciones y la utilización de nuevos servicios, redes y tecnologías con el propósito de asegurar el acceso en condiciones de igualdad a todas las personas. Para garantizar el cumplimento de sus objetivos, la ley exige a los distintos operadores la homologación y certificación de equipos, así como el uso de la tecnología adecuada, a fin de lograr el acceso universal a la comunicación.

BASES TEÓRICAS

Entre los tópicos teóricos que contempla este trabajo de grado se relacionan, los siguientes:

SEGURIDAD

En general, "seguridad" en un sistema, indica que el mismo está libre de peligro, daño, riesgo, y fallas. La seguridad en Internet requiere atención especial, ya que esta

red está cambiando muchas de las suposiciones que históricamente se han hecho sobre la seguridad computacional y la publicación de información:

- Internet es una red de dos sentidos. Así como hace posible que los servidores Web divulguen información a millones de usuarios, permite también a personas o entidades no autorizadas (hackers, crackers, criminales, vándalos) irrumpir en las mismas computadoras donde se ejecutan los servidores Web. Estos riesgos no existen en prácticamente ningún otro medio informativo.

- Las empresas y los gobiernos utilizan cada vez más Internet para distribuir información importante y realizar transacciones comerciales.

- Aunque Internet es fácil de utilizar, los servidores y navegadores Web son piezas de software extremadamente complicadas y tienen diversas fallas de seguridad potenciales.

- Muchas veces se han agregado nuevas funciones sin prestar suficiente atención a su impacto en la seguridad. Por ello, aun el software bien instalado puede representar amenazas de seguridad.

- Una vez que violen los navegadores y servidores Web, los atacantes pueden ocuparlos como base para iniciar otros ataques contra usuarios y organizaciones.

- Existen (y existirán) muchos usuarios principiantes de los servicios que dispone Internet.

- La generación actual de software les exige tomar decisiones de seguridad relevantes a diario, sin proporcionarles información suficiente para tomar una decisión informada.

REQUERIMIENTOS DE SEGURIDAD

Los requerimientos básicos de seguridad son disponibilidad, integridad, confidencialidad (privacidad) y autenticidad. A continuación se dará una breve definición de cada uno:

Disponibilidad: Es la garantía de que la información y los servicios de la red estarán accesibles para los usuarios autorizados. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

Integridad: Se refiere a la protección que se da a los activos informáticos para que sólo puedan ser modificados por las personas autorizadas. La integridad afecta directamente al correcto desempeño de las funciones de una organización.

Confidencialidad: Se refiere a controlar que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados.

Autenticidad: Propiedad fundamental de la información de ser confrontada en cualquier momento de su ciclo de vida contra su origen real (verdadero/falso). Contra la autenticidad se dan suplantaciones y engaños que buscan realizar un fraude. La autenticidad es la base para poder luchar contra el repudio y como tal, fundamenta el

comercio electrónico o la administración electrónica, permitiendo confiar sin papeles ni presencia física.

Otros requerimientos de seguridad son:

No repudio: Registro e identificación inequívoca de los participantes en una transacción electrónica, de tal manera que no puedan negarla en ningún momento. Es necesario en casos como los siguientes por ejemplo: transacción de retiro de una cuenta bancaria desde Internet o por medio de un cajero electrónico, donde posteriormente el cliente podría negar (repudiar) que hizo la transacción.

Identificación y control de acceso: Se refiere a verificar la identidad de las personas. Autorizar y controlar quién y cómo se accede a los datos y los recursos de un sistema.

Registro: Este requerimiento se refiere a que toda acción dentro de un sistema informático (aplicaciones, redes, computadores, bases de datos) sea registrada con fines de hacer una auditoría posterior, es decir que se puedan saber lo que se hace dentro del sistema y quién lo hace.

POLÍTICAS DE SEGURIDAD

En general, la seguridad informática depende de la articulación eficiente de varios factores, uno de los cuales es ese conjunto de políticas de seguridad, las cuales

representan el marco normativo para el establecimiento de cualquier solución de seguridad para las organizaciones.

¿Por qué se necesitan políticas de seguridad? La información es un recurso muy valioso para las organizaciones y es de vital importancia protegerla, particularmente porque está expuesta a múltiples amenazas externas e internas por la interconectividad que proporcionan las redes y la amplia difusión de la tecnología. Esta responsabilidad de protegerla es de todos los estamentos de la organización, desde la alta gerencia hasta los niveles operativos, para lo cual es necesario dar conciencia y sensibilizar a todos los miembros de la organización sobre el uso apropiado y seguro de la información. Éste es el propósito de las políticas de seguridad en una organización.

¿Qué son las políticas de seguridad informática? Las políticas son directrices escritas divulgadas por la gerencia que expresan la posición de la organización respecto a las acciones a tomar en situaciones generales o particulares relacionadas con la seguridad de la información. Las políticas son de carácter general, de larga duración y van dirigidas a un auditorio amplio dentro, y en ocasiones fuera, de la organización. En cierto sentido son reglas del negocio y por consiguiente su cumplimiento es obligatorio. Las excepciones requieren autorización especial.

Según la International Standards Organization (ISO) el término política de seguridad se suele definir como el conjunto de requisitos definidos por los responsables directos o indirectos de un sistema que indica en términos generales qué está y qué no está permitido en el área de seguridad durante la operación general de dicho sistema.

Parker (1994), señala que cualquier política ha de contemplar los siguientes seis elementos claves en la seguridad de un sistema informático.

- Disponibilidad Es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesitan, especialmente la información crítica.

- Utilidad: Los recursos del sistema y la información manejada en el mismo ha de ser útil para alguna función.

- **Integridad** La información del sistema ha de estar disponible tal y como se almacenó por un agente autorizado.

- **Autenticidad**
  El sistema ha de ser capaz de verificar la identidad de sus usuarios y los usuarios la del sistema.

- **Confidencialidad**
  La información sólo ha de estar disponible para agentes autorizados, especialmente su propietario.

- **Posesión**
  Los propietarios de un sistema han de ser capaces de controlarlo en todo momento; perder este control en favor de un usuario malicioso compromete la seguridad del sistema hacia el resto de usuarios.

Para cubrir de forma adecuada los seis elementos anteriores, con el objetivo permanente de garantizar la seguridad corporativa, una política se suele dividir en puntos más concretos a veces llamados **normativas**. El estándar ISO 17799 define las siguientes líneas de actuación:

- **Seguridad organizacional:** Aspectos relativos en la gestión de la seguridad dentro de la organización (cooperación con elementos externos, *outsourcing*, estructura del área de seguridad, etc.).

- **Clasificación y control de activos:** Inventario de activos y definición de sus mecanismos de control, así como etiquetado y clasificación de la información corporativa.

- **Seguridad del personal:** Formación en materias de seguridad, cláusulas de confidencialidad, reporte de incidentes, monitoreo de personal.

- **Seguridad física y del entorno:** Bajo este punto se engloban aspectos relativos a la seguridad física de los recintos donde se encuentran los diferentes recursos, incluyendo las personas de la organización y de los sistemas en sí, así como la definición de controles genéricos de seguridad.

- **Gestión de comunicaciones y operaciones:** Este es uno de los puntos más interesantes desde un punto de vista estrictamente técnico, ya que engloba aspectos de la seguridad relativos a la operación de los sistemas y telecomunicaciones, como los controles de red, la protección frente a *malware*, la gestión de copias de seguridad o el intercambio de *software* dentro de la organización.

- **Controles de acceso:** Definición y gestión de puntos de control de acceso a los recursos informáticos de la organización: contraseñas, seguridad perimetral, monitoreo de accesos...

- **Desarrollo y mantenimiento de sistemas:** Seguridad en el desarrollo y las aplicaciones, cifrado de datos, control de *software*...

- **Gestión de continuidad de negocio:** Definición de planes de continuidad, análisis de impacto, simulacros de catástrofes...

- **Requisitos legales:** Evidentemente, una política ha de cumplir con la normativa vigente en el país donde se aplica. Si una organización se extiende a lo largo de diferentes países, su política tiene que ser coherente con la normativa del más restrictivo de ellos. En este apartado de la política se establecen las relaciones con cada ley: derechos de propiedad intelectual, tratamiento de datos de carácter personal, junto a todos los aspectos relacionados con registros de eventos en los recursos (*logs*) y su mantenimiento.

ATAQUES Y VULNERABILIDADES

Los ataques pueden clasificarse en: Ataques al hardware, software y a los datos.

Ataques al hardware: Hay muchas formas accidentales o intencionales de atacar un sistema a fin de limitar o impedir su disponibilidad. El robo y la destrucción son las formas más utilizadas. Los gerentes de centros de computación conocen las vulnerabilidades de sus equipos y a menudo instalan sistemas de *seguridad física* para protegerlos.

Ataques al software: Un programa es modificado ya sea para que falle durante su ejecución o para que haga alguna otra cosa. El software es relativamente fácil de modificar: con cambiar un solo bit, puede que el programa deje de funcionar o puede ser que funcione hasta que llegue a alguna rutina que active la parte modificada. Con

cierta habilidad el cambio puede ser mucho más sutil, de manera que el cambio trabaja bien la mayor parte de las veces, pero falla en ciertas circunstancias.

Ataques a los datos: El ataque a los datos es más generalizado y serio que al hardware o al software. Los datos a menudo poseen un valor más grande que el hardware y el software. Porque pueden ser recogidos interviniendo las líneas de comunicación, monitoreando la radiación electromagnética, sobornando empleados o simplemente solicitándolos. Debido a que los datos a menudo están disponibles en forma legible por los humanos, su confidencialidad es un punto de gran preocupación en el ámbito de la seguridad.

Una **debilidad** o **vulnerabilidad** en los sistemas de seguridad puede ser aprovechada para causar daños o pérdidas. Se define como la situación por la cual un recurso es susceptible de ser atacado. Las personas se aprovechan de la vulnerabilidad para intentar un ataque sobre el sistema. Los riesgos en un sistema son circunstancias que potencialmente pueden causar pérdidas o daños, un ataque humano es un ejemplo de riesgo, así como desastres naturales, errores no intencionales y fallas en hardware o software del sistema.

Aunque las personas podrían ser la fuente más grande de problemas de seguridad, no son la única fuente. Basta mencionar los peligros naturales tales como inundación e incendio, que tiene que ver directamente con la vulnerabilidad física de un sistema.

A continuación se mencionan brevemente algunos aspectos bastante obvios de la seguridad física.

Desastres naturales: Los equipos de red están sujetos a los mismos desastres naturales que pueden afectar a casas, oficinas y automóviles. Los aspectos a ser considerados incluyen el costo de reemplazar el equipo, la rapidez con cual el equipo puede ser reemplazado, la necesidad de su disponibilidad y el costo o la dificultad de cargar de nuevo los datos y los programas.

Vándalos humanos: Ataques de fuerza bruta pueden ser muy efectivos, pero ataques más sutiles también pueden ser bastante graves. Un vándalo con pocas habilidades podría tratar el ataque de fuerza bruta, destruyendo equipos electrónicos y los medios de soporte de la información.

El acceso no autorizado: A medida que los sistemas distribuidos, las aplicaciones cliente-servidor e Internet se vuelven más generalizados, proteger al sistema del acceso desde afuera se hace más difícil y más importante. Se necesita la protección tanto para prevenir que usuarios no autorizados tengan acceso al sistema como para verificar la identidad de usuarios autorizados.

Además de los peligros que amenazan la seguridad física de las redes (es decir el hardware), existen en la actualidad los peligros que amenazan la integridad de los datos (es decir el software). Entre estos, los de mayor preocupación son los denominados *virus informáticos* y sus semejantes (caballos de Troya, bombas lógicas).

CRIPTOGRAFÍA

Hoy día hay una fuerte necesidad de seguridad, ya que las redes sufren muchas amenazas como es el redirigir el tráfico, insertar paquetes falsos, modificar paquetes, montar ataques de negación del servicio, e introducir software dañino en los sistemas.

Una manera de contrarrestar estos ataques es mantener un estricto control de acceso a la red restringiendo el acceso solo a los usuarios en los que se confía. Para obtener el necesario nivel de seguridad y complementar el control de acceso, entonces se debe proteger el tráfico de la red.

Se hace, por lo tanto, necesario trasladar también los sistemas de seguridad a este contexto en el que el principal problema reside en que no existe contacto directo entre las partes implicadas.

¿Cómo se resuelve este problema? Utilizando mecanismos criptográficos. La criptografía proporciona las técnicas básicas que se necesitan para construir soluciones de comunicaciones seguras, siendo como principales propósitos mantener la confidencialidad de los mensajes y garantizar la integridad de los mismos, donde la confidencialidad viene dada por el cifrado, en tanto que la integridad se puede proporcionar mediante códigos de autentificación o firma electrónica, término que se explicará más adelante.

El termino criptografía consta de dos vocablos griegos kriptos: ocultar y graphos: escritura. La criptografía es la rama matemática que transforma mensajes legibles, denominados “texto en claro”**,** en otros que sólo puedan entender las personas autorizadas para ello, conocidos como “criptograma” o “texto cifrado”. El método o sistema empleado para cifrar el texto en claro se denomina algoritmo de cifrado**.** El cifrado de textos es una actividad que ha sido ampliamente usada a lo largo de la historia humana, sobre todo en el campo militar y en aquellos en los que es necesario enviar mensajes con información confidencial y sensible a través de medios no seguros.

La criptografía se remonta al Imperio Romano, en la época del Emperador Julio César, el cual utilizaba un esquema criptográfico simple pero efectivo para comunicarse con sus generales. El esquema consistía en desplazar cada letra del alfabeto un número determinado de posiciones. Por ejemplo, la letra "A" podría ser codificada como "M", la "B" como "N", la "C" como "O”... así sucesivamente. En este caso, el número que se sumaría a cada letra para realizar la codificación sería el 13.

Así pues, el mensaje "ATAQUEN HOY AL ENEMIGO" podría transformarse en "MFMCGQZ TAK MX QZQYUSA", sin poder ser reconocido por el enemigo.

El método de cifrado introducido por Julio César introduce el concepto de "clave criptográfica". El "desplazamiento de 13 letras" es la clave que se utiliza para cifrar el mensaje, necesitándose la misma clave para descifrarlo. El ejemplo de César muestra un esquema criptográfico de clave simétrica en el que se utiliza la misma clave para cifrar y descifrar el mensaje.

La criptografía provee múltiples beneficios que son requeridos para implementar un sistema de firma electrónica:

- **Confidencialidad**: Esto es, asegurar que sólo la persona autorizada tenga acceso a la información cifrada.
- **Integridad**: Asegurar que la información no ha sido alterada en su trayecto o almacenamiento.
- **Autenticación**: Verificar la identidad de uno o ambos comunicantes.

Los esquemas criptográficos usan algoritmos usualmente públicos (aunque algunos son secretos), y el conocer el algoritmo es condición necesaria pero no suficiente para descifrar la información. El valor secreto (clave) para descifrar el mensaje es compartido sólo por los comunicantes, y es condición suficiente para descifrar la información.

CRIPTOGRAFÍA DE CLAVE PRIVADA

La criptografía convencional es también llamada de clave secreta o privada, o sistema de cifrado simétrico. Su característica fundamental es que la misma clave que se utiliza para cifrar se usa también para descifrar. Los algoritmos simétricos presentan la particularidad de presentar una sola clave, que se usa tanto para cifrar como para descifrar.

Figura 2.1 Seguridad con solo una clave

En la figura 2.2, se observa cómo funciona, donde la seguridad del sistema reside en mantener en secreta dicha clave

:

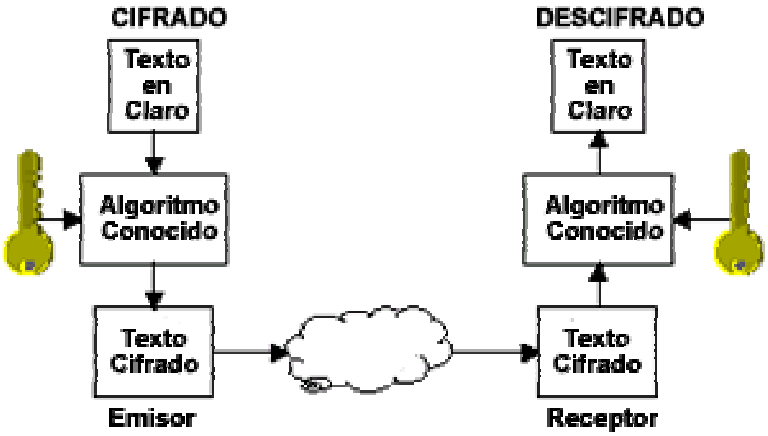


Figura 2.2 Algoritmo simétrico

El emisor utiliza la clave representada por la clave amarilla para cifrar el "texto en claro" y cuando este llega al receptor utiliza la misma clave amarilla para descrifar el texto y así poder entenderlo. Esto se convierte en un inconveniente ya que la clave debe estar tanto en el emisor como en el receptor. Al mismo tiempo tiene como fortaleza la longitud de sus claves, ya que cuanto más larga sea, dura más tiempo para

descifrarla y se hace más segura. Los algoritmos simétricos son muy rápidos para cifrar y descifrar gran cantidad de datos, lo que los hace apropiados para cifrar un archivo completo, un ejecutable de un programa, o una imagen.

ALGORITMOS SIMÉTRICOS DE CIFRADO

Entre los algoritmos más importantes, se tiene:

- RCX (X=2,4,5)
- DES
- 3DES
- AES
- IDEA
- BLOWFISH
- TWOFISH

RCX (X=2, 4, 5): Algoritmo propuesto por Ron Rivest, el método no es público ni está patentado, era un secreto industrial. Cifra bloques de 64 bits con claves de longitud variable. El RC2 se usa en SMIME con longitudes de clave de 40, 64 y 128 bits. El RC4 está incorporado al Nestcape Navigator.

DES (Estándar de Cifrado de Datos): Es un algoritmo de cifrado simétrico DES o Data Encryption Standard es un algoritmo de cifrado por bloques, en donde se manejan bloques de datos de 64 bits y una clave de cifrado/descifrado de 64 bits de

los cuales realmente 56 bits corresponden a la clave como tal y 8 bits se usan para control (cheksum). Puede ser implementado tanto en hardware como en software y en firmware.

Este algoritmo fue desarrollado por IBM en la década de los 70s y hacia finales de misma década fue adoptado como el estándar de cifrado oficial del gobierno americano para información no confidencial.

Por muchos años se consideró inviolable, hasta que en 1998 se realizó un concurso para romperlo y finalmente se logró. Desde ese momento y cada vez más (debido al poder de cómputo de los nuevos computadores y a las capacidades de procesamiento distribuido con que se cuenta) este algoritmo ahora es considerado poco fiable.

3DES: Como ya se mencionó DES ya fue roto y como una alternativa para seguirlo utilizando aparece 3DES. El mayor problema de DES estaba relacionado con el tamaño de clave de 64 bits (56 bits de clave y 8 de paridad). Para responder a esto, 3DES maneja claves de 128 bits (112 bits de clave y 16 de paridad). Consiste en tres aplicaciones del cifrado DES en modo CDC (Cifrado-Descifrado-Cifrado) con claves independientes.

AES (*Estándar de cifrado avanzado*): AES o Advanced Encryption Standard es un nuevo mecanismo de cifrado simétrico de datos que reemplazó a DES. En 1997 el gobierno de Estados Unidos realizó un concurso abierto en la búsqueda de un nuevo mecanismo de cifrado para reemplazar al viejo DES y su sucesor 3DES. Dicho concurso tenía como requisitos los siguientes:

- Ser un algoritmo simétrico por bloques.
- Ser algoritmo público, para que el poder del mecanismo no estuviese en el desconocimiento o secreto del algoritmo sino en el poder de cómputo que implicaría tratar de romperlo sin conocer la clave de cifrado.
- Manejar tamaños de claves de 128, 192 y 256 bits.
- Finalmente, la implementación del algoritmo vía hardware y por software.

IDEA: Es un algoritmo europeo usado en el correo electrónico PGP, aunque ahora ya no es el que PGP usa por defecto, puesto que requiere de licencia para ser usado comercialmente. Opera con 8 rondas con un tamaño de bloque de 64 bits que utiliza claves de 128 bits. IDEA es resistente al criptoanálisis. Actualmente, no se conoce ninguna manera de romper IDEA aparte de la fuerza bruta. Se considera generalmente que IDEA es seguro y tanto el desarrollo del algoritmo como su base teórica han sido abierta y ampliamente discutidos. Los mejores ataques conocidos contra IDEA son:

- Ataque diferencial con clave elegida en una versión muy debilitada del algoritmo con sólo 3 rondas.
- Ataque temporizado sólo con "texto cifrado" y clave elegida sobre el algoritmo completo que requiere 5x217 peticiones de claves relacionadas, cada una de ellas usada para realizar 220 bloques de "texto en claro" sin nombre y aleatorios.
- Una combinación de criptoanálisis diferencial y lineal que requiere 229 pares de texto en claro elegido y una carga de trabajo de 249 sumas módulo 216+1 en una versión muy debilitada del algoritmo con sólo 3 rondas.

BLOWFISH: Es un criptosistema simétrico inventado (y no patentado) por Bruce Schneier, publicado en Abril de 1994 en la edición del Journal del Dr. Dobb's. Cifra bloques de texto de 64 bits, tamaño de clave de 32 hasta 448 bits. También apareció en la segunda edición de "Criptografía Aplicada". Blowfish es bastante compacto, requiere sólo 5K de memoria y es 5 veces mas veloz que el DES, su fortaleza puede variar según la longitud de la clave.

TWOFISH: Es un cifrador simétrico de bloques de 128 bits con claves de 128, 192 o 256 bits, cuyo algoritmo está bajo código abierto o software libre, finalista en el AES (Advanced Encryption Standard) pero que no fue seleccionado para la estandardización, siendo estudiado a fondo por criptólogos que han demostrado su consistencia.

En la mayoría de las plataformas Twofish es ligeramente más lento que Rijndael (el algoritmo elegido AES) para las claves de 128-bits, pero algo más rápido para las claves de 256-bits.

CRIPTOGRAFÍA DE CLAVE PÚBLICA

La característica principal de este algoritmo es que presenta un par de claves complementarias, para el cifrado y descifrado, en lugar de una sola, como los simétricos.

Figura 2.3 Clave pública

Al igual que con los algoritmos simétricos, la longitud de las claves es la que determinará la robustez de la seguridad del algoritmo, mientras más largas sean las claves, más seguras son.

Los algoritmos asimétricos son normalmente más lentos que los simétricos debido a su complejidad matemática. A cambio, presentan la posibilidad de brindar más servicios de los definidos como necesarios ante ataques a la seguridad en Internet.

En la figura 2.4, tanto el emisor como el receptor hacen pública una de sus claves (será su clave pública) y mantienen en secreto la otra (su clave privada). Por ello, el cifrado asimétrico se denomina también cifrado de clave pública. Se observa el esquema de cifrado con una clave de color azul, y descifrado con la otra clave correspondiente de color rojo.

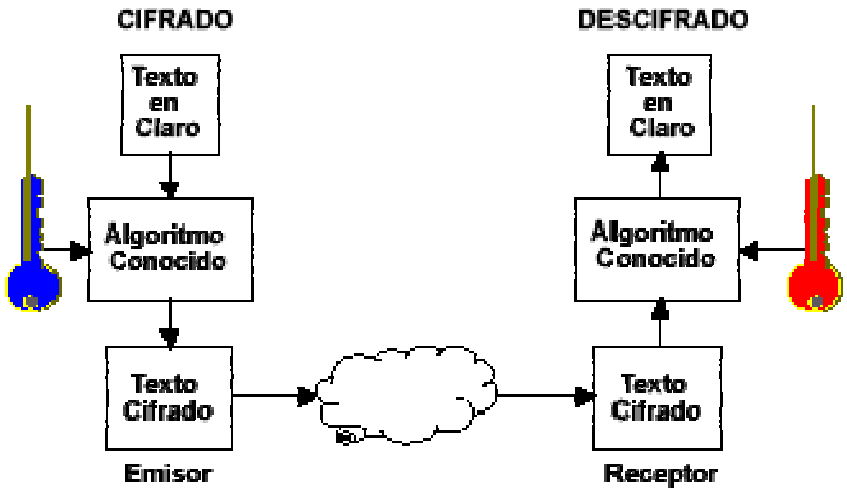


Figura2.4 Algoritmo asimétrico o de clave pública

ALGORITMOS ASIMÉTRICOS DE CIFRADO

Entre los algoritmos más importantes, se tiene:

- RSA
- ELGamal
- Curvas Elípticas

RSA: Un buen método, que satisfacía los requerimientos planteados por Diffie-Hellman[1], fue desarrollado por un grupo en el Massachusett Institute of Technology (M.I.T.) [2] compuesto por Rivest, Shamir y Adleman en 1978, el cual llamaron RSA[RSA78] en honor a sus creadores.

El algoritmo brinda solución a muchos de los problemas de ataques analizados. La mayor fortaleza de este algoritmo reside en la dificultad técnica de factorizar números primos de gran magnitud. Tanembaum (2003) De acuerdo con Rivest y sus colegas, la factorización de un número de 500 dígitos requiere 1025 años de tiempo de cómputo utilizando el mejor algoritmo conocido y una computadora con un tiempo de instrucción de 1 μseg.

El algoritmo para definición de la clave es el siguiente:

1. Se escogen dos primos grandes, p y q, generalmente mayores de **10^100.**
2. Se calcula el valor **n = p * q, y z = (p − 1) * (q − 1).**
3. Se escoge un **d,** menor que **n** y primo relativo con **z**, es decir, **d** y **z** tienen factor común solo a 1**.**
4. Se encuentra un número **e,** de tal forma que **e x d = 1 mod z.**

[1] Whithfield Diffie y Martin Hellman en 1976 crearon un algoritmo para intercambio de claves. Este mecanismo esta especificado en el RFC 2631 y es el primer paso en busca de los algoritmos de cifrado asimétrico.

[2] El Instituto Tecnológico de Massachusetts, conocido habitualmente como MIT (acrónimo de Massachusetts Institute of Technology), es una de las principales instituciones dedicadas a la docencia y a la investigación, especialmente en ciencia, ingeniería y economía.

Para cifrar un mensaje P, se calcula **C = P^e mod n.** Para descifrar **C**, se calcula **P = C^d mod n.** Se puede demostrar, lo cual está fuera de los alcances de este documento, que la función de cifrado y descifrado son inversas para **P** en el rango **0 ≤ P < n.** Para realizar el cifrado se necesita **e y n**, para realizar el descifrado se necesita d y n, por lo que la clave pública está constituida por **(e, n)** y la clave privada por **(d, n).** Al valor **n** se le llama módulo y al valor e exponente público.

Debido a que el largo del mensaje debe estar en el rango **[0, n[**, cuando un mensaje es más largo se puede dividir en bloques de texto de tal forma que cada bloque, **P**, esté en el intervalo **0 ≤ P ≤ n** y a continuación se cifra cada bloque.

ELGAMAL (firma): Es un criptosistema de clave pública basado en la intratabilidad computacional del problema del algoritmo discreto, desarrollado por Taher ElGamal durante 1984 y a985.

Aunque generalmente no se utiliza de forma directa, ya que la velocidad de cifrado y autenticación es inferior a la obtenida con RSA, y las formas producidas son más largas (el doble de largo que el texto original), el algoritmo de ELGamal es de gran importancia en el desarrollo del DSS (*Digital Signatura Standard*), del NIST (*National Institute of Standards and Techonology*) estado unidense.

CURVAS ELÍPTICAS: Los sistemas criptográficos de curvas elípticas (Elliptic Curve Cryptosystems (ECC)) fueron inventados por Neal Koblitz en 1937 y Víctor Miller en 1985 y son el estado del arte de la criptografía moderna.

En forma muy resumida, los criptosistemas basados en curvas elípticas pueden ser vistos en forma análoga y los sistemas criptográficos que basan su seguridad en el problema del logaritmo discreto (por ejemplo DSA o ElGamal) pero el conjunto donde se escogen los primos se reemplaza por los puntos de una curva elíptica sobre un campo finito.

Los sistemas criptográficos de curvas elípticas basan su seguridad entonces en el problema del logaritmo discreto sobre curvas elípticas. Debido a que este problema es significativamente más complejo, la seguridad por cada bit de la clave es sustancialmente mayor en los sistemas de curvas elípticas que en los convencionales, lo que permite obtener niveles equivalentes de seguridad con claves de menor tamaño. Por ejemplo, el nivel de seguridad logrado con una clave de 160 bits en curvas elípticas, equivale a 1024 bits en RSA. La ventaja de utilizar parámetros más pequeños incluye más velocidad (cálculos más rápidos) y menor tamaño de claves y certificados. Lo anterior es especialmente importante en ambientes donde el poder de cálculo, espacio de almacenamiento, ancho de banda y consumo de energía es limitado (teléfonos móviles, agendas electrónicas, dispositivos de hardware, etc.).

El algoritmo “Elliptic Curve Digital Signature Algorithm (ECDSA)” es el análogo a DSA y al igual que éste, está estandarizado como Federal Information Processing Standard (FIPS 186-2).

FUNCIÓN HASH

La criptografía asimétrica permite identificar al emisor y al receptor del mensaje. Para identificar el mensaje propiamente dicho, se utilizan las llamadas funciones resumen (en inglés, *hash*). Una función hash es una operación que se realiza sobre un conjunto

de datos de cualquier tamaño de tal forma que se obtiene como resultado otro conjunto de datos, en ocasiones denominado *resumen* de los datos originales, de tamaño fijo e independiente del tamaño original que, además, tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es prácticamente imposible encontrar dos mensajes distintos que tengan un resumen hash idéntico.

Son tres las aplicaciones principales de las funciones hash:

- Contraseñas: Las funciones hash son ampliamente usadas para almacenar contraseñas. Por su característica de irreversibilidad, almacenar un valor hash de una contraseña es más seguro que almacenarla en forma criptográfica.

- Firmas Digitales: Realizar operaciones de firmas digitales sobre mensajes grandes puede consumir mucho tiempo por los algoritmos de firmas digitales. En su lugar, al mensaje se le aplica la función hash y el algoritmo de firma digital se aplica al valor hash obtenido de menor tamaño.

- Integridad y autentificación de un mensaje: Un mensaje puede ser considerado íntegro si su valor hash ya fue calculado antes de cualquier transmisión. Este valor es comparado con el valor hash del mensaje recibido.

Hay muchos algoritmos de este tipo. Uno de los más conocidos es SHA, que se utiliza habitualmente para firmas electrónicas. Entre las funciones hash más conocidas destacan:

- MD5
- SHA-1

- RIPEM-160

MD5 (*Message Digest Algorithm*): Se trata de uno de los más populares algoritmos de generación hash, siendo el resultado de una serie de mejoras sobre el algoritmo MD4, diseñado en 1991 por Ron Rivest. Procesa los mensajes de entrada en bloques de 512 bits, y produce una cadena de salida de 128 bits de longitud. El mensaje se alarga hasta que su longitud es exactamente 64 bits inferior a un múltiplo de 512 bits.

SHA-1: Es un algoritmo de resumen seguro desarrollado por el NIST[3]. SHA-1 es una versión corregida del algoritmo publicado en 1994. El algoritmo es un estándar ANSI. El algoritmo toma un mensaje de menos de 2^{64} bits y genera un resumen de 160 bits. Es más lento que el MD5, pero la mayor longitud de clave lo hace más resistente a ataques de colisión por fuerza bruta y de inversión, otras nuevas propuestas conocidas son SHA-256 y SHA-512.

RIPEM-160: Desarrollado en el proyecto europeo RIPE de 1996. Produce resumen de 160 bits.

FIRMA ELECTRÓNICA

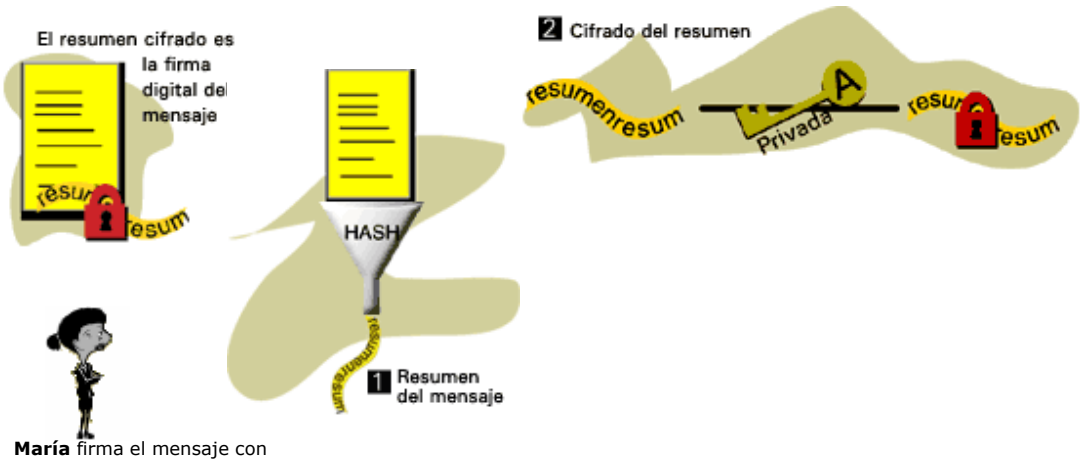
El concepto de firma electrónica y/o digital, fue introducido por Diffie y Hellman en 1.976. Básicamente una firma electrónica es un conjunto de datos asociados a un

[3] Instituto Nacional de Estándares y Tecnología en inglés National Institute of Standards and Technology, http://www.nist.gov

mensaje electrónico, que permite asegurar la identidad del firmante y la integridad del mensaje.

La firma electrónica puede ser definida como una secuencia de datos electrónicos (bits) que se obtienen mediante la aplicación a un mensaje determinado de un algoritmo (fórmula matemática) de cifrado asimétricos o de clave pública, y que equivale funcionalmente a la firma del emisor del mensaje. Desde el punto de vista material, la firma electrónica es una simple cadena o secuencia de caracteres que se adjunta al final del cuerpo del mensaje firmado digitalmente. Esto permite que del lado del receptor, el proceso de verificar la imagen recibida resultado del algoritmo de cifrado con la nueva imagen producida se realiza en una computadora en cuestión de segundos, y el mensaje sólo será aceptado si ambas son idénticas. A continuación un caso practico de firma electrónica:

En la figura 2.5 se muestra como generar una firma electrónica, con dos premisas: **María** y **Pedro** tienen su par de claves (pública y privada). **María** escribe un mensaje firmado a **Pedro.** Como resultado **Pedro** puede verificar realmente que el mensaje es de María, porque ella utilizó su firma electrónica.



María firma el mensaje con su clave privada

1. **Resume el mensaje mediante una función hash.**
2. **Cifra el resultado de la función hash con su clave privada. De esta forma obtiene su firma digital.**
3. **Envía a Pedro el mensaje original junto con la firma.**

Pedro recibe el mensaje junto a la firma electrónica. Entonces Deberá comprobar la validez de ésta para dar por bueno el mensaje y reconocer al autor del mismo (integridad y autenticación).

4. **Descifra el resumen del mensaje mediante la clave pública de María.**
5. **Aplica al mensaje la función hash para obtener el resumen.**
6. **Compara el resumen recibido con el obtenido a partir de la función hash. Si son iguales, Pedro puede estar seguro de que quien ha enviado el mensaje es María y que éste no ha sido modificado.**

Figura 2.5 De la Fábrica Moneda y Timbre de España, disponible en: http://www.cert.fnmt.es/pilotos/soporte.htm

En el ejemplo, María envía un mensaje electrónico a Pedro, dicho mensaje firmado cumple con los siguientes requisitos:

- Autenticidad, que implica poder atribuir de forma indubitada el mensaje electrónico recibido a una determinada persona como autora del mensaje.

- Integridad, que implica la certeza que el mensaje recibido por Pedro es exactamente el mismo mensaje emitido por María que lo envía, sin que haya sufrido alteración alguna durante el proceso de transmisión de María hacia Pedro.

- No repudio o no rechazo en origen, denota que el emisor del mensaje (María) no pueda negar en ningún caso que el mensaje ha sido enviado por ella.

A los tres requisitos anteriores, se une un cuarto elemento, que es la confidencialidad, que no es un requisito esencial de la firma electrónica, sino accesorio de la misma. La confidencialidad implica que el mensaje no haya podido ser leído por terceras personas distintas del emisor y del receptor durante el proceso de transmisión del mismo.

CERTIFICADO ELECTRÓNICO

Un certificado electrónico y/o digital, es un documento que identifica cada clave pública con su propietario correspondiente. Para que un certificado tenga validez, es necesario que vaya firmado por una Autoridad de Certificación en la que confían el emisor y el receptor y que certifica sus identidades. Los certificados, por tanto, son emitidos y firmados por la Autoridad Certificadora y están identificados por un número de serie y un período de validez.

La mayoría de los certificados digitales que se usan hoy día en las transacciones electrónicas seguras son del tipo X.509. Estos certificados son emitidos por Autoridades de Certificación privadas o públicas, tales como VeriSign, Thawte y British Telecom. Hay distintas clases de certificados digitales, de acuerdo al uso que se le vaya a dar y al nivel de confianza. En la figura siguiente se ilustra la estructura

de un certificado X.509 v3, recomendado por la Unión Internacional de Comunicaciones (UIT).

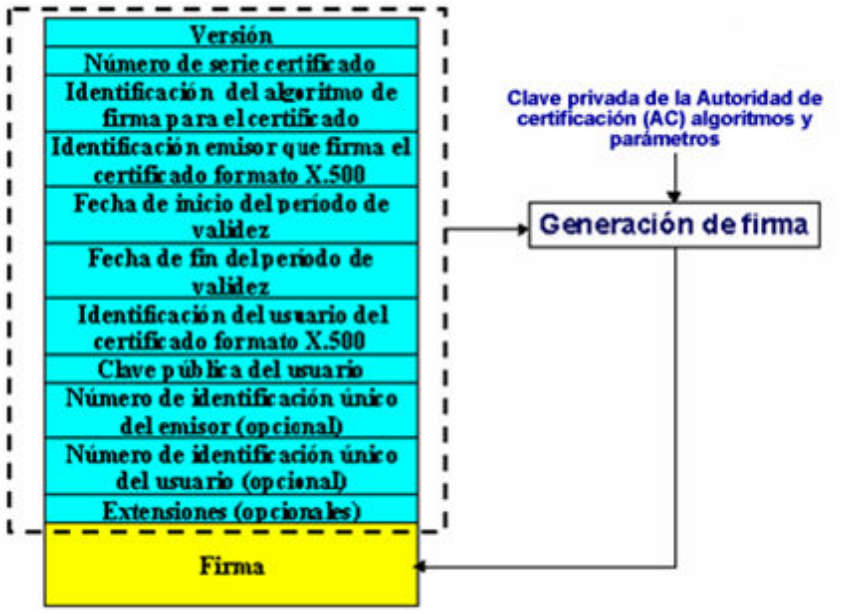


Figura 2.6 Formato de un certificado según norma X.509 v3.

Los datos que figuran generalmente en un certificado típicamente son los siguientes:

- ***Versión*:** Versión del estándar X.509. La versión 3 es la más reciente.
- ***Número de serie certificado*:** Número identificador del certificado, único para cada certificado expedido por una Autoridad Certificadora determinada.

- ***Identificación del algoritmo de firma para el certificado*:** Algoritmo criptográfico usado para la firma digital.
- ***Identificación emisor que firma el certificado formato X.500 (Autoridad de Certificación)*:** Datos sobre la autoridad que expide el certificado.
- ***Fecha de inicio del periodo de validez del certificado*:** Define la fecha de inicio de validez del mismo, que generalmente es de un año.
- ***Fecha de fin del periodo de validez del certificado*:** Define el fin del periodo valido del mismo.
- ***Identificación del usuario formato X.500 (Propietario)*:** Persona o entidad que es titular del certificado.
- ***Clave pública del usuario*:** Representación de la clave pública vinculada a la persona o entidad (en hexadecimal), junto con el algoritmo criptográfico para el que es aplicable.
- ***Algoritmo de identificación:*** Especifica el algoritmo de firma utilizado.
- ***Firma de la Autoridad Certificación*:** Asegura la autenticidad del mismo, porque el certificado fue firmado con la clave privada de la Autoridad de Certificación superior.
- ***Información adicional*:** Como por ejemplo tipo de certificado.

Además, los certificados electrónicos pueden contener *extensiones*. Ellas se utilizan para introducir información sobre, por ejemplo, políticas de certificación e infraestructura de los entornos de seguridad que utilizan los certificados, y dichas extensiones pueden ser marcadas como críticas o indispensables tomado del estándar

X509 y del RFC 3280, lo que significa que las aplicaciones de validación de certificados no las pueden ignorar.

INFRAESTRUCTURA DE CLAVE PÚBLICA

Es el conjunto de componentes y políticas necesarias para crear, gestionar y revocar certificados electrónicos que pueden ser utilizados para autenticar cualquier aplicación, persona, proceso u organización de una red de empresa, Extranet o Internet, además de cumplir con los componentes de seguridad básicos, como los son: confidencialidad, integridad y no-repudio.

El modelo de confianza basado en Tercera Parte Confiable (TPC) es la base de la definición de la Infraestructuras de Clave Pública (ICP o PKI). Este modelo es fundamental en cualquier entorno de clave pública de tamaño considerable debido a que es posible que los usuarios no hayan tenido relaciones previas antes de intercambiar información cifrada, entonces otro agente ajeno asegura que los usuarios son los que dicen ser. Además la mejor forma de permitir la distribución de las claves públicas (o certificados electrónicos) de los distintos usuarios es que algún agente o entidad en quien todos los usuarios confíen se encargue de su publicación en algún repositorio al que todos los usuarios tengan acceso.

Entonces se podrá tener confianza en el certificado electrónico de un usuario al que previamente se conoce si dicho certificado está avalado por una tercera parte en la

que sí se confía. La forma en que esa tercera parte avala que el certificado es de fiar es mediante su firma electrónica sobre el certificado. Por tanto, se podrá confiar en cualquier certificado electrónico firmado por una tercera parte en la que se confía. La TPC que se encarga de la firma electrónica de los certificados de los usuarios de un entorno de clave pública se conoce con el nombre de Autoridad de Certificación (AC).

COMPONENTES DE LA INFRAESTRUCTURA DE CLAVE PÚBLICA

A continuación en la siguiente figura, se indican los componentes de la ICP.

Figura 2.7 Componentes de la Infraestructura de Claves Públicas (ICP)

- ***Autoridad de Certificación (AC)***: Es la entidad encargada de firmar y revocar todos los certificados digitales. La Autoridad de Certificación es quien da validez a los certificados mediante la firma digital de estos con su clave privada. La confianza de los usuarios en ella es fundamental para el buen funcionamiento del servicio.

- ***Autoridad de Registro (AR)***: Establece las relaciones entre los usuarios y las AC. Es la que se encarga del registro de los usuarios, de la confirmación y validación de la identidad de los usuarios.

- ***Políticas de Seguridad***: Establecen y definen los niveles de seguridad de la información para una organización, así como los procedimientos a utilizar. Por lo general, incluye:

    - Una clasificación de los usuarios que solicitan el certificado.
    - Los procedimientos: método de registro, renovación de certificados, revocación de certificados.
    - Los controles técnicos de seguridad: controles de ciclo de vida, seguridad física, compatibilidad con estándares.
    - Cuestiones de responsabilidad, obligaciones y leyes.
    - Limitaciones referentes al uso de certificados y claves asociadas.

- ***Sistema de Distribución de Certificados***: Los certificados se pueden distribuir de varias formas, dependiendo de la estructura del entorno ICP. Se pueden distribuir, por ejemplo, manualmente (usuario-usuario), a través de un servicio de directorio o por vía e-mail.

- ***Aplicaciones de ICP***: Son aquéllas que están habilitadas para el uso de ICP. Algunos ejemplos de éstas aplicaciones pueden ser:
    - Comunicaciones entre servidores y navegadores de Internet.
    - Correo electrónico.
    - Intercambio Electrónico de Datos (IED).
    - Transacciones con tarjeta de crédito en Internet.
    - Factura Electrónica.
    - Redes Privadas Virtuales (VPN).

En otras palabras, la infraestructura de certificación para la criptografía con clave pública o ICP se define como el conjunto de elementos de hardware/software necesarios para su operación, los usuarios con sus claves públicas/privadas y las políticas y procedimientos necesarios para crear, gestionar, almacenar, distribuir y revocar certificados basados en criptografía de clave pública**.**

TOPOLOGÍA PARA LA AUTORIDAD DE CERTIFICACIÓN RAÍZ

Según Segovia (2004) el modelo para la AC Raíz es el jerárquico subordinado. Este permite establecer relaciones de confianza basadas en el modelo de árbol en el cual desde una raíz específica, surge toda la estructura de confianza del sistema. Este modelo de certificación además de ser simple en su diseño, es fácil de comprender para el usuario común. Por la simplicidad, este modelo es el de mayor acogida a nivel mundial y en particular es el modelo que han implantado los grandes proveedores

comerciales de servicios de certificación como Verisign, y además de Venezuela han sido adoptado en naciones como Brasil, India, Arabia Saudita.

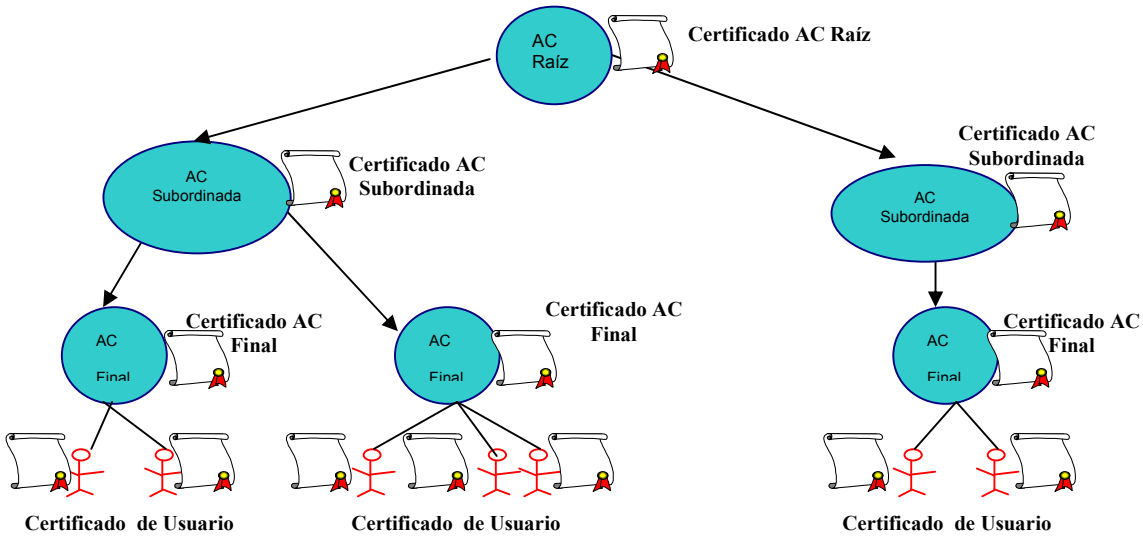


Figura 2.8 Estructura jerárquica subordinada

En la figura 2.8, la Autoridad de Certificación (AC) Raíz es el ancla de confianza común para todas las entidades destino. Por definición, es la Autoridad de Certificación con más confianza y todas las demás relaciones de confianza salen a partir de ella. Certifica el siguiente conjunto más bajo de AC Subordinadas con un conjunto de relaciones de confianza unidireccionales. En este modelo, solamente la AC superior expide certificados a sus subordinados, destacando que las AC Subordinadas no certifican a sus superiores.

Como las relaciones de confianza se construyen desde la AC de más confianza, no existe otra Autoridad de Certificación que pueda firmar el certificado de la AC Raíz. Como resultado, la AC crea un certificado autofirmado o autoexpedido por si misma, ver figura 2.9.

El certificado autofirmado es un caso específico donde el titular y el emisor del certificado electrónico serán el mismo. La AC usa su clave privada para firmar su clave pública que esta contenida en su certificado electrónico, entonces la clave pública en el certificado autofirmado se usa para verificar la firma electrónica en el certificado cuanto éste se vaya a validar.

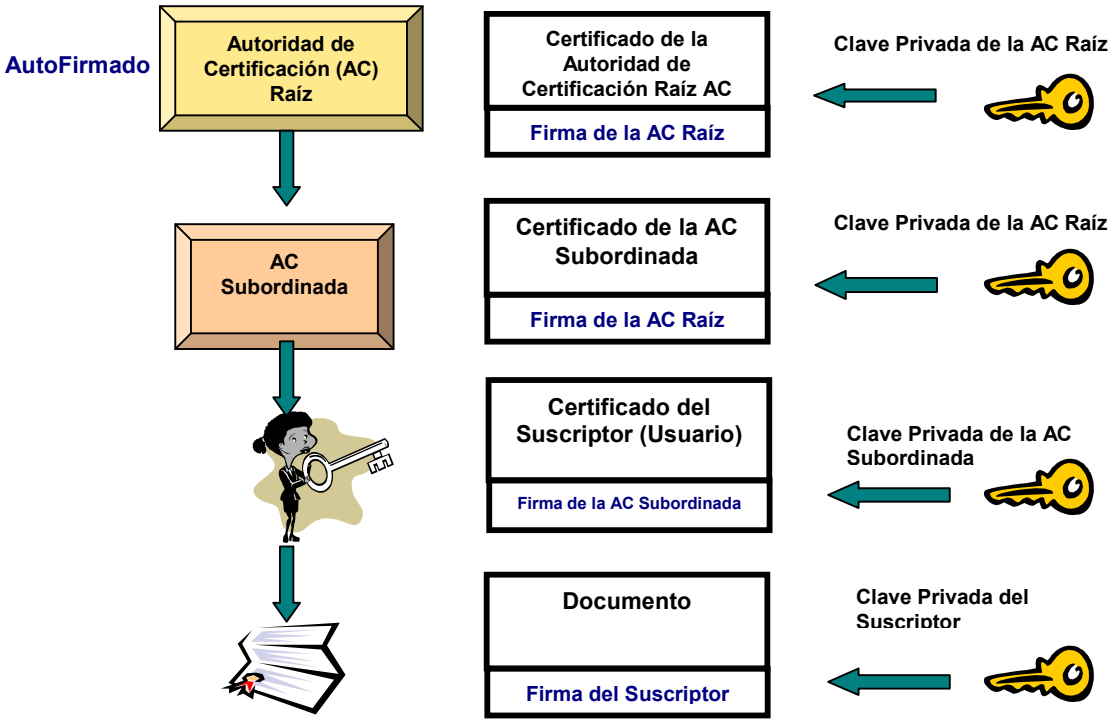


Figura 2.9 Certificado autofirmado por la AC Raíz

certificado electrónico autofirmado de la AC Raíz, luego utilizando su clave privada firma el certificado electrónico de la AC Subordinada, para luego la AC Subordinada firmar con su clave privada los certificados de los subscriptores o usuarios finales. Una vez que el subscriptor tiene su certificado electrónico y el par de claves (pública y privada) puede utilizar la firma electrónica y su certificado electrónico.

El certificado de la AC Raíz se debe distribuir a todos los usuarios de certificados, en el modelo de jerarquía subordinada, todas las rutas incluirán el certificado de la AC Raíz y cualquier compromiso o pérdida de confianza de la clave privada de la AC Raíz ocasionará desconfianza para el modelo de infraestructura de clave pública. La pérdida de confianza en la operación del modelo de confianza afectará a todos los usuarios de certificados. De hecho, las claves de la AC Raíz tendrán que ser revocadas y se deberán expedir y distribuir un nuevo certificado raíz a todos los usuarios de certificados. Además, es necesario reemplazar cualquier certificado subordinado y las claves que fueran sospechosas.

Las AC Raíz además pueden proporcionar copias de su clave pública en sitios Web públicos. Confiar en una AC Raíz, supone confiar en todas las ACs subordinadas a la AC Raíz.

HARDWARE CRIPTOGRAFICO

A medida que la criptografía de clave pública ha ido consolidándose como base de la seguridad informática, el punto débil de la seguridad ha ido desplazándose desde los datos en sí hacia las claves que los protegen. Los datos sólo son seguros en la medida en que lo sean dichas claves. Para solucionar el problema, es posible utilizar productos que almacenan las claves con la debida seguridad, en el interior de módulos hardware (en ingles Hardware Security Module, HSM), protegidos y fiables.

Adicionalmente, es necesario un proceso de control del ciclo de vida de las claves protegidas por el HSM para lo que se requiere un software que actúe como interfaz entre el HSM y el mundo externo.

El HSM se utiliza para la protección de la clave privada asociada a la clave pública utilizada por una Autoridad de Certificación para firmar los certificados electrónicos y las listas de certificados revocados, así como para la aceleración de los algoritmos criptográficos.

El dispositivo criptográfico HSM posee un conjunto de tarjetas inteligentes criptográficas, en las cuales se almacenan las claves de los administradores y operadores de dicho dispositivo. Para activar el HSM es necesario tener el conjunto de tarjetas inteligentes configuradas en el dispositivo para iniciar el proceso de firma de certificados electrónicos y esto lo hace mucho más seguro.

TARJETAS INTELIGENTES

Las tarjetas inteligentes hace décadas que se encuentran cumpliendo un rol en la sociedad moderna. Ya sea que almacenen datos de identidad, monetarios, de pasajes en medios de transporte, entre otras. Básicamente, las tarjetas inteligentes son un pequeño microprocesador con memoria incorporada dentro de un trozo de plástico del tamaño de una tarjeta de crédito. Sus niveles de uso van desde el tipo de las tarjetas para llamadas telefónicas sencillas hasta complejos dispositivos ICP que soportan la aceleración criptográfica.

Las tarjetas inteligentes se construyen de acuerdo con un conjunto de estándares, de los cuales el ISO7816 es uno de los más importantes. Este estándar define la forma, el grosor, las posiciones de contacto, las señales eléctricas, los protocolos y algunas funciones de sistema operativo con que deben contar algunas tarjetas inteligentes. Estos dispositivos se reconocen por el hecho de que habitualmente tienen lo que parece un pequeño sello dorado en una de sus caras. Como se muestra en la siguiente figura.

Figura 2.10 De la tarjeta inteligente ceres de la Fábrica Nacional de Moneda y Timbre de España

Las tarjetas inteligentes se encuentran disponibles en varios modelos con características y usos diferentes. Entre los modelos existentes se encuentran:

- **Las tarjetas de memoria** para almacenar información no sensible, por ejemplo almacén de datos no confidenciales.
- **Las tarjetas con microprocesador** con chip que incluye capacidades de seguridad para datos sensibles como datos confidenciales.
- **Las tarjetas criptográficas** con chip que incluye un sistema operativo y algoritmos criptográficos especialmente diseñados para ICP.

En la ICP se utilizan las tarjetas criptográficas para generar el par de claves (pública y privada) de los operadores del software ICP o los usuarios finales subscriptos a una

AC subordinada a la AC Raíz. La clave pública se mantiene publicada mientras que la clave privada nunca deja la tarjeta, ni siquiera en el momento de generación. Sólo la clave pública puede ser leída por el computador, cuando comienza el proceso de solicitud del certificado electrónico.

Una vez obtenido, el certificado electrónico puede también almacenarse en la tarjeta inteligente criptográfica, que posee una estructura de datos similar a los directorios de los computadores. Esta separación de datos permite que se almacene más de un certificado, y más de un juego de claves pública y privada. La movilidad propia de su formato físico la hace apta para que el usuario pueda operar con su certificado electrónico y su clave privada en más de una computadora, en el trabajo, el hogar, etc.

Las tarjetas inteligentes poseen funciones de control de acceso a datos e instrucciones, que sólo son activadas si se coloca un número de identificación personal (PIN). Esto es opcional, pero de activarse, resuelve el problema de robo o extravío de la tarjeta inteligente (y el certificado y la clave privada que contienen).

Otra característica interesante es que posee capacidad multifunción. Esto significa que la misma tarjeta puede servir para varias funciones. Por ejemplo, podría utilizarse como medio de identificación en Internet (con su juego de claves, certificado electrónico, proceso RSA, hash y DES). Podría utilizarse como monedero electrónico, para hacer micropagos en el mundo real o el virtual, mediante el almacenaje y proceso seguro de un saldo, off-line del banco. Podría utilizarse para el pago de transporte, como control de acceso al sitio de trabajo, etc.

ESTÁNDARES APLICABLES A LA FIRMA ELECTRÓNICA

Las prácticas y políticas de certificación establecen un marco de estandarización de las actividades que permite la operación efectiva de la firma electrónica desde el punto de vista técnico.

A continuación se describen los estándares de certificación electrónica, agrupados según su nivel de operación:

DECLARACIÓN DE PRÁCTICAS Y POLÍTICA DE CERTIFICACIÓN

Dos de las normas importantes sobre declaración de políticas y prácticas de certificación son:

- ANSI X9.79: Public Key Infrastructure (PKI) – Practices and Policy Framework.
- RFC 2527: Internet X.509, Public Key Infrastructure, Certificate Policy and Certification Practices Framework.
- RFC 3647: Internet X.509, Public Key Infrastructure, Certificate Policy and Certification Practices Framework.

SEGURIDAD

Algunas de las normas que se aplican a la seguridad en este ámbito son:

- ISO/IEC 17799:2000 Information Technology - Code for information security management.

- ISO-27001 Sistemas de Gestión Seguridad de la Información.

- BS 7799 Part 2 The specification for information security management systems, 1998, en la cual se basó la norma ISO/IEC 17799 parte 1.

- ISO IS 15408 Common criteria version 2.1 (2000).

- FIPS PUB 140-2. Security requirements for cryptography modules.

ESTRUCTURA DE CERTIFICADOS

La definición de la estructura de los certificados de firma electrónica más utilizada en la infraestructura de clave pública se define en los siguientes documentos:

- ITU-T X.509 Information technology-Open systems interconnection-The Directory: Public-key and attribute certificate frameworks.

- ISO/IEC 9594

REPOSITORIO DE INFORMACIÓN

A continuación se mencionan algunos documentos de referencia sobre los repositorios de información utilizados para implementar ICP:

- RFC 1777 Yeong, W. Et al., Lightweight Directory Access Protocol, Marzo 1995.

- RFC 2251 Wahl, M. Et al. Lightweight Directory Access Protocol v3, Diciembre 1997.

- RFC 2559 Boeyen, S. Et al. Internet X.509 Public Key Infrastructure. Operational Protocols – LDAPv2, Abril 1999.

- RFC 2585 Housley, R., Hoffman, P., X.509 Internet Public Key Infrastructure. Operational Protocols: FTP and HTTP, Mayo 1999.

- RFC 2587 Boeyen, S. Et al., Internet X.509 Public Key Infrastructure. LDAPv2 Schema, Junio 1999.

- X.500 ITU-T Recommendation X.500, Information technology – Open Interconnection – The Directory: Overview of concepts, models and services, 1997.

SUSCERTE Y SU ORGANIZACIÓN

ANTECEDENTES

La Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), fue creada a través del Decreto con fuerza de Ley Nº 1.204 de fecha 10 de Febrero de 2001, de Mensaje de datos y Firmas Electrónicas (LSMDFE), publicado en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 37.148 del 28 de Febrero de 2001, cuyo desarrollo de sus normas se encuentra a partir del Capítulo V, artículo 20, donde expresamente se indica la creación de la Superintendencia de Servicios de Certificación Electrónica, como un servicio autónomo con autonomía presupuestaria,

administrativa, financiera y de gestión, en las materias de su competencia, dependiente del Ministerio de Ciencia y Tecnología.

Con la institucionalización de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), se da apertura a una nueva etapa en el sector de la ciencia y la tecnología, con un marco legal acorde con la realidad del país, que asegura otorgar y reconocer eficiencia y valor jurídico a la firma electrónica, al mensaje de datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como la regulación en cuanto a la acreditación, supervisión y control, en los términos previstos en el referido Decreto - Ley y sus reglamentos, a los Proveedores de Servicios de Certificación públicos o privados.

MISIÓN

Acreditar, supervisar y controlar, en los términos previstos en el Decreto con Fuerza de Ley Nº 1.204 de Mensaje de Datos y Firmas Electrónicas y sus reglamentos, a los Proveedores de Servicios de Certificación públicos o privadas del país.

VISIÓN

Ser un organismo impulsor por excelencia en el uso de los medios electrónicos, con una estructura organizativa flexible y un personal altamente capacitado, quien a través de la promoción y difusión efectiva de los mismos en el ámbito nacional, fomente la participación de todos los sectores en los intercambios de información.

OBJETIVOS DE LA ORGANIZACIÓN

En relación a las competencias de SUSCERTE de acuerdo a lo contemplado en el Decreto con Fuerza de Ley Nº 1.204 en el artículo 22 de Mensajes de Datos y Firmas Electrónicas se pueden mencionar:

- Acreditar y renovar la acreditación a los Proveedores de Servicios de Certificación Electrónica.
- Mantener, procesar, clasificar, resguardar, y custodiar el registro de los Proveedores de Servicios de Certificación públicos o privados.

- Verificar el cumplimiento de los requisitos establecidos en el Decreto con Fuerza de Ley Nº 1.204 de Mensaje de Datos y Firmas Electrónicas.

- Supervisar las actividades de los Proveedores de Servicios de Certificación.

- Imponer las sanciones establecidas en le Decreto con Fuerza de Ley Nº 1.204 de Mensaje de Datos y Firmas Electrónicas.

- Liquidar, recaudar y administrar las tasas y multas establecidas en el Decreto con Fuerza de Ley Nº 1.204 de Mensaje de Datos y Firmas Electrónicas.

- Coordinar con organismos nacionales e internacionales aspectos relacionados con el cumplimiento de su gestión.

- Inspeccionar y fiscalizar la instalación, operación y prestación de servicios de los Proveedores de Servicios de Certificación.

- Actuar como mediador en conflictos entre los Proveedores de Servicios de Certificación y sus usuarios a petición de las partes.

- Las demás que establezca la ley y los reglamentos.

ESTRUCTURA ORGANIZATIVA

La Estructura Organizativa de SUSCERTE se encuentra conformada por las siguientes unidades, Ver figura 2.1:

- **Despacho del Superintendente:** Tiene como finalidad definir las políticas para la promoción y desarrollo de los mensajes de datos y las firmas electrónicas. De igual forma, se encarga de promover el desarrollo de un marco jurídico que permita el uso de firmas electrónicas para el gobierno electrónico y los negocios del sector privado. Su principal propósito es contribuir a la construcción del Gobierno Electrónico a través del desarrollo de los lineamientos y políticas para la implantación de la Infraestructura Nacional de Certificación Electrónica.

- **Oficina de Gestión Administrativa:** Tiene como objeto prestar apoyo técnico y logístico en materia de administración del capital humano, físico y financiero para la formulación, ejecución y control del gasto de los servicios de SUSCERTE con la finalidad de garantizar la operatividad y funcionamiento eficiente de SUSCERTE.

- **Dirección de Registro y Acreditación:** Se encarga de implantar las políticas de promoción y divulgación para el otorgamiento de las acreditaciones a los proveedores. Administra y gestiona el proceso de acreditación en los términos de Decreto con Fuerza de ley Nº 1.204 de Mensaje de Datos y Firmas Electrónicas y de mantener y resguardar el Registro de Proveedores de Servicios de Certificación. Define los estándares tecnológicos y mejores prácticas de seguridad para la operación de los Proveedores de Servicios de Certificación.

- **Dirección de Investigación y Desarrollo Tecnológico:** Está encargada del diseño, implantación y mantenimiento para la plataforma tecnológica requerida para la gestión de procesos de SUSCERTE. Además de su promoción y divulgación, en lo referente al objeto del organismo y el apoyo a la creación de líneas de investigación en las tecnologías relacionadas con la Firma Electrónica y los mecanismos de certificación de la misma.

- **Dirección de Inspección y Fiscalización:** Su finalidad es realizar el control, inspección y auditoria de los Proveedores de Servicios de Certificación, vigilando que se cumplan las normativas de SUSCERTE, de conformidad con lo establecido en el Decreto con Fuerza de Ley Nº 1.204 de Mensaje de Datos y Firmas

Electrónicas (LSMDFE), así como el desarrollo de lineamientos y políticas para el desarrollo de metodologías propias de auditoría.

Otro aspecto importante de destacar está contemplado en el artículo 27, Capitulo IV, del Decreto con Fuerza de ley Nº 1.204 de Mensaje de Datos y Firmas Electrónicas, donde se establece que SUSCERTE podrá adoptar las medidas preventivas o correctivas necesarias para garantizar la confiabilidad de los servicios prestados por los Proveedores de Servicios de Certificación. A tal efecto, podrá ordenar, entre otras medidas, el uso de estándares o prácticas internacionalmente aceptadas para la prestación de los servicios de certificación electrónica, o que el Proveedor se abstenga de realizar cualquier actividad que ponga en peligro la integridad o el buen uso del servicio.

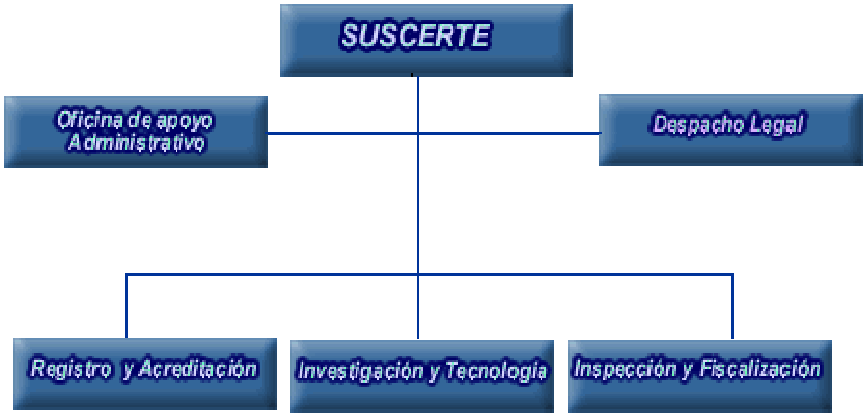


Figura 2.11 Estructura organizativa de SUSCERTE

MARCO METODOLÓGICO

El presente capítulo expone el modelo, nivel y diseño de investigación e instrumento de recolección de las muestras y análisis de los datos para lograr los objetivos del trabajo de grado.

MODELO DE LA INVESTIGACIÓN

De acuerdo al problema planteado y en función de sus objetivos, el estudio se emprende siguiendo el modelo de investigación denominada Proyecto Especial. En el Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales. Normas UPEL (2003), "la modalidad proyecto especial permite la presentación de trabajos que llevan a creaciones tangibles, susceptibles de ser utilizadas como soluciones a problemas demostrados o que responden a necesidades e intereses de tipo cultural. Se incluye en esta categoría los trabajos de elaboración de libros de texto, de materiales de apoyo educativo, el desarrollo de software, prototipos y de productos tecnológicos en general, así como también los de creaciones literarias y artísticas" (p.91).

El proyecto especial se refiere a la propuesta de la Infraestructura de Clave Pública (ICP) para la Administración Pública Nacional (APN) y la Declaración de Prácticas de Certificación (DPC) para la Autoridad de Certificación raíz de Venezuela, en función de los objetivos que se plantearon en el capítulo anterior, se tiene una modalidad de proyecto especial apoyado en un diseño no experimental con un nivel descriptivo y una investigación de tipo de campo.

NIVEL DE LA INVESTIGACIÒN

El nivel de investigación para este trabajo es de tipo descriptivo según Arias (2003), "el nivel de investigación descriptiva consiste en la caracterización de un hecho, fenómeno o grupo con el fin de establecer su estructura o comportamiento (…) mide de forma independiente las variables". (p.48). Al respecto Méndez (2001)

expresa que “los estudios descriptivos acuden a técnicas especificas en la recolección de información, como la observación, las entrevistas, los cuestionarios. También pueden utilizarse informes y documentos elaborados por otros investigadores”, (p. 137).

De acuerdo a estas definiciones mencionadas, el nivel de la investigación es descriptivo porque son interpretadas las realidades de hechos, incluyendo la descripción, el registro, el análisis e interpretación de la naturaleza actual, basados en documentos elaborados en materia de certificación electrónica con la finalidad de satisfacer necesidades para la creación y funcionamiento del Sistema Nacional de Certificación Electrónico impulsado por SUSCERTE.

Con respecto a la utilidad de este trabajo de investigación es de tipo aplicada, debido a que permite resolver un problema determinado en la institución, cabe destacar citar a Sabino (2000): “ La investigación aplicada persigue, en cambio, fines más directos e inmediatos”. (p.60).

DISEÑO DE LA INVESTIGACIÓN

El diseño de la investigación se refiere a la manera de dar respuesta a las interrogantes formuladas en la investigación, relacionadas con las estrategias a seguir en búsqueda de soluciones al problema planteado. La estrategia asumida en este proyecto especial es el diseño de campo. La definición dada por la Universidad Pedagógica Experimental Libertador (2001) de investigación de campo, es: “El

análisis sistemático de problemas en la realidad, con el propósito bien sea de describirlos, interpretarlos, entender su naturaleza y factores constituyentes, explicar sus causas y efectos, o predecir su ocurrencia, haciendo uso de métodos característicos de cualquiera de la realidad; en ese sentido se trata de investigaciones a partir de datos originales o primarios". (p.5).

De acuerdo a esta definición, vale la pena resaltar que el presente proyecto especial parte del estudio hecho por la Superintendencia en materia legal a través del marco jurídico vigente para los mensajes de datos y firmas electrónicas y en el área técnica con el modelo de Infraestructura de Clave Pública (ICP) para la nación venezolana.

POBLACIÓN Y MUESTRA

Según Selltiz; (cit. Hernández, Fernández y Baptista, 2001) la población es el conjunto de todas las cosas que concuerdan con una serie de especificaciones. (p. 204).

Para Arias (2003) “La población de una investigación es el conjunto de unidades de las que se desea obtener información y sobre las que se van a generar conclusiones. La población puede ser definida como el conjunto finito o infinito de elementos, personas o cosas pertinentes a una investigación y que generalmente suele ser inaccesible”. (p.93).

De acuerdo a estas definiciones, de la población se obtendrán los datos de la investigación. En el presente trabajo la población corresponde a la Administración Pública Nacional (APN) porque la Raíz de la ICP nacional está bajo la custodia de SUSCERTE ente autónomo adscrito al Ministerio de Ciencia y Tecnología (MCT) de la República Bolivariana de Venezuela y el control del Proveedor de Servicios de Certificación (PSC) para la APN será de la Fundación del Instituto de Ingeniería (FII) organismo adscrito al MCT.

La muestra es definida por Sudman; (cit. Hernández Fernández y Baptista, 2001) como un subgrupo de la población. (p. 204). Entonces se considera como muestra en este trabajo, SUSCERTE y la FII, por ser parte representativa del universo de la población seleccionada para la investigación. Por ser SUSCERTE el ente rector en la materia de certificación electrónica y responsable de iniciar y mantener en el tiempo el uso de la firma electrónica y los certificados electrónicos en el país y la FII será el primer Proveedor de Servicios de Certificación (PSC) de carácter público acreditado ante SUCERTE que prestará los servicios de certificación electrónica para la APN.

INSTRUMENTO A UTILIZAR

La técnica a utilizar en este trabajo de investigación para recopilar los datos se compone básicamente de dos procedimientos: investigación documental y encuesta. La investigación documental se emplea con el fin de obtener una visión generalizada de los datos y establecer la relación, estudio de diversos documentos, manuales y en

general obras que contienen o tratan el tema que se desarrolla en la situación objeto de estudio, la encuesta se realiza para formular preguntas al personal de SUSCERTE y del FII con la finalidad de recolectar los datos de la investigación.

VALIDEZ Y CONFIABILIDAD DEL INSTRUMENTO

Validez del Instrumento

Para establecer la validez del instrumento de recolección de los datos, son consultados por SUSCERTE tres expertos en el área de ingeniería los cuales son: un ingeniero en electrónica, y dos ingenieros en sistemas, y dos expertos en el área de ingeniería pertenecientes a la FII los cuales son ingenieros en sistemas. La validación del instrumento permite asegurar que las respuestas llevarán a los resultados esperados de acuerdo con los objetivos de la investigación.

Confiabilidad del Instrumento

La confiabilidad de este instrumento es certificada a través de que los ítems descritos en ese documento cumplieron con los objetivos de la investigación.

PROCEDIMIENTO DE LA INVESTIGACIÓN

Según Márquez (2003) en el trabajo se desarrollan tres fases (p.81):

Fase 1: Planeación

En esta fase se realiza el levantamiento de la información para realizar el planteamiento del problema, los objetivos trazados, la justificación e importancia de la investigación, la investigación de las definiciones utilizadas en el trabajo formando el marco teórico y finalmente la elaboración del anteproyecto.

Fase 2: Ejecución

Una vez aprobado el anteproyecto, se procede al diseño de los instrumentos de recolección de datos.

Fase 3: Divulgación

Posteriormente se redacta el borrador del informe del trabajo de grado para el tutor a fin de su revisión y corrección, para finalizar la redacción del trabajo definitivo y luego ser sometido a su evaluación.

ANÁLISIS DE LA INFORMACIÓN RECOLECTADA

A través de la técnica de recolección de datos antes mencionada y el uso del instrumento elegido para la obtención de la información se obtuvieron los siguientes resultados:

Pregunta N° 1:

¿Existen antecedentes de documentación de Declaración de Prácticas de Certificación (DPC) y Políticas de Certificados (PC) que deben consignar los Proveedores de Servicios de Certificación ante SUSCERTE?

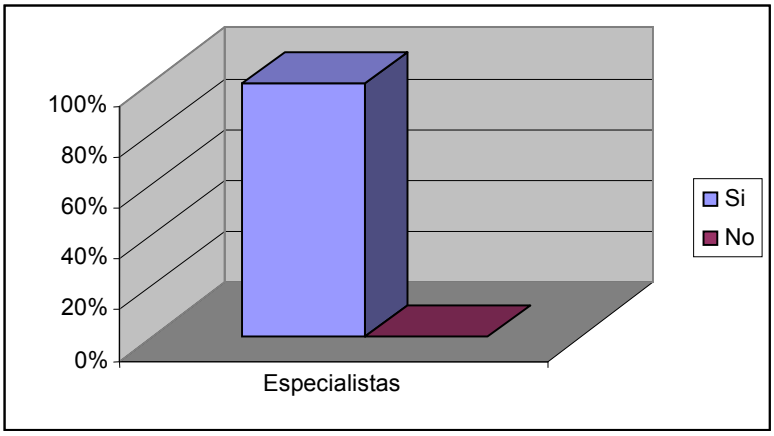


Figura 3.1 Gráfica de los documentos existentes de la DPC y PC de los PSC acreditados ante SUSCERTE

Resultado:

De una población de cinco especialistas en el área que conforman el 100% entre SUSCERTE y la FII se obtuvo que todos los especialistas tienen conocimiento de la existencia de un documento modelo de estructura de DPC realizado por SUSCERTE, es decir el 100%. Entonces se recopiló la información referente a la existencia de la estructura modelo para la DPC vigente realizado por una investigación anterior en SUSCERTE, documento que debe ser consignado ante la Superintendencia por los entes interesados a optar por la acreditación.

Pregunta N° 2:

¿Existe el documento de Declaración de Prácticas de Certificación y Políticas de Certificados para la Autoridad de Certificación Raíz en SUSCERTE?

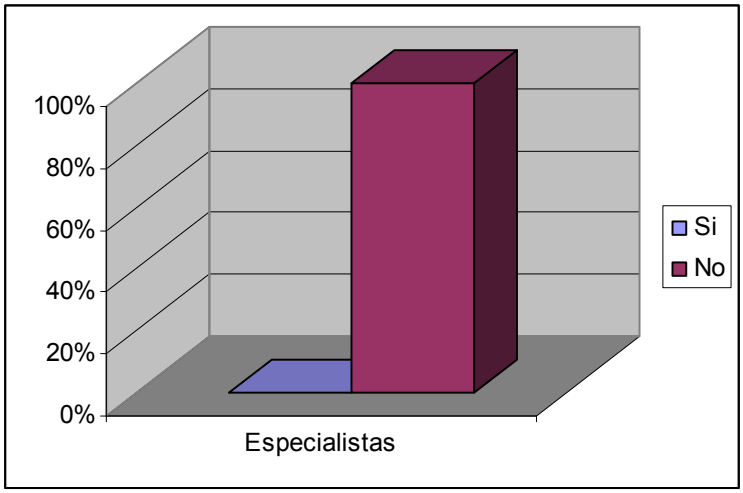


Figura 3.2 Gráfica del documento existente de la DPC de la AC Raíz

Resultado:

De una población de tres especialistas en el área que conforman el 100% de SUSCERTE se obtuvo que todos los especialistas no tienen conocimiento de la existencia de un documento de DPC para la AC Raíz en SUSCERTE.

Una vez recopilada la información, se concluyó que no existe dicho documento para la administración de los certificados electrónicos generados por la AC Raíz.

Pregunta N° 3:

¿Es entonces necesario que la Autoridad de Certificación Raíz de la Infraestructura de Clave Pública de Venezuela tenga su propia Declaración de Prácticas de Certificación?

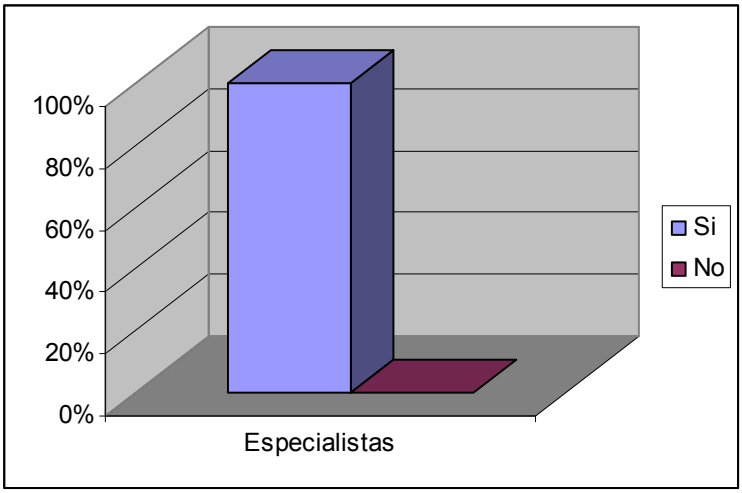


Figura 3.3 Gráfica de la importancia de la propia DPC de la AC Raíz

Resultado:

De una población de tres especialistas en el área que conforman el 100% de SUSCERTE se obtuvo que todos los especialistas estuvieran de acuerdo con la elaboración del documento de la Declaración de Prácticas de Certificación para la AC Raíz, del cual parte toda la cadena de confianza generada en el Sistema Nacional de Certificación Electrónica.

Pregunta N° 4:

¿Podría ser adecuado el modelo existente de Declaración de Prácticas de Certificación (DPC) y Política de Certificados de los Proveedores de Servicios de Certificación para la DPC de la Autoridad de Certificación (AC) Raíz de Venezuela?

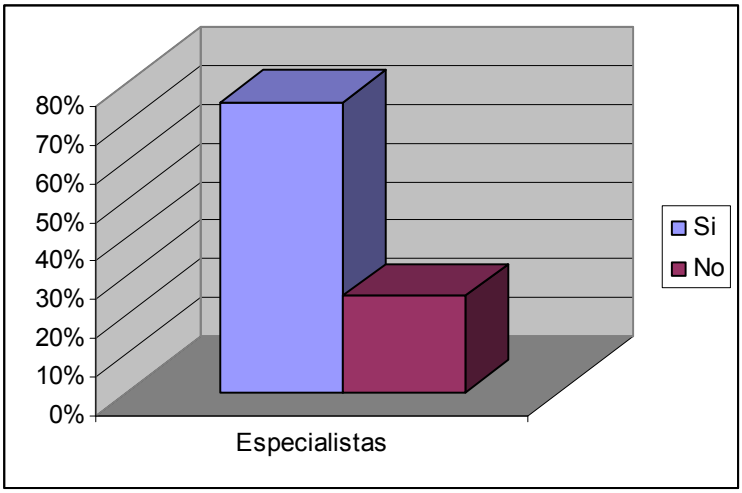


Figura 3.4 Gráfica de seguir la estructura del documento de la DPC existente en SUSCERTE

Resultado:

De una población de tres especialistas en el área que conforman el 100% de SUSCERTE se obtuvo que dos especialistas de los encuestados estaban de acuerdo, es decir un 66.6% considera seguir la estructura del modelo de DPC existente en SUSCERTE para la AC Raíz porque es necesario que la Raíz o ancla de confianza cumpla al igual que los PSC con los requisitos para mantener conocimiento de los tipos de certificados emitidos, frecuencia de publicación de los revocados, suspensión, controles de seguridad, auditaría, resguardo seguro de sus claves y plan de contingencia en caso que se vea comprometida la clave privada de la AC Raíz. Por otro lado un 33.3% equivalente a un especialista de los encuestados no estuvo de acuerdo porque consideraba que por ser un caso particular la Raíz existirán apartados de la DPC que no se aplican a la Raíz o apartados que se deban incorporar.

Se concluye que a pesar de emitir la diferencia en un 33.3% de no seguir con la DPC existente, la DPC para la AC Raíz se elaborará siguiendo la estructura presente.

Pregunta N° 5:

¿Existe un diseño de Infraestructura de Clave Pública (ICP) del Proveedor de Servicios de Certificación (PSC) de carácter público, para cumplir con lo especificado en la disposición final tercera de la Ley sobre Mensajes de Datos y Firma Electrónica (LSMDFE) de Venezuela?

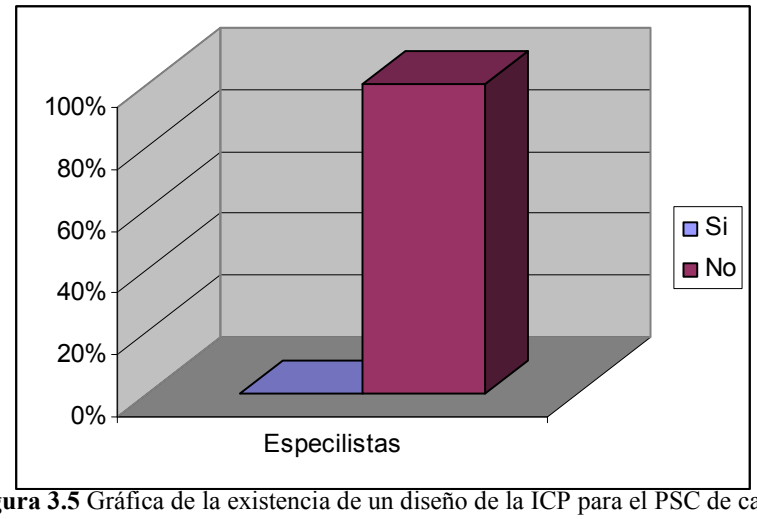


Figura 3.5 Gráfica de la existencia de un diseño de la ICP para el PSC de carácter público

Resultado:

De una población de cinco especialistas en el área que conforman el 100% entre SUSCERTE y la FII, se obtuvo que todos los especialistas no tienen conocimiento de la existencia de un modelo de diseño para la ICP del PSC y consideraban que es importante partir del diseño con la finalidad de implementarlo para cumplir con la (LSMDF) de Venezuela.

Pregunta N° 6:

¿Deberá el Proveedor de Servicios de Certificación (PSC) de carácter público, seguir el mismo modelo escogido para la Infraestructura de Clave Pública (ICP) Nacional?

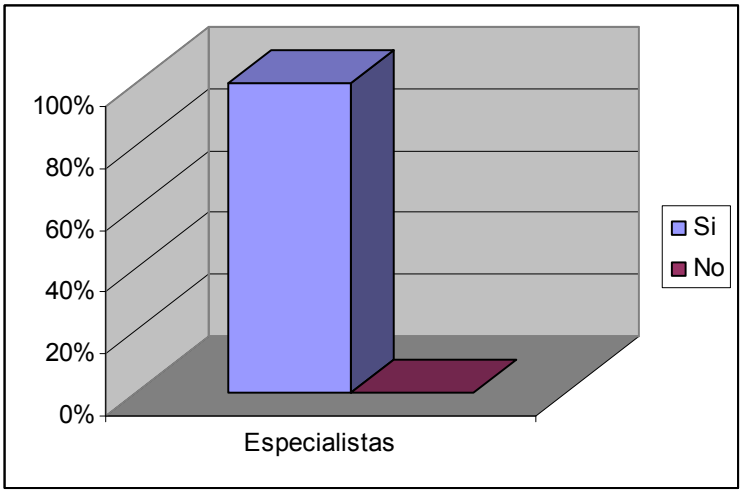


Figura 3.6 Gráfica de seguir el modelo de la ICP Nacional por el PSC de carácter público

Resultado:

De una población de cinco especialistas en el área que conforman el 100% entre SUSCERTE y la FII, se obtuvo que todos los especialistas estaban de acuerdo en mantener el modelo jerárquico subordinado, que tiene una única raíz del cual se desprende toda la confianza en el Sistema Nacional de Certificación Electrónica, y el PSC de carácter público que prestará los servicios de certificación electrónica en la Administración Pública Nacional forma parte del sistema.

PROPUESTA DE LA INFRAESTRUCTURA DE CLAVE PÚBLICA (ICP) PARA LA ADMINISTRACIÓN PÚBLICA NACIONAL (APN)

El presente capítulo expone la propuesta de la arquitectura y los componentes de la Infraestructura de Clave Pública (ICP) para la Administración Pública Nacional (APN), con una única raíz o ancla de confianza que genera seguridad a todo el Sistema Nacional de Certificación Electrónica.

SELECCIÓN DEL MODELO DE LA INFRAESTRUCTURA DE CLAVE PÚBLICA

Después de un estudio de las diferentes topologías de Autoridad de Certificación (AC), la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE)

concluye que el modelo que posee mejores atributos para ser implantado en la ICP Nacional es la arquitectura **jerárquica subordinada**.

Este modelo es también adoptado para el Proveedor de Servicios de Certificación (PSC) de carácter público que prestará servicios de certificación a la APN porque forma parte del Sistema Nacional de Certificación Electrónica.

DISEÑO DE LA ARQUITECTURA DE LA ICP

En la figura 4.1 se establecen las relaciones de confianza basadas en el modelo de árbol con una única raíz, punto inicial que deriva toda la confianza del sistema. Este modelo de certificación además de ser simple en su diseño, es fácil de comprender para el usuario común.

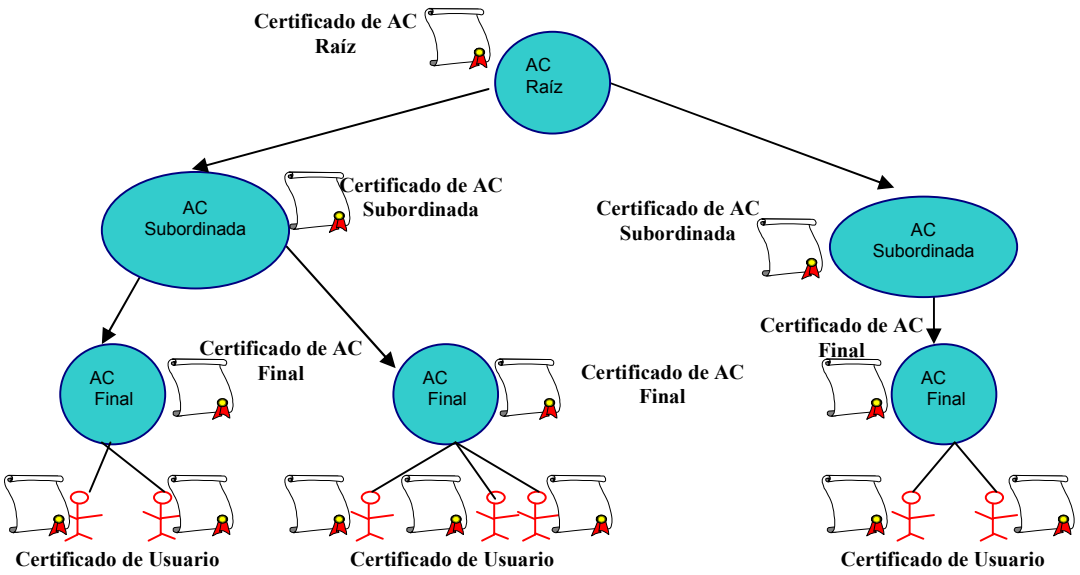


Figura 4.1 Estructura jerárquica de la ICP de Venezuela

SUSCERTE como ente rector y líder de la utilización de la firma electrónica y los certificados electrónicos en Venezuela a través del proyecto de la Autoridad de Certificación (AC) Raíz, garantiza el control para el buen funcionamiento de la ICP Nacional.

La AC Raíz genera un certificado raíz que será posteriormente utilizado por todas las AC Subordinadas, también llamada en el marco jurídico venezolano Proveedor de Servicios de Certificación (PSC) del sector público y privado, acreditados ante SUSCERTE.

La estructura propuesta agrupa las posibles comunidades de usuarios y las AC de organismos, instituciones, empresas públicas y privadas del país, como se observa en la siguiente figura.

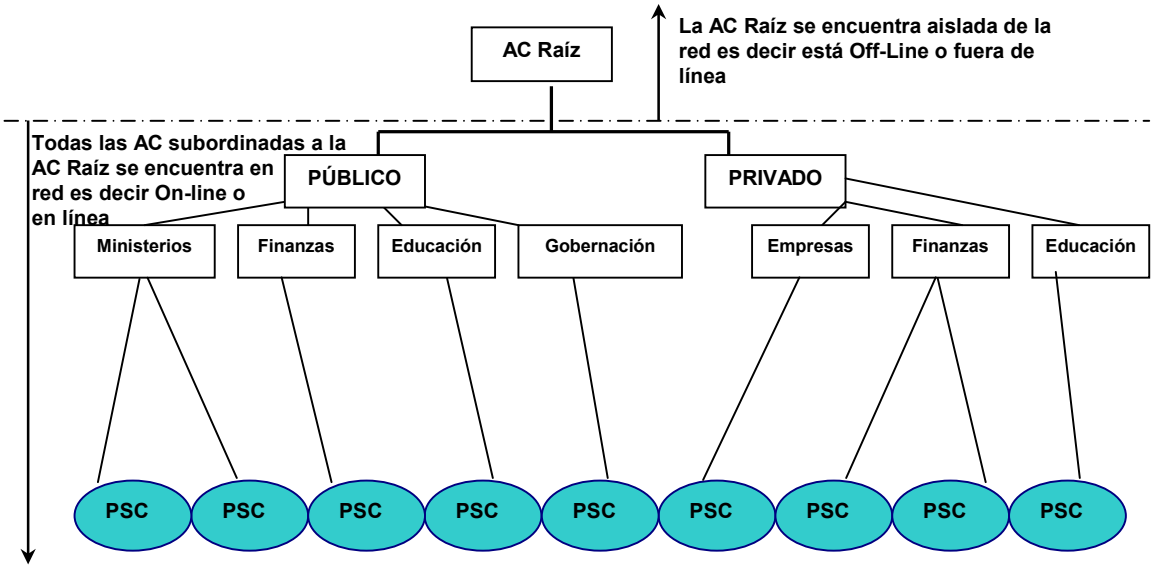


Figura 4.2 Estructura de (ICP) para los sectores público y privado de Venezuela

La AC Raíz es operada por SUSCERTE en forma "Off-Line[4]", porque este mecanismo permite proteger la clave privada de la AC Raíz, ancla de la cadena de confianza de la ICP de Venezuela, para que no quede comprometida su clave privada, es decir, para que no sea vulnerada. En adelante las comunicaciones de los proveedores acreditados se encuentran en forma "On-Line"[5], porque estos son los que finalmente se encargarán de emitir los certificados electrónicos a los usuarios finales del sistema.

Esta esquema general permite a otras personas que poseen el certificado electrónico, verificar la firma electrónica de cualquier mensaje de datos firmado con la clave privada de la AC acreditada, pero además permite que el receptor del mensaje de datos pueda tener la certeza de que el signatario o emisor del mensaje es quien dice ser, siempre y cuando el receptor tenga suficiente confianza en la honestidad y profesionalismo de la autoridad que certificó la identidad del signatario o emisor.

Los elementos de la estructura de la figura 4.2, corresponden a:

AC Raíz, que trabaja fuera de línea aislada por razones de seguridad para así proteger su clave privada de ataques de intrusos a través de la red. Su función principal es gestionar y emitir certificados a todos los sectores del país, tales como:

Sector Público: Se encarga de brindar servicios de certificación electrónica al conjunto de instituciones u organismos que forman parte del Poder Público del Estado Venezolano con competencia a nivel nacional, acreditando a los entes del gobierno o APN tales como: Ministerios, Asamblea Nacional, Gobernación, Alcaldías, Tribunal

[4] Fuera de línea, se mantiene aislada de la red por seguridad.

[5] En línea, está conectada a la red.

Supremo de Justicia (TSJ), Defensoría del Pueblo, Fiscalía General de la República, Procuraduría General de la República, Contraloría General de la República, Consejo Nacional Electoral, SENIAT, entre los principales. Se debe garantizar la interoperabilidad con las Autoridades de Certificación (AC) que ya se encuentran operativas en algunos organismos públicos.

Sector Privado: Se encarga de brindar servicios de certificación electrónica al sector privado venezolano incluyendo grandes, medianas y pequeñas empresas. También en el sector de educación privada, instituciones, sector de la banca privada entre otros, garantizando la interoperabilidad de la AC dentro de las empresas, con la ICP de Venezuela.

Sector Finanzas: *S*e encarga de brindar servicios de certificación electrónica a la banca tanto del sector público como para el privado en el aspecto financiero en general, respetando la compatibilidad con diferentes Autoridades de Certificación (AC) que actualmente estén ya operando.

Sector Educación: Proporciona los servicios de certificación electrónica a las instituciones cuyo objeto sea la educación, como universidades, institutos de investigación entre otros, tanto del sector público como privado.

COMPONENTES DE LA ICP DE LA APN DE VENEZUELA

La infraestructura basada en el esquema anterior debe contar con los siguientes componentes. (Ver figura 4.3):

- **Autoridad de Administración de Políticas (AAP)**
- **Autoridad Certificadora (AC) Raíz**
- **Autoridades Certificadoras Subordinadas (AC)**
- **Autoridades de Registro (AR)**
- **Usuario final**

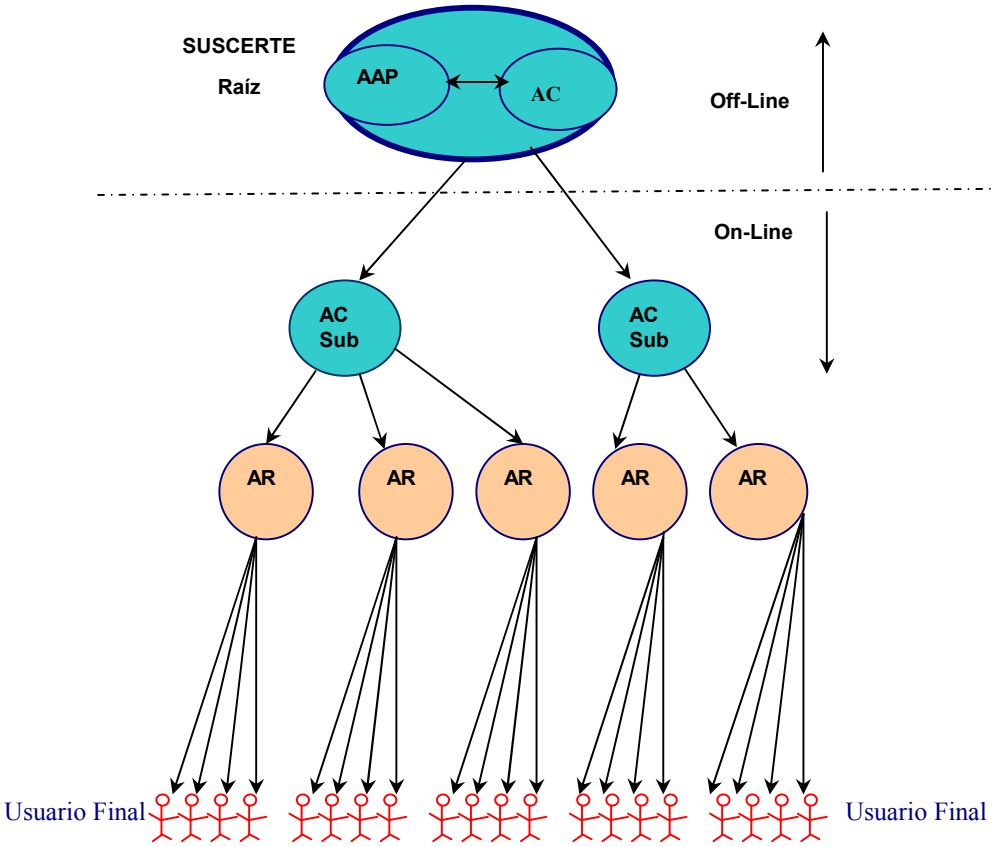


Figura 4.3 Componentes de la ICP de Venezuela

En el escenario de la figura 4.3 se modela la actuación de diferentes organismos. Esta propuesta de arquitectura podría cambiar considerando el apoyo tecnológico y

las políticas que brinden cada uno de ellos. También pueden incorporarse nuevos entes que provean a la comunidad de la certificación electrónica.

La Superintendencia, como ente encargado de acreditar, supervisar, y controlar, en los términos previstos en el Decreto con Fuerza Ley sobre Mensaje de Datos y Firmas Electrónicas (LSMDFE) y su Reglamento Parcial de la LSMDFE para los Proveedores de Servicios de Certificación públicos o privados, es responsable de la operación, mantenimiento de la AC Raíz de Venezuela y de garantizar los servicios de certificación electrónica en el sector público para cumplir con la disposición final tercera de la LSMDFE. Por otro lado, la AC Raíz establece relaciones de confianza unidireccional con las AC subordinadas. Esto se debe a que en esta jerarquía. Solamente la AC superior expide certificados a sus subordinadas y las AC Subordinadas no certifican a sus superiores.

Funciones de la Autoridad de Certificación (AC)-Raíz

Es responsable del:

- Resguardo seguro del ancla punto más alto de confianza, para la emisión y gestión de los Proveedores de Servicios de Certificación Electrónica (PSC).
- Puesta en Marcha de los Servicios de Certificación Electrónica en el sector público, a través de la acreditación del primer PSC de carácter público par la APN.
- Registro de los certificados asignados a los Proveedores de Servicios de Certificación Electrónica (PSC).

- Registro de una lista de certificados revocados generados por ella y una segunda lista de los certificados revocados de otras autoridades de certificación, de la ICP de Venezuela.

Función de la Autoridad de Administración de Políticas (AAP)- Raíz

Define las políticas de administración y seguridad para la operación de la ICP del Estado Venezolano, condensadas en un detallado documento conocido como la Declaración de Prácticas de Certificación (DPC) y Políticas de Certificación (PC) de la AC Raíz.

Funciones de la Autoridad de Certificación (AC) Subordinadas o PSC

- Cumplir con los lineamientos, estándares y normativas puestas por la Ley y por SUSCERTE.
- Archivar todos los certificados y las listas de revocación de certificados generados por el mismo.
- Resguardo de la clave privada en un medio o dispositivo criptográfico seguro.
- Elaborar su propia DPC y PC acorde al modelo que proporciona SUSCERTE.

Funciones de la Autoridad de Registro (AR) del PSC

- Verificar la identidad de los solicitantes.
- Comunicación con la AC para la emisión de los certificados electrónicos.
- Entrega de los certificados electrónicos y claves públicas y privadas a los solicitantes en dispositivos criptográficos seguros.

Continuando con la propuesta de la arquitectura, se incorporan los sectores público y privado.

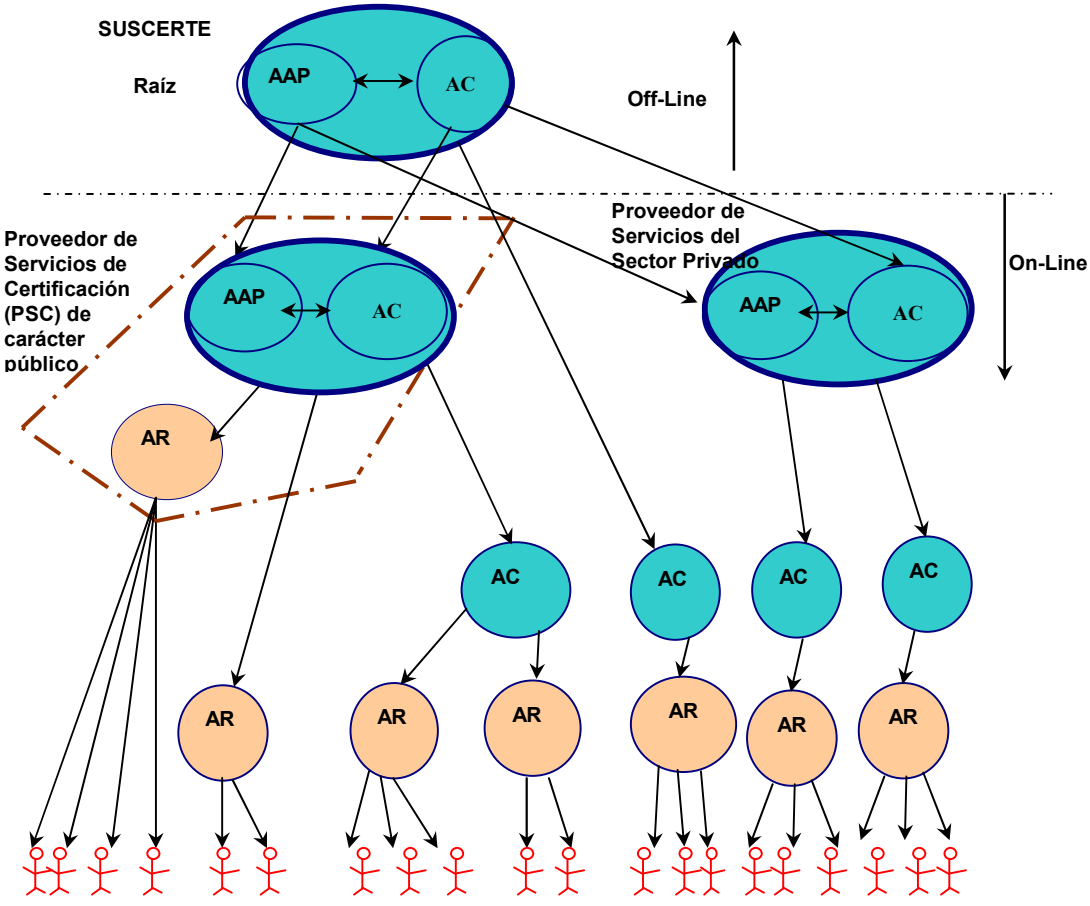


Figura 4.4 ICP dotada de una Entidad Pública de Certificación para el Proveedor de Servicios de Certificación del Estado

En la figura 4.4, las AC generalmente cumplen con un modelo de confianza que permite asegurar en un nivel alto la autenticación de sus suscriptores, administrado por organizaciones públicas y privadas que cumplen políticas y realizan prácticas estrictas manteniendo de esta manera la confianza en los servicios que ellas prestan. Una AC puede también funcionar para autenticar la identidad de otras AC, y a través de este procedimiento, se pueden construir modelos de confianza más robustos y escalables.

En el último nivel de la arquitectura propuesta se tienen las personas titulares (usuarios finales) de una o varias firma y certificados electrónicos, responsables de la custodia de su clave privada. Considerando que esta sólo será conocida por su propietario, normalmente es utilizado un medio de resguardo físico con un alto nivel de confianza como son las tarjetas inteligentes criptográficas.

COMPONENTES DE LA AUTORIDAD DE CERTIFICACION (AC) RAÍZ

Para la creación de configuración e inicio de operaciones de la AC raíz, ancla de la cadena de confianza la Infraestructura de Clave Pública (ICP) Nacional, se definen los componentes que deben estar presentes para la correcta operación en correspondencia con las políticas y normas legales dictadas en materia de certificación electrónica.

Se plantea un modelo de seguridad de 3 aristas para resolver el problema propuesto. La visión de seguridad de tres aristas consiste en considerar tres aspectos, tales como:

- Hardware
- Software
- Modelos y políticas

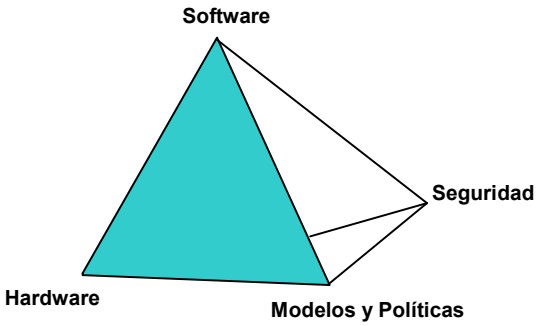


Figura 4.5 Modelo de seguridad de 3 aristas

Las tres aristas incorporan elementos de los dos aspectos: técnico y operacional, que se agrupan de la siguiente manera:

DE TIPO TÉCNICO

Software

Debido a que la infraestructura opera para dar servicios en operaciones electrónicas (software), este componente es de vital importancia. El software se

refiere a todos los programas y aplicaciones libres y/o propietarios que funcionan sobre cualquier hardware que forma parte de la AC Raíz, y que en principio están asociados a la ejecución de determinada tarea o la prestación de determinado servicio, tales como: servidores de datos, control de acceso, protección de claves, identificación, registro de acceso, replicación, sistemas operativos, manejadores de dispositivos, entre otros.

En la validación y aseguramiento del software, al utilizar el software libre se debe hacer el chequeo de integridad del código fuente, que se logra a través del uso de firmas electrónicas, y herramientas de generación de resumen (hash) que sellen el estado y validez de cada elemento de software.

Por otra parte en el caso de ser necesario utilizar algún software de tipo propietario, es importante tener acuerdos de confidencialidad con la empresa que provea el software así como también contar con la posibilidad de certificación de los binarios y/o códigos fuentes.

Las tareas asociadas al software para la operación de la AC Raíz, son la:

1. Generación y protección de claves privadas

2. Generación de claves públicas y certificados

3. Acreditación de Autoridades de Certificación

4. Firma de certificados

5. Publicación de certificados

6. Control de identidad de usuarios

7. Registro de tareas y acciones

8. Control de acceso físico

Hardware

Es conocido que el uso de elementos de hardware especializados aumenta los niveles de seguridad y la eficiencia de los procesos o procedimientos que se realice con la ayuda de herramientas o sistemas de cómputo, ya que para poder quebrantar la seguridad de un sistema "seguro" es imprescindible el contacto físico con los elementos de hardware, además de no poderse realizar copias del material a vulnerar y tener en muchas ocasiones que utilizar herramientas de difícil traslado y ocultamiento.

Una de las tareas más importantes de la AC Raíz, es la protección de las claves privadas del certificado autofirmado. Generalmente para ello se utiliza un dispositivo denominado **Módulo de Seguridad en Hardware**[6], que funciona como una caja de seguridad resistente a condiciones extremas, en la cual se depositan las claves privadas, y que solo puede ser accedida de forma restringida conforme a políticas de seguridad estrictas.

El hardware es utilizado en la identificación de usuarios o control de acceso a sistemas. Para que una determinada persona (empleado, administrador, gerente,

[6] (Hardware Security Module, HSM por sus siglas en inglés)

usuario, etc.) acceda a un sistema, debe tener algún elemento que lo identifique. En un nivel básico, se utiliza algo que sabe la persona, como por ejemplo, una contraseña o frase oculta. Pero hoy día para incrementar la seguridad se utilizan elementos de hardware como tarjetas, discos, que contengan información digital protegida. En un grado más alto de seguridad es posible utilizar dispositivos de reconocimiento biométrico como captadores de huellas digitales, reconocedoras de forma de la cara o mano, entre otros dispositivos.

Acceso Físico

El acceso físico es uno de los aspectos fundamentales en la creación de una AC Raíz. Este aspecto tiene que ver con las condiciones físicas donde se encuentra el hardware y software que sirven para operarla.

En general, se debe disponer de un cuarto de seguridad o bóveda o bunker, con por lo menos tres controles de acceso basados en identificación de nivel 2 (de identificación), nivel 3 (biométrico) y pin de acceso. También es conveniente disponer de sistemas de TV en circuito cerrado, y vigilancia total (24x365) con personal de seguridad armado.

DE TIPO OPERACIONAL

Políticas

Es el componente que coordina todos los procedimientos y reglas en la conformación y operación adecuada de la AC Raíz. Las políticas tienen la función de

asegurar la operación de la raíz. En general se hace uso de herramientas de hardware y software para que puedan ser implementadas.

El documento de políticas debe ser conciso y coherente, tomando en cuenta los lineamientos y estándares de seguridad, que tengan que ver directamente con el flujo de operación de la AC Raíz. También debe normar tareas y la estructura de los elementos que conforman la raíz.

Operadores y Administradores

En la ejecución de procedimientos de la AC Raíz participan personas que deben ser responsables de las acciones que en éste se ejecuten. Cada una de estas personas debe tener un rol o conjunto de actividades definidas dentro del flujo de trabajo de operación del nodo.

Es conveniente contar con esquemas de trabajo de responsabilidad compartida o en jerarquía, que garanticen que un procedimiento tan delicado cuente con la aprobación necesaria de diferentes actores para poder ejecutarse.

Auditorías

Los procesos de auditorías certifican que el flujo de operación de la AC Raíz se realice dentro de los parámetros adecuados y en el marco de las políticas previamente definidas.

Se deben realizar cada cierto tiempo y deben también estar definidas en el documento de políticas. Es conveniente que los auditores cuenten con acceso a información y herramientas que les permitan evaluar y certificar códigos, procedimientos, registros y demás elementos.

COMPONENTES DE LA AUTORIDAD DE CERTIFICACION (AC) PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN (PSC) PARA LA APN

Los componentes de la AC del PSC de carácter público para la APN tienen características similares a las de la AC Raíz. Se diferencian en el nivel de seguridad y en el escalamiento que experimenta una AC Subordinada al bajar en la jerarquía.

El nivel de seguridad de la AC Raíz debe ser superior al de la AC Subordinada, ya que es el punto central de la jerarquía y de ella depende toda la infraestructura. El nivel de seguridad debe ir en concordancia con las políticas y con el costo que implicará el robo o violación de las claves privadas que guarda la AC. Este costo puede ser calculado y asignado a una póliza de seguro en función de minimizar daños a usuarios o entidades finales.

En el tema de escalamiento, en la AC del PSC de la APN es necesario incorporar manejo de datos a media y alta escala, para ello por lo general, se utilizan manejadores de base de datos relacionales, que están diseñados para soportar acceso a datos de forma segura y eficiente.

En la automatización de procesos como la firma y publicación de certificados, se pueden incorporar procedimientos por lotes (batch) que faciliten al operador las tareas que debe realizar manteniendo los parámetros de seguridad establecidos. Una de las características que no necesariamente es incorporada en la AC Raíz, pero si es necesario en la AC del PSC de la APN por la conexión en línea o fuera de ella con la Autoridad de Registro (AR).

La AR tiene la función de acreditar y confirmar los datos dados por la entidad final (usuario final) y exportar en un formato estándar y comprensible por el componente AC. La AC del PSC de la APN debe tener una conexión en línea o fuera de línea con el componente publicador, por lo general es un esquema de directorio unificado, como por ejemplo OpenLDAP (Lighweight Directory Access Protocol) o algún tipo de repositorio con interfaces de publicación, como bases de datos relacionales o repositorios de documentos XML.

APLICACIÓN ROOTVE: COMPONENTE DE SOFTWARE DE LA AC RAÍZ

En concordancia con la definición general del componente de software para la AC Raíz, la aplicación ROOTVE desarrollada bajo software libre por FUNDACITE Mérida organismo adscrito al MCT, tiene las siguientes características:

Protección de las claves privadas

La clave privada de la AC Raíz se crea a través de un módulo de seguridad[7] generada en un dispositivo de **Módulo de Seguridad en Hardware (HSM)** y nunca saldrá del mismo, para mantener en resguardo las claves privadas del certificado autofirmado. Las copias de seguridad han sido realizadas, también dentro del HSM y extraídas en varias partes con el objeto de garantizar una mayor seguridad.

El proveedor del HSM utilizado es nCipher, que ofrece integración inmediata con numerosas aplicaciones comerciales de seguridad mediante interfaces basadas en normas, además de una gama de soluciones para que los desarrolladores realicen aplicaciones especiales e implementaciones incrustadas.

[7] En el módulo HSM nShield deben existir k partes del secreto para que pueda ser leído en su totalidad. El secreto es compartido con la generación de clave privada de tres operadores y tres administradores del HSM cada uno tiene en su tarjeta inteligente un pedazo de la clave privada del HSM, para generar la clave privada de la AC Raíz dentro del HSM

Repositorio cifrado

Se utiliza la Base de Datos Berkeley DB[8] esta aplicación de repositorio de datos ofrece un esquema no relacional pero con un nivel de seguridad alto, ya que no es necesario la apertura de puertos del sistema operativo y no presenta un configuración conocida de la información que pueda ser accedido por otra aplicación cliente. Aunque BerkeleyDB es una base de datos basada en archivos locales, soporta transacciones, replicación y multihilos; también lleva un registro de todas las operaciones realizadas sobre los datos. Toda la información es cifrada y solo puede ser accedida utilizando un esquema de secreto compartido.

Doble repositorio y firma cruzada

La aplicación ROOTVE para la emisión de certificados electrónicos de los PSC acreditados ante SUSCERTE, utiliza dos tipos de repositorios: uno basado en una base de datos integrada y otro basado en un esquema relacional en un entorno cliente-servidor. Inicialmente ROOTVE maneja Berkeley DB como base de datos integrada y Postgres como base de datos relacional.

Los dos repositorios pueden estar en diferentes elementos de memoria. Por ejemplo, la base de datos Postgres puede estar en una memoria portable (pen-drive) y la base de datos integrada puede estar en otro tipo de dispositivo, como un disco duro, u otra memoria portátil.

La firma cruzada consiste en que la aplicación ROOTVE realiza el proceso de firma de los datos de los elementos de los repositorios con la finalidad de mantener la

integridad. La firma se almacena de forma cruzada, es decir, se firman las tablas del repositorio relacional y se almacena en el repositorio cifrado, luego se firman los registros y claves del repositorio cifrado y se almacenan en el repositorio relacional. Para firmar una tabla del repositorio relacional o cifrado, se le indica al usuario al final de su sesión los elementos modificados: tablas, lista de acciones (registro), claves, y la opción para cargar su clave privada, según se muestra en la siguiente figura:

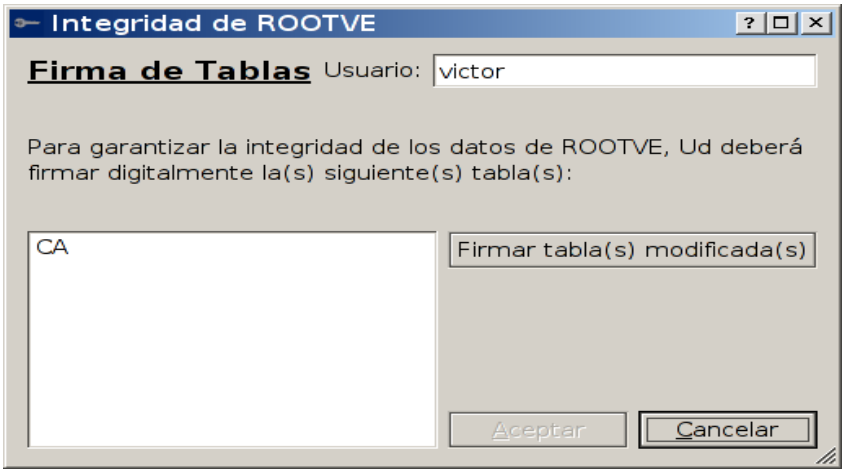


Figura 4.6 Pantalla de Integridad de la aplicación ROOTVE para firmar las tablas modificadas

[8] www.sleepycat.com

Módulo de Seguridad en Hardware (HSM: Hardware Security Module)

El diseño de la aplicación ROOTVE permite incorporar un repositorio basado en hardware especializado tal como un HSM de fabricante NCipher[9] bajo el estándar establecido en la Norma Federal de Procesamiento de la Información (FIPS) 140-2 nivel 3, Este nivel impide la exportación de claves fuera del sistema. Estos equipos proveen una Interfaz de Programación de Aplicación o API[10] que permite realizar las operaciones de generación, comprobación, firma de certificados, perfectamente integrables con los demás componentes de ROOTVE. Un módulo de seguridad en hardware se muestra en la figura 4.7 (modelo nSHIELD F3 nCipher):

Figura 4.7 Modelo nSHIELD F3 nCipher

Uso de Tarjetas Inteligentes Criptográficas (Smartcard):

Para el control de acceso de usuarios autorizados de la aplicación ROOTVE, se utiliza un esquema de comprobación clave pública-privada. Una de los puntos importantes de este esquema es la distribución de claves privadas a los administradores de la AC, y se realiza a través de la asignación y entrega de tarjetas

[9] http://www.ncipher.com
http://www.ncipher.com/downloads/international/ncipher_products_spanish.pdf

inteligentes contentivas de la respectiva clave privada. También cada parte del secreto compartido[4] se asigna a un administrador, y se coloca en la tarjeta inteligente asignada. La aplicación ROOTVE tiene compatibilidad con tarjetas de la empresa española C3po S.A.[11], que distribuye un combo (en inglés kit) compuesto de una tarjeta inteligente llamada "Ceres" y un lector modelo LTC31, además del software necesario para dar soporte a sistemas GNU/Linux. Una tarjeta Ceres tiene la apariencia que se muestra en la figura 2.10 del marco teórico del presente documento.

Las tarjetas inteligentes criptográficas son un componente de la ICP que da soporte a la generación y almacenamiento de claves públicas y privadas así como mecanismos y algoritmos criptográficos para garantizar integridad, confidencialidad y el no repudio en origen, entre ellos la firma electrónica.

Características de la tarjeta Ceres

Entre las características esenciales están: tarjeta criptográfica con sistema de almacenamiento de certificados, sistema de alta seguridad y criptografía asimétrica (RSA), capacidades de 16kb y 32kb. La tarjeta Ceres está especialmente diseñada para las infraestructuras de claves públicas.

Se encuentran implementados algoritmos para generación de números aleatorios, pares de claves pública/privada. Cumple con los estándares reconocidos de diseño, construcción y manipulación para tarjetas inteligentes como lo son: norma ISO 7816-1/-2/-3, estándar PKCS#11 y PKCS#15.

[10] API, por sus siglas en inglés Application Programming Interface
[11] www.c3po.es

En las aplicaciones que se están desarrollando, las tarjetas inteligentes se utilizan como un dispositivo de generación y almacenamiento de pares de claves pública/privada que permiten que la aplicación ROOTVE autentique a los usuarios operadores. Esta autenticación garantiza el acceso a la aplicación a través de un mecanismo de seguridad de nivel 2. El nivel de seguridad 2 implica que el usuario conoce algo (el número de identificación personal – PIN – de la tarjeta) y posee algo (la tarjeta misma). Las clave privadas generadas dentro de las tarjetas nunca salen de la misma. Adicionalmente se utilizan las tarjetas como mecanismo para exportación de certificados en hardware de los usuarios de las aplicaciones, almacén de secretos compartidos para el acceso de la clave privada de la autoridad de certificación raíz, entre otros usos.

Hoy día, la tarjeta Ceres de la RCM-FNMT [12](Real Casa de la Moneda - Fábrica Moneda y Timbre de España) constituye un soporte para los certificados digitales que se emiten en la Autoridad de Certificación Española y que están siendo utilizados en operaciones de gobierno electrónico en los siguientes organismos: presidencia de gobierno, agencia estatal de administración tributaria, comisión del mercado de las telecomunicaciones, seguridad social, ministerio del trabajo y asuntos sociales, Ministerio de Economía y Hacienda, entre otros.

Herramientas necesarias para ROOT.VE

Para la implementación de la aplicación ROOT.VE, el sistema operativo utilizado fue Debian Sarge y con las siguientes herramientas instaladas:

[12] http://www.cert.fnmt.es/pilotos/tarjeta.htm

Berkeley DB 4.2.52

De esta herramienta se utiliza el archivo fuente db_cxx.h y las librerías libdb, libdb-4.2, libdb_cxx, y libdb_cxx-4.2. Se requiere configurar la herramienta con la opción: $ ./configure --enable-cxx

OpenSSL

De esta herramienta se utilizan los archivos fuente openssl/opensslv.h y la librería libcrypto. Se recomienda una versión reciente de OpenSSL específicamente mayor o igual a la versión 0.97d.

Crypto++

Se utiliza esta librería para la creación de secretos compartidos asociados al password de acceso a la base de datos de las claves privadas de ROOT.VE. Esta herramienta se encuentra disponible entre las fuentes de la distribución de ROOT.VE y está comprimida en formato .zip.

Para instalar la librería se descomprime el archivo en un directorio destino con el comando unzip -a cryptopp521.zip creando el subdirectorio crypto++. Luego se compilan los fuentes con el comando make. Una vez compilados las fuentes se genera la librería libcryptopp.a que debería ser copiada en el directorio /usr/lib del sistema de archivos. De esta forma la librería estará disponible durante la compilación de las fuentes de ROOTVE.

Postgres-7.4.2

ROOT.VE utiliza una base de datos Postgres para almacenar información relevante de solicitudes de firma de certificados, certificados, sujetos que emiten solicitudes, organizaciones, autoridades de certificación y de los usuarios de la aplicación.

ROOT.VE utiliza las fuentes de Postgres para el construir el manejador (driver) QPSQL7 de la librería Qt así como para funciones particulares como la creación inicial de la base de datos y ejecución del script sql que define la estructura de las tablas.

Qt 3.3.3

ROOT.VE es una aplicación desarrollada completamente con la librería Qt versión 3.3.3 para proporcionar la funcionalidad gráfica. La compilación de ROOT.VE requiere que la librería Qt haya sido instalada con soporte para threads; eso se logra al momento de compilar la librería con los comandos:

$ ./configure -threads

$ make

$ make install

Plug-in QPSQL7

Para manipular la información de la base de datos Postgres, ROOT.VE requiere un driver o manejador para conectarse a la misma. El driver utilizado es el QPSQL7. Este driver o controlador, en forma de plug-in, puede ser construido durante la instalación de la librería o posteriormente.

Otras herramientas

Para la compilación de ROOT.VE se requiere el compilador GNU C++ en una versión mayor o igual a 2.95 y GNU make.

Las fuentes de la aplicación y el paquete rootve.deb están disponibles en http://cnsi.funmrd.gov.ve/cnsi/modulos/descargas/index.php

PROCESO DE FIRMA DE CERTIFICADOS ELECTRÓNICOS DE LA AC RAÍZ

Para la firma de certificados electrónicos se necesitan los siguientes elementos:

1. Acceso a la clave privada del certificado autofirmado de la AC Raíz que se encuentra en el HSM.

2. Certificado electrónico autofirmado de la AC Raíz.

3. Documento de Solicitud de Firma de Certificado (CSR Certificate Signing Request, por sus siglas en inglés) del PSC a la AC Raíz.

La aplicación ROOT.VE provee todos los elementos para realizar el proceso de firma utilizando los tres documentos enumerados con anterioridad. El flujo de trabajo para realizar el proceso de firma es el siguiente:

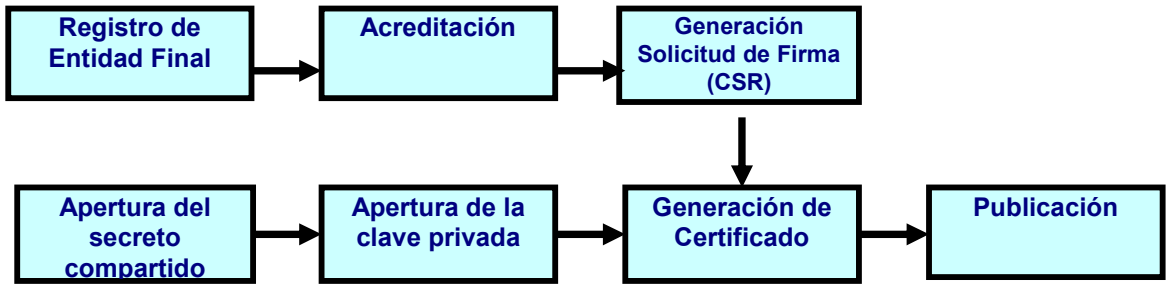


Figura 4.8 Proceso de firma de los certificados electrónicos por parte de la AC Raíz

MODELO FUNCIONAL DEL PSC DE CARÁCTER PÚBLICO PARA LA APN

SUSCERTE tiene como compromiso garantizar los servicios y las autoridades de registro para operar bajo un Sistema Nacional de Certificación Electrónica (SNCE).

En el SNC es importante tener bien definidas todas las partes involucradas para que tengan suficiente claridad respecto a las obligaciones y responsabilidades de cada cual, y así poder anticipar de manera segura las consecuencias y efectos respecto al uso de los certificados digitales bajo cualquier circunstancia.

Por lo tanto se plantea el modelo del Proveedor de Servicios de Certificación Electrónica (PSC) de carácter público de acuerdo a lo establecido en la Disposición Final Tercera del Decreto Ley sobre Mensajes de Datos y Firmas Electrónicas (DLSMDFE).

El PSC debe llevar de manera adecuada las operaciones, e informar respecto a todos los procedimientos aplicables a SUSCERTE.

En la figura 4.9, se muestra el modelo funcional del PSC de carácter público, cuyo responsable será la Fundación del Instituto de Ingeniería (FII) organismo adscrito al Ministerio de Ciencia y Tecnología (MCT) responsable de la administración del Proveedor de Servicios de Certificación Electrónica (PSC) de carácter público, decisión tomada por el ejecutivo nacional.

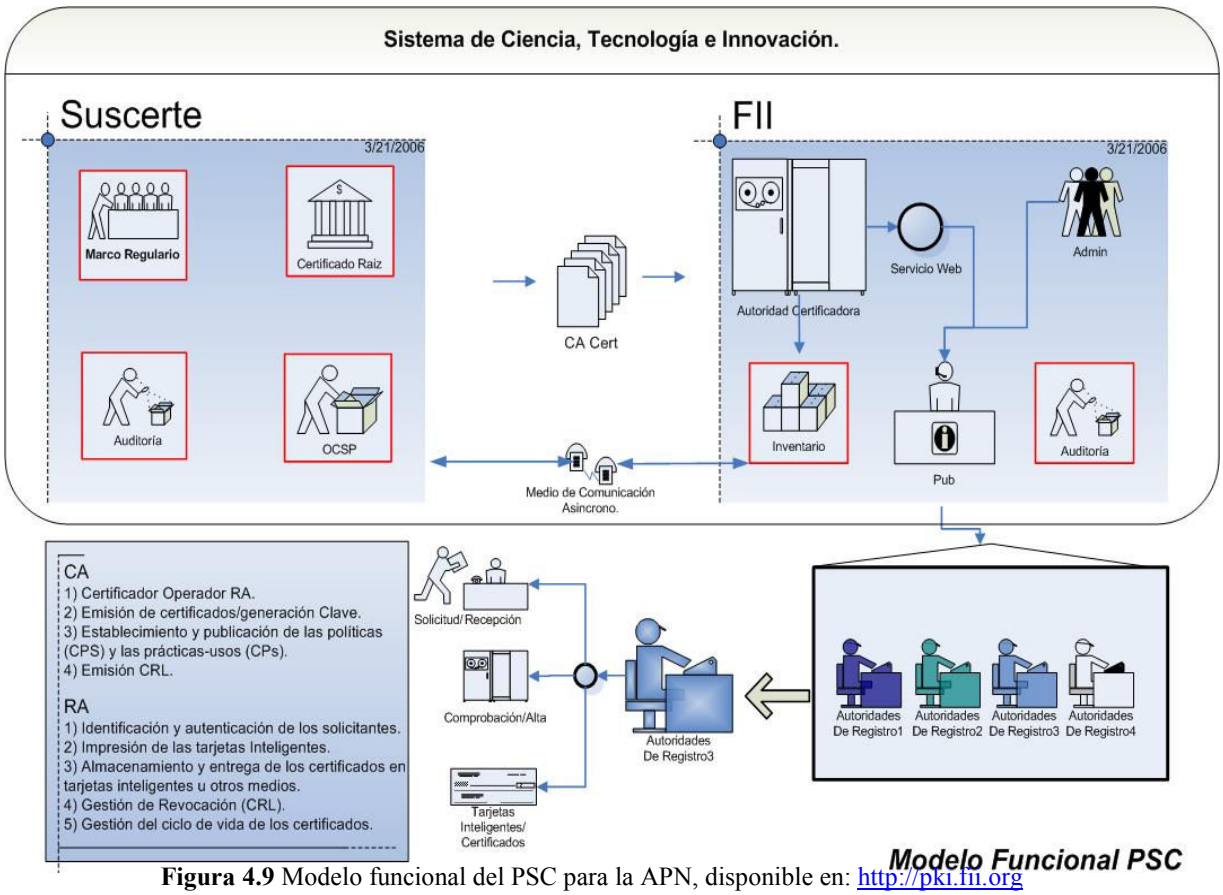


Figura 4.9 Modelo funcional del PSC para la APN, disponible en: http://pki.fii.org

SUSCERTE como ente regulador en la materia, debe velar que el PSC cumpla con:

- La Ley sobre Mensajes de Datos y Firmas Electrónicas
- Reglamento de la Ley sobre Mensajes de Datos y Firmas Electrónicas
- Estándares y lineamientos tecnológicos dictados por SUSCERTE
- Normas y procedimientos de acreditación dictados por SUSCERTE
- Normas y procedimientos de la auditoría dictados por SUSCERTE

A continuación se resumen de lineamientos y estándares para la acreditación del PSC ante SUSCERTE:

Para la implementación de la estructura de los certificados electrónicos, se debe tomar en cuenta que:

- La estructura de datos que conforma el certificado de firma electrónica emitido, debe estar en conformidad al estándar ISO/IEC 9594-8.
- El certificado por parte del proveedor de ICP debe tener por lo menos:
  - Un código de identificación único del certificado.
  - Nombre o razón social, RIF, dirección de correo electrónico, antecedentes de su acreditación y su propia firma electrónica, los datos de la identidad del signatario (nombre, dirección de correo electrónico, cédula de identidad, y plazo de vigencia).
- En el campo de Certificate Policies (Políticas de Certificado) de las extensiones del certificado del formato X-509 v3, su texto debe ser:"Certificado para firma electrónica".

Para la implementación de la estructura de la lista de certificados de revocados (CRL):

- La lista de certificados revocados de firma electrónica debe contener la información y estructura que especifica el estándar X.509, y debe ser firmada por el proveedor de ICP.
- Debe a lo menos tener la siguiente información:

- Versión (debe tener el valor 3).
- Algoritmo de firma.
- Nombre del emisor (que emitió y firmó la lista de certificados revocados).
- Fecha actual (fecha y hora en que fue emitida la lista de certificados revocados).
- Próxima actualización.
- Certificados revocados.

Para la implementación del registro de acceso público, se debe hacer:

- La elaboración de un sitio Web de información pública, con al menos:
  - El registro de certificados emitidos, indicando código y su estado.
  - Copia de la Lista de Certificados Revocados (CRL) actualizada las 24 horas.
  - Indicar si el certificado ha sido traspasado de otro proveedor acreditado o ha sido homologado.
  - El acceso seguro a los signatarios para realizar la revocación o suspensión de certificados vigentes.
- La Política del Certificado de firma electrónica.
- La Declaración de sus Prácticas de Certificación.

Para la estructura del plan de administración de claves, se debe cumplir con:

- Documento del ciclo de vida completo de las claves criptográficas, esto es:
  - Generación de las claves de la Autoridad Certificadora (AC) de forma electrónica del proveedor de ICP.
  - Almacenamiento, respaldo y recuperación de la clave privada de la AC de firma electrónica.
  - Distribución de la clave pública de la AC de firma electrónica.
  - Uso de la clave privada por parte de la AC de firma electrónica.
  - Término del ciclo de vida de la AC de firma electrónica.
    - Administración del ciclo de vida del hardware criptográfico utilizado por la AC.
    - Servicios de administración de las claves de los signatarios suministradas por la AC (generación de clave y revocación después de vencimiento).
    - Preparación de los dispositivos seguros de los signatarios.
    - A su vez el plan debe ser consistente con la Política de los Certificados de firma electrónica.

Para la evaluación de la plataforma tecnológica, se debe tener un:

- Modelo criptográfico:
  - Generar pares de clave privada y pública de 4096 bits.
  - Capacidad de firma y cifrado.

- Existencia del sistema de control de acceso para acceder a la clave privada.
- Existencia de controles de acceso para acceder a funcionalidades de firma y cifrado.
- Capacidad de respaldar la clave privada, en forma segura.
- Capacidad de recuperar la clave privada del back-up.
- Capacidad de generar log auditable para administración de contingencia y accesos maliciosos.

Para la Política de Certificados (PC) electrónicos, tanto para el signatario como para las entidades involucradas y los que reciben el documento con la firma electrónica, se deberá verificar:

- El registro del signatario. La autenticación, verificación de su identidad en forma fehaciente y forma de la política para comprobar el nombre del signatario, y así poder utilizar el certificado para la firma digital.
- La Política de Certificados Digitales deberá permitir la interoperabilidad con otros Proveedores de Servicios de Certificados (PSC) electrónicos.
- Las Prácticas de Certificación deberán establecer cómo el PSC entrega la confianza establecida en la Política de Certificados.

Para la Declaración de Prácticas de Certificación (DPC), se debe:

- Conocer la práctica de certificación de firma digital con las responsabilidades y obligaciones tanto del PSC, como del sujeto a ser identificado digitalmente.
- Tener explicito el ciclo de vida de los certificados.

En el modelo operacional de la Autoridad Certificadora, se debe poseer:

- Los servicios prestados por la AC del PSC.
- Cómo se interrelacionan los diferentes servicios.
- En qué lugares opera.
- Qué tipos de certificados se entregarán.
- Cómo se entregan, incluyendo a terceros.
- Cómo se protegerán los activos.

En el modelo operacional de la Autoridad de Registro (AR), se debe saber:

- Cuáles son los servicios de registro prestados por el PSCE.
- En qué lugares se ofrecerán dichos servicios.
- Qué tipos de certificados se entregarán.
- Cómo se pretende hacer esto, incluyendo los servicios por terceros.

En el modelo de operaciones de Autoridad Certificadora, se debe por lo menos:

- Ser consistente con la Política de Certificación.
- Incluir la interacción entre la AC y la AR.

- Describir los controles de seguridad física, de red, del personal y de procedimientos.
- Incluir los procedimientos adoptados para el manejo de claves públicas y privadas.

En el manual de operaciones de la Autoridad de Registro, se debe:

- Ser consistente con la Política de Certificación.
- Describir el plan de entrenamiento de los empleados.
- Incluir la forma en que se verifica la identidad de las personas.
- Incluir procedimientos de entrega y uso de la clave privada por los signatarios de los certificados.
- Incluir la metodología adoptada para manejar el análisis de riesgos, plan de recuperación de desastres, plan de seguridad e incluir la interacción entre las unidades internas que cumplen la función de AC y AR.

Una vez preparado el PSC con los requisitos legales, técnicos y administrativos para la acreditación. Si cumple con todos los requerimientos para la acreditación SUSCERTE otorga la acreditación al PSC, esta decisión es publicada en Gaceta Oficial para que sea de conocimiento público. El siguiente paso es la generación del certificado electrónico del PSC y finalmente el acto de la ceremonia de claves del PSC. El Acto público es avalado por un notario público y por los custodios de la clave privada de la AC Raíz operada fuera de línea que se encuentra dentro del HSM.

Los custodios son tres operadores de cinco siguiendo el método esquema límite (k,n) de Shamir, para garantizar seguridad al momento de utilizar la clave privada de la AC Raíz y firmar el certificado electrónico proveniente del PSC. Como resultado el PSC pasa a ser parte de la cadena de confianza del modelo de jerarquía subordina de infraestructura de clave pública nacional.

A partir de ese momento el PSC forma parte del Sistema Nacional de Certificación Electrónica y comienza la operación de la/las AR para la operación y administración de los certificados electrónicos que emite, con las funciones descritas en los puntos 4.3.3 y 4.3.4 de la presente propuesta.

Los usuarios finales que desean obtener certificados electrónicos del PSC, lo solicitan a través de su Autoridad de Registro (AR), que se mantiene en comunicación en línea con la AC del PSC. Es entonces cuando la AC firma el certificado lo envía a la AR y es allí cuando se le entrega el certificado electrónico al usuario final en un medio seguro. Se recomienda utilizar la tarjeta inteligente.

Una vez puesta en marcha el PSC, se cumple con la disposición final tercera de la LSMDFE y aquellos organismos de la APN que requieran de los servicios electrónicos podrán solicitarlos al PSC de carácter público. Así el gobierno nacional usará la firma y los certificados electrónicos, con la ventaja que le otorga plena validez legal a la firma electrónica.

DECLARACIÓN DE PRACTICAS DE CERTIFICACIÓN (DPC) DE LA AC RAÍZ

En este capítulo se presenta la normativa y condiciones generales de los servicios de certificación electrónica que presta la Infraestructura de Clave Pública (ICP) de la Raíz en Venezuela.

INTRODUCCIÓN

La *Declaración de Prácticas de Certificación* (DPC) de la Autoridad de Certificación (AC) Raíz de Venezuela establece los elementos necesarios para la gestión y emisión de certificados a los Proveedores de Servicios de Certificación (PSC) del sector público y privado y la Política de Certificados (PC), junto con los tipos de certificados y el conjunto de reglas que indican los procedimientos seguidos en la prestación de servicios de certificación creando el Sistema de Certificación Electrónica confiable, dentro de la Infraestructura de Clave Pública (ICP) de Venezuela.

La AC Raíz es la autoridad de certificación Raíz de la Infraestructura de Clave Pública de Venezuela cuya función principal es emitir los certificados digitales a los PSC, donde un certificado digital es un documento digital que asocia la identidad de un sujeto (entidad, individuo, dispositivo, etc.) con su correspondiente clave pública y uno o más atributos.

El caso específico de un certificado raíz, se corresponde a un certificado que ninguna entidad de confianza superior firma digitalmente como raíz, es decir se trata de un certificado autofirmado, y es a partir de allí, donde comienza la cadena de

confianza. Este proceso de autofirmado hace que los campos del certificado raíz cumplan con los estándares internacionales y aplicables que garantizan la interoperabilidad.

Entonces la AC Raíz dispone de un certificado autofirmado con su clave privada, con el que firma los certificados de clave pública de los PSC, que a su vez emplean sus claves privadas, para firmar los certificados de las entidades finales, de modo que toda la jerarquía se encuentra cubierta por la confianza de la AC Raíz.

La aplicación para la ICP de la AC Raíz ha sido desarrollada por FUNDACITE Mérida, organismo adscrito al Ministerio de Ciencia y Tecnología (MCT) en software libre siguiendo el Decreto Presidencial 3390 sobre software libre.

Los certificados digitales de clave pública son generados de acuerdo al estándar X.509 versión 3 (1996).

La arquitectura general, a nivel jerárquico, de la ICP de la certificación electrónica de Venezuela es la siguiente:

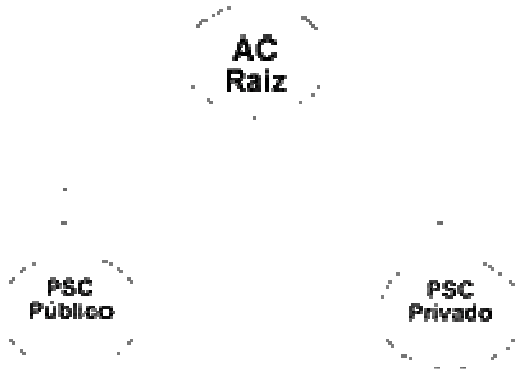


Figura 5.1 Arquitectura general de la ICP de Venezuela

En la figura 5.1, la arquitectura jerárquica parte de la Raíz, ancla de la Cadena de Confianza de la certificación electrónica, llamada Autoridad de Certificación (AC) Raíz. Las relaciones de confianza se construyen desde la AC de más confianza hasta las que tenga la ICP, donde no existe otra AC superior, que pueda firmar el certificado de la AC Raíz.

Este es el único caso, en el que la AC Raíz crea un certificado autofirmado por sí misma, para luego una vez acreditado ante SUSCERTE, según la Ley sobre Mensaje de Datos y Firma Electrónica (LSMDFE) firme el certificado electrónico de los PSC del sector público y privado además de la Lista de Certificados Revocados (LCR).

En el siguiente paso se encuentra las AC Subordinadas de la AC Raíz llamado PSC. Una vez acreditados ante SUCERTE según la LSMDFE, emitirán los certificados según el propósito de los certificados electrónicos especificados en su propia DPC y PC. Además de la LSMDFE, existe el Reglamento Parcial de la Ley sobre Mensajes de Datos y Firmas Electrónicas.

Es importante resaltar que el personal de SUSCERTE es el responsable de elaborar y su directiva de aprobar la presente DPC, así como sus modificaciones, siguiendo el modelo que la misma SUSCERTE proporciona para su elaboración. Si se considera necesario modificar la estructura, entonces la elegida será el modelo a seguir por todos los que soliciten ser PSC acreditados, además de evaluar la elaboración de la DPC de cada PSC de la ICP de Venezuela.

Al finalizar se tendrá en la DPC las especificaciones de los requisitos empleados por la AC Raíz, para la generación, publicación y administración de certificados de firma electrónica a los PSC subordinados basados en el RFC (Request for Comments) 2527. La RFC 2527[13] con titulo "Internet x.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" proviene del IETF[14] (Internet Engineering Task Force) donde se enumera las partes y requisitos necesarios para una DPC y Políticas de Certificados (PC).

IDENTIFICACIÓN

El documento de DPC se identificará con los siguientes campos:

- Nombre del documento
- Versión del documento
- Estado del documento
- Fecha de emisión

[13] RFC 2527 disponible en http://www.ietf.org/rfc/rfc2527.txt?number=2527

[14] IETF: es una organización internacional abierta de normalización que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, tales como transporte, encaminamiento, seguridad. Creada en EEUU en 1986.

- Identificador Único de Objeto (OID)

En particular, el **OID** se caracteriza por ser único y es 2 16 862 1 1.

COMUNIDAD DE USUARIO Y APLICABILIDAD

Las entidades que forman parte de la jerarquía de ICP, son:

Autoridad de Certificación (AC) Raíz

La AC Raíz es la Autoridad de Certificación origen de la jerarquía de certificación electrónica de la ICP en Venezuela, responsable de emitir los certificados que acreditan la validez de los PSC subordinados del sector público y privado.

Para proteger la AC Raíz ancla de confianza de la certificación electrónica, ella permanece por seguridad la mayor parte de su vida operativa fuera de línea (OFF-Line) con sus claves aseguradas en un dispositivo de hardware criptográfico seguro. Se destaca que se usa con poca frecuencia, ya que de forma esporádica se realiza la acreditación a un PSC.

Los PSC en la jerarquía de la ICP de Venezuela, emiten los certificados a los signatarios finales. Cada PSC debe elaborar su propia DPC y una Política de Certificados (PC) coherente con los tipos de certificados que emitirá y los requisitos generales establecidos por el Decreto-Ley sobre Mensaje de Datos y Firmas Electrónicas (LSMDFE), su Reglamento, el modelo de estructura del documento y otros que considere necesario SUSCERTE.

Autoridad de Registro (AR)

El modelo de funcionamiento define una AC Raíz, que opera en conjunto con la AR, la cual le envía directamente las solicitudes de firma a la AC Raíz.

Proveedor de Servicios de certificación (PSC) Subordinados

Las AC subordinadas son llamadas PSC por la LSMDFE, están subordinados en la jerarquía a la AC Raíz, donde requieren que la AC Raíz les firme su certificado para que ellos a su vez emitan certificados a los signatarios finales siguiendo con la cadena de confianza desde el punto raíz de la ICP de Venezuela. Cada uno de estos PSC debe elaborar su propia DPC y Política de Certificados coherente con los requisitos generales establecidos por la LSMDFE, su Reglamento y otros que considere necesario SUSCERTE.

Aplicabilidad

La AC Raíz emite los certificados firmados a los PSC que cumplen los requisitos establecidos en la LSMDFE y su Reglamento en paralelo con la emisión y firma de la Lista de de Certificados Revocados (LCR).

Así los PSC sólo podrán emplear su certificado para firmar sus entidades finales y la CRL en la ICP de Venezuela.

CONTACTOS

Cualquier sugerencia o pregunta relacionada con este documento deberá formularse a SUSCERTE.

Dirección: Av. Universidad, Esquina El Chorro. Torre MCT. Caracas - Venezuela
***Telf.*:** (058-212) 564.8028
Fax: (058-21) 564.5993
Sitio Web: www.suscerte.gob.ve/icp
(En estos momentos está en construcción)
***Correo Electrónico*:** superintendencia@suscerte.gob.ve

RESPONSABILIDADES DE PUBLICACIÓN Y REPOSICIÓN

OBLIGACIONES

Obligaciones de la Autoridad de Certificación (AC) Raíz

Asegurar la protección de las claves privadas de las autoridades de certificación de los PSC y de la misma AC Raíz.

- Verificar que los PSC cumplen los requisitos necesarios para ser miembros de la jerarquía de confianza de la ICP.
- Publicar en la página Web de SUSCERTE la DPC de la AC Raíz.
- Asegurar que su clave pública y la DPC están disponibles para cualquier interesado que lo requiera.
- Garantizar la adopción de las medidas necesarias para evitar la falsificación de los certificados electrónicos y de las firmas electrónicas que proporcionen.
- Realizar auditorías internas a la aplicación ICP de la AC Raíz
- Revocar o suspender el certificado de un PSC si se da alguna de las causas expuestas en la LSMDFE, su Reglamento o la DPC.

- Mantener un registro actualizado de los certificados de los PSC que han sido otorgados, revocados o suspendidos.
- Revocar o suspender aquellos certificados que habiendo sido emitidos, se sospeche o conozca que ha sido revelada la clave privada.
- Conservar toda la información y documentación relativa a los certificados, en medios electrónicos o magnéticos o lo que establezca la legislación vigente, para su consulta durante 10 años.

Obligaciones de la Autoridad de Registro (AR)

Sin contenido[15].

Obligaciones del Proveedor de Servicios de Certificación (PSC)

EL Proveedor de Servicios de Certificación (PSC) deberá:

1. Tener conocimiento de los pasos necesarios para la acreditación ante SUSCERTE.

2. Actuar con diligencia para evitar el uso no autorizado de su firma electrónica.

3. Garantizar y proteger sus claves privadas en dispositivos criptográficos.

4. Notificar a la AC Raíz que su firma electrónica ha sido indebidamente utilizada, cuando tenga conocimiento de ello.

5. Mantener el esquema de la arquitectura de Infraestructura de Clave Pública (ICP) con la jerarquía en forma de árbol, para las entidades que partan de ella.

6. Emitir, distribuir, revocar o suspender los certificados de las Autoridades de Certificación Subordinadas al PSC.

7. Elaborar su propia DPC y PC.

8. Cumplir con el Artículo 35 de las Obligaciones de los Proveedores del Capítulo VI de los Proveedores de Servicios de Certificación de la LSMDFE.

RESPONSABILIDADES

Responsabilidad de la Autoridad de Certificación (AC) Raíz

La Autoridad de Certificación asume el cumplimiento de las obligaciones que le impone la legislación aplicable y el procedimiento de emisión de los certificados, establecido en las presentes condiciones de utilización de los certificados aceptadas por los signatarios.

Debe revocar cualquier certificado en cuanto le sea notificado o se detecte compromiso o mal uso del mismo, algún incumplimiento de los requisitos establecidos LSMDFE.

---

[15] Cuando en el apartado se tiene "Sin contenido", se hace la referencia a él, porque es parte de la estructura del modelo DPC que hizo en el trabajo de grado Marifrancy Falcón (2005), pero para la DPC de la AC Raíz de la ICP de Venezuela ese apartado no aplica.

Debe proteger la clave privada de la AC Raíz, mediante el uso de un módulo criptográfico que cumpla con el estándar FIPS 140-2 nivel 3[16].

La AC Raíz debe permanecer fuera de línea (Off-Line) a partir de ella la jerarquía de los PSC ante la Raíz, se encuentran todos en línea.

La AC Raíz no responderá por los daños y perjuicios que se deriven de las actuaciones negligentes o dolosas por parte de terceros con relación a los certificados por él emitidos en favor de un determinado signatario.

Responsabilidad de la Autoridad de Registro (AR)

Sin contenido.

RESPONSABILIDAD FINANCIERA

Sin contenido

Responsabilidad financiera de la Autoridad de Certificación (AC) Raíz

Sin contenido.

[16] El HSM está validado conforme a lo establecido en la Norma Federal de Procesamiento de la Información (FIPS) 140-2 Nivel 3. Este nivel impide la exportación de claves fuera del sistema, por lo

INTERPRETACIÓN Y LEGALIDAD

Legislación aplicable

Para la AC Raíz no aplica ningún tipo de legislación por tratarse de la autoridad de certificación raíz de la ICP de la nación venezolana. Sin embargo, debe cumplir con todas las normas, políticas, lineamientos y estándares internacionales en la materia.

Por otro lado los PSC acreditados deben seguir la LSMDFE, su reglamento, los estándares internacionales, las normas y procedimientos de acreditación, auditorías, y otros que SUSCERTE considere necesario.

Formación de Interpretación y aplicación

Sin contenido.

Procedimientos de resolución de conflictos

Sin contenido.

---

que la clave privada utilizada durante la emisión del certificado a los PSC es totalmente inaccesible.

ARANCELES

La AC Raíz de la ICP de Venezuela no está sujeta al pago de aranceles. Sólo los PSC acreditados ante la SUSCERTE, son los que están obligados a cumplir con las tasas impuestas en la LSMDFE.

Está especificado en el Artículo 24 Capítulo V de la LSMDFE la tasa que la Superintendencia de Servicios de Certificación Electrónica cobrará a los PSC. Los PSC constituidos por entes públicos de la nación venezolana estarán exentos del pago de las tasas de este artículo.

Tasas de registro por la expedición y renovación de Acreditación

En este caso específico, por tratarse de la AC Raíz, son las AC subordinadas a ella, es decir PSC, los que deben pagar las tasas de registro por la expedición y renovación de acreditación ante SUSCERTE.

1. Por la acreditación de los PSC, AC subordinadas de la AC Raíz de Venezuela, SUSCERTE cobrará una tasa de un mil unidades tributarias (1.000 U.T).

2. Por la renovación de la acreditación de los PSC se cobrará una tasa de quinientas unidades tributarias (500 U.T).

Tasas de registro por cancelación de Acreditación

Por la cancelación de la acreditación de los PSC ante SUSCERTE, se cobrará una tasa de quinientas unidades tributarias (500 U.T).

Tasas de registro por los certificados otorgados por PSC extranjeros

A Los PSC extranjeros, se cobrará una tasa de quinientas unidades tributarias (500 U.T).

PUBLICACIÓN Y REPOSITORIOS

Publicación de información del la AC Raíz

Los interesados pueden acceder, a través de un servidor Web, al repositorio de la AC Raíz https://www.suscerte.gob.ve/icp donde se publicará la siguiente información:

- Lista de Certificados Revocados (LCR)
- Políticas de Certificados (PC)
- La clave pública de la AC Raíz
- Versiones anteriores y actualizadas de la DPC
- Los datos de contacto de SUSCERTE
- Manual de procedimientos de la AC Raíz.
- Toda otra información considerada relevante a los certificados emitidos
-

Frecuencia de publicación

Lista de Certificados Revocados

La Lista de Certificados Revocados (LCR) se publicará con la frecuencia establecida en el punto 5.4.4.9.

Declaración de Prácticas de Certificación

La AC Raíz publicará en el repositorio, las nuevas versiones de la DPC[17], inmediatamente tras la aprobación de la misma.

Clave Pública

El certificado de la AC Raíz se encuentra publicado en el repositorio. En el caso de generar un nuevo certificado autofirmado, se procederá a publicarlo, inmediatamente, en el servidor Web.

Controles de acceso a la información

El acceso a la información publicada por la AC Raíz sólo será de consulta y no podrá ser modificada por terceros. Solo será actualizada por el personal encargado de esta función que labora en SUSCERTE.

Además se garantiza la consulta de la LCR[18], PC[19] correspondiente y a su manual de procedimientos, DPC en sus versiones anteriores y actualizadas.

Repositorios

El repositorio de la AC Raíz es de disponibilidad pública para consulta, además de brindar integridad, es decir no puede ser modificado.

[17] Declaración de Prácticas de Certificación.
[18] Lista de Certificados Revocados.
[19] Política de Certificados.

AUDITORÍAS

Este componente indica los aspectos específicos al proceso de auditoría.

Frecuencia del cumplimiento de las auditorías

La AC Raíz se somete periódicamente a auditorías internas, con el objeto de evaluar el grado de cumplimiento de las políticas definidas en esta DPC.

Auditores

Las auditorías son realizadas por expertos técnicos de reconocido prestigio como los auditores que estén inscritos en el Registro de Auditores de SUSCERTE.

Contenido de las auditorías

Son objeto de auditoría todos los requisitos técnicos, funcionales y organizativos entre ellos:

- La DPC y PC utilizadas.
- Políticas de seguridad.
- Administración de la AC Raíz
- Consideraciones de confidencialidad.
- Seguridad física.
- Modelo de respaldo.
- Plan de contingencia y recuperación ante desastres.

- Plan de continuidad de las actividades.
- Personal operativo.

Resultados de la auditoría

Si el resultado de la auditoría detecta cualquier anomalía, la AC Raíz se compromete a subsanarla en el menor tiempo posible.

Comunicación de resultados

El resultado de la auditoría es considerado confidencial conforme a lo previsto en el siguiente punto.

CONFIDENCIALIDAD

La AC Raíz se compromete a proteger todos los datos a los que tenga acceso como consecuencia de su actividad como entidad de certificación de la ICP de Venezuela.

No obstante, AC Raíz se reserva el derecho a revelar a los empleados y consultores, externos o internos, los datos confidenciales necesarios para realizar sus actividades como AC Raíz. En este caso los empleados y/o consultores son informados sobre las obligaciones de confidencialidad.

Estas obligaciones no se aplican si la información calificada como “confidencial” es requerida por los tribunales u órganos administrativos competentes o impuesta por una ley.

Información confidencial

Se considera información confidencial:

- Información de registro. Todos los datos relativos al registro de certificados son considerados confidenciales.
- Información sobre la vida de los certificados. Todos los datos relativos a la emisión y revocación (salvo su publicación en la LCR) de certificados de los PSC.

Información no confidencial

Se considera información no confidencial:

- Contenido de los certificados emitidos
- Lista de Certificados Revocados (LCR)
- La clave pública de la AC Raíz
- Las versiones de la DPC
- Las Políticas de Certificado (PC)

- Los siguientes documentos: informes de auditoría, plan de contingencia y recuperación ante desastres, plan de seguridad de sistemas y en general cualquier documento que la AC Raíz requiera para su operación.
- La LSMDFE y su Reglamento Parcial.
- Cualquier otra información que SUSCERTE considere como pública.

Publicación de información sobre la revocación o suspensión de un certificado

La AC Raíz publica en su portal Web un listado de los certificados revocados (LCR) en la siguiente dirección electrónica: http://www.suscerte.gob.ve/lcr

Divulgación de información a autoridades judiciales

La AC Raíz puede revelar datos calificados como confidenciales a la autoridad judicial pertinente que lo requiera formalmente.

Divulgación de información como parte de un proceso judicial o administrativo

La AC Raíz puede revelar datos calificados como confidenciales a la autoridad judicial pertinente que lo requiera formalmente.

Divulgación de información por solicitud del titular

La AC Raíz puede revelar datos calificados como confidenciales (por ejemplo resultado de su auditoría) a petición del PSC que lo requiera formalmente.

Otras circunstancias de divulgación de información

Sin contenido.

DERECHOS DE PROPIEDAD INTELECTUAL

La propiedad y los derechos de propiedad intelectual del Documento de Prácticas son de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) organismo adscrito al Ministerio de Ciencia y Tecnología (MCT) de Venezuela.

IDENTIFICACIÓN Y AUTENTICACIÓN

REGISTRO INICIAL

Tipos de nombres

La AC Raíz sólo genera y firma certificados con un DN (Distinguished Name) autenticado del estándar X. 500.

El DN de los certificados electrónicos debe proporcionar al menos los siguientes:

EJEMPLOS	
Nombre del emisor del certificado	**Nombre del sujeto**

Identifica la AC que generó y firmó el certificado. El DN de los certificados electrónicos asociado al emisor está compuesto por los siguientes atributos, por ejemplo:	Identifica la entidad o individuo asociado con el certificado. El DN de los certificados electrónicos asociado al sujeto está compuesto por los siguientes atributos, por ejemplo:
E = superintendencia@suscerte.gob.ve OU = Sistema Nacional de Certificación Electrónica O = SUSCERTE ST = Caracas L = Caracas C = VE CN = rootca	E = cnsi@funmrd.gob.ve OU = Sistema Nacional de Certificación Electrónica O = CNSI ST = Mérida L = Mérida C = VE CN = PSCMerida

SUSCERTE establece como política la emisión de un tipo de certificado que por tratarse de la AC Raíz será identificado por un OID (Object Identifier) único, incluido en el certificado, dentro de la extensión X509 Certificate Policies

Tipo Certificado Autoridad

Los certificados de Autoridad se emitirán a entidades que se constituyen en AC, dentro de la jerarquía de la ICP de Venezuela llamados Proveedor de Servicios de Certificación (PSC), y a la AC Raíz, cuyo único certificado es autofirmado por tratarse de un caso especial como la raíz o ancla de confianza de la ICP de Venezuela.

Necesidad de nombre significativos

La AC Raíz verifica que sean apropiados los siguientes nombres de los PSC:

- **CommonName**: Debe corresponder a la unidad operativa responsable del servicio.

- **OrganizationalUnitName**: Puede contener a las unidades operativas relacionadas con el servicio.

- **OrganizationName**: Debe coincidir con la inscripción en el Registro Mercantil (para personas jurídicas) o con la denominación oficial del organismo (para Organismo Públicos).

Reglas para la interpretación de nombres

Las reglas aplicables para el tratamiento de nombres corresponderán a lo indicado en el estándar X.500 de referencia en la ISO/IEC 9594.

Unicidad de nombres

El DN de los certificados de los PSC subordinados es único e inequívoco.

Procedimiento de resolución de disputas sobre nombres

La AC Raíz no tiene responsabilidad en el caso de disputas de nombres. La AC Raíz no deberá determinar que un solicitante de certificados tiene derecho sobre el nombre que aparece en una solicitud de certificado. Asimismo, no actuará como árbitro o mediador, ni de ningún otro modo deberá resolver disputa alguna concerniente a la propiedad de nombres de personas u organizaciones, nombre de dominio, marcas o nombres comerciales.

La AC Raíz se reserva el derecho de rechazar una solicitud de certificado debido a conflicto de nombres.

Reconocimiento, autenticación y rol de las marcas registradas

Sin contenido.

Método para probar la posesión de la clave privada

La clave privada asociada al certificado electrónico emitido por la AC Raíz autofirmado, es siempre generada exclusivamente en el hardware criptográfico, donde se encuentra la AC Raíz. El método de prueba de posesión de la clave privada será PKCS#10.

Autenticación de la identidad de personas jurídicas, organismos públicos o aplicaciones.

El mecanismo específico utilizado para autenticar las identidades de los PSC del sector público o privado requerirá la presencia física de los representantes de los mismos, está expresado en las normas de acreditación de SUSCERTE. La norma se llama "procedimiento de entrega de la credencial al representante legal del solicitante" disponible en www.suscerte.gob.ve/icp/normas.

Autenticación de la identidad de personas físicas.

La autenticación requerirá la presencia física de los individuos, verificando los datos identidad para culminar con la emisión del certificado y siguiendo lo especificado en el apartado 5.3.1.8.

GENERACIÓN DE NUEVO PAR DE CLAVES

Para generar el par de claves de la AC Raíz se realiza la "ceremonia de claves". En la ceremonia primero se deben generar las claves de los tres operadores y tres administradores del HSM de la AC Raíz, en las tarjetas inteligentes. Una vez listo, se inicia la generación de las claves con la autenticación de al menos dos operadores de los tres operadores del HSM. La configuración del HSM es "No permanente" y esto quiere decir que es necesario permanecer en el lector USB del HSM, conectada la ultima tarjeta inteligente del último operador autenticado para poder crear las claves de la AC Raíz, porque sino se cierra la comunicación de la aplicación de la AC Raíz con el HSM. Una vez establecido el canal de comunicación entre la AC Raíz y el

HSM, entonces se genera el par de claves desde la aplicación de la AC Raíz, quedando resguardada la clave privada en el HSM y la clave pública en el repositorio de acceso público.

Los PSC también generan su par de claves siguiendo el proceso utilizado por la AC Raíz, con la diferencia que le envían la solicitud de firma de certificado a la AC Raíz, una vez firmado ésta bajo la jerarquía de la ICP de Venezuela.

GENERACIÓN DE NUEVO CERTIFICADO (POSTERIOR A REVOCACIÓN)

Al momento de sospechar la invalidez del certificado electrónico de la AC Raíz, se debe informar a todos los PSC acreditados, para generar de nuevo la ceremonia de claves de la AC Raíz y firmar de nuevo los certificados de los PSC.

La revocación del certificado electrónico del PSC tiene como consecuencia principal la terminación inmediata del período operativo del certificado electrónico, el que legalmente pasa a ser **No Valido**, ver apartado 5.4.4.3.

REQUERIMIENTO DE REVOCACIÓN

La revocación del certificado electrónico responderá a cualquiera de los siguientes casos:

- Solicitud de suspensión temporal del PSC.

- Culminación del periodo de validez del certificado.
- Cuando el certificado del PSC posee datos falsos.
- Cuando es solicitado por una autoridad competente de conformidad con la ley.
- Por incumplimiento de obligación principal derivada del contrato de acreditación del PSC ante SUSCERTE.
- Por ser vulnerado el sistema de seguridad del PSC que afecte la integridad y confiabilidad del certificado electrónico.

CICLO DE CERTIFICADO: REQUERIMIENTOS OPERATIVOS

REQUERIMIENTO DE CERTIFICADO

Los procedimientos operativos establecidos por SUSCERTE para la acreditación son efectuados por los PSC bajo una solicitud siguiendo un proceso de acreditación en forma personal dirigiéndose ante las oficinas de SUSCERTE o a través de la solicitud de acreditación visitando la dirección electrónica:

http://150.180.8.235:8080/suscerte_cliente.

Una vez aprobada la solicitud por la directiva de SUSCERTE significa que el PSC debe presentar las garantías necesarias para obtener la acreditación como PSC de la ICP de Venezuela, y en la cadena de confianza, pasa a ser una AC Subordinada de la AC Raíz.

La acreditación de los PSC establece que los mismos operan en conformidad con las políticas y procedimientos establecidos por SUSCERTE.

EMISIÓN DEL CERTIFICADO

La información necesaria para la solicitud de la acreditación de los PSC ante SUSCERTE que gestiona la AC Raíz de la ICP de Venezuela son los que se establecen en el Articulo 3 del Reglamento Parcial del Decreto Ley sobre Mensajes de Datos y firmas Electrónicas.

ACEPTACIÓN DEL CERTIFICADO

Presentadas las garantías y verificadas por la SUSCERTE, ésta procederá a realizar la acreditación al PSC mediante la publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

En el Artículo 31 de la LSMDFE, se especifica los requisitos que debe cumplir el PSC.

SUSPENSIÓN Y REVOCACIÓN DE CERTIFICADOS

Causas de revocación

Las causas de revocación de un certificado de PSC son las siguientes:

4. Revelación de la clave privada de la AC Raíz.

5. Revelación o sospecha de la clave privada asociada al certificado del PSC.

6. Cuando el PSC solicite a la AC Raíz la suspensión temporal de su certificado.

7. Cuando el PSC tenga conocimiento del uso indebido de la firma electrónica.

8. Por resolución judicial o administrativa que lo ordene.

Autorizados a solicitar la revocación

Son autorizados a solicitar la revocación de acreditación de un PSC de la ICP de Venezuela, los siguientes entes:

- Autoridad competente de conformidad con la ley.
- El mismo PSC.

El procedimiento para la solicitud de revocación de un PSC ante SUSCERTE es:

***Primero**, la Dirección de Registro y Acreditación (DRA) de SUSCERTE:*

- Recibe del directorio la resolución donde se determina la suspensión de la acreditación de un PSC.
- Acata la instrucción donde se le solicita participe al PSC de la resolución tomada.

***Luego**, el PSC:*

- Recibe la notificación de suspensión de la acreditación como PSC, resuelta por el Directorio de SUSCERTE.

- Suspende de inmediato la negociación con nuevos usuarios, manteniendo el servicio de los signatarios existentes, hasta nuevo aviso.

- Decide acción para solventar la problemática, en función del razonamiento dado por el Directorio a la suspensión:

  - Acata medida por estar de acuerdo con la misma.

  - U objeta decreto de suspensión de su acreditación por el directorio.

- Expone planteamiento ante SUSCERTE.

***Entonces**, la DRA[20] de SUSCERTE conviene con el PSC sobre las acciones a llevar a cabo, de acuerdo a su planteamiento de:*

- Acordar el mecanismo para activar la suspensión de la que fue objeto, en el lapso de los quince días que tiene para ello.

- O recibir sus fundamentos en contra de la suspensión de la Acreditación, utilizando los diez días que la Ley Orgánica de Procedimientos Administrativos (LOPA) le asigna para exponer alegatos.

***Después**, El PSC:*

Ejecuta las acciones convenidas con la DRA de SUSCERTE:

- Envía a SUSCERTE plan de mejoras para solventar la problemática que originó la suspensión de su acreditación, si está de acuerdo con la decisión del directorio.

[20] Dirección de Registro y Acreditación

- O remite a SUSCERTE informe justificando las razones de su desacuerdo ante suspensión de la acreditación.

***Entonces**, la DRA de SUSCERTE:*

- Recibe del PSC las comunicaciones y soportes de sus planteamientos y actúa en consecuencia:
  - Presenta al Directorio el plan de mejoras del PSC interesado en reactivar su acreditación.
  - O presenta al directorio los fundamentos del PSC, donde alega inconformidad con la decisión del directorio justificando su motivación.

***El Directorio** de SUSCERTE*:

- Admite los documentos del PSC, decidiendo en consonancia con las sustentaciones**:**
  - Ajusta y aprueba el plan de mejoras del PSC, autorizándolo para su aplicación en el tiempo determinado, apoyando su ejecución para solucionar el estado de suspensión de la acreditación.
  - O analiza reclamo interpuesto por el PSC:
    - Reafirma la suspensión de la acreditación, al comprobar nuevamente los incumplimientos que la originaron.

- O reajusta la decisión, si los alegatos del PSC tienen fundamento, reactivando la acreditación por medio de una resolución.

- Participa a la DRA de SUSCERTE las disposiciones.

- Autoriza a la DRA de SUSCERTE el envío de comunicación informativa al PSC.

***Entonces**, la DRA de SUSCERTE:*

- Comunica al PSC decisión del directorio:

  - Insta al PSC para que ponga en práctica el plan de mejoras aprobado por el Directorio.

  - O informa en relación a su reclamo:

    - Señala que su acreditación continúa suspendida, y de no aplicar algún plan de mejoras, le será revocada, destacando el tiempo que le queda para ello.

    - O da parte de la resolución emitida por el directorio, donde reactiva la acreditación suspendida.

***Y** el PSC:*

- Recibe notificación de la DRA de SUSCERTE:

  - Inicia las mejoras que tiene que efectuar, para solventar la problemática que originó la suspensión de su acreditación, si está de acuerdo con la decisión del Directorio.

- Resuelve, con relación a su reclamo:
    - Elaborar un plan de mejoras, para evitar la revocación de su acreditación, en el tiempo que le queda para ello.
    - Reiniciar sus actividades ordinarias.
- Informa a la DRA de SUSCERTE los resultados de su gestión.

***Finalmente** la DRA de SUSCERTE:*

- Periódicamente verifica la situación del PSC en relación con el estado de la suspensión de la acreditación y las acciones en ejecución y actúa de acuerdo:
    - Reactiva la acreditación del PSC que logra cumplir con todos los requisitos y obligaciones exigidos por el Decreto-Ley 1.204, Reglamento Parcial y Normas de SUSCERTE.
    - O revoca la acreditación del PSC que incumple con los requisitos y obligaciones exigidos por el Decreto-Ley 1.204, Reglamento Parcial y Normas de SUSCERTE.

Plazo para la solicitud de revocación

Es el mismo del apartado 5.4.4.1

Causas de suspensión

Sin contenido.

Autorizados a solicitar la suspensión

Sin contenido.

Procedimientos para la solicitud de suspensión

Los pasos para la solicitud de suspensión del servicio del PSC ante SUSCERTE, son:

Primero**, la DRA de SUSCERTE:**

- Recibe del PSC, con la antelación prevista, el plan de mantenimiento y/o mejoras a sus instalaciones, equipos y sistemas, con anexo del cronograma de suspensión temporal del servicio por tales actividades.
- Revisa la planificación de las actividades y el cronograma de suspensión temporal para comprobar la correspondencia entre ambos, siempre pendiente de no permitir que se exceda de los lapsos previstos.
- Solicita al PSC que ajuste la planificación y el cronograma, de no estar conforme.
- Aprueba el plan y el cronograma, cuando estos se adecuen a las disposiciones del Decreto-Ley 1.204 y a las normativas internas de SUSCERTE.
- Envía al PSC el plan y el cronograma de suspensión del servicio temporal aprobados, autorizándolo para ejecutar dicha suspensión en la fecha y hora programada, por el período acordado.

***Luego**, el PSC*:

- Recibe de SUSCERTE el plan y el cronograma de suspensión del servicio prestado.
- Envía a sus signatarios el cronograma de suspensión del servicio, aprobado por SUSCERTE.
- Remite a SUSCERTE ejemplar de la notificación con la cual informó a sus signatarios del cronograma de suspensión del servicio.

***Después**, la DRA* de SUSCERTE:

- Recibe un ejemplar de la notificación donde los signatarios del PSC son informados del cronograma de suspensión temporal del servicio.
- Queda pendiente de controlar las acciones a realizar por el PSC para suspender el servicio, en la fecha y hora aprobadas.

***Y el** PSC*:

- Envía comunicación a sus signatarios donde les notifica la fecha y hora de la suspensión del servicio.
- Remite ejemplar a SUSCERTE de la notificación enviada a sus signatarios.
- Suspende el servicio en su oportunidad, en la fecha y hora establecidas.
- Reinicia el servicio, cumpliendo con el lapso aprobado para la suspensión.

- Informa a sus signatarios del reinicio del servicio.
- Despacha a SUSCERTE un ejemplar de la notificación del reinicio del servicio que le enviará a sus signatarios.

Finalmente *la DRA de SUSCERTE*:

- Recibe del PSC copia de la notificación del reinicio del servicio.
- Constata cumplimiento de la programación establecida.
- Participa al PSC la adecuada aplicación de las disposiciones legales y normativas de SUSCERTE.
- Queda a la espera de la próxima programación de la suspensión del servicio por parte del PSC.

Límites del periodo de suspensión de un certificado

En un plazo no mayor a cuarenta y ocho horas.

Frecuencia de emisión de la LCR

La AC Raíz dispone de un servidor Web accesible desde Internet para cualquiera que necesite consultarlo. El acceso a la información del servidor está disponible 24 horas al día, 7 días a la semana.

Los certificados revocados permanecen insertados en la LCR hasta la fecha de caducidad que se especificó en su emisión. La frecuencia de emisión de cada LCR es de cada seis meses, salvo que se revoque un certificado, en cuyo caso se emite una nueva LCR inmediatamente.

La LCR indica la fecha de publicación de la siguiente lista y sus puntos de distribución específicos. La LCR es emitida y firmada por la AC Raíz.

Requisitos para verificación de la LCR

La información relativa al estado de los certificados LCR de los PSC se encuentra disponible en la siguiente dirección: www.suscerte.gob.ve/icp/lcr.

Disponibilidad en línea del servicio de revocación del estado del certificado

Sin contenido.

Requisitos para la verificación en línea del estado de revocación

Sin contenido.

Otras formas disponibles para la divulgación de la revocación

A través de la dirección electrónica www.suscerte.gob.ve/icp y en la Gaceta Oficial de la República Bolivariana de Venezuela.

Requisitos para la verificación de otras formas de divulgación de revocación

Sin contenido.

Requisitos específicos para casos de revelación de claves

Sin contenido.

PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

La AC Raíz almacena registros electrónicos de eventos (logs) relativos a su actividad como entidad de certificación de la ICP de Venezuela.

Estos registros son guardados, de manera automatizada y en los demás casos en formato papel u otros medios. Están a disposición del auditor en los casos en que sea necesario.

Tipos de eventos registrados

Cada registro de eventos incluye datos relativos a:

- Fecha y hora en que se produjo
- Número de serie o secuencia de entrada en el registro
- Identificación del personal según su rol que introdujo el evento

Los eventos que registra la AC Raíz son los siguientes

1. *Eventos de sistema*:

   - Instalación del Sistema Operativo
   - Instalación del software de la AC Raíz
   - Instalación de los módulos de hardware criptográfico (HSM)
   - Cambio de módulo de hardware criptográfico (HSM)
   - Eliminación del módulo criptográfico
   - Sistema de inicio del software de la AC Raíz
   - Intentos de acceso a la AC Raíz
   - Configuración de cambios al equipo de la AC Raíz, en concreto:

     ✓Hardware

     ✓Software

     ✓Sistema Operativo

     ✓Usuarios

     - Perfiles de seguridad

     ✓Privilegios de administrador

     ✓Auditorías

2. *Acceso físico:*

- Acceso del personal a la sala segura
- Acceso del personal al sistema
- Conocimiento o sospecha de violación de la seguridad física

3. *Anomalías inesperadas:*

- Fallas en el chequeo de la integridad del software;
- Ataques a la red (confirmados o bajo sospecha);
- Fallas en la red
- Fallas en el equipamiento
- Fallas de energía
- UPS cíclica
- No cumplimiento de las Prácticas de Certificación
- Reinicio del Sistema Operativo

4. *Acciones de los operadores de AC Raíz:*

- Gestión de cuentas
- Realización de copias de seguridad de las bases de datos
- Almacenamiento de las bases de datos
- Manipulación de registros
- Envío al directorio de cualquier documento o archivo;

- Acceso a las bases de datos
- Firma de las tablas que utiliza en la aplicación
- Uso indebido de las claves privadas
- Acciones tomadas en respuesta a cualquier solicitud
- Carga de la tarjeta inteligente con certificados
- Envío de las claves al modulo criptográfico

Notificación de las auditorías

Cada vez que se audita un evento, el administrador de seguridad no informa previamente al autor del mismo. Sin embargo, cuando un operador conoce algún evento susceptible de auditoría, debe informar inmediatamente al administrador de seguridad para que proceda en función de la gravedad del evento.

Evaluación de las vulnerabilidades

La AC Raíz dispone de un documento interno denominado "Políticas de Seguridad (PS)" del Centro de Cómputo de Datos de SUSCERTE, disponible en www.suscerte.gob.ve/ps, en el que se especifican las medidas de seguridad adoptadas para evitar el acceso no autorizado al sistema de gestión de certificados, así como la evaluación periódica de los riesgos y vulnerabilidades detectadas.

ARCHIVO DE REGISTROS

La política de archivo de registros de AC Raíz es la siguiente:

Tipos de registros archivados

1. *Respecto al ciclo de vida de las claves de AC Raíz.*

   - Generación de las claves de la AC Raíz
   - Instalación de las claves criptográficas
   - Copia de respaldo de las claves
   - Almacenamiento de las claves
   - Recuperación de las claves criptográficas
   - Depósito de las claves
   - Uso de las claves
   - Destrucción de claves
   - Custodia de claves y de aparatos o cualquier otro soporte de claves

2. *Relacionados con el ciclo de vida de los certificados:*

   - Recepción de solicitudes para certificados
   - Sometimiento de claves públicas para certificación
   - Generación de certificados
   - Distribución de las claves públicas
   - Revocación de certificados
   - Solicitudes de validación de certificados y respuestas

3. *Relacionados con el ciclo de vida de los dispositivos criptográficos:*

- Recepción de dispositivos
- Entrada o traslado al lugar de almacenamiento
- Uso de dispositivos
- Desinstalación de dispositivos
- Designación del dispositivo para el servicio o reparación
- Retiro de dispositivos

4. *Otros:*

- Actualización de la DPC
- Modificaciones de las obligaciones contractuales
- Trazas de auditoría
- Accesos y modificaciones de la documentación solicitada por los auditores.

Período de conservación de los archivos

Las trazas de los archivos son conservadas durante un período de diez años.

Protección de los archivos

Las medidas de seguridad definidas están destinadas a proteger los archivos de accesos (internos o externos) no autorizados, de modo que sólo ciertas personas pueden consultar, modificar o eliminar los archivos.

Los archivos son almacenados en un lugar seguro fuera de las instalaciones con las mismas medidas de seguridad tomadas en el centro principal de cómputo, necesarias para protegerlos de factores naturales.

Procedimientos de respaldo de archivos

En el documento "Políticas de Seguridad" disponible en www.suscerte.gob.ve/ps, se definen los procedimientos empleados para realizar copias de seguridad de todos los archivos.

Requisitos de sellado de tiempo de los registros

Por los momentos los registros no llevan sellado de tiempo porque no se dispone de la Autoridad de Estampado de Tiempo en Venezuela. Este servicio incluirá la fecha y la hora exacta que emite el Observatorio Cajigal de Venezuela organismo encargado de garantizar la hora legal en Venezuela en los documentos electrónicos.

Sistema de recopilación de archivos

La recopilación y almacenamiento de los archivos es realizado por personal cualificado autorizado por SUSCERTE conforme al procedimiento definido en las "Políticas de Seguridad" disponible en www.suscerte.gob.ve/icp/ps.

Procedimientos para verificar y obtener información de archivos

El contenido de los archivos es recabado y verificado conforme al procedimiento definido en las "Políticas de Seguridad" de SUSCERTE disponible en www.suscerte.gob.ve/ps.

CAMBIO DE CLAVES

Las claves de los certificados emitidos por AC Raíz dejarán de tener validez en el mismo momento en que lo haga su certificado autofirmado. Una vez expirado, la AC Raíz generará un nuevo certificado.

PLAN DE RECUPERACIÓN ANTE DESASTRES

Los requisitos de notificación y los procedimientos de recuperación en caso de compromiso de la clave privada o desastre se activan en los siguientes casos:

Los recursos hardware, software, y/o datos fueron o existe sospecha de haber sido modificados

La AC Raíz dispone de un plan de continuidad de actividades que le permite seguir operando si el hardware, software y/o los datos son alterados (pero no destruidos). También actualiza periódicamente este plan con el fin de asegurar su vigencia en todo momento.

El plan incluye los procedimientos necesarios para garantizar la continuidad de la actividad durante el período de tiempo transcurrido entre el desastre y el restablecimiento de la situación original (dando prioridad a la publicación de las LCR).

Debilitamiento de la clave privada de la AC Raíz

En el plan de continuidad de la AC Raíz es considerado la revelación de su clave privada como un desastre. En este caso en el documento se prevé la publicación y difusión, inmediatamente, de la revocación de su certificado electrónico con el objeto de no confiar más en el mismo.

La clave pública de la AC Raíz es revocada

El plan de continuidad de la AC Raíz prevé la revocación del certificado electrónico como consecuencia inmediata de la divulgación de la clave privada.

Seguridad de las instalaciones tras un desastre natural o de otro tipo

La AC Raíz dispone de sitios externos para mantener almacenadas las copias de seguridad, para minimizar los efectos en caso de desastre natural o de otro tipo sobre las instalaciones primarias.

CESE DE ACTIVIDAD

La AC Raíz no podrá nunca culminar de sus actividades de servicios de certificación porque se trata de la raíz única de la jerarquía de confianza de la ICP del país. En caso de estar divulgada su clave privada deberá inmediatamente crear un nuevo certificado electrónico autofirmado y firmar los certificados vigentes de los PSC acreditados.

CONTROLES DE SEGURIDAD FÍSICA, FUNCIONALES Y PERSONALES

CONTROLES DE SEGURIDAD FÍSICA

Las políticas y procedimientos de seguridad de la AC Raíz se enmarcan dentro de la documentación de las políticas y normas de seguridad de SUSCERTE. Esto es a consecuencia de compartir recursos e instalaciones en el Centro de Cómputo de Datos de SUSCERTE.

En términos generales estas políticas (definidas en un documento interno denominado "Políticas de Seguridad") disponible en www.suscerte.gob.ve/ps, regulan el desarrollo de las normas y procedimientos de seguridad, que se pueden resumir en las medidas adoptadas más relevantes descritas en los siguientes apartados:

Localización y construcción

Las instalaciones de la AC Raíz están protegidas físicamente con todas las medidas de seguridad necesarias para salvaguardar la información y los equipos ubicados en la infraestructura de la torre MCT.

Para ello la ubicación y el tipo de construcción, así como otras medidas de seguridad, tales como bóveda o bunker (estructuras fuertes utilizadas para el resguardo físico), cámaras de circuito cerrado, sistema de alarmas, garantizan una protección adecuada contra el acceso no autorizado a los equipos y la información de la AC Raíz.

Acceso físico

El acceso físico a las instalaciones de la AC Raíz está protegido por diversos controles de acceso, de modo que sólo el personal autorizado puede ingresar a las mismas. Estos controles están basados en la identificación de nivel 2 con tarjeta inteligente, nivel 3 de huella biométrica, con sistemas de video de circuito cerrado de televisión todos los días del año (es decir 24x365), adecuados para registrar cada uno de los accesos a las instalaciones, archivando periódicamente los mismos.

Los controles específicos, el personal que debe estar autorizado, el número de accesos permitidos, la tecnología empleada y demás aspectos relativos al acceso físico se encuentra definidos en el documento "Políticas de Seguridad" del Centro de Cómputo de SUSCERTE disponible en www.suscerte.gob.ve/ps.

Electricidad y aire acondicionado

Los armarios donde están ubicados los equipos cuentan con las condiciones de potencia y ventilación necesarias para evitar fallas de potencia u otras anomalías eléctricas o en los sistemas.

El cableado de los equipos está protegido para evitar intercepciones o daños y se han adoptado medidas especiales para evitar la pérdida de información provocadas por la interrupción en el flujo de suministro eléctrico, conectando los componentes más críticos a UPS para asegurar un suministro continuo de energía eléctrica, con una potencia suficiente para mantener la red eléctrica funcionando y para proteger a los equipos frente fluctuaciones eléctricas que los pudieran dañar.

Exposiciones al agua

La instalación de la AC Raíz está protegida para evitar las exposiciones al agua, mediante detectores de humedad, inundación y otros mecanismos de seguridad apropiados al medio.

Prevención y protección contra el fuego

La instalación de la AC Raíz cuenta con sistema de detección y extinción de incendios para aminorar cualquier emergencia posible.

Medios de almacenamiento

La AC Raíz cuenta con un lugar de almacenamiento interno y externo con acceso restringido por personal autorizado, donde se guarda toda la información, registros y copias de seguridad generada.

5.5.1 Eliminación desechos

La AC Raíz mantiene mecanismos de revisión de todos los materiales desechables donde se almacena información (disco extraíble, papel, cintas de respaldo, etc.) los cuales son chequeados, antes de su eliminación o reutilización, con el objeto de comprobar si contienen información sensible, siendo físicamente destruidos, salvo que puedan reutilizarse como medio de soporte, en cuyo caso se elimina la información de manera segura.

Almacenamiento de las copias de seguridad

Todas las copias de seguridad son almacenadas en otro edificio ubicado en otro estado del país, con una replica de la AC Raíz. Este segundo edificio está protegido con los medios y mecanismos de seguridad definidos anteriormente.

CONTROLES FUNCIONALES

Roles de confianza

La AC Raíz cuenta con un personal que por sus actividades es sometido a procedimientos de controles especiales debido a que su actividad es esencial para el correcto funcionamiento de la ICP de Venezuela. Tienen la condición de roles de confianza:

- Administrador de Seguridad: Responsable de implementar las prácticas de seguridad, así como aprobar la generación y revocación de certificados
- Administrador de Sistemas: Autorizado para instalar, configurar y mantener el sistema de ICP para el registro, emisión y revocación de certificados, así como la provisión de los dispositivos de generación de claves.
- Operadores de Sistemas: Responsables de utilizar el sistema operativo y de realizar copias de seguridad y recuperación
- Auditores de Sistemas: Autorizados para visualizar y mantener los archivos y logs de auditoría de los sistemas del PSC.

- Administradores del HSM (Modulo Hardware Seguro): Encargados de la definición de claves de administración del HSM, de su custodia, de su configuración y puesta en marcha.

- Operadores HSM: Encargados de configurar el acceso al HSM por parte de las aplicaciones, de la inicialización del token PKCS#11, de asistir en las tareas de exportación e importación del material criptográfico del HSM.

Como medida de seguridad las responsabilidades están compartidas entre los distintos roles y personas, de modo que la actitud negligente o dolosa de alguno de ellos no afecta gravemente a la actividad de SUSCERTE como AC Raíz de la ICP de Venezuela.

Número de personas requeridas por tarea

Se requiere de un número de tres personas con capacidad profesional suficiente para realizar las tareas correspondientes al administrador del sistema y tres personas para las correspondientes a las de los operadores del HSM.

Identificación y autenticación para cada rol

El personal de activación de la AC Raíz es identificado y autenticado en los HSM mediante técnicas de secreto compartido en tarjetas criptográficas específicas de los HSM, antes de acceder.

La autenticación tanto a las instalaciones generales como a la sala donde está ubicado el sistema de la AC Raíz es conforme a los procedimientos definidos en el

documento “Políticas de Seguridad” del Centro de Cómputo de Datos de la SUSCERTE, disponible en www.suscerte.gob.ve/ps.

CONTROLES PERSONALES

Requisitos del personal de los roles de confianza

SUSCERTE posee unas prácticas de personal (definidas en el documento “Políticas de Seguridad”) disponible en www.suscerte.gob.ve/ps, con lo cual se garantiza la aptitud del personal de confianza, así como unos procedimientos de control adecuados para el cumplimiento de los derechos y obligaciones establecidos en el presente documento. Las prácticas de selección y reclutamiento de personal han sido definidos teniendo en cuenta requisitos de experiencia, calificación e historial precisos para cada puesto, sea de un rol de confianza o no.

Procedimientos de verificación del historial

Periódicamente se inspecciona al personal relacionado con la gestión de claves y certificados para verificar que continúan cumpliendo los requisitos establecidos en el presente documento. Si algún empleado no supera la inspección, es trasladado a otro puesto distinto o despedido.

Requisitos de formación

El personal de SUSCERTE es entrenado para poseer el conocimiento y la experiencia en certificación electrónica y calificación necesaria para prestar los

servicios ofertados, especialmente en conocimientos de ICP, tecnología de firma electrónica y procedimientos de seguridad.

Períodos y procedimientos de formación

SUSCERTE ofrece a los empleados cursos de formación para actualizar sus conocimientos.

Frecuencia y serie de rotaciones de trabajo entre varios roles

SUSCERTE implanta rotaciones de trabajo entre los distintos roles, con el objeto de incrementar la seguridad y asegurar la continuidad de la actividad en caso de ausencia de alguno de los trabajadores.

Sanciones

Las prácticas del personal de SUSCERTE definen el procedimiento sancionador para los empleados que incumplen las mismas, especificando las sanciones por efectuar una acción no autorizada, el uso no autorizado de la autoridad o el uso no autorizado de los sistemas.

En cualquier caso si SUSCERTE sospecha que algún empleado está efectuando una acción no autorizada, automáticamente bloquea su permiso de acceso.

Documentación suministrada al personal

SUSCERTE proporciona a sus empleados toda la documentación necesaria para el correcto desempeño de sus tareas.

Entre la documentación se encuentran los manuales de operación, mantenimiento, administración, instalación y utilización de herramientas de de la AC Raíz bajo Software Libre (SL), libros sobre materias técnicas para revisión, Declaración de Prácticas de Certificación (DPC), Políticas de Certificados (PC), acceso a Internet para obtener información adicional, entre otros.

CONTROLES DE SEGURIDAD TÉCNICA

GENERACIÓN E INSTALACIÓN DE CLAVES

Generación del par de claves

La AC Raíz genera su par de claves (pública y privada) en un hardware criptográfico que cumple (HSM) el FIPS 140-2 Nivel 3. La generación se realiza en el mismo dispositivo seguro en el que es utilizado el par de claves (ver apartado 5.3.2).

El procedimiento de generación de las claves para los PSC acreditados ante SUSCERTE es idéntico al de la AC Raíz.

Entrega de la clave privada al suscriptor

Para los PSC su clave privada quedará resguardada en su propio HSM. A diferencia de la AC Raíz, el certificado del PSC deberá ser firmado por la AC Raíz, así permanecerá bajo la jerarquía de la ICP de Venezuela.

Para los suscriptores del certificado emitidos por el PSC, se les entregará en una tarjeta inteligente el/los certificados electrónicos con el par de claves (pública y privada) asociado. Para que dicho suscriptor tenga acceso a la tarjeta inteligente es necesario que introduzca el PIN que protege a dicha tarjeta.

Entrega de la clave pública al emisor del certificado

Una vez enviada la solicitud del PSC codificada con el estándar PKCS#1 a la AC Raíz, se firma la clave pública del PSC para luego publicar en el repositorio

disponible en acraiz.suscerte.gob.ve/certificados el certificado electrónico y su clave pública.

Disponibilidad de la clave pública

Siempre debe estar disponible la clave pública de la AC Raíz, en acraiz.suscerte.gob.ve/certificados las 24 horas del día los 7 días de la semana de forma continua.

Tamaño de claves

Los algoritmos criptográficos empleados por la AC Raíz para firmar los certificados y las LCR son RSA.

La longitud de la clave con el algoritmo RSA de la AC Raíz es de 4096 bits, del PSC es de 2048 bits.

Generación de parámetros de claves asimétricas

La AC Raíz utiliza uno de los mejores métodos de compartición de secretos conocido. El método esquema límite (k,n) de Shamir, consiste en partir una clave en **n** partes y se tiene como mínimo (límite) el número **k** de partes para reconstruir la clave. Es decir, cualquiera **k** de los **n** custodios pueden reconstruir la clave, pero ningún subgrupo de **(k-1)** custodios podrá hacerlo.

La creación del juego de tarjetas de los operadores y administradores del HSM es bajo este esquema K de N para acceso a la clave privada.

Verificación de la calidad de los parámetros

Como se define en el apartado 5.0

Generación de claves por hardware y software

La AC Raíz sólo genera sus claves en modulo de hardware criptográfico (HSM). Para la autenticación contra el HSM se utilizan las claves de al menos 2 operadores de 3 del HSM siguiendo el esquema K de N (ver aparatado 6.1.6) con el modo no persistente en el HSM, donde es necesario tener físicamente conectado el último juego de tarjetas en el lector del HSM, para que la AC Raíz pueda utilizar la clave privada y pueda firmar los certificados. Una vez retirada la ultima tarjeta en el lector del HSM, se cierra la comunicación desde la AC Raíz hasta el HSM. Por ende la AC Raíz no podrá firmar con su clave privada a menos que se autentiquen de nuevos los operadores y dejen en el lector del HSM la última tarjeta del operador.

Propósitos de utilización de claves

Los certificados emitidos por la AC Raíz incluyen la extensión ***keyusage*** establecido en el estándar X.509, para restringir el propósito de la clave pública del certificado, indicando que la clave sólo es para:

- Firma certificado

2.3.5.1 Firma CRL

PROTECCIÓN DE LA CLAVE PRIVADA

La clave privada de la AC Raíz se genera en un módulo de hardware criptográfico (HSM) y nunca saldrá del mismo. Las clave privadas son extraídas en varias partes con el esquema k de n a través de los operadores y administradores del HSM, con el objeto de garantizar una mayor seguridad.

Estándares para módulos criptográficos

El HSM utilizado por la AC Raíz, para generar sus claves está validado conforme a lo establecido en la Norma Federal de Procesamiento de la Información (FIPS) 140-2 Nivel 3.

La clave privada se almacena en el HSM, mientras que la clave pública se almacena en formato electrónico firmado, de modo que están protegidas de fallos electrónicos y/o problemas con la potencia eléctrica.

Control "N de M" de clave privadas

Cuando la AC Raíz generó su clave privada, ésta se creó y guardó en un entorno seguro (HSM) protegiéndose a través de un sistema de seguridad dividido en varias partes (m), de modo que la clave privada sólo puede manipularse si se unen todas las (n) partes.

Cada vez que la AC Raíz genera una nueva clave privada, el procedimiento es el mismo que el definido en este apartado.

Recuperación de la clave privada

Sin contenido.

Copia de seguridad de la clave privada

La AC Raíz, realiza varias copias de seguridad por cada par de claves generadas. Las copias de seguridad de las claves privadas generadas por la AC Raíz se almacenan en un segundo HSM de reserva.

Archivo de clave privada

Las claves privadas generadas por la AC Raíz son archivadas conforme a lo previsto en el apartado 5.0 del presente documento.

Inserción de claves privadas en módulos criptográficos

Las distintas partes de la clave simétrica son generadas en el HSM.

Método de activación de claves privadas

La clave privada de la AC Raíz sólo puede activarse insertando la clave simétrica, generada en el HSM.

Una vez activada la clave, ésta permanecerá así hasta que el HSM sea reinicializado tras la finalización de la sesión.

Método de desactivación de claves privadas

La AC Raíz sólo permite el acceso a la clave privada al personal autorizado, permitiendo la manipulación de la misma dentro de un entorno seguro.

Si la clave no es utilizada durante un determinado período de tiempo, ésta es desactivada, guardándose el HSM en un lugar seguro.

Método de destrucción de claves privadas

La AC Raíz eliminará su clave privada cuando expire su plazo de vigencia o haya sido revocada.

La destrucción se realizará utilizando los comandos establecidos para borrar físicamente de la memoria del HSM la parte en la que estaba grabada la clave. Lo mismo ocurrirá con sus copias de seguridad.

OTROS ASPECTOS DE ADMINISTRACION DE CLAVES

Archivo de clave pública

La clave pública de la AC Raíz es archivada según el formato estándar PKCS#7.

Periodo de uso de clave pública y privada

El periodo del uso de la clave privada y pública de la AC Raíz es permanente mientras no se sospeche de su invalidez. Por otra parte el plazo de vigencia de los certificados emitidos por la AC Raíz a los PSC es de un año.

DATOS DE ACTIVACIÓN

Generación e instalación de datos de activación

La manipulación de la clave privada de la AC Raíz está protegida con una clave simétrica generada por el HSM y a su vez esa clave se puede bloquear a través de un PIN que sólo es conocido por el usuario autorizado.

Protección de datos de activación

La AC Raíz utiliza un cuarto de seguridad (bóveda o bunker), con por lo menos tres controles de acceso basados en identificación de nivel 2 (tarjeta o disco de identificación) y nivel 3 (biométrico). También es conveniente disponer de sistemas de video en circuito cerrado, y vigilancia total (24x365) con personal de seguridad para proteger la activación de las claves.

Otros aspectos referidos a los datos de activación

Sin contenido.

CONTROLES DE SEGURIDAD DEL COMPUTADOR

Requisitos técnicos específicos

SUSCERTE ha definido en el documento "Políticas de Seguridad" disponible en www.suscerte.gob.ve/ps los controles de seguridad técnica aplicables a los equipos informáticos. Estos controles se refieren a aspectos tales como el uso de los equipos, controles de acceso discrecional y obligatorio, auditorias, identificación y autenticación, etiquetas, tests de seguridad y de intrusión.

Calificaciones de seguridad computacional

SUSCERTE utiliza productos certificados, al menos, por el Nivel E3 de las normas de Certificación de Criterios de Evaluación de la Seguridad Informática (ITSEC).

Los niveles de evaluación de la ITSEC se definen dentro del contexto de los criterios de corrección. La evaluación de la corrección investiga si las funciones y mecanismos dedicados a la seguridad están implementados correctamente.

CONTROLES TÉCNICOS DE CICLO DE VIDA

Controles de desarrollo de sistemas

Las "Políticas de Seguridad" disponibles en www.suscerte.gob.ve/ps aplicables a la AC Raíz recogen diversas medidas de control para el desarrollo de las aplicaciones y la seguridad en las instalaciones, así como el uso e implementación de técnicas y diseños de seguridad contra fallos.

Controles de administración de seguridad

El documento "Políticas de Seguridad" disponible en www.suscerte.gob.ve/ps establece una metodología de control que incluye la utilización de diversas herramientas, así como la implantación de procedimientos para asegurar que sus sistemas y redes se vinculan a la seguridad definida.

Calificaciones de seguridad del ciclo de vida

El documento "Políticas de Seguridad" disponible en www.suscerte.gob.ve/ps prevé la revisión periódica con controles técnicos en cada etapa del ciclo de vida de los sistemas.

CONTROLES DE SEGURIDAD DE RED

El HSM empleado por SUSCERTE en la AC Raíz para generar su certificado cumple el estándar FIPS 140-2 Nivel 3.

CONTROLES DE INGENIERIA DE MÓDULOS CRIPTOGRÁFICOS

Sin contenido.

PERFILES DE CERTIFICADOS Y DE LISTAS DE CERTIFICADOS REVOCADOS

PERFIL DEL CERTIFICADO

Número de versión

La AC Raíz utiliza y emite certificados X. 509 versión 3.

Extensiones

Las extensiones del certificado de la AC Raíz permiten codificar información adicional en los certificados sin requerir modificación en el formato del mismo.

Las extensiones estándar las define X.509 incluye los siguientes campos:

•SubjectKeyIdentifier

•AuthorityKeyIdentifier

•BasicConstraints

- KeyUsage
- CRLDistributionPoint

•AuthorityInformationAccess

Identificadores de algoritmos

Los OID de los algoritmos criptográficos utilizados por la AC Raíz son:

•PKCS #1 SHA256 con RSA

Formatos de nombre

El certificado de la AC Raíz contiene como DN, en formato X. 500, los nombres del emisor y titular del certificado en los campos emisor (issuer) y sujeto (subject). Los campos son los que se encuentran en el apartado 5.3.1.1 del presente documento.

Restricción de nombres

Sin contenido

OID de la Política de Certificados

El OID de la Política de Certificado de la AC Raíz es 2 16 862 1 1.

Uso de extensión "Restricciones de políticas"

Sin contenido

Sintaxis y semánticas de calificadores de políticas

Sin contenido.

Semántica de procesamiento para extensiones criticas

Sin contenido.

PERFIL DE LA LISTA DE CERTIFICADOS REVOCADOS

Número de versión

La AC Raíz, emite LCR con formato X. 509 v. 2.

Extensiones de LCR

Las extensiones de las LCR emitidas por la AC Raíz, son las definidas por el IETF en su RFC (Request for Comments) 2459, es decir:

- Authority Key Identifier
- CRL Number
- Issuing Distribution Point

ADMINISTRACIÓN DE ESPECÍFICACIONES

PROCEDIMIENTOS DE CAMBIOS DE ESPECIFICACIONES

SUSCERTE revisa la DPC contenida en el presente documento con el objeto de actualizar su contenido, adoptando las modificaciones necesarias por el personal especializado.

POLÍTICAS DE PUBLICACIÓN Y NOTIFICACIÓN

Cuando se realice un nuevo cambio a la DPC, SUSCERTE procederá a publicarlo inmediatamente, en su portal Web.

PROCEDIMIENTOS DE APROBACIÓN

La presente DPC ha sido aprobada por la directiva de SUSCERTE y publicada en Gaceta Oficial.

ANEXO DE LA DPC

GLOSARIO DE DEFINICIÓN

Acreditación: Es el titulo que otorga la Superintendencia de Servicios de Certificación Electrónica a los Proveedores de Servicios de Certificación para proporcionar certificados electrónicos, una vez cumplidos los requisitos y condiciones establecidos en el Decreto-Ley 1.204.

Auditores: Son los expertos técnicos en la materia, inscritos en el Registro de Auditores de la Superintendencia de Servicios de Certificación Electrónica.

Certificado de Firma Electrónica: Instrumento electrónico que autentica el vínculo entre el firmante o titular del Certificado Electrónico y la Firma Electrónica.

Declaración de Practicas de Certificación: Documento en el cual el Proveedor de Servicios de Certificación Electrónica define los procedimientos relacionados con el manejo de los certificados electrónicos que emite.

Ley 1.204 sobre Mensajes de Datos y Firmas Electrónicas: Decreto con fuerza de Ley, de fecha 10 de febrero de 2001, publicado en Gaceta Oficial de la República Bolivariana de Venezuela Nº 37.148, de fecha 28 de febrero de 2001, que tiene por objeto otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y a los Certificados Electrónicos.

Política de Certificados: Documento en el cual el Proveedor de Servicios de Certificación Electrónica, define las reglas a seguir para el uso de un Certificado Electrónico en una comunidad de usuarios o aplicación determinados y sus requerimientos de seguridad.

Reglamento parcial del decreto-ley 1.204: Decreto Nº 3.335 de fecha 14 de diciembre de 2004, que desarrolla en forma parcial lo establecido en el Decreto 1.204 con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas, regulando la Acreditación de los PSCs ante SUSCERTE, la creación del Registro de Auditores, así como los estándares, planes y procedimientos de seguridad.

Repositorio: Sistema de información utilizado para el almacenamiento y acceso de los certificados electrónicos y la información asociada a los mismos.

Solicitud de Acreditación: Petición dirigida a SUSCERTE y que tiene por objeto obtener la Acreditación para proporcionar certificados electrónicos y demás actividades previstas en el Decreto-Ley 1.204.

Superintendencia de Servicios de Certificación Electrónica (SUSCERTE): Servicio Autónomo adscrito al Ministerio de Ciencia y Tecnología y cuyo objeto es acreditar, supervisar y controlar, en los términos previstos en el Decreto-Ley 1.204 (LSMDFE) y sus reglamentos, a los Proveedores de Servicios de Certificación Electrónica públicos o privados.

X.509: Es el estándar fundamental que define la estructura del certificado de clave pública.

SIGLAS

AC: Autoridad de Certificación

AL: Asesoría Legal

AR: Autoridad de Registro

DPC: Declaración de Practicas de Certificación

DRA: Dirección de Registro y Acreditación

HSM: Hardware Security Modules (en español Módulo de Hardware Criptográfico)

ICP: Infraestructura de Clave Pública

IETF: Internet Engineering Task Force (Grupo de Trabajo en Ingeniería de Internet)

LOAP: Ley Orgánica de Administración Pública

LOPA: Ley Orgánica de Procedimientos Administrativos

LSMDFE Iniciales que identifican el Decreto con fuerza de Ley 1.204 Sobre Mensajes de Datos y Firmas Electrónicas.

PKCS: Public Key Cryptography Standards. Estándares de ICP desarrollados por

RSA Laboratories y aceptado internacionalmente.

PSC: Proveedor de Servicios de Certificación.

PC: Políticas de Certificados.

RFC: Request For Comments (Estándar emitido por la IETF).

RECOMENDACIONES

- Tomar consejo de personas u organismos internacionales que han construido una ICP con éxito, porque las decisiones basadas en su experiencia ayudarán a crear una ICP exitosa para la organización.

- Capacitar al personal técnico en el uso de esta nueva tecnología para darle mantenimiento y continuidad a la ICP de la organización.

- Se debe continuar con el modelo jerárquico subordinado e incrementar la cantidad de Proveedores de Servicios de Certificación (PSC) acreditados ante SUSCERTE para crecer y fortalecer la infraestructura de clave pública nacional.

- Continuar con la divulgación de las ventajas y beneficios proporcionados al incorporar en las aplicaciones la firma electrónica y los certificados electrónicos.

- Continuar con el equipo valioso de FUNDACITE Mérida en conjunto con el personal de SUSCERTE para gestionar y crear las herramientas hechas en software libre para mejorar las funcionalidades en la ICP de Venezuela.

- Mantener conocimiento constante acerca de las nuevas tecnologías que brindan seguridad en las transacciones electrónicas.

- Realizar un Plan Piloto para probar y adquirir experiencia al utilizar la tecnología de firma electrónica, aprovechando las capacidades existentes en el estado coordinado por SUSCERTE

- Participar en mesas de trabajos con otros países para establecer alianzas y digitalizar los procesos de certificación que operan manualmente para aplicar la certificación electrónica, a través del uso de las tecnologías que garantice la autenticidad, confiabilidad, integridad y la aceptación del mismo.

- Fortalecer la certificación electrónica a través del desarrollo e implementación de librerías de código y aplicaciones bajo software libre para facilitar la integración de la firma electrónica en las aplicaciones existentes.

- Crear la Autoridad de Estampado de Tiempo para dar validez a los registros de la AC Raíz al momento de una auditoría. Incluir como servicio el estampado de tiempo en los documentos electrónicos, y aplicaciones de la organización para asegurar que los datos originales del documento como la información del estado de los certificados, se generaron en un instante de tiempo validado por la hora legal de Venezuela.

- Actualizar la DPC con el RFC 3647 más reciente por IETF (Internet Engineering Task Force) para los procedimientos y políticas de certificación de una Infraestructura de Clave Pública.

CONCLUSIONES

En la actualidad, Venezuela avanza aceleradamente hacia la actualización en materia de tecnologías de información y de las comunicaciones. La particularidad de estas tecnologías de información es que utilizan medios electrónicos y redes nacionales e internacionales adecuadas para ello, y constituyen una herramienta ideal para realizar intercambios de todo tipo incluyendo el comercial a través de la transferencia de informaciones de un computador a otro sin necesidad de la utilización de documentos

escritos en papel, lo que permite ahorros de tiempo y dinero. Soportado en nuestra legislación nacional al otorgarse la misma validez jurídica a la firma electrónica de la manuscrita dada por el Decreto con fuerza de Ley Nº 1.204 de fecha 10 de Febrero de 2001, de Mensaje de datos y Firmas Electrónicas (LSMDFE).

SUSCERTE como ente regulador de los servicios de certificación electrónica en Venezuela, es el responsable de regular el Sistema Nacional de Certificación Electrónica (SNCE) que sigue un modelo jerárquico con una única raíz o ancla de confianza del cual se deriva toda la cadena de confianza para el resto de los componentes del sistema. En el sistema se prestan los servicios de certificación electrónica a los ciudadanos a través de la criptografía y certificados electrónicos para obtener la autenticación correcta de autenticidad, confidencialidad, integridad y no repudio de un documento o mensaje electrónico.

Es importante señalar que este trabajo de grado diseña la Infraestructura de Clave Pública (ICP) del Proveedor de Servicios de Certificación (PSC) de carácter público responsable de brindar los servicios electrónicos a la comunidad de la Administración Pública Nacional (APN) con la descripción de sus componentes. Una vez listo el diseño el siguiente paso será la implementación del sistema, la puesta en marcha corresponderá a la Fundación del Instituto de Ingeniería, organismo adscrito al Ministerio de Ciencia y Tecnología. Sin embargo, corresponderá a SUSCERTE la regulación del funcionamiento del PSC una vez acreditado.

Por otro lado se logró la elaboración del la primera versión de la Declaración de Prácticas de Certificación (DPC) para la operación, mantenimiento y administración de la AC Raíz. Este documento estará disponible al público en general.

El documento de la DPC de la AC Raíz es importante porque en el se describe el ciclo de vida del certificado electrónico además de ser una excelente oportunidad para realizar la celebración de la ceremonia de claves de la Raíz y la emisión del certificado autofirmado de la Raíz para generar las claves y el almacenamiento seguro de la clave privada de la AC Raíz en el dispositivo criptográfico (HSM).

De esta manera se arranca el SNCE y se impulsa el uso de la firma electrónica y los certificados electrónicos en el país avanzando hacia gobierno electrónico transmitiendo confianza a los ciudadanos venezolanos en las actividades prestadas por medios electrónicos.

Asimismo se espera incrementar el número de PSC acreditados ante SUSCERTE del sector público y privado para fortalecer el SNCE del país. Y establecer alianzas con otros países para validación de los certificados electrónicos como es el caso de MERCOSUR y poder mejorar e incrementar los servicios a los ciudadanos.

ANEXO A. GLOSARIO DE TÉRMINOS

En este Anexo se exponen algunos de los conceptos básicos o términos de la seguridad y tecnología aplicada Infraestructura de Clave Pública (ICP).

ACTION PLAN DE OASIS: Es un software PKI, con una fuerte participación de Sun el Comité Técnico de OASIS (Organization for the Advencement of Structured Information Standards) para tecnologías PKI (Public Key Infrastructure). Impulsa la

adopción de estándares para el área de e-business, exige pruebas de interoperabilidad, mejores materiales de formación y métodos para reducir costos en la implantación de PKI, tecnología utilizada en muchos estándares, como SSL o IPsec, para la seguridad en las conexiones de red.

ACRÓNIMO (del griego *akros*, 'punta, altura' y *ónoma*, 'nombre') es una palabra que resulta de la unión de las letras iniciales de una o más palabras.

ALGORITMO: Una función matemática, como las que se usan para cifrar información.

AMENAZA: Evento o circunstancia que potencialmente puede provocar una pérdida de disponibilidad, confidencialidad o integridad de la información.

ANÁLISIS DE RIESGOS: Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización.

AUTENTICACIÓN: La acción de verificar información, como identidad, propiedad o autorización. Los métodos de autenticación incluyen contraseñas, hardware de identificadores, software de identificadores, tarjetas inteligentes, software de tarjetas inteligentes y dispositivos biométricos.

AUTENTIFICACIÓN SIMPLE: Procedimiento para autentificar a una entidad haciendo uso de una clave.

AUTENTIFICACIÓN FUERTE: Autentificación basada en credenciales cifradas.

AUTENTICACIÓN DE DOS FACTORES: Una forma de autenticación que requiere dos elementos distintos para garantizar la autenticidad del usuario; los factores podrían incluir un identificador de prenda, un número de identificación personal (PIN), un dispositivo biométrico o una tarjeta inteligente.

AUTORIDAD DE CERTIFICACIÓN (AC): Es una entidad, digna de confianza para los usuarios, con capacidad para crear y asignar certificados. Opcionalmente puede generar la clave pública y privada de un usuario. El término más usual para referirnos a una autoridad de certificación es la abreviatura en inglés, **CA** (Certification Authority).

AUTORIDAD DE CERTIFICACIÓN RAÍZ: Es normalmente una de las entidades certificadoras más confiables de la ICP, ya que ocupa la posición más alta dentro de la jerarquía de certificados, donde terminan todas las cadenas de certificados. Como no existe una entidad certificadora de orden superior, normalmente las AC Raíz firman sus propios certificados. Este certificado se lo denomina "certificado con auto-firma". Estos son los que vienen incluidos directamente en los navegadores.

BALTIMORE UNICERT: Es un software PKI para publicar certificados en cualquier directorio X.500.

CERTIFICADO: Es la clave pública de un usuario, junto con otra información. Un certificado es emitido y firmado digitalmente por una autoridad de certificación.

CERTIFICADO X.509: Información digital firmada por una autoridad de certificación. Un certificado X.509 contiene información relacionada con el sujeto que enlaza a un usuario específico con su clave pública RSA, el nombre del expedidor y la firma digital.

CIFRAR: La transformación de "texto en claro" en una forma aparentemente menos legible (llamada texto cifrado) a través de un proceso matemático. El texto cifrado lo puede leer cualquiera que tenga la clave que lo descifra.

CIFRADO ASIMÉTRICO: Un método criptográfico que usa una clave para cifrar un mensaje y una clave diferente para descifrarlo. Es el fundamento de la Infraestructura de Clave Pública.

CIFRADO DE CLAVE PÚBLICA: Este esquema de cifrado usa dos claves: una pública, que cualquiera puede usar, y una clave privada correspondiente, que posee sólo la persona que la creó. Con este método, cualquiera puede enviar un mensaje cifrado con la clave pública del receptor, pero sólo el receptor tiene la clave privada necesaria para descifrarla.

CIFRADO DE SESIÓN: Cifrado que se usa para la duración de una sesión de comunicación, como durante una conexión segura en un servidor Web que usa SSL.

CIFRADO SIMÉTRICO: Un método que usa el mismo algoritmo o clave para cifrar y descifrar información.

CLAVE: El secreto usado par cifrar o descifrar texto cifrado; la seguridad del cifrado depende de mantener en secreto la clave.

CLAVE PÚBLICA: Dentro de un sistema criptográfico basado en criptografía asimétrica, es la clave de usuario conocida públicamente.

CLAVE PRIVADA: Dentro de un sistema criptográfico basado en criptografía asimétrica, es la clave de usuario conocida únicamente por él.

CRIPTOGRAFÍA: Técnica que permite hacer ilegible un mensaje.

CRIPTOGRAFÍA ASIMÉTRICA: Sistema criptográfico que emplea dos claves, una para cifrar el texto normal y una segunda para descifrar el texto cifrado. Normalmente se conoce como **criptografía de clave pública**. Ejemplos de algoritmos de clave pública son RSA y ElGamal.

CRIPTOGRAFÍA SIMÉTRICA: Sistema criptográfico que emplea la misma clava para cifrar y descifrar. Normalmente se conoce como **criptografía de clave secreta**. DES e IDEA son ejemplos de algoritmos de clave secreta.

CONFIANZA: En tecnología de seguridad, la definición de la relación entre dos partes o computadoras, a través de la cual se conceden ciertos derechos o privilegios a la parte en que se confía.

CONFIDENCIALIDAD: Limitar la comunicación del contenido privado a las partes autorizadas.

CRIPTOGRAFÍA: ciencia que trata del enmascaramiento de la comunicación de modo que sólo resulte inteligible para la persona que posee la clave, o método para averiguar el significado oculto, mediante el criptoanálisis de un texto aparentemente incoherente.

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACION (DPC): Define la práctica y los procedimientos para la emisión de los certificados.

DOCUMENTO ELECTRÓNICO: Toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.

ESTAMPADO DE TIEMPO: Es un procedimiento mediante el cual es posible dar el servicio de la fecha y la hora exacta de un mensaje o un documento electrónico.

ESTÁNDARES: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son situaciones obligatorias que buscan hacer cumplir las políticas. Los estándares sirven como especificaciones para la implementación de las políticas; son diseñados para promover la implementación de las políticas de alto nivel de la organización antes que crear nuevas políticas.

ENTRUST/PKI: Es un software PKI, para publicar certificados en su directorio, Entrust/Directory; en un directorio X.500, como el directorio ICL i500; o en un directorio LDAP (Lightweight Directory Access Protocol), como Netscape Directory Server.

FIRMA DIGITAL: Consiste en aplicar una función hash de un sentido a un texto y después cifrar con la clave privada del firmante.

FUNCIÓN DE UN SENTIDO: Es una función matemática f, tal que es sencillo calcular f(x), pero muy difícil, en términos computacionales, a partir de y obtener un valor x tal que f(x) = y.

FUNCIÓN HASH: Es una función matemática que toma un mensaje grande y genera una secuencia de longitud fija. La bondad de una función hash se mide por la distribución (aleatoriedad) de los resultados. Habitualmente se denomina **hash**. Ejemplos de algoritmos hash son MD5 y SHA.

HASH: Una función de hash es una función matemática para calcular un código "resumen" (*hash*), de un mensaje o documento electrónico. Las características principales de una función de hash son: Todos los *hashes* tienen el mismo tamaño independientemente del tamaño del mensaje original, es fácil y rápido calcular una función de hash con el uso de un computador, pero es "imposible" reconstruir el mensaje original a partir de su hash, es "imposible" generar un mensaje para obtener un hash determinado.

GENERACIÓN DE JUEGO DE CLAVES: Es un mecanismo seguro para la creación de la clave privada y su correspondiente claves pública.

GESTIÓN DE RIESGOS: Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.

ICP (INFRAESTRUCTURA DE CLAVE PÚBLICA): También en inglés **PKI** (Public Key Infrastructure) es el término utilizado para referirse a la infraestructura de seguridad, basada en criptografía de clave pública, que permite la gestión de certificados digitales.

IETF (INTERNET ENGINEERING TASK FORCE): Comunidad internacional compuesta por gran cantidad de ingenieros, diseñadores, vendedores y expertos que investigan y promueven las distintas tendencias, estándares e investigaciones relacionadas con Internet.

INFORMACIÓN: Es un activo que, como otros activos importantes de la institución, tiene valor para la organización y requiere en consecuencia una protección adecuada.

ISO 17799: Es una guía de buenas prácticas de seguridad de la información que presenta una extensa serie de controles de seguridad. Es la única norma que no sólo cubre la problemática de la seguridad de tecnología de información sino que hace una aproximación holística a la seguridad de la información corporativa, abarcando todas las funcionalidades de una organización en cuanto a la seguridad de la información que maneja.

JUEGO DE CLAVES: Una clave privada siempre tendrá su correspondiente clave pública. La clave pública se utiliza para verificar una firma electrónica creada utilizando la correspondiente clave privada y para cifrado de mensajes hacia el dueño de la clave privada.

LDAP: Es una descripción del método de acceso y el protocolo que se utilizan para localizar información en un directorio.

MENSAJES DE DATOS: Toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio.

MIT: El Instituto Tecnológico de Massachusetts, conocido habitualmente como MIT (acrónimo de **M**assachusetts **I**nstitute of **T**echnology), es una de las principales instituciones dedicadas a la docencia y a la investigación, especialmente en ciencia, ingeniería y economía.

NO-REPUDIO: La imposibilidad de negar una transacción legítimamente realizada.

PLAN DE SEGURIDAD: Conjunto de reglas de seguridad que permiten materializar las decisiones de gestión de riesgos.

POLÍTICA DE CERTIFICADOS: Define las características de los certificados que serán emitidos por una Autoridad Certificadora.

POLÍTICA DE SEGURIDAD: Es el conjunto de reglas establecidas por la autoridad competente encargada de la seguridad en los servicios.

PROTOCOLO: es el conjunto de acciones coordinadas que realizan dos o más partes o entidades con el objeto de llevar a cabo un intercambio de datos o información.

PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA DEL ESTADO (PSCE): Consiste en una Infraestructura de Clave Pública dotada de una Entidad Pública de Certificación que permite autentificar y garantizar la confidencialidad e integridad de las comunicaciones entre ciudadanos, empresas u otras instituciones y administraciones públicas a través de las redes abiertas de comunicación.

RIESGO: Probabilidad de que se materialice como consecuencia de una vulnerabilidad existente.

RSA: Es una compañía privada que ofrece toda una gama de productos de seguridad. Su sitio en Internet está lleno de información correcta sobre seguridad.

SEGURIDAD: Es la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

SISTEMA CRIPTOGRÁFICO, CRIPTOSISTEMA: Es una serie de transformaciones que convierten un texto normal en texto cifrado, y viceversa. Las transformaciones emplean algoritmos matemáticos.

UIT- LA UNIÓN INTERNACIONAL DE TELECOMUNICACIONES: Es una organización mundial en la que el sector público y el sector privado cooperan para desarrollar las telecomunicaciones y armonizar las políticas nacionales relativas a las telecomunicaciones.

VULNERABILIDAD: Debilidad que frente a una amenaza puede provocar pérdida de confidencialidad, integridad o disponibilidad de la información.

ANEXO B. ESTÁNDARES CRIPTOGRÁFICOS DE CLAVE PÚBLICA

En este anexo se introducen los estándares criptográficos tomados para la implementación de la Infraestructura de Claves Públicas (PKI).

Los Estándares Criptográficos de Clave Pública (traducción literal de la denominación PKCS) son un intento por parte de *RSA Data Security, Inc.* Para proporcionar una norma para la industria que permita una interfaz estándar con la criptografía de clave pública. A diferencia de otros estándares, respaldados por organismos internacionales, se trata de una norma creada por una única empresa. Aunque muchas empresas han participado en el desarrollo de estos estándares, RSA se reserva la última palabra en su promulgación y revisión.

Aunque no son realmente estándares, son una aproximación al mundo de la criptografía, con la ventaja de que múltiples fabricantes los soportan. En la actualidad se trata de:

PKCS#1 (*RSA Encryption Standard*) describe un método para la utilización del algoritmo RSA. Su propósito es producir firmas digitales de mensajes y "sobres digitales" (mensajes cifrados) utilizando la sintaxis definida en el estándar PKCS#7. Las firmas digitales se producen aplicando una función de *hash* al mensaje y cifrando la huella digital resultante con la clave privada del firmante. El mensaje y su firma digital se representan tal como indica PKCS#7. Para conseguir los sobres digitales, el mensaje se cifra primero con una clave simétrica y, después, se cifra dicha clave con la clave pública del destinatario del mensaje. Ambos componentes (sobre y clave cifrada) se representan juntos según PKCS#7. También describe una sintaxis, idéntica a X.509 para las claves públicas y privadas y tres algoritmos de firmado digital (MD2 y RSA, MD4 y RSA y MD5 y RSA).

PKCS#2 y **PKCS#4** han sido incorporadas a PKCS#1.

PKCS#3 (*Diffie-Hellman Key-Agreement Standard*) describe un método para implementar el intercambio de claves Diffie-Hellman.

PKCS#5 (*Password-Based Encryption Standard*) describe un método para cifrar mensajes con una clave secreta derivada de una passphrase. Su objetivo primario es permitir la transmisión cifrada de claves privadas entre dos computadoras, como se describe en el PKCS#8, aunque puede ser usada para cifrar mensajes. Emplea MD2 o MD5 para producir una clave a partir de una frase de paso. Esta clave se utiliza para cifrar con DES (en modo CBC) el mensaje en cuestión.

PKCS#6 (*Extended-Certificate Syntax Standard*) describe una sintaxis para "certificados extendidos", entendiendo por tales un superconjunto de X.509, de modo que se pueden extraer certificados X.509 de estos certificados. Se incluyen atributos adicionales como puede ser la dirección electrónica. Una lista no exhaustiva de tales atributos se define en PKCS#9.

PKSC#7 (*Cryptographic Message Syntax Standard*) es una sintaxis general para datos que pueden tener alguna operación criptográfica asociada, ya sea cifrado ("sobres digitales") o firmado (firmas digitales). La sintaxis es recursiva, de modo que se pueden anidar sobres digitales o cifrar datos cifrados previamente. También se

permiten atributos adicionales, como marcas temporales (*time stamps*). Una forma límite de utilización de esta sintaxis proporciona un método para distribuir certificados o listas de revocación de certificados. En este sentido, PKCS#7 es compatible con varias arquitecturas de gestión de claves basadas en certificados.

PKCS#8 (*Private-Key Information Syntax Standard*) describe una sintaxis para la información de la clave privada, la cual incluye una clave privada y una serie de atributos, y una sintaxis para claves privadas cifradas (un algoritmo de cifrado basado en palabras de paso, como el descrito en el PKCS#5, podría ser usado para cifrar la información de clave privada). Una lista parcial de atributos puede encontrarse en PKC#9.

PKCS#9 (*Selected Attribute Types*) define algunos atributos para su uso en los certificados extendidos del PKCS#6, los mensajes firmados digitalmente de PKCS#7, la información de clave privada de PKCS#8 y para las peticiones de firmado de certificados definidas en PKCS#10.

PKCS#10 (*Certification Request Syntax Standard*) describe una sintaxis para las peticiones de certificados. Una petición de certificados consiste en un nombre distinguido (*distinguished name*), una clave pública y una serie de atributos opcionales (parcialmente definidas en PKCS#9), todo ello firmado colectivamente con la clave privada de la persona que hace la petición. Las peticiones se envía a una Autoridad de Certificación, la cual transforma la petición en un certificado X.509 v.3 o en un certificado extendido (PKCS#6). Las autoridades de certificación pueden precisar procedimientos de petición no electrónicos y responder no electrónicamente. Estos procedimientos son específicos de cada autoridad y están fuera del estándar.

PKCS#11 (*Cryptographic Token Interface Standard*) especifica una interfaz de programación llamada *Cryptoki* para su uso con dispositivos criptográficos de cualquier tipo (conocidos como *tokens*). *Cryptoki* tiene un enfoque basado en objetos permitiendo que aplicaciones realicen operaciones criptográficas sin conocer los detalles de la tecnología de los dispositivos. También define conjuntos de algoritmos que el *token* puede soportar.

PKCS#12 (*Personal Information Exchange Syntax Standard*) describe la sintaxis para almacenar en *software* las claves públicas de un usuario, proteger sus claves privadas, certificados y cualquier otra información de relevancia criptográfica. Su propósito es permitir el uso de un único archivo de claves accesible por cualquier aplicación.

PKCS#13 (*Elliptic Curve Cryptography Standard*) describe, de modo similar a como lo hace PKCS#1, un método para la utilización de algoritmos de curva elíptica. Describe la generación y validación de parámetros, la generación y validación de claves, el procedimiento de firmado y de cifrado.

PKCS#15 (*Smart Card File Format*). Este PKCS, aún en borrador, surge para cubrir ciertos aspectos no contemplados por PKCS#11. Para ello, trata de uniformizar la estructura de directorios y archivos de las tarjetas inteligentes, el contenido de ciertos archivos (como el de certificados) y el modo de acceder a ellos, de modo que se asegure la interoperabilidad entre aplicaciones, de modo que no dependan de la tarjeta instalada.

ANEXO C. DECRETO CON FUERZA DE LEY SOBRE MENSAJES DE DATOS Y FIRMAS ELECTRÓNICAS

En este anexo se introduce la Ley sobre mensajes de Datos y Firmas Electrónica (LSMDFE)

LEY SOBRE MENSAJES DE DATOS Y FIRMAS ELECTRONICAS

Gaceta Oficial Nº 37.148 de fecha 28 de febrero de 2001

Decreto Nº 1.204 – 10 de febrero de 2001

HUGO CHÁVEZ FRIAS

PRESIDENTE DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA

En ejercicio de la atribución que le confiere el numeral 8 del artículo 236 de la Constitución de la República Bolivariana de Venezuela, en concordancia con el artículo 1, numeral 5, literal b de la Ley que Autoriza al Presidente de la República para dictar Decretos con Fuerza de Ley en las Materias que se delegan, en Consejo de Ministros,

Dicta

El siguiente,

DECRETO CON RANGO Y FUERZA DE LEY SOBRE MENSAJES DE DATOS Y FIRMAS ELECTRONICAS

CAPITULO I

AMBITO DE APLICACIÓN Y DEFINICIONES

Objeto y aplicabilidad del Decreto-Ley.

Artículo 1.- El presente Decreto-Ley tiene por objeto otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos.

El presente Decreto-Ley será aplicable a los Mensajes de Datos y Firmas Electrónicas independientemente de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en un futuro. A tal efecto, sus normas serán desarrolladas e interpretadas progresivamente, orientadas a reconocer la validez y eficacia probatoria de los Mensajes de datos y Firmas Electrónicas.

La certificación a que se refiere el presente Decreto-Ley no excluye el cumplimiento de las formalidades de registro público o autenticación que, de conformidad con la ley, requieran determinados actos o negocios jurídicos.

Definiciones.

Artículo 2.- A los efectos del presente Decreto-Ley, se entenderá por:

Persona: Todo sujeto jurídicamente hábil, bien sea natural, jurídica, pública, privada, nacional o extranjera, susceptible de adquirir derechos y contraer obligaciones.

Mensajes de datos: Toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio.

Emisor: Persona que origina un Mensaje de Datos por sí mismo, o a través de terceros autorizados.

Firma Electrónica: Información creada o utilizada por el Signatario, asociada al Mensaje de Datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado.

Signatario: Es la persona titular de una Firma Electrónica o Certificado Electrónico.

Destinatario: Persona ha quien va dirigido el Mensaje de Datos.

Proveedor de Servicios de Certificación: Persona dedicada a proporcionar Certificados Electrónicos y demás actividades previstas en este Decreto-Ley.

Acreditación: Es el título que otorga la Superintendencia de servicios de Certificación Electrónica a los Proveedores de Servicios de Certificación para proporcionar certificados electrónicos, una vez cumplidos los requisitos y condiciones establecidos en este Decreto-Ley.

Certificado Electrónico: Mensaje de Datos proporcionado por un Proveedor de Servicios de Certificación que le atribuye certeza y validez a la Firma Electrónica.

Sistema de Información: Aquel utilizado para generar, procesar o archivar de cualquier forma Mensajes de Datos.

Usuario: Toda persona que utilice un sistema de información.

Inhabilitación técnica: Es la incapacidad temporal o permanente del Proveedor de Servicios de Certificación que impida garantizar el cumplimiento de sus servicios, así como, cumplir con los requisitos y condiciones establecidos en este Decreto-Ley para el ejercicio de sus actividades.

El reglamento del presente Decreto-Ley podrá adaptar las definiciones antes señaladas a los desarrollos tecnológicos que se produzcan en el futuro. Así mismo, podrá establecer otras definiciones que fueren necesarias para la eficaz aplicación de este Decreto-Ley.

Adaptabilidad del Decreto-Ley.

Artículo 3.- El Estado adoptará las medidas que fueren necesarias para que los organismos públicos puedan desarrollar sus funciones, utilizando los mecanismos descritos en este Decreto-Ley.

CAPITULO II

DE LOS MENSAJES DE DATOS

Eficacia Probatoria.

Artículo 4.- Los Mensajes de Datos tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos, sin perjuicio de lo establecido en la primera parte del artículo 6 de este Decreto-Ley. Su promoción, control, contradicción y evacuación como medio de prueba, se realizará conforme a lo previsto para las pruebas libres en el Código de Procedimiento Civil.

La información contenida en un Mensaje de Datos, reproducida en formato impreso, tendrá la misma eficacia probatoria atribuida en la ley a las copias o reproducciones fotostáticas.

Sometimiento a la Constitución y a la ley.

Artículo 5.- Los Mensajes de Datos estarán sometidos a las disposiciones constitucionales y legales que garantizan los derechos a la privacidad de las comunicaciones y de acceso a la información personal.

Cumplimiento de solemnidades y formalidades.

Artículo 6.- Cuando para determinados actos o negocios jurídicos la ley exija el cumplimiento de solemnidades o formalidades, éstas podrán realizarse utilizando para ello los mecanismos descritos en este Decreto-Ley.

Cuando para determinados actos o negocios jurídicos la ley exija la firma autógrafa, ese requisito quedará satisfecho en relación con un Mensaje de Datos al tener asociado una Firma Electrónica.

Integridad del Mensaje de Datos.

Artículo 7.- Cuando la ley requiera que la información sea presentada o conservada en su forma original, ese requisito quedará satisfecho con relación a un Mensaje de Datos si se ha conservado su integridad y cuando la información contenida en dicho Mensaje de Datos esté disponible. A tales efectos, se considerará que un Mensaje de Datos permanece íntegro, si se mantiene inalterable desde que se generó, salvo algún cambio de forma propio del proceso de comunicación, archivo o presentación.

Constancia por escrito del Mensaje de Datos.

Artículo 8.- Cuando la ley requiera que la información conste por escrito, ese requisito quedará satisfecho con relación a un Mensaje de Datos, si la información que éste contiene es accesible para su ulterior consulta.

Cuando la ley requiera que ciertos actos o negocios jurídicos consten por escrito y su soporte deba permanecer accesible, conservado o archivado por un período determinado o en forma permanente, estos requisitos quedarán satisfechos mediante la conservación de los Mensajes de Datos, siempre que se cumplan las siguientes condiciones:

3.6.2 Que la información que contengan pueda ser consultada posteriormente.

3.6.3 Que conserven el formato en que se generó, archivó o recibió o en algún formato que sea demostrable que reproduce con exactitud la información generada o recibida.

3.6.4 Que se conserve todo dato que permita determinar el origen y el destino del Mensaje de Datos, la fecha y la hora en que fue enviado o recibido.

Toda persona podrá recurrir a los servicios de un tercero para dar cumplimiento a los requisitos señalados en este artículo.

CAPITULO III

DE LA EMISIÓN Y RECEPCIÓN DE LOS MENSAJES DE DATOS

Verificación de la emisión del Mensaje de Datos.

Artículo 9.- Las partes podrán acordar un procedimiento para establecer cuándo el Mensaje de Datos proviene efectivamente del Emisor. A falta de acuerdo entre las partes, se entenderá que unos Mensajes de Datos proviene del Emisor, cuando éste ha sido enviado por:

2. El propio Emisor.

3. Persona autorizada para actuar en nombre del Emisor respecto de ese mensaje.

4. Por un Sistema de Información programado por el Emisor, o bajo su autorización, para que opere automáticamente.

Oportunidad de la emisión.

Artículo 10.- Salvo acuerdo en contrario entre las partes, el Mensaje de Datos se tendrá por emitido cuando el sistema de información del Emisor lo remita al Destinatario.

Reglas para la determinación de la recepción.

Artículo 11.- Salvo acuerdo en contrario entre el Emisor y el Destinatario, el momento de recepción de un Mensaje de Datos se determinará conforme a las siguientes reglas:

- Si el Destinatario ha designado un sistema de información para la recepción de Mensajes de Datos, la recepción tendrá lugar cuando el Mensaje de Datos ingrese al sistema de información designado.
- Si el Destinatario no ha designado un sistema de información, la recepción tendrá lugar, salvo prueba en contrario, al ingresar el Mensaje de Datos en un sistema de información utilizado regularmente por el Destinatario.

Lugar de emisión y recepción.

Artículo 12.- Salvo prueba en contrario, el Mensaje de Datos se tendrá por emitido en el lugar donde el Emisor tenga su domicilio y por recibido en el lugar donde el Destinatario tenga el suyo.

Del acuse de recibo.

Artículo 13.- El Emisor de un Mensaje de Datos podrá condicionar los efectos de dicho mensaje a la recepción de un acuse de recibo emitido por el Destinatario.

Las partes podrán determinar un plazo para la recepción del acuse de recibo. La no recepción de dicho acuse de recibo dentro del plazo convenido, dará lugar a que se tenga el Mensaje de Datos como no emitido.

Cuando las partes no establezcan un plazo para la recepción del acuse de recibo, el Mensaje de Datos se tendrá por no emitido si el Destinatario no envía su acuse de recibo en un plazo de veinticuatro (24) horas a partir de su emisión.

Cuando el Emisor reciba el acuse de recibo del Destinatario conforme a lo establecido en el presente artículo, el Mensaje de Datos surtirá todos sus efectos.

Mecanismos y métodos para el acuse de recibo.

Artículo 14.- Las partes podrán acordar los mecanismos y métodos para el acuse de recibo de un Mensaje de Datos. Cuando las partes no hayan acordado que para el acuse de recibo se utilice un método determinado, se considerará que dicho requisito se ha cumplido cabalmente mediante:

- Toda comunicación del Destinatario, automatizada o no, que señale la recepción del Mensaje de Datos.

- Todo acto del Destinatario que resulte suficiente a los efectos de evidenciar al Emisor que a recibido su Mensaje de Datos.

Oferta y aceptación en los contratos.

Artículo 15.- En la formación de los contratos, las partes podrán acordar que la oferta y aceptación se realicen por medio de Mensajes de Datos.

CAPITULO IV

DE LAS FIRMAS ELECTRONICAS

Validez y eficacia de la Firma Electrónica. Requisitos.

Artículo 16.- La Firma Electrónica que permita vincular al Signatario con el Mensaje de Datos y atribuir la autoría de éste, tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa. A tal efecto, salvo que las partes dispongan otra cosa, la Firma Electrónica deberá llenar los siguientes aspectos:

2.3.13.1 Garantizar que los datos utilizados para su generación puedan producirse sólo una vez, y asegurar, razonablemente, su confidencialidad.

2.3.13.2 Ofrecer seguridad suficiente de que no pueda ser falsificada con la tecnología existente en cada momento.

2.3.13.3 No alterar la integridad del Mensaje de Datos.

A los efectos de este artículo, la Firma Electrónica podrá formar parte integrante del Mensaje de Datos, o estar inequívocamente asociada a éste; enviarse o no en un mismo acto.

Efectos jurídicos. Sana critica.

Artículo 17.- La Firma Electrónica que no cumpla con los requisitos señalados en el artículo anterior no tendrá los efectos jurídicos que se le atribuyen en el presente Capítulo, sin embargo, podrá constituir un elemento de convicción valorable conforme a las reglas de la sana crítica.

La certificación.

Artículo 18.- La Firma Electrónica, debidamente certificada por un Proveedor de Servicios de Certificación conforme a lo establecido en este Decreto-Ley, se considerará que cumple con los requisitos señalados en el artículo 16.

Obligaciones del signatario.

Artículo 19.- El Signatario de la Firma Electrónica tendrá las siguientes obligaciones:

Actuar con diligencia para evitar el uso no autorizado de su Firma Electrónica.

Notificar a su Proveedor de Servicios de Certificación que su Firma Electrónica ha sido controlada por terceros no autorizados o indebidamente utilizada, cuando tenga conocimiento de ello.

El Signatario que no cumpla con las obligaciones antes señaladas será responsable de las consecuencias del uso no autorizado de su Firma Electrónica.

CAPITULO V

DE LA SUPERINTENDENCIA DE SERVICIOS

DE CERTIFICACIÓN ELECTRÓNICA

Creación de la Superintendencia.

Artículo 20.- Se crea la Superintendencia de Servicios de Certificación Electrónica, como un servicio autónomo con autonomía presupuestaria, administrativa, financiera y de gestión, en las materias de su competencia, dependiente del Ministerio de Ciencia y Tecnología.

Objeto de la Superintendencia.

Artículo 21.- La Superintendencia de Servicios de Certificación Electrónica tiene por objeto acreditar, supervisar y controlar, en los términos previstos en este Decreto-Ley y sus reglamentos, a los Proveedores de Servicios de Certificación públicos o privados.

Competencias de la Superintendencia.

Artículo 22.- La Superintendencia de Servicios de Certificación Electrónica tendrá las siguientes competencias:

1. Otorgar la acreditación y la correspondiente renovación a los Proveedores de Servicios de Certificación una vez cumplidas las formalidades y requisitos de este Decreto-Ley, sus reglamentos y demás normas aplicables.

2. Revocar o suspender la acreditación otorgada cuando se incumplan las condiciones, requisitos y obligaciones que se establecen en el presente Decreto-Ley.

3. Mantener, procesar, clasificar, resguardar y custodiar el Registro de los Proveedores de Servicios de Certificación públicos o privados.

4. Verificar que los Proveedores de Servicios de Certificación cumplan con los requisitos contenidos en el presente Decreto-Ley y sus reglamentos.

5. Supervisar las actividades de los Proveedores de Servicios de Certificación conforme a este Decreto-Ley, sus reglamentos y las normas y procedimientos que establezca la Superintendencia en el cumplimiento de sus funciones.

6. Liquidar, recaudar y administrar las tasas establecidas en el artículo 24 de este Decreto-Ley.

7. Liquidar y recaudar las multas establecidas en el presente Decreto-Ley.

8. Administrar los recursos que se le asignen y los que obtenga en el desempeño de sus funciones.

9. Coordinar con los organismos nacionales o internacionales cualquier aspecto relacionado con el objeto de este Decreto-Ley.

10. Inspeccionar y fiscalizar la instalación, operación y prestación de servicios realizados por los Proveedores de Servicios de Certificación.

11. Abrir, de oficio o a instancia de parte, sustanciar y decidir los procedimientos administrativos relativos a presuntas infracciones a este Decreto-Ley.

12. Requerir de los Proveedores de Servicios de Certificación o sus usuarios, cualquier información que considere necesaria y que esté relacionada con materias relativas al ámbito de sus funciones.

13. Actuar como mediador en la solución de conflictos que se susciten entre los Proveedores de Servicios de Certificados y sus usuarios, cuando ello sea solicitado por las partes involucradas, sin perjuicio de las atribuciones que tenga el organismo encargado de la protección, educación y defensa del consumidor y el usuario, conforme a la ley que rige esta materia.

14. Seleccionar los expertos técnicos o legales que considere necesarios para facilitar el ejercicio de sus funciones.

15. Presentar un informe anual sobre su gestión al Ministerio de adscripción.

16. Tomar las medidas preventivas o correctivas que considere necesarias conforme a lo previsto en este Decreto-Ley.

17. Imponer las sanciones establecidas en este Decreto-Ley.

18. Determinar la forma y alcance de los requisitos establecidos en los artículos 31 y 32 del presente Decreto-Ley.

19. Las demás que establezcan la ley y los reglamentos.

Ingresos de la Superintendencia.

Artículo 23.- Son ingresos de la Superintendencia de Servicios de Certificación Electrónica:

I Los recursos que le sean asignados en la Ley de Presupuesto a través del Ministerio de Ciencia y Tecnología.

II Los provenientes de su gestión conforme a lo establecido en esta Ley.

III Cualquier otro ingreso permitido por ley.

De las tasas.

Articulo 24.- La Superintendencia de Servicios de Certificación Electrónica cobrará las siguientes tasas:

2.3.5.1.1 Por la acreditación de los Proveedores de Servicios de Certificación se cobrará una tasa de un mil unidades tributarias (1.000 U.T.).

2.3.5.1.2 Por la renovación de la acreditación de los Proveedores de Servicios de Certificación se cobrará una tasa de quinientas unidades tributarias (500 U.T.).

2.3.5.1.3 Por la cancelación de la acreditación de los Proveedores de Servicios de Certificación se cobrará una tasa de quinientas unidades tributarias (500 U.T.).

2.3.5.1.4 Por la autorización que se otorgue a los Proveedores de Servicios de Certificación debidamente acreditados en relación a la garantía de los Certificados Electrónicos proporcionados por Proveedores de Servicios de Certificación extranjeros, conforme a lo establecido en el artículo 44 del presente Decreto-Ley, se cobrará una tasa de quinientas unidades tributarias (500 U.T.).

Los Proveedores de Servicios de Certificación constituidos por entes públicos estarán exentos del pago de las tasas previstas en este artículo.

Mecanismos de control.

Artículo 25.- La Contraloría Interna del Ministerio de Ciencia y Tecnología, ejercerá las funciones de control, vigilancia y fiscalización de los ingresos, gastos y bienes

públicos sobre este servicio autónomo, de conformidad con la ley que regula la materia.

De la supervisión.

Artículo 26.- La Superintendencia de Servicios de Certificación Electrónica supervisará a los Proveedores de Servicios de Certificación con el objeto de verificar que cumplan con los requerimientos necesarios para ofrecer un servicio eficaz a sus usuarios. A tal efecto, podrá directamente o a través de expertos, realizar las inspecciones y auditorias que fueren necesarias para comprobar que los Proveedores de Servicios de Certificación cumplen con tales requerimientos.

Medidas para garantizar la confiabilidad.

Artículo 27.- La Superintendencia de Servicios de Certificación Electrónica podrá adoptar las medidas preventivas o correctivas necesarias para garantizar la confiabilidad de los servicios prestados por los Proveedores de Servicios de Certificación. A tal efecto, podrá ordenar, entre otras medidas, el uso de estándares o prácticas internacionalmente aceptadas para la prestación de los servicios de certificación electrónica, o que el Proveedor se abstenga de realizar cualquier actividad que ponga en peligro la integridad o el buen uso del servicio.

Designación del Superintendente.

Artículo 28.- La Superintendencia de Servicios de Certificación Electrónica estará a cargo de un Superintendente, será de libre designación y remoción del Ministro de Ciencia y Tecnología.

Requisitos para ser Superintendente.

Artículo 29.- El Superintendente de Servicios de Certificación Electrónica, debe reunir los siguientes requisitos:

- Ser venezolano.

- De reconocida competencia técnica y profesional para el ejercicio de sus funciones.

No podrá ser Superintendente, los miembros directivos, agentes, comisarios, administradores o accionistas de empresas o instituciones sometidas al control de la Superintendencia. Tampoco podrá ejercer tal cargo el que tenga parentesco hasta el cuarto grado de consanguinidad o segundo de afinidad con personas naturales también sometidas al control de la Superintendencia.

Atribuciones del Superintendente.

Artículo 30.- Son atribuciones del Superintendente:

- Dirigir el Servicio Autónomo Superintendencia de Servicios de Certificación Electrónica.

- Suscribir los actos y documentos relacionados con las materias especificadas en el artículo 22 de este Decreto-Ley.

- Administrar los recursos e ingresos del Servicio Autónomo Superintendencia de Servicios de Certificación Electrónica.

- Celebrar previa delegación del Ministro de Ciencia y Tecnología, convenios con organismos públicos o privados, nacionales e internacionales, derivados del cumplimiento de las atribuciones que corresponden a la Superintendencia de Servicios de Certificación Electrónica.

- Elaborar el proyecto de presupuesto anual, de conformidad con las previsiones legales correspondientes.

- Proponer escalas especiales de remuneración para el personal de la Superintendencia, de conformidad con las disposiciones legales aplicables.

- Presentar al Ministro de Ciencia y Tecnología el Proyecto de Reglamento Interno.

- Celebrar previa delegación del Ministro de Ciencia y Tecnología, los contratos de trabajo y de servicios de personal, que requiera la

Superintendencia de Servicios de Certificación Electrónica para su funcionamiento.

- Elaborar anualmente la memoria y cuenta de la Superintendencia de Servicios de Certificación Electrónica.

- Las demás que le sean asignadas por el Ministro de Ciencia y Tecnología.

CAPITULO VI

DE LOS PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN

Requisitos para ser Proveedor.

Artículo 31. Podrán ser Proveedores de Servicios de Certificación, las personas, que cumplan y mantengan los siguientes requisitos:

- La capacidad económica y financiera suficiente para prestar los servicios autorizados como Proveedor de Servicios de Certificación. En el caso de organismos públicos, éstos deberán contar con un presupuesto de gastos y de ingresos que permitan el desarrollo de esta actividad.

- La capacidad y elementos técnicos necesarios para proveer Certificados Electrónicos.

- Garantizar un servicio de suspensión, cancelación y revocación, rápido y seguro, de los Certificados Electrónicos que proporcione.

- Un sistema de información de acceso libre, permanente, actualizado y eficiente en el cual se publiquen las políticas y procedimientos aplicados para la prestación de sus servicios, así como los Certificados Electrónicos que hubiere proporcionado, revocado, suspendido o cancelado y las restricciones o limitaciones aplicables a éstos.

- Garantizar que en la emisión de los Certificados Electrónicos que provea se utilicen herramientas y estándares adecuados a los usos internacionales, que estén protegidos contra su alteración o modificación, de tal forma que garanticen la seguridad técnica de los procesos de certificación.

- En caso de personas jurídicas, éstas deberán estar legalmente constituidas de conformidad con las leyes del país de origen.

- Personal técnico adecuado con conocimiento especializado en la materia y experiencia en el servicio a prestar.

- Las demás que señale el reglamento de este Decreto-Ley.

El incumplimiento de cualesquiera de los requisitos anteriores dará lugar a la revocatoria de la acreditación otorgada por la Superintendencia de Servicios de Certificación Electrónica, sin perjuicio de las sanciones previstas en este Decreto-Ley.

De la acreditación.

Artículo 32.- Los Proveedores de Servicios de Certificación presentarán ante la Superintendencia de Servicios de Certificación Electrónica, junto con la correspondiente solicitud, los documentos que acrediten el cumplimiento de los requisitos señalados en el artículo 31. La Superintendencia de Servicios de Certificación Electrónica, previa verificación de tales documentos, procederá a recibir y procesar dicha solicitud y deberá pronunciarse sobre la acreditación del Proveedor de Servicios de Certificación, dentro de los veinte (20) días hábiles siguientes a la fecha de presentación de la solicitud.

Una vez aprobada la solicitud del Proveedor de Servicios de Certificación, éste presentará, a los fines de su acreditación, garantías que cumplan con los siguientes requisitos:

II Ser expedidas por una entidad aseguradora o bancaria autorizada para operar en el país, conforme a las disposiciones que rigen la materia.

III Cubrir todos los perjuicios contractuales y extracontractuales de los signatarios y terceros de buena fe derivados de actuaciones dolosas, culposas u omisiones atribuibles a los administradores, representantes legales o empleados del Proveedor de Servicios de Certificación.

El Proveedor de Servicios de Certificación deberá mantener vigente la garantía aquí solicitada por el tiempo de vigencia de su acreditación. El incumplimiento de este requisito dará lugar a la revocatoria de la acreditación otorgada por la Superintendencia de Servicios de Certificación Electrónica.

Negativa de la acreditación.

Artículo 33.- La Superintendencia de Servicios de Certificación Electrónica podrá negar la solicitud a que se refiere el artículo anterior, en caso que el solicitante no reúna los requisitos señalados en este Decreto-Ley y sus reglamentos.

Actividades de los Proveedores de Servicios de Certificación.

Artículo 34.- Los Proveedores de Servicios de Certificación realizarán entre otras, las siguientes actividades:

- Proporcionar, revocar o suspender los distintos tipos o clases de Certificados Electrónicos.
- Ofrecer o facilitar los servicios de creación de Firmas Electrónicas.
- Ofrecer servicios de archivo cronológicos de las Firmas Electrónicas certificadas por el Proveedor de Servicios de Certificación.
- Ofrecer los servicios de archivo y conservación de mensajes de datos.
- Garantizar Certificados Electrónicos proporcionados por Proveedores de Servicios de Certificación extranjeros.
- Las demás que se establezcan en el presente Decreto-Ley o en sus reglamentos.

Los Certificados Electrónicos proporcionados por los Proveedores de Servicios de Certificación garantizarán la validez de las Firmas Electrónicas que certifiquen, y la titularidad que sobre ellas tengan sus Signatarios.

Obligaciones de los Proveedores.

Artículo 35.- Los Proveedores de Servicios de Certificación tendrán las siguientes obligaciones:

- Adoptar las medidas necesarias para determinar la exactitud de los Certificados Electrónicos que proporcionen y la identidad del Signatario.

- Garantizar la validez, vigencia y legalidad del Certificado Electrónico que proporcione.

- Verificar la información suministrada por el Signatario para la emisión del Certificado Electrónico.

- Mantener en medios electrónicos o magnéticos, para su consulta, por diez (10) años siguientes al vencimiento de los Certificados Electrónicos que proporcionen, un archivo cronológico con la información relacionada con los referidos Certificados Electrónicos.

- Garantizar a los Signatarios un medio para notificar el uso indebido de sus Firmas Electrónicas.

- Informar a los interesados en sus servicios de certificación, utilizando un lenguaje comprensible en su pagina en la Internet o en cualquier otra red mundial de acceso público, los términos precisos y condiciones para el uso del Certificado Electrónico y, en particular, de cualquier limitación sobre su responsabilidad, así como de los procedimientos especiales existentes para resolver cualquier controversia.

- Garantizar la integridad, disponibilidad y accesibilidad de la información y documentos relacionados con los servicios que proporcione. A tales efectos, deberán mantener un respaldo confiable y seguro de dicha información.

- Garantizar la adopción de las medidas necesarias para evitar la falsificación de Certificados Electrónicos y de las Firmas Electrónicas que proporcionen.

- Efectuar las notificaciones y publicaciones necesarias para informar a los signatarios y personas interesadas acerca del vencimiento, revocación, suspensión o cancelación de los Certificados Electrónicos que proporcione, así como de cualquier otro aspecto de relevancia para el público en general, en relación con dichos Certificados Electrónicos.

- Notificar a la Superintendencia de Servicios de Certificación Electrónica cuando tenga conocimiento de cualquier hecho que pueda conllevar a su Inhabilitación Técnica.

El incumplimiento de cualesquiera de los requisitos anteriores dará lugar a la suspensión de la acreditación otorgada por la Superintendencia de Servicios de

Certificación Electrónica, sin perjuicio de las sanciones establecidas en el presente Decreto-Ley.

La contraprestación del servicio.

Artículo 36.- La contraprestación por los servicios que los Proveedores de Servicios de Certificación presten, estará sujeta a las reglas de la oferta y la demanda.

Notificación del cese de actividades.

Artículo 37.- Cuando los Proveedores de Servicios de Certificación decidan cesar en sus actividades, lo notificarán a la Superintendencia de Servicios de Certificación Electrónica, al menos con treinta (30) días de anticipación a la fecha de cesación.

En el caso de Inhabilitación Técnica, el Proveedor de Servicios de Certificación notificará inmediatamente a la Superintendencia de Servicios de Certificación Electrónica.

Recibida cualesquiera de las notificaciones señaladas en este artículo, la Superintendencia de Servicios de Certificación Electrónica emitirá un acto por el cual se declare públicamente la cesación de actividades del Proveedor de Servicios de Certificación como prestador de ese servicio, sin perjuicio de las investigaciones que pueda realizar a fin de determinar las causas que originaron el cese de las actividades del Proveedor, y las medidas que fueren necesarias adoptar con el objeto de salvaguardar los derechos de los usuarios. En ese acto la Superintendencia podrá ordenar al Proveedor que realice los trámites que considere necesarios para hacer del conocimiento público la cesación de esas actividades, y para garantizar la conservación de la información que fuere de interés para sus usuarios y el público en general.

En todo caso, el cese de las actividades de un Proveedor de Servicios de Certificación conllevará su retiro del registro llevado por la Superintendencia de Servicios de Certificación Electrónica.

CAPITULO VII

CERTIFICADOS ELECTRONICOS

Garantía de la autoría de la Firma Electrónica.

Artículo 38.- El Certificado Electrónico garantiza la autoría de la Firma Electrónica que certifica así como la integridad del Mensaje de Datos. El Certificado Electrónico no confiere la autenticidad o fe pública que conforme a la ley otorguen los funcionarios públicos a los actos, documentos y certificaciones que con tal carácter suscriban.

Vigencia del Certificado Electrónico.

Artículo 39.- El Proveedor de Servicios de Certificación y el Signatario, de mutuo acuerdo, determinarán la vigencia del Certificado Electrónico.

Cancelación.

Artículo 40.- La cancelación de un Certificado Electrónico procederá cuando el Signatario así lo solicite a su Proveedor de Servicios de Certificación. Dicha cancelación no exime al Signatario de las obligaciones contraídas durante la vigencia del Certificado, conforme a lo previsto en este Decreto-Ley.

El Signatario estará obligado a solicitar la cancelación del Certificado Electrónico cuando tenga conocimiento del uso indebido de su Firma Electrónica. Si el Signatario en conocimiento de tal situación no solicita dicha cancelación, será responsable por los daños y perjuicios sufridos por terceros de buena fe como consecuencia del uso indebido de la Firma Electrónica certificada mediante el correspondiente Certificado Electrónico.

Suspensión temporal voluntaria.

Artículo 41.- El Signatario podrá solicitar la suspensión temporal del Certificado Electrónico, en cuyo caso su Proveedor deberá proceder a suspender el mismo durante el tiempo solicitado por el Signatario.

Suspensión o revocatoria forzosa.

Artículo 42.- En los contratos que celebren los Proveedores de Servicios de Certificación con sus usuarios, se deberán establecer como causales de suspensión o revocatoria del Certificado Electrónico de la Firma Electrónica, las siguientes:

- Sea solicitado por una autoridad competente de conformidad con la ley.
- Se compruebe que alguno de los datos del Certificado Electrónico proporcionado por el Proveedor de Servicios de Certificación es falso.
- Se compruebe el incumplimiento de una obligación principal derivada del contrato celebrado entre el Proveedor de Servicios de Certificación y el Signatario.
- Se produzca una Quiebra Técnica del sistema de seguridad del Proveedor de Servicios de Certificación que afecte la integridad y confiabilidad del certificado contentivo de la Firma Electrónica.

Así mismo, se preverá en los referidos contratos que los Proveedores de Servicios de Certificación podrán dejar sin efecto la suspensión temporal del Certificado Electrónico de una Firma Electrónica al verificar que han cesado las causas que originaron dicha suspensión, en cuyo caso el Proveedor de Servicios de Certificación correspondiente estará en la obligación de habilitar de inmediato el Certificado Electrónico de que se trate.

La vigencia del Certificado Electrónico cesará cuando se produzca la extinción o incapacidad absoluta del Signatario

Contenido de los Certificados Electrónicos.

Artículo 43.- Los Certificados Electrónicos deberán contener la siguiente información:

- Identificación del Proveedor de Servicios de Certificación que proporciona el Certificado Electrónico, indicando su domicilio y dirección electrónica.

- El código de identificación asignado al Proveedor de Servicios de Certificación por la Superintendencia de Servicios de Certificación Electrónica.
- Identificación del titular del Certificado Electrónico, indicando su domicilio y dirección electrónica.
- Las fechas de inicio y vencimiento del periodo de vigencia del Certificado Electrónico.
- La Firma Electrónica del Signatario.
- Un serial único de identificación del Certificado Electrónico.
- Cualquier información relativa a las limitaciones de uso, vigencia y responsabilidad a las que esté sometido el Certificado Electrónico.

Certificados electrónicos extranjeros.

Artículo 44.- Los Certificados Electrónicos emitidos por proveedores de servicios de certificación extranjeros tendrán la misma validez y eficacia jurídica reconocida en el presente Decreto-Ley, siempre que tales certificados sean garantizados por un Proveedor de Servicios de Certificación, debidamente acreditado conforme a lo previsto en el presente Decreto-Ley, que garantice, en la misma forma que lo hace con sus propios certificados, el cumplimiento de los requisitos, seguridad, validez y vigencia del certificado. Los certificados electrónicos extranjeros, no garantizados por un Proveedor de Servicios de Certificación debidamente acreditado conforme a lo previsto en el presente Decreto-Ley, carecerán de los efectos jurídicos que se atribuyen en el presente Capítulo, sin embargo, podrán constituir un elemento de convicción valorable conforme a las reglas de la sana crítica.

CAPITULO VIII

DE LAS SANCIONES

A los Proveedores de Servicios de Certificación.

Artículo 45.- Los Proveedores de Servicios de Certificación serán sancionados con multa de Quinientas Unidades Tributarias (500 U.T.) a Dos Mil Unidades Tributarias (2.000 U.T.), cuando incumplan las obligaciones que les impone el artículo 35 del presente Decreto-Ley.

Los Proveedores de Servicios de Certificación serán sancionados con multa de Quinientas Unidades Tributarias (500 U.T.) a Dos Mil Unidades Tributarias (2.000 U.T.), cuando dejen de cumplir con alguno de los requisitos establecidos en el artículo 31 del presente Decreto-Ley.

Las sanciones serán impuestas en su término medio, pero podrán ser aumentadas o disminuidas en atención a las circunstancias agravantes o atenuantes existentes.

Circunstancias agravantes y atenuantes.

Artículo 46.- Son circunstancias agravantes:

- La reincidencia y la reiteración.
- La gravedad del perjuicio causado al Usuario.
- La gravedad de la infracción.
- La resistencia o reticencia del infractor para esclarecer los hechos.

Son circunstancias atenuantes:

13. No haber tenido la intención de causar el hecho imputado de tanta gravedad.
14. Las que se evidencien de las pruebas aportadas por el infractor en su descargo.

En el proceso se apreciará el grado de la culpa para agravar o atenuar la pena.

Prescripción de las sanciones.

Artículo 47.- Las sanciones aplicadas prescriben por el transcurso de tres (3) años, contados a partir de la fecha de notificación al infractor.

Falta de acreditación.

Artículo 48.- Serán sancionadas con multa de dos mil (2000) a cinco mil (5000) Unidades Tributarias (U.T.), las personas que presten los servicios de Proveedores de Servicios de Certificación previstos en este Decreto-Ley, sin la acreditación de la Superintendencia de Servicios de Certificación Electrónica, alegando tenerla.

Procedimiento ordinario.

Artículo 49.- Para la imposición de las multas previstas en los artículos anteriores, la Superintendencia de Servicios de Certificación Electrónica aplicará el procedimiento administrativo ordinario previsto en la Ley Orgánica de Procedimientos Administrativos.

CAPITULO X

DISPOSICIONES FINALES

Primera.- El presente Decreto-Ley entrará en vigencia a partir de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

Segunda.- Los procedimientos, trámites y recursos contra los actos emanados de la Superintendencia de Servicios de Certificación Electrónica, se regirán por lo previsto en la Ley Orgánica de Procedimientos Administrativos.

Tercera.- Sin limitación de otros que se constituyan, el Estado creará un Proveedor de Servicios de Certificación de carácter público, conforme a las normas del presente Decreto-Ley. El Presidente de la República determinará la forma y adscripción de este Proveedor de Servicios de Certificación.

Cuarta.- La Administración Tributaria y Aduanera adoptará las medidas necesarias para ejercer sus funciones utilizando los mecanismos descritos en este Decreto-Ley, así como para que los contribuyentes puedan dar cumplimiento a sus obligaciones tributarias mediante dichos mecanismos.

ANEXO D. REGLAMENTO PARCIAL DE LA LEY SOBRE MENSAJES DE DATOS Y FIRMAS ELECTRÓNICAS

En este anexo se introduce el Reglamento Parcial de la Ley sobre Mensajes de Datos y Firmas Electrónica (LSMDFE) normativa que regula la acreditación de los Proveedores de Servicios de Certificación ante la SUSCERTE

HUGO CHÁVEZ FRÍAS

Presidente de la República

En ejercicio de la atribución que le confiere el numeral 10 del artículo 236 de la Constitución de la República Bolivariana de Venezuela, en concordancia con el Articulo 87 de la Ley Orgánica de la administración Publica

DECRETA

El siguiente,

REGLAMENTO PARCIAL DE LA LEY SOBRE MENSAJES DE DATOS Y FIRMAS ELECTRÓNICAS

CAPITULO I

DISPOSICIONES GENERALES

Objeto

Artículo 1 El presente reglamento tiene por objeto desarrollar la normativa que regula la acreditación de los Proveedores de Servicios de Certificación ante la Superintendencia de Servicios de Certificación Electrónica; la creación del Registro de Auditores; así como los estándares, planes y procedimientos de seguridad.

Definiciones

Artículo 2 A los efectos del presente reglamento se entenderá por:

Declaración de Prácticas de Certificación: Documento en el cual el Proveedor de Servicios de Certificación Electrónica define los procedimientos relacionados con el manejo de los Certificados Electrónicos que emite.

Política de Certificados: Documento en el cual el Proveedor de Servicios de Certificación Electrónica define las reglas a seguir para el uso de un Certificado Electrónico en una comunidad de usuarios o aplicación determinados y sus requerimientos de seguridad.

Datos de Generación de Firma Electrónica: Valor o valores numéricos que utilizados conjuntamente con un procedimiento matemático sirven para crear la Firma Electrónica asociada a un Mensaje de Datos.

Datos de Verificación de la Firma Electrónica: Valor o valores numéricos que son utilizados para comprobar que la Firma Electrónica fue creada con los datos de generación de Firma Electrónica del signatario.

Repositorio: Sistema de Información utilizado para el almacenamiento y acceso de los Certificados Electrónicos y la información asociada a los mismos.

Auditores: Son los expertos técnicos inscritos en el registro de auditores de la Superintendencia de Servicios de Certificación Electrónica.

CAPITULO II

DE LA ACREDITACION DE LOS PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN

Presentación de la solicitud de Acreditación

Artículo 3 El Proveedor de Servicios de Certificación Electrónica presentará la solicitud de Acreditación ante la Superintendencia de Servicios de Certificación Electrónica, con los siguientes recaudos e información:

- Identificación completa del solicitante**.**
- Información económica y financiera con la cual se demuestre la capacidad suficiente para prestar servicios como Proveedor de Servicios de Certificación**.**
- Copia de los contratos correspondientes a aquellos servicios que sean prestados por terceros en caso de haberlos**.**
- Proyecto de contrato a ser suscrito con los Signatarios**.**
- Políticas de Certificados y Declaración de Prácticas de Certificación**.**

- Estados financieros auditados y declaraciones del impuesto sobre la renta de los dos últimos ejercicios fiscales.

- Informe de auditoría de acuerdo con lo establecido en el artículo 5 de este reglamento, elaborado por Auditores independientes, no vinculados e inscritos en el registro que a tal efecto lleva la Superintendencia de Servicios de Certificación Electrónica.

- Documento con la descripción detallada de la infraestructura, planes y procedimientos establecidos en el Capítulo VIII de este reglamento. En caso que toda o parte de la infraestructura sea prestada por un tercero debe incluirse copia de los contratos o convenios con éste.

Admisibilidad de la solicitud

Artículo 4 La Superintendencia de Servicios de Certificación Electrónica tendrá veinte (20) días hábiles de conformidad con el artículo 32 de la Ley de Mensajes de Datos y Firmas Electrónicas para pronunciarse sobre la solicitud de la Acreditación.

La Superintendencia de Servicios de Certificación Electrónica informará al solicitante, dentro de los cinco (5) días siguientes a la presentación de la solicitud de Acreditación, la omisión o incumplimiento de algún requisito, de conformidad con la Ley que rige los procedimientos administrativos. Dicho pronunciamiento será debidamente notificado al solicitante

Contenido del informe de Auditoria

Artículo 5 El informe de auditoría deberá contener al menos:

1. Nombre e identificación de los auditores.

2. Fecha de inicio y terminación de la auditoría.

3. Declaración de conformidad de cada una de las condiciones previstas en el artículo 31 de la Ley Sobre Mensajes de Datos y Firmas Electrónicas y las demás previstas en este reglamento.

4. Manifestación del cumplimiento de los estándares indicados en el Capítulo VII de este reglamento.

5. Firma del auditor.

Inspecciones y visitas

Artículo 6 Durante todo el procedimiento de Acreditación, la Superintendencia de Servicios de Certificación Electrónica podrá solicitar información adicional a la ya suministrada, así como realizar visitas a las instalaciones del solicitante por intermedio de sus funcionarios o por expertos especialmente autorizados para tal fin.

Pronunciamiento de la Superintendencia de Servicios de Certificación Electrónica sobre las garantías

Artículo 7 Aprobada la solicitud el Proveedor de Servicio de Certificación deberá presentar las garantías necesarias para su Acreditación.

Presentadas las garantías y verificadas por la Superintendencia de Servicios de Certificación Electrónica, ésta procederá a Acreditar al Proveedor de Servicio de Certificación Electrónica mediante decisión publicada en la Gaceta Oficial de la República Bolivariana de Venezuela.

La Superintendencia de Servicios de Certificación Electrónica negará la Acreditación, mediante auto motivado, cuando encuentre que las garantías presentadas por el Proveedor de Servicio de Certificación no cumplan los requisitos establecidos en el artículo 32 de la Ley de Mensaje de Datos y Firmas Electrónicas. Dicho pronunciamiento será debidamente notificado al solicitante.

Cumplimiento continuo de los requisitos

Artículo 8 De conformidad con lo establecido en el numeral 4 del artículo 22 de la Ley Sobre Mensajes de Datos y Firmas Electrónicas, la Superintendencia de Servicios de Certificación Electrónica verificará el cumplimiento continuo, por parte de los Proveedores de Servicios de Certificación, de los requisitos establecidos en la Ley y sus reglamentos.

Duración de la Acreditación

Artículo 9 La Acreditación de los Proveedores de Servicios de Certificación ante la Superintendencia de Servicios de Certificación Electrónica, tendrá la duración de un (1) año.

Renovación de la Acreditación

Artículo 10 El Proveedor de Servicios de Certificación deberá solicitar la renovación de la Acreditación dentro de los cuarenta y cinco (45) días continuos previos al vencimiento de la Acreditación.

Al momento de la solicitud de la renovación el Proveedor de Servicios de Certificación deberá presentar nuevamente todos los recaudos que son necesarios para la Acreditación.

La Superintendencia de Servicios de Certificación Electrónica tendrá veinte (20) días de conformidad con la ley que rige los procedimientos administrativos, para el pronunciamiento de la renovación de la Acreditación.

La Superintendencia de Servicios de Certificación Electrónica informará al Proveedor de Servicios de Certificación, dentro de los cinco (5) días siguientes a la presentación de la solicitud de renovación, la omisión o incumplimiento de algún requisito.

Revocación de la Acreditación

Artículo 11 De conformidad con lo establecido en el numeral 2 del artículo 22 de la Ley Sobre Mensajes de Datos y Firmas Electrónicas, la Superintendencia de

Servicios de Certificación Electrónica podrá revocar la Acreditación de un Proveedor de Servicios de Certificación en los siguientes casos:

1. Por pérdida de las condiciones que sirvieron de fundamento para la Acreditación, la que será calificada por la Superintendencia de Servicios de Certificación Electrónica.

2. Por el incumplimiento de las obligaciones que establece la Ley y sus reglamentos, previa apertura del procedimiento administrativo correspondiente.

Notificación de la Revocatoria de la Acreditación

Artículo 12 Los Proveedores de Servicio de Certificación cuya Acreditación haya sido revocada, deberán comunicar inmediatamente este hecho a los titulares de los Certificados Electrónicos por ellos emitidos. Sin perjuicio de ello, la Superintendencia de Servicios de Certificación Electrónica publicará en un diario de los de mayor circulación nacional un aviso dando cuenta de la revocación. El costo de dicho aviso será a cargo del Proveedor de Servicios de Certificación.

A partir de la fecha de publicación en la Gaceta Oficial de la República Bolivariana de Venezuela, de la decisión de la Superintendencia de Servicios de Certificación Electrónica, por la cual revoca la acreditación de un Proveedor de Servicios de Certificación, las Firmas Electrónicas generadas con los Datos de Creación de Firma emitidos por dicho Proveedor de Servicios Certificación perderán la validez y eficacia probatoria que la Ley otorga.

Responsabilidad por los perjuicios causados por la revocación

Artículo 13 Los perjuicios que pueda causar la revocatoria de la Acreditación del Proveedor de Servicios de Certificación a los titulares de los Certificados Electrónicos que se encontraban vigentes, así como los costos de transferencia a otro proveedor acreditado, serán de responsabilidad del Proveedor de Servicios de Certificación cuya Acreditación se revocó.

CAPITULO III

DE LOS PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN ACREDITADOS

Artículo 14 Además de lo establecido en el articulo 31 de la Ley de Mensajes de Datos y Firmas Electrónicas los Proveedores de Servicios de Certificación Acreditados deberán cumplir y mantener las obligaciones establecidas en los artículos 15, 18, 19, 20, 23, 27, 37, 38 y 40 de este reglamento.

Obligaciones de los Proveedores de Servicios de Certificación Acreditados

Artículo 15 Acorde a lo previsto en el artículo 35 de la Ley Sobre Mensajes de Datos y Firmas Electrónicas, los Proveedores de Servicios de Certificación electrónica deberán:

1. Comprobar presencialmente la identidad de los solicitantes de los Certificados Electrónicos y verificar cualesquiera otras circunstancias relevantes, en forma previa a la expedición, conservando la documentación que respalda dicha identificación por el tiempo señalado en numeral 4 del artículo 35 de la Ley Sobre Mensajes de Datos y Firmas Electrónicas.

2. Mantener a disposición permanente del público en su página en la Internet o en cualquier otra red mundial de acceso público y con un acceso desde su página inicial, la declaración de Prácticas de Certificación y las Políticas de Certificados vigentes.

3. Cumplir cabalmente con las Políticas de Certificados y la Declaración de Prácticas de Certificación vigente.

4. Informar en la forma establecida en el numeral 4º del artículo 31 y 6º del artículo 35 de la Ley Sobre Mensajes de Datos y Firmas Electrónicas, el nivel de confiabilidad de sus Certificados Electrónicos, los límites de responsabilidad del Proveedor de Servicios de Certificación y las obligaciones que el Signatario asume como usuario del servicio de certificación.

5. Garantizar la prestación permanente e ininterrumpida del servicio. Quedan a salvo las suspensiones que autorice la Superintendencia de Servicios de Certificación Electrónica de conformidad con la ley y sus reglamentos.

6. Garantizar de manera fácil y permanente el acceso de los Signatarios y terceros al repositorio.

7. Informar a la Superintendencia de Servicios de Certificación Electrónica de manera inmediata la ocurrencia de cualquier evento que comprometa la prestación del servicio.

8. Abstenerse de almacenar los Datos de Generación de Firma del Signatario y garantizar un método de creación de los mismos que impida mantener copia una vez que éstos hayan sido entregados al Signatario.

9. Mantener actualizado el registro de los Certificados Electrónicos revocados.

10. Informar al signatario dentro de las 24 horas siguientes de la suspensión o revocatoria de su Certificado Electrónico.

11. Mantener el control exclusivo de sus Datos de Generación de Firma Electrónica como Proveedor de Servicios de Certificación y establecer las medidas de seguridad necesarias para que esta no se divulgue o comprometa.

Cambio o actualización de datos de un Proveedor de Servicios de Certificación

Artículo 16 Si el Proveedor de Servicios de Certificación realizara cualquier reforma de los Estatutos Sociales de la empresa, así como la ubicación de sus oficinas principales, deberá notificarlo a la Superintendencia de Servicios de Certificación Electrónica dentro de los diez (10) días siguientes a la modificación o cambio a los fines de mantener actualizada la información.

Modificación de la Declaración de Practicas de Certificación y las Políticas de Certificados

Artículo 17 El Proveedor de Servicios de Certificación acreditado deberá someter a la autorización de la Superintendencia de Servicios de Certificación Electrónica cualquier modificación en su declaración de Prácticas de Certificación. Igualmente deberá someter a la autorización de la Superintendencia de Servicios de Certificación

Electrónica cualquier creación, modificación o eliminación de sus Políticas de Certificados.

Información periódica

Artículo 18 Para fines estadísticos, el Proveedor de Servicios de Certificación acreditado, deberá enviar a la Superintendencia de Servicios de Certificación Electrónica dentro de los primeros diez (10) días del inicio de cada trimestre un reporte sobre la actividad del trimestre anterior, discriminada mes a mes con la siguiente información:

- Cantidad de Certificados Electrónicos emitidos, de acuerdo con las Políticas de Certificados autorizados por la Superintendencia de Servicios de Certificación Electrónica para dicho Proveedor de Servicios de Certificación.
- Cantidad de Certificados Electrónicos vigentes, de acuerdo con las Políticas de Certificados autorizados por la Superintendencia de Servicios de Certificación Electrónica para dicho Proveedor de Servicios de Certificación.
- Cantidad de Certificados Electrónicos revocados, de acuerdo con las Políticas de Certificados autorizados por la Superintendencia de Servicios de Certificación Electrónica para dicho Proveedor de Servicios de Certificación.

Suspensión del Servicio por Mantenimiento y Mejoras del Sistemas

Artículo 19 Los Proveedores de Servicios de Certificación podrán cesar temporalmente la prestación del servicio a fin de hacer mantenimiento o mejoras a su sistema, hasta por setenta y dos (72) horas acumulativas por cada año calendario.

Cuando la suspensión deba exceder el lapso indicado en el parágrafo anterior, el Proveedor de Servicios de Certificación deberá solicitar a la Superintendencia de Servicios de Certificación Electrónica la autorización correspondiente.

El Proveedor de Servicios de Certificación deberá informar al Signatario la suspensión con no menos de veinticuatro (24) horas de anticipación y deberá remitir

a la Superintendencia de Servicios de Certificación Electrónica la constancia de dicho aviso durante las veinticuatro (24) horas siguientes de haber informado al signatario.

Suspensión del Servicio por Caso Fortuito o Fuerza mayor

Artículo 20 Cuando por caso fortuito o fuerza mayor se ocasione la suspensión de la prestación de sus servicios, el Proveedor de Servicios de Certificación deberá notificarlo a sus usuarios dentro de las 24 horas siguientes al inicio de la misma y remitir constancia de dicha notificación a la Superintendencia de Servicios de Certificación Electrónica; adicionalmente deberá consignar ante este servicio autónomo, un informe contentivo de las causas y periodo de la suspensión en un plazo no mayor de 48 horas luego del restablecimiento del servicio.

Indicación de Acreditación

Artículo 21 El Proveedor de Servicios de Certificación podrá señalar en cualquier medio en el cual publicite sus servicios que ha sido debidamente Acreditado ante la Superintendencia de Servicios de Certificación Electrónica.

CAPITULO IV

DE LOS PROVEEDORES DE SERVICOS DE CERTIFICACION EXTRANJEROS

Requisitos para garantizar Certificados Electrónicos Extranjeros

Artículo 22 Para garantizar Certificados Electrónicos extranjeros en la forma establecida en el artículo 44 de la Ley Sobre Mensajes de Datos y Firmas Electrónicas, el Proveedor de Servicios de Certificación Electrónica acreditado, deberá demostrar a la Superintendencia de Servicios de Certificación Electrónica que el proveedor extranjero cuyos certificados se garantizarán cumplen con normas técnicas equivalentes a las establecidas en Venezuela para el desarrollo de esta actividad.

Notificación de la Garantía de Certificación

Artículo 23 El Proveedor de Servicios de Certificación acreditado que garantice Certificados Electrónicos extranjeros deberá comunicar a la Superintendencia de Servicios de Certificación Electrónica la fecha a partir de la cual dicha garantía será efectiva en sus sistemas.

La forma y alcance de la garantía de los certificados extranjeros deberán estar establecidos en la Declaración de Prácticas de Certificación del garante.

Efectos de la Garantía del Certificado Extranjero

Artículo 24 El efecto de la garantía de cada certificado extranjero, se limitará a las características establecidas en la Política de Certificado correspondiente y por el período de validez del mismo.

Los Signatarios de los Certificados Electrónicos garantizados y los terceros interesados tendrán idénticos derechos que los signatarios y terceros interesados de los Certificados Electrónicos propios del Proveedor de Servicios de Certificación que hace el reconocimiento.

CAPITULO V

DE LA SUPERVISIÓN DE LOS PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN ACREDITADOS POR LA SUPERINTENDENCIA DE SERVICIOS DE CERTIFICACIÓN ELECTRONICA

Realización de Inspecciones

Artículo 25 De conformidad con las competencias establecidas en la Ley Sobre Mensajes de Datos y Firmas Electrónicas, la Superintendencia de Servicios de Certificación Electrónica ejercerá la facultad inspectora sobre los Proveedores de Servicios de Certificación ante ella acreditados y podrá, a tal efecto, requerir información correspondiente y realizar las visitas a sus instalaciones con el fin de comprobar el cumplimiento de sus obligaciones.

Inspecciones Ordinarias y Extraordinarias

Artículo 26 La Superintendencia de Servicios de Certificación Electrónica podrá realizar inspecciones ordinarias y extraordinarias a los Proveedores de Servicios de Certificación.

La inspección ordinaria consiste en una visita anual a las instalaciones del Proveedor de Servicios de Certificación acreditado y el requerimiento en forma semestral de información sobre el desarrollo de sus actividades.

La inspección extraordinaria será practicada por denuncia de terceros sobre inconsistencias en la prestación del servicio, o por oficio.

Ejecución de las Inspecciones

Artículo 27 La Superintendencia de Servicios de Certificación Electrónica realizará las inspecciones a través de sus funcionarios y podrá hacerse asistir de los expertos técnicos o legales que considere necesarios para facilitar el ejercicio de sus competencias.

La Superintendencia de Servicios de Certificación Electrónica podrá requerir al Proveedor de Servicios de Certificación toda la información técnica, financiera o de cualquier otra naturaleza que considere necesaria, dentro del ámbito de sus competencias.

Confidencialidad de la información suministrada

Artículo 28 La Superintendencia de Servicios de Certificación Electrónica, así como el personal que actúe bajo su dependencia o por cuenta de ella, deberá mantener la confidencialidad de la información y documentos entregados por los Proveedores de Servicios de Certificación, cuando dicha información revista tal carácter en virtud de alguna norma legal.

CAPITULO VI

DEL REGISTRO DE AUDITORES

Informe de Auditoria

Artículo 29 A los efectos de lo establecido en el artículo 26 de la Ley Sobre Mensajes de Datos y Firmas Electrónicas, las auditorias a las que se refiere la mencionada Ley y sus reglamentos, serán realizadas por auditores debidamente inscritos ante la Superintendencia de Servicios de Certificación Electrónica, de conformidad con lo dispuesto en el presente reglamento.

Solamente los informes de los auditores inscritos ante la Superintendencia de Servicios de Certificación Electrónica podrán hacerse valer como parte de los requisitos de Acreditación exigidos, o en cualquier otro caso en que se requiera de conformidad con la Ley Sobre Mensajes de Datos y Firmas Electrónicas y sus reglamentos.

Creación del Registro de Auditores

Artículo 30 Con base en la disposición contenida en el numeral 14 del artículo 22 de la Ley Sobre Mensajes de Datos y Firmas Electrónicas, la Superintendencia de Servicios de Certificación Electrónica creará un registro de auditores con el propósito de inscribir a las personas autorizadas para la realización de los Informes de auditoría.

Solicitud de inscripción en el registro

A los fines de la inscripción en el Registro de Auditores de la Superintendencia de Servicios de Certificación Electrónica, los interesados deberán hacer su solicitud por escrito cumpliendo con los requisitos que a tal efecto establezca la Superintendencia de Servicios de Certificación Electrónica**.**

Decisión de inscripción en el registro

Artículo 31 Recibida la solicitud la Superintendencia de Servicios de Certificación Electrónica dispondrá del lapso de veinte (20) días hábiles de conformidad con lo que

establece la ley que rige los procedimientos administrativos para decidir sobre la inscripción en el Registro de Auditores.

La Superintendencia de Servicios de Certificación Electrónica informará al solicitante, dentro de los cinco (5) días siguientes a la presentación de la solicitud de renovación, la omisión o incumplimiento de algún requisito, de conformidad con la ley que rige los procedimientos administrativos, dicho pronunciamiento será debidamente notificado al solicitante.

Vigencia de la inscripción en el registro

Artículo 32 Decidida favorablemente la inscripción en el registro, la Superintendencia de Servicios de Certificación Electrónica expedirá una certificación de inscripción que tendrá una vigencia de tres (3) años.

Renovación de la inscripción

Artículo 33 El Auditor deberá solicitar la renovación del registro dentro de los cuarenta y cinco (45) días continuos previos al vencimiento.

Al momento de la solicitud de la renovación el Auditor deberá presentar nuevamente todos los recaudos que son necesarios para la inscripción.

La Superintendencia de Servicios de Certificación Electrónica tendrá veinte (20) días de conformidad con la ley que rige los procedimientos administrativos, para el pronunciamiento de la renovación de la inscripción.

La Superintendencia de Servicios de Certificación Electrónica informará al Auditor dentro de los cinco (5) días siguientes a la presentación de la solicitud de renovación, la omisión o incumplimiento de algún requisito, de conformidad con la ley que rige los procedimientos administrativos.

Dicho pronunciamiento será debidamente notificado al solicitante

CAPITULO VII

LOS CERTIFICADOS ELECTRÓNICOS Y

DE LAS FIRMAS ELECTRÓNICAS

Contenido de los Certificados Electrónicos

Artículo 34 Además de la información requerida por el artículo 43 de la Ley Sobre Mensajes de Datos y Firmas Electrónicas, los Certificados Electrónicos emitidos por los Proveedores de Servicios de Certificación acreditados por la Superintendencia de Servicios de Certificación Electrónica, podrán incluir información adicional siempre y cuando ésta no dificulte o impida su lectura o impida el reconocimiento de dichos certificados por terceros.

Manejo de los datos de Generación de Firma Electrónica

Artículo 35 Los Datos de Generación de la Firma Electrónica creados por el Proveedor de Servicios de Certificación Electrónica, deberán ser entregados al Signatario en forma personal y de manera inmediata quedando comprobada la recepción de los mismos mediante acuse de recibo. A partir de este momento, el Signatario pasará a ser responsable del uso y resguardo de los Datos de Generación de Firma Electrónica.

El Proveedor de Servicios de Certificación Electrónica no podrá mantener copia de los datos de generación de la Firma Electrónica del Signatario.

CAPITULO VIII

DE LOS ESTÁNDARES, PLANES Y PROCEDIMIENTOS DE SEGURIDAD

Políticas, Planes y Procedimientos de Seguridad

Artículo 36 El Proveedor de Servicios de Certificación debe definir y poner en práctica políticas, planes y procedimientos de seguridad orientados a garantizar la prestación continua de los servicios de certificación y el resguardo de los registros, que deberán ser revisados y actualizados periódicamente. Estos deben incluir al menos:

1. Políticas y procedimientos de seguridad de las instalaciones físicas y los equipos.
2. Políticas de acceso a los sistemas e instalaciones del proveedor y monitoreo constante de los mismos.
3. Planes y procedimientos de actualización de hardware y software, utilizados para la operación de Proveedores de Servicios de Certificación.
4. Planes y procedimientos de contingencia en cada uno de los riesgos potenciales que atenten en contra del funcionamiento del Proveedor de Servicios de Certificación, según estudio que se actualizará periódicamente.
5. Plan de manejo, control y prevención de virus informático.

Cumplimiento de los Requisitos Técnicos

Artículo 37 De conformidad con el artículo 31, incisos 2, 3, 4, 5 y 8, de la Ley de Mensajes de Datos y Firmas Electrónicas, el Proveedor de Servicios de Certificación Electrónica deberá contar con el personal calificado, infraestructura física y tecnológica y sistemas de seguridad que cumplan con las siguientes obligaciones técnicas:

1. Generar las firmas electrónicas propias, y prestar los servicios para los cuales ha sido autorizado en la correspondiente Acreditación.
2. Garantizar el cumplimiento de lo previsto en la Declaración de Prácticas de Certificación y las Políticas de Certificados.
3. Garantizar que los certificados expedidos cumplan con lo previsto en el artículo 43 de la Ley sobre Mensajes de Datos y Firmas Electrónicas y por lo menos, con alguno de los estándares de certificados admitidos por la Superintendencia de Servicios de Certificación Electrónica.

4. Establecer sistemas de seguridad en las instalaciones, con monitoreo permanente de la infraestructura física, y con acceso restringido a los equipos de sistemas de operación del Proveedor.

5. Someter los datos de generación de firma electrónica al procedimiento propio de seguridad que evite el acceso físico o de otra índole, a personal no autorizado.

6. Garantizar que los sistemas que cumplan las funciones de certificación sólo sean utilizados para ese objeto y fin y no puedan realizar ninguna otra función.

7. Garantizar que todos los sistemas que participen directa o indirectamente en la función de certificación estén protegidos por sistemas y procedimientos de autenticación y seguridad de alto nivel de protección, que serán actualizados de acuerdo a los avances tecnológicos para garantizar la correcta prestación del servicio.

Estándares

Artículo 38 La Superintendencia de Servicios de Certificación Electrónica de conformidad con la facultad que le confiere el artículo 27 de la Ley Sobre Mensajes de Datos y Firmas Electrónicas, establecerá los estándares o las prácticas aceptadas para la prestación de los Servicios de Certificación Electrónica.

Infraestructura Prestada por un Tercero

Artículo 39 Cuando el Proveedor de Servicios de Certificación requiera o utilice infraestructura o servicios tecnológicos prestados por un tercero, los contratos deberán prever que a la terminación de los mismos, se establezca un tiempo suficiente para que el Proveedor de Servicios de Certificación tome las medidas necesarias para garantizar la continuidad de la prestación de sus servicios sin ningún perjuicio para los signatarios.

La contratación de esta infraestructura o servicios no exime al Proveedor de Servicios de Certificación de la presentación de los informes de auditoria previstos en este reglamento, los cuales deben incluir los sistemas y seguridades del tercero contratado.

CAPITULO VIII

DISPOSICIONES FINALES

Artículo 40 Cualquiera de los requisitos establecidos en este reglamento deberán presentarse en idioma castellano o traducido al castellano por intérprete público.

Artículo 41 La Superintendencia de Servicios de Certificación Electrónica será el órgano encargado de la ejecución del presente Decreto.

Artículo 42 El presente Decreto entrará en vigencia a partir de la fecha de su publicación en la Gaceta Oficial de la Republica Bolivariana de Venezuela.

Dado en Caracas, a los días del mes de del año dos mil tres (2003). Año 193º de la Independencia y 144º de la Federación".

(L.S.)

HUGO RAFAEL CHÁVEZ FRIAS

PRESIDENTE DE LA REPÚBLICA

(L.S.)

JOSE VICENTE RANGEL

VICEPRESIDENTE EJECUTIVO

(L.S.)

Refrendado

Todos los Ministros

ANEXO E ENTIDADES REGULADORAS EN FIRMAS Y CERTIFICADOS DIGITALES EN EL MUNDO

En este anexo se presentan las entidades reguladoras en la certificación electrónica en el mundo para identificarlas y conocerlas

	PAÍS	ENTIDAD REGULADORA
	Alemania	Regulatory Authority for Telecommunications and Posts
	Australia	Australian Government's strategy for the use of Public Key Infrastructure (PKI) - Gatekeeper
	Austria	Supervisory Authority for Electronic Signatures
	Bélgica	Centre d' Information sur la Signature Electronique
	Brasil	ICP-Brasil - Infra-estrutura de Chaves Públicas Brasileira Instituto Nacional de Tecnologia da Informação Autoridade Certificadora Raiz da ICP
	Canadá	Government of Canada Public Key Infrastructure
	Chile	Entidad Acreditadora de Firma Electrónica Empresa Nacional de Certificación Electrónica Organismo Nacional de Certificación Electrónica Certificación Digital
	Colombia	Colombia: Superintendencia de Industria y Comercio
	EEUU	Federal Public Key Infrastructure Steering Committee NIST PKI Program Federal Bridge Certification Authority (FBCA)
	Eslovenia	Government Centre for Informatics
	España	Fábrica Nacional de Moneda y Timbre - Proyecto CERES Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información

	Finlandia	Finnish Communications Regulatory Authority
	Francia	Le site du programme d'action de l'Etat pour la société de l'information Serveur Thématique sur la Sécurité des Systèmes dInformation
	Hong Kong	Electronic Service Delivery Infrastructure
	India	Controller of Certifying Authorities
	Italia	CNIPA:Centro Nazionale per Informatica nella Pubblica Amministrazione
	Luxemburgo	Office Luxembourgeois d'Accreditation et de Surveillance
	Noruega	Norwegian Post and Telecommunication Authority
	Nueva Zelanda	Secure Electronic Environment PKI
	Panamá	Proyecto Firma Digital y Comercio Electrónico (SENACYT)
	Perú	INDECOPI - Acreditación de entidades de certificación
	Reino Unido	The National Technical Authority for Information Authority Government Gateway
	República de Corea	Korea Certification Authority Central
	Singapur	Controller of Certification Authorities
	Suecia	Swedish Board for Accreditation and Conformity Assessment
	Venezuela	Superintendencia de Servicios de Certificación Electrónica

ANEXO F BREVE REFERENCIA DEL RFC 2527

En este anexo se presenta una breve referencia del RFC 2527. Presenta un esqueleto para asistir a los que escriben la política de certificación o las prácticas de certificación para las autoridades de certificación de la ICP.

En particular, el esqueleto provee una lista comprensiva de tópicos que potencialmente (a discreción de los escritores) necesitan ser cubiertas en una Política de Certificación (PC) o Declaración de Práctica de Certificación (DPC).

En particular, el esqueleto identifica los elementos que deben ser considerados durante la formulación. El propósito es que no se definan PCs o DPCs particulares, para cada Autoridad de Certificación.

El rango de aplicación de este documento está limitado a la discusión de contenidos de la Política de Certificación (como se define en la X.509) o DPC (como se define en la ABA Guideline). El esqueleto presentado para ser usado según el formato X.509 versión 3 pero puede ser adaptado a nuevos formatos.

El documento presenta las siguientes definiciones:

- **Política de certificación, PC (en ingles Certificate policy, CP**): Conjunto de reglas que indican la aplicabilidad de un certificado en una comunidad y/o clase de aplicación con requerimientos de seguridad comunes.

- **Trayectoria o camino de certificación (Certificate path):** Es una secuencia ordenada de certificados con los cuales, en conjunto con una clave pública del

objeto inicial en la ruta o trayectoria (path), se puede proceder a obtener el objeto final en la ruta o trayectoria (path).

- **Declaración de prácticas de Certificación, DPC (en inglés Certification practice statement, CPS):** Es una declaración de las prácticas que la autoridad certificadora emplea para la emisión de certificados.

- **Campos del certificado (Certificate fields):** En el X.509 existen los siguientes campos para soportar las políticas de certificación:

    - Políticas de certificación (Certificate Policies Extension). Esta extensión tiene dos variantes, críticas y no críticas.

    - Mapeo de la política (Policy Mappings Extension). Puede ser utilizado únicamente en los certificados de las PSC. Permite indicar si ciertas políticas en su propio dominio pueden ser consideradas equivalentes a otras políticas en el dominio de la PSC usuaria.

    - Restricciones de la política (Policy Contrains Extension). Soporta dos características opcionales. La primera habilita a la PSC para requerir de una política de certificación explícita que debe estar presente en todos los caminos de certificación subsecuentes cuando el certificado abandona el dominio de confianza. La segunda característica opcional es habilitar a la PSC a desactivar el mapeo de la política, con lo cual la PSC evita que una PSC de mayor jerarquía imponga su dominio de confianza a una PSC usuaria.

- **Calificadores de Política (Policy Qualifiers):** Permite la utilización de políticas estandarizadas (o definida por parámetros), punteros a sitios donde se publican la DPC, etc. El X.509 no determina el propósito de este campo.