

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

**PROPUESTA DE METODOLOGÍA MODELO PARA INCORPORAR LA  
INFRAESTRUCTURA DE CLAVE PÚBLICA (ICP) EN LOS  
PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN (PSC) DEL  
ESTADO VENEZOLANO A TRAVÉS DE LA SUPERINTENDENCIA DE  
SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA (SUSCERTE)**

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

**AUTOR: Ing. Jessica O. Villegas Sánchez**

CARACAS, DICIEMBRE 2.007

## **TRABAJO ESPECIAL DE GRADO**

# **PROPUESTA DE METODOLOGÍA MODELO PARA INCORPORAR LA INFRAESTRUCTURA DE CLAVE PÚBLICA (ICP) EN LOS PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN (PSC) DEL ESTADO VENEZOLANO A TRAVÉS DE LA SUPERINTENDENCIA DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA (SUSCERTE)**

TUTOR Académico: Prof.: Vicenzo 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 Ing. Jessica O. Villegas Sánchez

CARACAS, DICIEMBRE 2.007

## DEDICATORIA

    Mi tesis la dedico  
    Con todo mi amor y cariño a  
Ti DIOS que me diste la oportunidad de vivir  
    Y de regalarme una familia maravillosa.  
    A todas aquellas persona  
    que me ayudaron de una u otra manera en  
especial a mi Madre que siempre me ha apoyado y me  
    ha dado fuerzas para salir de todas las  
adversidades, a mi hijo Samuel Alejandro  
    que con su amor y ternura ha sido  
    mi motor para seguir adelante,  
    a mi hermano Eduardo  
que sea un ejemplo para él este esfuerzo  
    de constancia y voluntad.

## AGRADECIMIENTOS

Esta tesis, si bien ha requerido de esfuerzo y mucha dedicación, no hubiese sido posible su finalización sin la cooperación desinteresada de todas y cada una de las personas que a continuación citaré y muchas de las cuales han sido un soporte muy fuerte en momentos de angustia y desesperación.

Primero y antes que nada, dar gracias a **Dios**, por estar conmigo en cada paso que doy, por llenarme de bendiciones, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante todo este período.

Agradecer hoy y siempre a mi Madre por su dedicación, empeño, por estar conmigo en los mejores momentos de mi vida y sobre todo ayudarme a levantar cada vez que caigo, por su amor y entrega incondicional y sobre todo por creer en mí. Siempre serás mi inspiración para alcanzar mis metas, por enseñarme que todo se aprende y que todo esfuerzo es al final recompensa. Tu esfuerzo, se convirtió en tu triunfo y el mío, TE AMO.

A mi porción de cielo que bajó hasta acá para hacerme la mujer más feliz y realizada del mundo, gracias porque nunca pensé que de tan pequeño cuerpecito emanara tanta fuerza y entusiasmo para sacar adelante a alguien. TE ADORO Samuel Alejandro que con tu alegría, amor, ternura y ocurrencias me has dado ánimo y fortaleza de seguir adelante, siendo mi motor principal para enfrentar los obstáculos que se me presenten para brindarte un mañana mejor.

A mi Hermano Eduardo, por apoyarme emocional y sentimentalmente con su compañía y palabras de aliento, ha logrado ser un verdadero orgullo para mí, lleno de entusiasmo y ganas de salir adelante sin ver hacia atrás, creyendo que los sueños se convierten en realidad con amor, empeño y dedicación.

Debo un especial reconocimiento al profesor Vincenzo Mendillo por la confianza que demostró en mí al concederme el honor de ser mi tutor Académico, con la

cual fue posible aventurarme en esta travesía, guiándome el camino para la culminación de esta especialización.

A mis amigas y compañeras Nelly, Sara, Coralia, Yralmy y María que con su compañerismo y colaboración creyeron en mí y en que este sueño se podría hacer realidad. Gracias por atenderme, escucharme, apoyarme, soportarme y regalarme el bello tesoro de la amistad, LAS VALORO.

A la Señora Gipsy por atenderme, apoyarme y colaborar en cuanto al proceso administrativo dentro de la Universidad, gracias por ser tan bondadosa con todos los que pasamos por estos trámites.

También agradezco especialmente al Ingeniero Sergio Torralba, por abrirme las puertas de la Superintendencia de Servicios de Certificación Electrónica, atenderme, enseñarme y darme la oportunidad de compartir con este bello grupo de trabajo.

No puedo olvidar a mis compañeros de labores con los cuales he compartido incontables horas de trabajo. Gracias por los excelentes momentos que hemos pasado.

# INDICE

<b>DEDICATORIA</b> .....	<b>III</b>
<b>AGRADECIMIENTOS</b> .....	<b>IV</b>
<b>RESUMEN</b> .....	<b>XI</b>
<b>INTRODUCCIÓN</b> .....	<b>12</b>
<b>CAPÍTULO I</b> .....	<b>16</b>
1. PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN .....	16
1.1.    CONTEXTO DEL PROBLEMA DE INVESTIGACIÓN .....	16
1.2.    OBJETIVO GENERAL DE LA INVESTIGACIÓN .....	18
1.3.    OBJETIVOS ESPECIFICOS DE LA INVESTIGACIÓN .....	18
1.4.    JUSTIFICACIÓN DE LA INVESTIGACIÓN.....	19
1.5.    ALCANCE Y LIMITACIONES DE LA INVESTIGACIÓN .....	19
<b>CAPÍTULO II</b> .....	<b>21</b>
2. MARCO TEORICO.....	21
2.1    ANTECEDENTES DE LA INVESTIGACIÓN .....	21
2.2    BASES LEGALES.....	24
2.3    BASES TEÓRICAS.....	29
2.3.1. <i>Seguridad</i> .....	29
2.3.2. <i>Políticas de Seguridad Informática</i> .....	36
2.3.3. <i>Auditoría</i> .....	40
2.3.4. <i>Infraestructura de Clave Pública (ICP)</i> .....	51
2.3.5. <i>Tarjetas Inteligentes</i> .....	66
2.3.6. <i>Contexto Organizacional de Suscerte</i> .....	70
<b>CAPÍTULO III</b> .....	<b>77</b>
3. MARCO METODOLÓGICO .....	77
3.1. MODELO DE LA INVESTIGACIÓN .....	77
3.2. DISEÑO DE LA INVESTIGACIÓN .....	78
3.3. POBLACIÓN Y MUESTRA .....	79
3.4. METODOLOGÍA A UTILIZAR .....	80
3.5. PROCEDIMIENTO DE LA INVESTIGACIÓN .....	80
3.6. ANÁLISIS DE LA INFORMACIÓN RECOLECTADA .....	81
<b>CAPÍTULO IV</b> .....	<b>86</b>
4. PROPUESTA .....	86
4.1. INTRODUCCIÓN .....	86
4.2. DEFINICIONES Y TERMINOLOGÍAS.....	88
4.3. SIMBOLOS Y ABREVIATURAS .....	90
4.4. INFRAESTRUCTURA NACIONAL DE CLAVES PÚBLICAS (INCP) .....	91
4.5. CERTIFICADOS DIGITALES .....	106
4.6. UNIDADES ORGANIZACIONALES REQUERIDAS PARA LA OPERACIÓN DEL PSC .....	123
4.6.1 <i>Dirección General del PSC</i> .....	124
4.6.2 <i>Unidad de Organización de Sistemas</i> .....	124
4.6.3 <i>Unidad de Auditoría</i> .....	124
4.6.4 <i>Unidad de Consultoría Jurídica</i> .....	125
4.6.5 <i>Unidad de Soportes a las Operaciones y Tecnología</i> .....	125
4.6.6 <i>Departamento de Investigación, Desarrollo e Innovación</i> .....	125

4.6.7	<i>Departamento del Apoyo Tecnológico</i> .....	125
4.6.8	<i>Unidades de Soporte de Comercialización</i> .....	127
4.7.	OPERACIONES DEL PSC .....	127
4.8.	ATENCIÓN A LA GARANTÍA DE CERTIFICADOS DIGITALES Y FIRMAS ELECTRÓNICAS .....	128
4.9.	PROCEDIMIENTO PARA LA EVALUACIÓN DE AUDITORIA AL PSC .....	131
<b>CONCLUSIONES</b> .....		<b>148</b>
<b>RECOMENDACIONES</b> .....		<b>150</b>
<b>LISTA DE REFERENCIAS</b> .....		<b>152</b>
<b>FUENTES ELECTRÓNICAS</b> .....		<b>153</b>
<b>ANEXOS</b> .....		<b>155</b>
ANEXO A.	ESTÁNDARES CRIPTOGRÁFICOS DE CLAVE PÚBLICA.....	156
ANEXO B.	DECRETO CON FUERZA DE LEY SOBRE MENSAJES DE DATOS Y FIRMAS ELECTRÓNICAS .....	159
ANEXO C.	REGLAMENTO PARCIAL DE LA LEY SOBRE MENSAJES DE DATOS Y FIRMAS ELECTRÓNICAS .....	169
ANEXO D.	ENTIDADES REGULADORAS EN FIRMAS Y CERTIFICADOS DIGITALES EN EL MUNDO .....	184
ANEXO E.	GLOSARIO DE TÉRMINOS .....	185
ANEXO F.	CONCEPTOS DEFINIDOS POR SUSCERTE EN SUS NORMAS 017, 018, 019, 020, 021, 023, 024 Y 025.....	191
ANEXO G.	IDENTIFICACIÓN DE ACRÓNIMOS QUE CONSIDERA LO EXPUESTO EN LAS NORMAS 017, 018, 019, 020, 021,023, 024 Y 025 EMITIDAS POR SUSCERTE.....	198
ANEXO H.	REQUERIMIENTOS GENERALES DE HARDWARE Y SOFTWARE PARA EL OTORGAMIENTO DE CERTIFICADOS DIGITALES.....	199
ANEXO I.	ESTRUCTURA DE LOS CERTIFICADOS DIGITALES .....	204
ANEXO L.	FORMATO DE REGISTRO DEL EXPEDIENTE DEL PSC .....	211
ANEXO M.	LISTA DE RECAUDOS LEGALES, ECONÓMICOS - FINANCIEROS Y TÉCNICOS .....	212

## Lista de Figuras

Figura 2.1 Modelo detallado a ser auditados al PSC .....	48
Figura 2.2 Estructura jerárquica de la INCP de Venezuela .....	54
Figura 2.3 Estructura de (INCP) para los sectores público y privado de Venezuela .....	55
Figura 2.4 Componentes de la ICP de Venezuela.....	59
Figura 2.5 HSM nCipher nShield F3 PCI.....	67
Figura 2.6 Estructura Organizativa actual de SUSCERTE.....	75
Figura 4.1 Relación de Confianza.....	94
Figura 4.2 Arquitectura Jerárquico General de la INCP .....	95
Figura 4.3 Estructura jerárquica de la INCP de Venezuela .....	96
Figura 4.4 Estructura de (INCP) para los sectores público y privado de Venezuela .....	97
Figura 4.5 Componentes de la ICP de Venezuela.....	101
Figura 4.6 Proceso de Emisión de Certificados .....	110
Figura 4.7 Proceso de Suspensión de Certificados .....	111
Figura 4.8 Proceso de Revocación de Certificados.....	116
Figura 4.10 Unidades Organizacionales del PSC .....	123
Figura 4.11 Proceso de Atención de Solicitudes de Cambio .....	128



## Lista de Tablas

Tabla N° 2.1 Solicitud de Auditoria a los PSC .....	46
Tabla N° 2.2 Procedimiento de Solicitud de Renovación .....	65
Tabla N° 4.1 Estructura de los datos del certificado de la AC Raíz.....	103
Tabla N° 4.2 Estructura de los datos del certificado del PSC .....	105
Tabla N° 4.3 Procedimiento de Solicitud de Renovación .....	113
Tabla N° 4.3 Procedimiento de Solicitud de Suspensión.....	115
Tabla N° 4.4 Procedimiento para la realización de la Auditoria.....	135
Tabla N° 4.5 Clasificación de criterios por áreas a ser evaluados a los Solicitante a PSC.....	147

## Lista de Gráficos

Gráfico 3.1 Existencia de una documentación.....	82
Gráfico 3.2 Facilidad de la documentación existente .....	82
Gráfico 3.3 Existencia de metodología modelo para incorporar la ICP para los PSC.....	83
Gráfico 3.4 Existencia de la necesidad de una metodología modelo a seguir por el PSC.....	84
Gráfico 3.5 Facilitaría al PSC su proceso de acreditación y la incorporación de la ICP, el contar con una metodología modelo .....	85

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

**PROPUESTA DE METODOLOGÍA MODELO PARA INCORPORAR LA  
INFRAESTRUCTURA DE CLAVE PÚBLICA (ICP) EN LOS  
PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN (PSC) DEL  
ESTADO VENEZOLANO**

Autor: Ing. Jessica O. Villegas Sánchez  
Tutor: Prof. Vincenzo Mendillo  
Diciembre 2007

**RESUMEN**

El objetivo principal de este trabajo es diseñar una propuesta de metodología modelo para incorporar la Infraestructura de Clave Pública (ICP) en los Proveedores de Servicios de Certificación (PSC) del Estado Venezolano, para dar una referencia clara y detallada de cuales son los pasos a seguir cuando se quiere diseñar una Infraestructura de Clave Pública, siguiendo las especificaciones solicitadas por SUSCERTE.

Para la consecución de los objetivos de este proyecto se llevaron a cabo diversas actividades entre las que destacan la realización del levantamiento de información inicial, considerando todo lo relacionado con los requisitos exigidos por SUSCERTE y se hicieron investigaciones sobre las necesidades de fomentar y detallar mejor la información sobre los requerimientos para incorporar una ICP en los PSC. Se identificaron y clasificaron las aplicaciones y servicios susceptibles a incorporar una ICP y las plataformas recomendadas de software y de hardware.

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.

## INTRODUCCIÓN

A lo largo de la historia el ser humano ha desarrollado sistemas de seguridad que le permitían comprobar la identidad del interlocutor en una comunicación.

Con el fin de asegurar la información del destinatario seleccionado se utilizó un correo certificado y para evitar su modificación se utilizó un mensaje notariado, pero el envío y recepción de información por las redes de computadoras bajo medios de comunicación inseguros y no supervisados generaron un problema de seguridad en las tecnologías de comunicación utilizadas en la actualidad.

En la mayor parte de los casos el sistema de seguridad se basa en la identificación física de la persona, información que se contrasta con el documento de identidad.

En contraste, las actividades ofimáticas como el intercambio de información se están trasladando al mundo electrónico a través de Internet, los programas de seguridad de la información son importantes para las organizaciones que quieren progresar y crecer en un mundo en línea cada vez más inseguro.

El crecimiento de los medios de comunicación trajo consigo el incremento de medios de interceptación de información por Sniffers y Hackers sin distinción de medios de transmisión, pudiendo ser éstos cable, inalámbricos y satélites entre otros, creando inseguridad en la transferencia de la información.

Por lo tanto, se hace 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.

Por ser esencial la seguridad, la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), quien es el gran motor impulsor del uso de la firma electrónica en el país, pilar fundamental para la existencia y puesta en marcha del gobierno electrónico, básicamente necesita prestar servicios como la autenticación de usuarios, para asegurarse de la identidad de un usuario, garantizar el acceso a servicios distribuidos en red, también impedir que una vez que el usuario ha realizado una operación se retracte o niegue haberlo hecho, prevenir la modificación deliberada o accidental de los datos, durante su transporte, almacenamiento o manipulación, en el correo electrónico, etc.

En resumen se desea garantizar la seguridad de las transacciones de los usuarios, por ello que se debe contar con mecanismos de autenticación e identificación de usuarios, control de acceso y privacidad de la información siendo estos transparentes para los mismos.

Esto se hace actualmente mediante certificados digitales los cuales permiten firmar digitalmente dichas transacciones u operaciones, siendo necesaria una Infraestructura de Clave Pública (ICP).

La Infraestructura de Clave Pública (ICP) es el conjunto de hardware y software necesarios para la creación, administración, distribución y revocación de certificados digitales. El propósito de esta infraestructura es la administración de claves y certificados digitales. Un certificado es una instrucción firmada digitalmente que contiene una clave pública y el nombre de un tema. El esquema de seguridad ICP tiene entre sus ventajas que permite que usuarios desconocidos entre sí, se comuniquen de manera segura en redes inseguras, permite la identificación electrónica confiable, la creación de relaciones de confianza y es la base para el uso de firmas digitales y no repudio. Puede utilizarse en una amplia gama de aplicaciones financieras, de comunicación, de comercio electrónico, intercambio electrónico de datos, Redes Privadas Virtuales (VPN) y otros.

Por esta razón se ha impulsado la prioridad de adoptar estas tecnologías de Firmas Electrónicas, y los Servicios de Certificación de las mismas. En relación a esto se crea la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), como un servicio autónomo adscrito al Ministerio del Poder

Popular para las Telecomunicaciones y la Informática (MPPTI); y cuyo objeto es acreditar, supervisar y controlar, a los proveedores de servicios de certificación (PSC) en los términos previsto en la Ley Sobre Mensaje de Datos y Firmas Electrónicas (LSMDFE) y su reglamento.

Es entonces SUSCERTE el encargado del diseño de la Infraestructura de Clave Pública (ICP), en inglés 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.

De esta forma SUSCERTE, como ente regulador para desempeño de su gestión en función de excelencia, debe establecer y describir los procedimientos 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 Proveedor SC 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 desarrollo y diseño de una Metodología modelo para incorporar la Infraestructura de Clave Pública (ICP) en los Proveedores de Servicios de Certificación (PSC) del Estado Venezolano para que sean de conocimiento público y establece los elementos mínimos requeridos para la operación de un Proveedor, incluyendo sistemas, políticas y procedimientos, aprobado por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE). De esta manera se generaría más confianza en el proceso de acreditación y un amplio control en el cumplimiento de sus recaudos solicitados.

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 límites del trabajo presentado.

**CAPITULO II:** Se presenta lo que se ha considerado esencial conocer sobre la seguridad electrónica, políticas de seguridad, Infraestructura de Clave Pública, modelos de confianza, Auditoría a los solicitantes a Proveedor de Servicios de Certificación 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 Metodología modelo para incorporar la Infraestructura de Clave Pública (ICP) en los Proveedores de Servicios de Certificación (PSC) del Estado Venezolano, especificando los elementos que componen la Infraestructura, estructura y tipos de certificados emitidos por los Proveedores, el modelo operacional del Proveedor y las auditorías que se les realiza por la Superintendencia.

Finalmente, se presentan las conclusiones y recomendaciones obtenidas como resultado del proyecto presentado.

# CAPÍTULO I

## 1. PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN

*En este capítulo se mostrará la manera en que la idea se desarrolla y se transforma en la descripción de la situación planteada y cual sería su solución inmediata.*

### 1.1. CONTEXTO DEL PROBLEMA DE INVESTIGACIÓN

Venezuela avanza aceleradamente hacia la actualización en materia de tecnologías de información y de las comunicaciones. En los últimos años esta evolución tecnológica ha revolucionado a nivel mundial las diferentes áreas del conocimiento y de las actividades humanas, fomentando el surgimiento de nuevas formas de trabajar, aprender, comunicarse y celebrar negocios, al mismo tiempo ha contribuido a borrar fronteras, comprimir el tiempo y acortar las distancias.

La particularidad de estas tecnologías de información es que utilizan medios electrónicos y las 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.

En consecuencia, se hace necesaria e inminente la regulación de las modalidades básicas de intercambio de información por medios electrónicos, de las cuales han de desarrollarse todas las nuevas modalidades de transmisión y recepción de información, conocidas y por conocerse.



Como complemento necesario a estas disposiciones se crea la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), adscrito al Ministerio del Poder Popular para las Telecomunicaciones y la Informática, que tiene por objeto acreditar, supervisar y controlar, en los términos previstos en la presente Decreto-Ley y sus Reglamentos, a los Proveedores de Servicios de Certificación, bien sean públicos o privados, a fin de verificar que cumplan con los requerimientos necesarios para ofrecer un servicio eficaz y seguro a los usuarios.

Estos Proveedores de Servicios de Certificación (PSC) una vez acreditados tendrán entre sus funciones emitir un documento contentivo de información “cerciorada” que vincule a una persona natural o jurídica y confirma su identidad, esto a fin de que el receptor pueda asociar inequívocamente la firma electrónica del mensaje a un emisor. El PSC da certeza de la autoría de un mensaje de datos mediante la expedición del certificado electrónico.

Cabe destacar que antes de que el PSC se acredite es necesario que cumpla y mantenga los requisitos señalados en el Decreto-Ley.

Los PSC presentan ante SUSCERTE, junto con la solicitud de acreditación, los documentos que acrediten el cumplimiento de los requisitos señalados en el Artículo 31 de la LSMDFE. SUSCERTE, previa verificación de tales documentos, procederá a recibir y procesar dicha solicitud y deberá pronunciarse sobre la acreditación del PSC.

Para dar cumplimiento a lo expresado en la LSMDFE, se hicieron varias investigaciones sobre el tema para determinar como será la operación de la ICP del PSC y se concluyó que no existe un documento con el alcance, responsabilidades, obligaciones, procedimiento de solicitud, los elementos que deben componer la ICP, los tipos de certificados digitales que emitirán, como deben especificar el proceso interno del modelo operativo con sus direcciones involucradas, los controles deben cumplir cuando se le efectúe la auditoría antes de ser acreditado un PSC.

Entonces se decidió que es importante elaborar el documento de la Metodología modelo para incorporar la Infraestructura de Clave Pública (ICP) en los Proveedores de Servicios de Certificación (PSC) del Estado Venezolano, para que sean de conocimiento público y establecer los elementos mínimos requeridos para la operación de un Proveedor de Servicios de Certificación Electrónica (PSC), incluyendo sistemas, políticas y procedimientos, aprobado por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE). De esta manera se generaría más confianza en el proceso de acreditación y un amplio control en el cumplimiento de los recaudos solicitados.

## **1.2. OBJETIVO GENERAL DE LA INVESTIGACIÓN**

La propuesta de metodología modelo para incorporar la Infraestructura de Clave Pública (ICP) en los Proveedores de Servicios de Certificación (PSC) del Estado Venezolano tiene como objetivo principal dar una referencia clara y detallada de cuales son los pasos a seguir cuando se quiere diseñar una Infraestructura de Clave Pública, siguiendo las especificaciones solicitadas por SUSCERTE.

## **1.3. OBJETIVOS ESPECIFICOS DE LA INVESTIGACIÓN**

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

- Identificar y clasificar las aplicaciones o servicios susceptibles a incorporar una Infraestructura de Clave Pública.
- Clasificar la distribución de los recaudos y evaluar de los requisitos a entregar por el solicitante a PSC.
- Analizar y comparar las legislaciones y regulaciones a nivel mundial sobre el uso de Firmas Electrónicas en aplicaciones de Gobierno.
- Investigar los diferentes estándares para gestión de documentos electrónicos de PKI.

- Seleccionar los estándares de desarrollo y mejores prácticas recomendadas a utilizar para implementar la ICP.
- Identificar las plataformas recomendadas de software y hardware.

#### **1.4. JUSTIFICACIÓN DE LA INVESTIGACIÓN**

El desarrollo del Modelo propuesto identificará perfectamente las especificaciones técnicas de la firma electrónica para su incorporación en el PSC, dando así a conocer las mejores prácticas tecnológicas desde el inicio del proceso hasta el cierre, tomando en consideración los lenguajes de programación específicos para su mejor ejecución, junto con las aprobaciones legales electrónicas, entre otros.

Este proyecto surge para dar respuesta a todos los solicitante a PSC de manera de aclarar las dudas encontradas en el cumplimiento de los requisitos solicitados por SUSCERTE, centralizando y unificando todo los alcances, responsabilidades, obligaciones, elementos que deben componer la ICP, los procesos internos del modelo operativo con sus direcciones involucradas y los controles deben ejecutar cuando se le efectúe la auditoria antes de ser acreditado.

El desarrollo de este documento se adaptará perfectamente a las normativas existentes en la Superintendencia. El diseño de esta metodología se concibe para que cause el menor impacto posible a los solicitantes a PSC en el momento de acreditarse a SUSCERTE, previendo que se realicen futuras modificaciones parciales a sus requerimientos.

Así mismo, SUSCERTE habría de disponer de procedimientos técnicos, administrativos y legales simplificados en línea para este procedimiento.

#### **1.5. ALCANCE Y LIMITACIONES DE LA INVESTIGACIÓN**

Los esfuerzos para desarrollar la administración electrónica van más allá del pensar en aplicaciones para que el ciudadano se pueda contactar por Internet. Si entre los alcances está facilitar los servicios al ciudadano, el primer paso debe ser dentro

de la Administración Pública Nacional y ya no solamente nos referimos al cambio de la cultura organizativa, sino también a la integración de sistemas tecnológicos que faciliten y aseguren el intercambio de datos entre administraciones.

A medida que la información digital se incorpora a más aspectos de la vida cotidiana, muchos trámites que tradicionalmente se realizaban en papel pasan a efectuarse de manera electrónica. Esto representa una ventaja para el tratamiento de la información.

Es por esta razón que este proyecto surge, para dar respuestas sobre Infraestructura de Clave Pública (ICP), mejores prácticas y su incorporación a los futuros Proveedores de Servicios de Certificación (PSC), bien sean éstos públicos o privados, a fin de verificar que cumplan con los requerimientos necesarios para ofrecer un servicio eficaz y seguro a los usuarios.

Además, contribuirá con asistencia tecnológica para las nuevas iniciativas de ICP. De esta manera las Administraciones Públicas Nacionales y demás organismos de todos los niveles habrían de esforzarse por explotar las nuevas tecnologías para hacerlas lo más accesible posible.

Así mismo, las Administraciones Públicas Nacionales, disfrutarían de procedimientos técnicos, administrativos y legales simplificados en línea disponibles para su incorporación.

Entre las limitaciones que se encuentran se pueden mencionar los pocos antecedentes de la investigación debido a que es un tema nuevo, no ha sido investigado previamente y las trabas presentadas para recopilar los datos e información sobre el mismo.

## CAPÍTULO II

### 2. MARCO TEORICO

#### OBJETIVO

*El presente capítulo expone trabajos previos de Infraestructura de Clave Pública y Firma Electrónica, la base legal, la base teórica con definiciones de una visión general de la misma, seguridad de Infraestructura de Clave Pública (ICP). Se proporciona información relevante sobre el área en estudio, facilitando de esta forma la comprensión de los conceptos básicos utilizados al desarrollar una Metodología modelo para incorporar la Infraestructura de Clave Pública en los Proveedores de Servicios de Certificación (PSC).*

#### 2.1 ANTECEDENTES DE LA INVESTIGACIÓN

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

Liendo, María del Carmen. (2006). Tesis **“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”**.

#### 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 sentó 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.

Palma, Marcelo (2005). Tesis **“Desarrollo de una Aplicación para Administración de Firmas y Certificados Digitales caso: Superintendencia de Telecomunicaciones”**.

## RESUMEN

La Superintendencia de Telecomunicaciones (SITTEL) tiene la potestad otorgada por el gobierno para administrar las telecomunicaciones en Bolivia desde 1995, entre sus principales Departamentos se encuentra el Departamento de Tecnologías de Información y Comunicación (TIC), que es nuestro objeto de estudio en el presente trabajo.

El Departamento de TIC surgió de la necesidad de administrar las tecnologías que apoyan el intercambio de información entre los diferentes usuarios internos e instituciones externas relacionadas con SITTEL, desde su creación como departamento de Sistemas fue adquiriendo nuevas tareas en pro de la Sociedad de la Información Boliviana.

En asociación con la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB) desde el 2002, el departamento de TIC de SITTEL participa en proyecto que proponen políticas, implementan estrategias y coordinan acciones tendientes a lograr un uso y aprovechamiento óptimo de las Tecnologías de

Información y Comunicación en contextos como la Estrategia Boliviana de Reducción de la Pobreza, los planes y acciones nacionales y/o regionales de desarrollo o estrategias consultivas como el Diálogo Nacional.

Para el logro de estos propósitos, resulta de gran utilidad proteger la información que genera SITTEL, a través de herramientas de tecnológicas que brinden seguridad en las intercomunicaciones internas y externas.

El contenido del presente proyecto de grado realiza un análisis de seguridad al departamento de TIC de SITTEL orientado hacia el uso de herramientas de control criptográfico para incrementar el nivel de seguridad de la información frente al uso de herramientas convencional como Pared de Fuego y productos de seguridad Microsoft que están orientados hacia la protección de la información externa de la institución gubernamental.

Al respecto las organizaciones mundiales en seguridad como la Asociación de Internautas (AI), International Communication Union (ITU), International Standard Association (ISO) determinaron que más de la mitad de los ataques informáticos son realizados dentro de las empresas y organizaciones (robo de información para ser vendida a la competencia, violación de la seguridad física y lógica, fraude a los sistemas, entre otros).

Los Estándares Internacionales y los Sistemas de Gestión de Seguridad de la Información (SGSI) desarrollados por la Norma Boliviana ISO/IEC 17799 hacen hincapié en el uso de herramientas criptográficas que coadyuvan al control por riesgos internos en la seguridad de la información en la empresas y organizaciones anteriormente mencionados, evitando que los mismos se materialicen en amenazas que pongan en riesgo la continuidad del negocio.

Los controles criptográficos son herramientas que aseguran la **integridad** (salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento), **disponibilidad** (garantizar que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera) y

**autenticación de la información** (garantizar que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella), los cuales son conceptos son la base de la Norma Boliviana ISO/IEC 17799 para los Sistemas de Gestión de Seguridad que fueron implantados en SITTEL a través de un Sistema de Administración de Firmas y Certificados Digitales.

## 2.2 BASES LEGALES

El objetivo principal del Decreto-Ley 1.204 de fecha 10 de Febrero de 2001, es adoptar un marco normativo que avale los desarrollos tecnológicos sobre seguridad en materia de comunicación y negocios electrónicos, para dar pleno valor jurídico a los mensajes de datos que hagan uso de estas tecnologías.

Como complemento necesario a estas disposiciones se crea la Superintendencia de Servicios de Certificación Electrónica, cuyo objetivo es acreditar, supervisar y controlar a los Proveedores de Servicios de Certificación, bien sean estos públicos o privados, a fin de que cumplan con los requisitos necesarios para ofrecer un servicio eficaz y seguro a los usuarios.

Estos Proveedores de Servicios de Certificación una vez acreditados, tendrán entre sus funciones emitir un documento contentivo de información “cerciorada” que vincule a una persona natural o jurídica y confirme su identidad, con la finalidad que el receptor pueda asociar inequívocamente la firma electrónica del mensaje del emisor.

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

1. Ley sobre Mensajes de Datos y Firmas Electrónicas.
2. Artículos 108 y 110 de la Constitución Nacional.
3. Reglamento Parcial del Decreto Ley Sobre Mensajes de Datos y Firmas



Electrónicas.

4. Ley Orgánica de Ciencia, Tecnología e Innovación.
5. Ley Orgánica de la Administración Pública.
6. Ley Especial sobre Delitos Informáticos.
7. Ley de Protección al Consumidor y al Usuario
8. Ley Orgánica de Telecomunicaciones

1 **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.

2 **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 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.

**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 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.

**6 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.

**7 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.

**8 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 cumplimiento 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.

## **2.3 BASES TEÓRICAS**

Como bien su nombre lo dice, las bases teóricas brindan todos aquellos conocimientos relacionados con la investigación, las cuales sirven como punto de apoyo para llevar cabo la misma. Éstas se tomaron de acuerdo a la relación que se tiene con la investigación y como incide en la propuesta de una metodología modelo para incorporar la Infraestructura de Clave Pública (ICP) en los Proveedores de Servicios de Certificación (PSC) del Estado Venezolano.

### **2.3.1. Seguridad**

Podemos entender como seguridad un estado de cualquier sistema (informático o no) que nos indica que el mismo está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados

que se obtienen del mismo. Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro.

La seguridad se define como la preservación de las siguientes características:

- **Confidencialidad:** Se garantiza que la información sea accesible sólo aquellas personas autorizadas a tener acceso a ella.
- **Integridad:** Se salvaguarda la exactitud y totalidad de la información, de los métodos de procesamiento.
- **Disponibilidad:** Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera.
- **Autenticación:** Se garantiza que el usuario que accede a la información sea realmente quien dice ser.

La seguridad se logra implementando un conjunto adecuado de controles, que abarca, políticas, prácticas, normas, procedimientos, estructuras organizacionales, estructuras físicas y lógicas, tecnológicas, recurso humano, entre otros.

Los medios de comunicación frecuentemente relatan incidentes que conciernen a amenazas de seguridad relacionados al Internet. Desde los problemas de seguridad con programas de navegación en Internet hasta ataques sofisticados que apuntan a comprometer servidores de comercio electrónico, servidores de correo, redes privadas, usuarios y otros, mientras que los administradores de redes deben abocarse a la creciente complejidad en el ambiente de seguridad.

Los ataques de hackers, los cuales incluyen virus, se han convertido en actividades cada vez más comunes. Grandes negocios en línea han probado ser vulnerables y han sido víctimas de serios ataques acarreando pérdidas considerables.

La Internet está disponible para cualquiera con una conexión de red y un acceso a un proveedor de servicios de Internet (ISP).

Términos relacionados con la seguridad informática:

- **Activo:** recurso del sistema de información o relacionado con éste, necesario

para que la organización funcione correctamente y alcance los objetivos propuestos.

- **Amenaza:** es un evento que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
- **Impacto:** consecuencia de la materialización de una amenaza.
- **Riesgo:** posibilidad de que se produzca un Impacto determinado en un Activo, en un Dominio o en toda la Organización.
- **Vulnerabilidad:** posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.
- **Ataque:** evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.
- **Desastre o Contingencia:** interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

Aunque a simple vista se puede entender que un Riesgo y una Vulnerabilidad se podrían englobar un mismo concepto, una definición más informal denota la diferencia entre ambos.

### ***2.3.1.1 Mecanismos de Seguridad específicos***

Ciertas técnicas pueden ser implementadas en diferentes niveles para proveer la seguridad, entre las cuales se encuentran las siguientes:

- ✓ **Mecanismos de Cifrados.** Estos encriptan los datos durante su transmisión entre dos sistemas o entre dos procesos en una máquina local.
- ✓ **Mecanismos de Firma Digital.** Éste es muy parecido a los mecanismos de cifrado, pero tienes ventajas adicionales para verificar que tanto el contenido como el remitente del mensaje son auténticos.

- ✓ **Mecanismos de control de acceso.** Estos son chequeos simples para determinar si realmente los usuarios están autorizados para llevar a cabo una tarea o un procedimiento.
- ✓ **Mecanismos de integridad de datos.** Técnicas para verificar que cada pieza de dato recibida o transmitida sobre un canal no haya sufrido modificaciones.
- ✓ **Mecanismos de autenticación.** Este mecanismo puede estar representado por un esquema de contraseña a nivel de usuario para determinar la autenticidad del usuario y reducir el acceso global y si una entrada no autorizada toma lugar.

### ***2.3.1.2 Establecimiento de los requerimientos de seguridad***

Es esencial que una organización identifique sus requerimientos de seguridad. Existen tres recursos principales para lograrlo.

- Evaluar los riesgos que enfrenta la organización. Mediante la evaluación o análisis de riesgos se identifican las amenazas a los activos, se evalúan las vulnerabilidades y probabilidades de ocurrencia y se estima el impacto potencial.
- Determinar los requerimientos legales, normativos, reglamentarios y contractuales que debe cumplir la institución y los proveedores de servicios.
- Establecer el conjunto específico de principios, objetivos y requisitos para el procesamiento de la información, que ha desarrollado la organización para respaldar sus operaciones.

### ***2.3.1.3 Selección de Controles***

Una vez identificados los requerimientos de seguridad, deben seleccionarse e implementarse controles para garantizar que los riesgos sean reducidos a un nivel aceptable. Los controles pueden seleccionarse sobre la base de este documento, de otros estándares o pueden diseñarse nuevos controles para satisfacer necesidades específicas según corresponda.



No obstante, es necesario reconocer que algunos controles no son aplicables a todos los sistemas o ambientes de información y podrían no resultar viables en todas las organizaciones.

Los controles deben seleccionarse teniendo en cuenta:

- El costo al ser implementados en relación con los riesgos a reducir y las pérdidas que podrían producirse de tener lugar una violación de la seguridad.
- Los factores no monetarios o intangibles, como el daño en la reputación y la pérdida de confianza.

Algunos controles pueden considerarse como principios rectores que proporcionan un buen punto de partida al implementar la seguridad de la información. Están basados en requisitos legales fundamentales o bien se consideran como práctica recomendada de uso frecuente concerniente a la seguridad de la información.

Los controles que se consideran esenciales para una organización, desde el punto de vista legal comprenden:

- Protección de datos y confidencialidad de la información personal.
- Protección de registros y documentos de la organización.
- Derechos de propiedad intelectual.

Otros controles son considerados como práctica recomendada al implementar la seguridad de la información, tales como:

- Documentación de la política de seguridad de la información.
- Asignación de responsabilidades en materia de seguridad de la información.
- Instrucción y entrenamiento en materia de seguridad de la información.
- Comunicación de incidentes relativos a la seguridad.
- Administración de la continuidad de la empresa.

Estos controles son aplicables a la mayoría de las organizaciones y en la mayoría de los ambientes, de todos modos, la relevancia de cada uno de ellos debe ser determinada teniendo en cuenta los riesgos específicos que afronta la organización.

#### **2.3.1.4 Seguridad Lógica**

Existe un viejo dicho en la seguridad informática que dicta que “todo lo que no está permitido debe estar prohibido” y esto es lo que debe asegurar la Seguridad Lógica, podemos pensar en la Seguridad Lógica como la manera de aplicar procedimientos que aseguren que sólo podrán tener acceso a los datos las personas o sistemas de información autorizados para hacerlo.

Los objetivos que se plantean serán:

1. Restringir el acceso a los programas y archivos.
2. Los operadores deben trabajar sin supervisión minuciosa y no podrán modificar ni programas archivos que no correspondan.
3. Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.
4. Asegurar que la información transmitida sea recibida sólo por el destinatario al cual ha sido dirigida y por ningún otro.
5. Asegurar que la información que el destinatario ha recibido sea la misma que ha sido transmitida.
6. Se debe disponer de sistemas alternativos de transmisión de información entre diferentes puntos.

#### **2.3.1.5 Seguridad Física**

Se argumenta que la seguridad perfecta sólo existe en una habitación sin puertas, pero eso naturalmente no es posible, en la actualidad el objetivo es prevenir, detectar y detener las rupturas de seguridad informática y de las organizaciones. ISO 17799 ofrece un marco para la definición de la seguridad informática en la organización y ofrece mecanismos para administrar el proceso de seguridad.

### 2.3.1.5.1 *Controles de Seguridad Física y de entorno. ISO 17799*

Este estándar proporciona a las organizaciones los siguientes beneficios, entre otros:

- Una metodología estructurada reconocida internacionalmente.
- Un proceso definido para evaluar, implementar, mantener y administrar seguridad informática.
- Una certificación que permite a una organización demostrar su 'status' en seguridad.

ISO 17799 contiene 10 controles de seguridad, los cuales se usan como base para la evaluación de riesgos, entre los 10 controles mencionados se encuentran aquellos orientados a garantizar la Seguridad Física y del entorno.

Los controles de Seguridad Física manejan los riesgos inherentes a las instalaciones de las empresas, e incluyen:

- **Ubicación:** Se deben analizar las instalaciones de la organización, considerando la posibilidad de un desastre natural.
- **Seguridad del perímetro físico:** El perímetro de seguridad de las instalaciones debe estar claramente definido y físicamente en buen estado, las instalaciones pueden dividirse en zonas, basándose en niveles de clasificación u otros requerimientos de la organización.
- **Control de accesos:** Las aperturas en el perímetro de seguridad de las instalaciones deben contar con controles de ingreso/salida proporcionales con el nivel de clasificación de la zona a la que afecta.
- **Equipamiento:** Los equipos deben estar situados en una zona de las instalaciones que asegure, físicamente y en su entorno, su integridad y disponibilidad.
- **Transporte de bienes:** Mecanismos para el ingreso o salida de bienes a través del perímetro de seguridad.

- **Generales:** Políticas y estándares, como la utilización de equipos de destrucción de documentos, almacenamiento seguro y regla de ‘escritorio limpio’, deben existir para administrar la seguridad operacional en el espacio de trabajo.

### **2.3.2. Políticas de Seguridad Informática**

Es frecuente que las personas involucradas con seguridad informática tengan una visión estrecha del que significa desarrollar las políticas de seguridad, pues no basta con escribirlas y pretender ponerlas en práctica. En ocasiones se incluye la asignación de responsables, se realizan actividades para dar a conocerlas y quizás, se supervise su cumplimiento; pero esto tampoco basta.

Es importante acotar que las políticas siempre deben estar en línea con los objetivos de la organización. Estas políticas establecen en marco de regulación para las actividades del negocio al definir de manera clara y precisa cada uno de los roles y responsabilidades que apoyan el progreso de la organización en continuo resguardo de todos los elementos que puedan considerarse como activos de importancia.

El proceso de definición de las políticas de seguridad informática de una organización, depende en gran medida de la naturaleza de las actividades de la institución, del ambiente en las que éstas se llevan a cabo, de la cultura organizacional y de muchos otros factores que determinan o condicionan la aplicabilidad o no de las políticas, normas y/o procedimientos de seguridad para la información.

#### **2.3.2.1. ¿Por qué tener Políticas escritas?**

Existen varias razones por las cuales es recomendable tener políticas escritas en una organización. La siguiente es una lista de algunas de estas razones:

- Para cumplir con regulaciones legales o técnicas.
- Como guía para el comportamiento profesional y personal.
- Permite unificar la forma de trabajo de personas en diferentes lugares o momentos que tengan responsabilidades y tareas similares.

- Permiten recoger comentarios y observaciones que buscan atender situaciones anormales en el trabajo.
- Permiten encontrar las mejores prácticas en el trabajo.
- Permiten asociar la filosofía de una organización (lo abstracto) al trabajo (al concreto).

#### 2.3.2.2. *Anatomía de una Política*

Considerar la anatomía de lo que es en sí una política, puede ayudar a identificar un error en su declaración. Toda política debe estar compuesta por las siguientes secciones:

- **Objetivo:** Declara y define el por qué de la necesidad de la política en la organización.
- **Alcance:** Define los objetos lógicos y/o físicos, personas, ambientes que estarán involucrados o se verán afectados por la política.
- **Cuerpo principal:** Descripción de la instrucciones de la gerencia o controles que se deben seguir.
- **Responsables:** Son aquellos que tienen que cumplir y hacer cumplir las políticas.
- **Características complementarias:** Estas pueden no encontrarse en todas las políticas pero sí deben ser consideradas. Características como la vigencia de una política, sanciones, disciplinas en caso de incumplimiento, canales formales de consulta para dudas sobre enunciados de políticas y los comentarios son solo algunas de todas las características que pueden ayudar a definir claramente una política.

Existen diferencias entre políticas, normas y procedimientos que deben ser identificadas para establecer correctamente dichas clasificaciones:

- **Políticas:** Instrucciones de la gerencia que reflejan los objetivos de la organización y están destinados a una gran audiencia. Por lo general son a largo

plazo.

- **Normas:** Son procesos o reglas que soportan a las políticas. Pueden estar dirigidas a grandes y pequeñas audiencias y por lo general son de duración limitada.
- **Procedimientos:** Son tareas específicas para ejecutar ciertas funciones y que por lo general tienen duración limitada. Los procedimientos, en su mayoría, están atados a la tecnología implantada en la organización, ya que muchas veces describen paso a paso cada una de las actividades a realizar dependiendo de la metodología o herramienta tecnológica sobre la cual se realizan dichas actividades.

Como ejemplo de los conceptos anteriores podemos decir que una política podría plantear o describir la necesidad de realizar respaldos, de tener almacenaje fuera de la sede y de salvaguardar los medios respaldados. La norma podría definir el software a utilizar para hacer los respaldos y cómo configurar dicho software. El procedimiento podría describir cómo usar el software de respaldo, cómo y cuándo sincronizar dichos respaldos y otros detalles.

#### ***2.3.2.3. Desarrollo de Políticas de Seguridad Informática***

La base metodológica para el desarrollo de las políticas debe partir de los objetivos y metas definidas en la planificación estratégica de la empresa, tomando en cuenta la tecnología de información como elemento habilitador de estas estrategias. Es de hacer notar, que en condiciones ideales, es necesario tomar en cuenta asesorías externas, que además de proveer el enfoque metodológico, aplican las mejores prácticas provenientes de empresas en donde la implantación de políticas haya reportado beneficios tangibles e intangibles. Finalmente, estos insumos constituyen el origen del desarrollo tanto de las políticas como de los procedimientos, lo cual demandará una serie de recursos para aplicabilidad.

El desarrollo de políticas de seguridad debe incluir ciertos aspectos, que garantice su funcionalidad y permanencia en la organización.

- Lograr que las políticas de seguridad cumplan con todos los principios de seguridad, a saber:
  - ◆ Autenticación.
  - ◆ Confidencialidad.
  - ◆ Integridad.
  - ◆ No repudio.
  - ◆ Disponibilidad de los recursos a personas autorizadas.
  - ◆ Control de Acceso.
  
- Identificación de estructura y requerimientos, cuyo objetivo principal es la identificación de la organización en términos de su misión, visión, políticas actuales, cultura organizacional y funcional de la empresa.
  
- Identificación de activos de información y riesgos. En esta fase se persigue el reconocimiento de los recursos o activos de información, para luego proceder a su clasificación según sus usos y niveles de acceso. Adicionalmente se detectan las vulnerabilidades y amenazas, analizando la factibilidad de que las mismas puedan ocurrir y examinado los controles que puedan ser aplicados.
  
- Elaboración de las políticas de seguridad de activos de información, la cual constituye el proceso de desarrollo propiamente dicho de las políticas de seguridad informática. En esta fase también se definen las sanciones en caso de incumplimiento de las políticas establecidas, por parte de la comunidad usuaria.
  
- Es de hacer notar, que mientras las políticas indican el “que”, los procedimientos indican el “cómo” y son estos últimos los que nos permiten llevar a cabo y aplicar las políticas. Ejemplos que requieren la creación de un procedimiento son:
  - ◆ Crear o eliminar una cuenta de usuario.
  - ◆ Otorgar o revocar privilegios de acceso en aplicaciones de negocios y

de automatización de oficina.

- ◆ Actualizar aplicaciones o software base.
  - ◆ Respaldar y restaurar información.
  - ◆ Manejar un incidente de seguridad, entre otros.
- Definir de la matriz de cobertura, que no es más que el alcance que debe tener las políticas para que las mismas estén orientadas al público adecuado. Esta matriz, está conformada con:
- ◆ **Audiencias:** determinan a quiénes va dirigida la política. Ejemplo: usuarios finales, gerentes, socios de negocios, entre otras.
  - ◆ **Categorías:** establecen la clasificación en donde la política se aplica. Ejemplo: hardware, software, comunicaciones, administración, seguridad física, personal, entre otros.
- Las acciones a seguir para el desarrollo de las políticas de seguridad informática deben:
- ◆ Identificar el punto sensible a proteger.
  - ◆ Establecer su prioridad en cuanto a acciones de seguridad de corto, mediano y largo plazo.
  - ◆ Definir la matriz de cobertura sin redundancias.
  - ◆ Definir acciones a tomar en caso de incumplimiento.
  - ◆ Redactar de forma clara y precisa el contenido.
  - ◆ Automatizar el mantenimiento y consulta de las políticas y procedimientos (ejemplo: base de datos, Web Site, etc.).

### 2.3.3. *Auditoría*

La auditoria en informática es la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización,



eficiencia y seguridad, de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

Una auditoría para que sea exitosa, debe constar de varias etapas esenciales durante las cuales el auditor debe adoptar varias perspectivas y roles para cumplir con los objetivos y principios de auditoría. Estos principios incluyen un análisis de riesgo, estrategias al conducir la auditoría y formas de proveer recomendaciones referentes a la seguridad.

Otra definición nos indica que la Auditoría Informática es aquella que tiene como objetivo evaluar los controles de la función informática, analizar la eficiencia de los sistemas, verificar el cumplimiento de las políticas y procedimientos de la empresa en este ámbito y revisar que los recursos materiales y humanos de esta área se utilicen eficientemente. El auditor informático debe velar por la correcta utilización de los recursos que la empresa dispone para lograr un eficiente y eficaz Sistema de Información.

### ***2.3.3.1 Alcance de la Auditoría Informática***

El alcance de la Auditoría Informática no es nada más que la precisión con que se define el entorno y los límites en que va a desarrollarse la misma y se complementa con los objetivos establecidos para la revisión. El alcance de la Auditoría Informática deberá definirse de forma clara en el Informe Final, detallando no solamente los temas que fueron examinados, sino también indicando cuales se omitieron.

### ***2.3.3.2 Importancia de la Auditoría Informática***

A pesar de ser una disciplina cuya práctica ha aumentado en nuestro país durante los últimos años, la Auditoría Informática es importante en las organizaciones por las siguientes razones:

- Se pueden difundir y utilizar resultados o información errónea si la calidad de

datos de entrada es inexacta o los mismos son manipulados, lo cual abre la posibilidad de que se provoque un efecto dominó y afecte seriamente las operaciones, toma de decisiones e imagen de la empresa.

- Las computadoras, servidores y los Centros de Procesamiento de Datos se han convertido en blancos apetecibles para fraudes, espionaje, delincuencia y terrorismo informático.
- La continuidad de las operaciones, la administración y organización de la empresa no deben descansar en sistemas mal diseñados, ya que los mismos pueden convertirse en un serio peligro para la empresa.
- Las bases de datos pueden ser propensas a atentados y accesos de usuarios no autorizados o intrusos.
- La piratería de software y el uso no autorizado de programas, con las implicaciones legales y respectivas sanciones que esto puede tener para la empresa.
- El robo de secretos comerciales, información financiera, administrativa, la transferencia ilícita de tecnología y demás delitos informáticos.
- Mala imagen e insatisfacción de los usuarios porque no reciben el soporte técnico adecuado o no se reparan los daños de hardware ni se resuelven los problemas en plazos razonables, es decir, el usuario percibe que está abandonado y desatendido permanentemente.
- En el Departamento de Sistemas se observa un incremento desmesurado de costos, inversiones injustificadas o desviaciones presupuestarias significativas.
- Evaluación de nivel de riesgos en lo que respecta a seguridad lógica, seguridad física y confidencialidad.
- Mantener la continuidad del servicio y la elaboración y actualización de los planes de contingencia para lograr este objetivo.
- Los recursos tecnológicos de la empresa incluyendo instalaciones físicas,

personal subalterno, horas de trabajo pagadas, programas, aplicaciones, servicios de correo, Internet, o comunicaciones; son utilizados por el personal sin importar su nivel jerárquico, para asuntos personales, alejados totalmente de las operaciones de la empresa o de las labores para las cuales fue contratado.

- El uso inadecuado de la computadora para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor y el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos.

### **2.3.3.3 Características de la Auditoría Informática**

La información de la empresa y para la empresa, siempre importante, se ha convertido en un Activo Real de la misma, como sus Stocks o materias primas si las hay. Por ende, han de realizarse inversiones informáticas, materia de la que se ocupa la *Auditoría de Inversión Informática*.

Del mismo modo, los Sistemas Informáticos han de protegerse de modo global y particular: a ello se debe la existencia de la *Auditoría de Seguridad Informática* en general, o a la auditoría de Seguridad de alguna de sus áreas, como pudieran ser Desarrollado o Técnica de Sistemas.

Cuando se producen cambios estructurales en la Informática, se reorganiza de alguna forma su función: se está en el campo de la *Auditoría de Organización Informática*.

Estos tres tipos de auditorías engloban a las actividades auditoras que se realizan en una auditoría parcial. De otra manera: cuando se realiza una auditoría del área de Desarrollo de Proyectos de la Informática de una empresa, es porque en ese Desarrollo existen, además de ineficiencias, debilidades de organización, o de inversiones, o de seguridad, o alguna mezcla de ellas.

### 2.3.3.3.1 Auditoria al Solicitante a Proveedor de Servicios de Certificación (PSC)

El Objetivo y campo de aplicación de esta auditoria es establecer los lineamientos y pasos a seguir para la planificación y realización de las auditorias a los PSC, a objeto de verificar la existencia, el cumplimiento y la eficacia de los procedimientos de control implantados, las normas y procedimientos de seguridad, la cobertura para minimizar los riesgos y determinar el cumplimiento de las garantías de calidad y sus niveles de servicios.

Los pasos para la auditoria al solicitante a PSC, son:

	ACTOR	ACCIÓN
1	SOLICITANTE A PSC	<ol style="list-style-type: none"> <li>1. Ingresar a la página Web de SUSCERTE sección Registro de Auditores.</li> <li>2. Revisa listado de Auditores Registrados y contacta el de su preferencia.</li> </ol>
2	AUDITOR REGISTRADO	<ol style="list-style-type: none"> <li>1. Recibe solicitud por parte del PSC para la realización de la Auditoria.</li> <li>2. Notifica a SUSCERTE la solicitud para la realización de la Auditoria.</li> <li>3. Elabora el Plan de Auditoria.</li> <li>4. Realiza reunión con el PSC: Resume los métodos y procedimientos que van a ser utilizados en la Auditoria y se clarifican los puntos dudosos sobre el Plan de Auditoria a ejecutarse.</li> <li>5. Envía al PSC el Plan de Auditoria, para su aprobación.</li> </ol>
3	SOLICITANTE A PSC	<ol style="list-style-type: none"> <li>1. Recibe el Plan de Auditoria y lo aprueba en conformidad.</li> <li>2. Envía al Auditor Plan de Auditoria aprobado.</li> </ol>

<p>4</p>	<p><b>AUDITOR REGISTRADO</b></p>	<ol style="list-style-type: none"> <li>1. Recibe el Plan de Auditoria aprobado y envía copia a SUSCERTE.</li> <li>2. Inicia la auditoria basándose en procesos sistemáticos, independientes, que le permitan verificar: la existencia, el cumplimiento y la eficacia de normas, políticas, planes y procedimientos de seguridad relacionados con Tecnología de Información y Comunicación (TIC), para minimizar los riesgos y determinar el cumplimiento de las garantías de calidad y sus niveles de servicios asociados, siguiendo la lista de chequeo establecida en la Norma SUSCERTE N° 044.</li> <li>3. Determina y describe las observaciones analíticas realizadas durante el proceso de auditoria.</li> <li>4. Realiza reunión con el responsable del PSC, informando las evidencias y/o hallazgos encontrados en la Auditoria.</li> <li>5. Encuentran evidencias y/o hallazgos:             <ol style="list-style-type: none"> <li>a) Si se encuentran evidencias y/o hallazgos indica las detecciones y llena el registro de detección de evidencias ó mejora. Espera tiempo solicitado y cierra auditoria.</li> <li>b) Si no se encuentran evidencias y/o hallazgos se procede al cierre de la Auditoria.</li> </ol> </li> <li>6. Realiza reunión de cierre: El objetivo de esta reunión es presentar las observaciones de la Auditoria y manifestar el comportamiento del desarrollo de la Auditoria e informar a los responsables de las áreas auditadas las evidencias y/o hallazgos encontrados.</li> <li>7. Culminado el proceso de Auditoria, emite Informe preliminar de Auditoria al PSC con los lineamientos establecidos en la Norma SUSCERTE N° 045, dejando claramente indicado un dictamen sobre la revisión efectuada.</li> </ol>
<p>5</p>	<p><b>SOLICITANTE A PSC</b></p>	<ol style="list-style-type: none"> <li>1. Recibe el Informe preliminar de Auditoria:</li> </ol>

		<p>a) Si hay evidencias y/o hallazgos elabora plan de acciones correctivas para subsanar las evidencias y/o hallazgos encontrados y envía plan de acciones correctivas al Auditor.</p> <p>b) Si no hay evidencias y/o hallazgos se procede a realizar el cierre de la Auditoria.</p>
6	<b>AUDITOR REGISTRADO</b>	<p>1. Hay evidencia y/o hallazgos:</p> <p>a) Si hay evidencias y/o hallazgos recibe plan de acciones correctivas y ejecuta el correctivo.</p> <p>b) Si no hay evidencias y/o hallazgos elabora Informe de Auditoria y entrega dos (2) originales, uno para el Solicitante a PSC y otro para ser consignado ante SUSCERTE. El tiempo para consignar el original del informe de Auditoria ante SUSCERTE no podrá exceder en cinco (5) días hábiles.</p>

**Tabla N° 2.1** Solicitud de Auditoria a los PSC

#### 2.3.3.3.1.1 **Criterios a Evaluar en la Auditoria a solicitante a PSC**

Los criterios a su vez son las áreas de control de alto nivel (generales) a ser objeto de revisión sobre los ambientes a ser revisados durante la ejecución del programa de auditoria, los cuales son:

➤ **Criterio de Administración de Certificaciones y Llaves Electrónicas:**

Comprobar que existan y se cumplan razonablemente las condiciones básicas de control sobre los criterios correspondientes a políticas, normas, procesos y procedimientos de Certificación, Certificados y Llaves Electrónicas que conforman el ambiente organizacional de un PSC.

➤ **Criterio de Seguridad y control del Ambiente Operacional:**

Comprobar que existan y se cumplan razonablemente las condiciones de seguridad y control sobre el ambiente operacional, en cuanto a: Organización de la seguridad, evaluación del riesgo y clasificación de activos, seguridad del

personal, seguridad física y ambiental, administración de las operaciones y las comunicaciones, control de acceso a los sistemas, y administración de la continuidad del negocio.

➤ **Criterio de Calidad, Confianza y Servicios:**

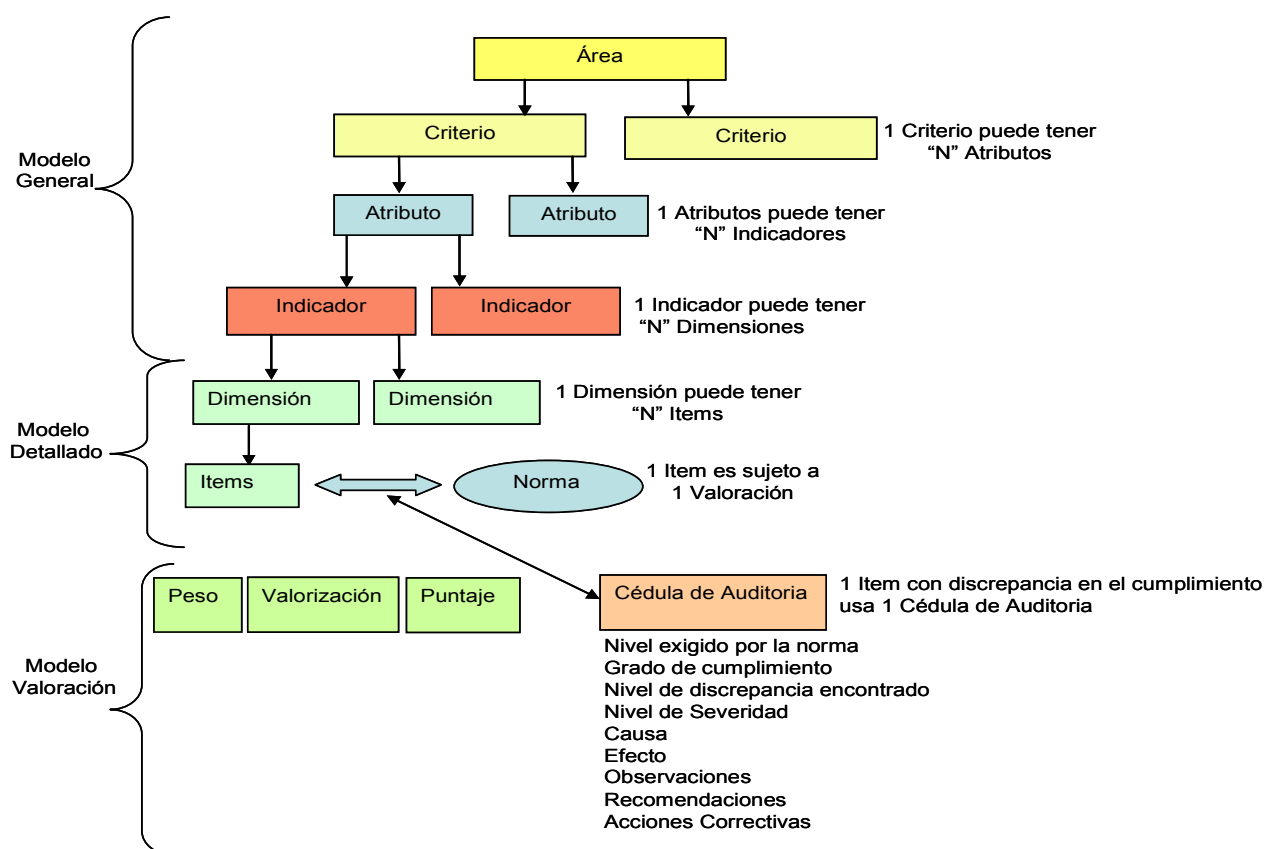
Constatar que el PSC cuenta con una política que regule los mecanismos relativos a los elementos de calidad, servicios, confianza, y como mecanismos asociado a la los servicios y la confianza, lo relativo al registro de acceso público.

Los atributos son a su vez un conjunto de elementos de control que caracterizan a cada criterio. Los atributos están integrados por grupos de indicadores. Los indicadores, están integrados a su vez por grupos de Dimensiones. A las Dimensiones, se asocian un conjunto de elementos de detalle, que son los objetos de directos a evaluarse. Todos los anteriores, excepto el más bajo nivel de detalle, forman parte del Modelo General.

El Modelo General, está entonces orientado a establecer:

- La Finalidad: relacionada esta al Área
- Fin: relacionado este al Criterio.
- Propósito: relacionado este al Atributo, y
- Objetivo de Control relacionado al Indicador.

Por su parte, las Dimensiones persiguen determinar las áreas puntuales a ser evaluadas. De esta forma, el Modelo de Auditoria se puede esquematizar de la siguiente forma:



**Figura 2.1** Modelo detallado a ser auditados al PSC

El Modelo Detallado, como su nombre lo indica, contiene cada una de las especificaciones a revisar de los aspectos contenidos en el Modelo General.

Contiene la operacionalización de los atributos del Modelo General, definiendo para cada una de las dimensiones, un conjunto de ítems, que vienen a ser los objetivos finales y desagregados de control para realizar las revisiones y evaluaciones objeto de la auditoría, los cuales se les asocia el marco legal y normativo (estándares, normas, mejores prácticas).

El Modelo de Valoración contiene la asignación de valores cualitativa /cuantitativa asociada a cada elemento.

Para cada uno de ellos, se asigna un peso en función al grado de importancia dentro de la dimensión y consecutivamente, dentro de cada uno de los elementos de agregación del modelo General.



Al peso, se le asocia una valuación.

La valuación o valor asignado, consiste en asignar cero “0” si no está presente lo indicado a evaluarse o no se corresponde con las exigencias de la norma, en caso contrario, o sea que está presente y se corresponde con la norma, a la valuación se le asigna valor uno “1”.

El siguiente nivel está dado por el producto de la valuación por el peso asignado, a lo que se denomina puntaje. Seguidamente, el modelo prevé la suma en cascada invertida de los valores encontrados a través de la valuación, a fin de que pueda conocerse el resultado final de la evaluación aplicada..

De esta forma, se totalizan los puntajes de los ítems como el valor de la Dimensión. De manera similar, se suman los valores de las Dimensiones y se totalizan como el valor del Indicador. Luego, se suman los valores totalizados de los indicadores, para obtener el valor correspondiente de su Atributo. Así mismo, se totalizan los valores de los atributos, para obtener el valor correspondiente a cada criterio.

Los valores totalizados de los criterios, se suman para obtener el valor de cada Área, y el valor de las tres (03) Áreas es sumado para obtener el resultado final de la evaluación realizada en el proceso de auditoría.

Cabe destacar, que el Modelo de Valoración empleado, facilita un alto grado de transparencia, eliminando la discrecionalidad del auditor, pues este sólo, a estos efectos, deberá identificar si algo se cumple o no se cumple para asignar los valores correspondientes.

Para aquellos casos en que exista un nivel de discrepancia entre lo encontrado y la norma, se deberá registrar la situación encontrada, en la cédula de auditoría.

La cédula de auditoría, deben contener para cada dimensión revisada: La reseña de la información recabada, el análisis de comportamiento realizado a la información recabada, revisando para esta información el y nivel de comportamiento exigido en la norma, y contrastándola con el nivel encontrado de comportamiento,

para determinar el/los indicador(es) de desviación, analizando la(s) causa(s), su efecto, aplicando los elementos cuantitativos de valoración, para determinar el nivel de criticidad, determinando posteriormente el grado de severidad que permita al auditor de los PSC indicar las observaciones y establecer las recomendaciones y las acciones correctivas a tomar. La cédula de auditoria debe tener anexo la evidencia de la información recabada.

#### ***2.3.3.3.2 Objetivo del empleo de normas, estándares y mejores prácticas internacionales, para realizar auditorías al PSC***

El empleo de normas, estándares y mejores prácticas internacionales, así como de otros documentos provenientes de organizaciones reconocidas en el desarrollo de la tecnología de información y comunicación y de las herramientas para certificación tiene, entre otros, los siguientes objetivos:

- Reflejar el estado del arte en materia de tecnologías de información y comunicación, así como de las herramientas que proveen estas tecnologías en materia de certificación de datos y firma electrónica; para que sean empleadas con: eficacia, eficiencia, productividad, tanto en los ambientes organizativos y de servicios, en los operacionales y de seguridad, como en los propiamente dichos del manejo especializado de la tecnología para certificar datos y manejar firmas electrónicas.
- Garantizar la interoperabilidad entre las entidades que conforman los PSC y de ésta con entidades e infraestructuras externas.
- Facilitar el proceso de actualización de estos criterios, mediante el seguimiento de las normas, estándares, mejores prácticas y documentos referenciados, y la eventual, así como para la incorporación de sus actualizaciones y modificaciones a este modelo y programa de auditoria, previa determinación de su aplicabilidad;
- Proveer una base consistente para la verificación del cumplimiento de las normas, estándares y mejores prácticas aplicables y la evaluación de los

distintos ambientes sujetos a la revisión y evaluación a efecto de auditoría.

- Generar una plataforma sólida de calidad organizacional y sobre los bienes o servicios entregados a los clientes / usuarios.
- Establecer compromisos de niveles de servicios, para satisfacer la expectativa y/o demanda de satisfacción de los clientes / usuarios.
- Generar y operar un sistema de garantías de calidad y niveles de servicio, que se base y soporte en la interacción proveedor / cliente, a fin de que además de capturar y validar sus expectativas y demandas sobre los bienes o servicios que se entregan, se garantice su acción proactiva en la evaluación de bien o servicio entregado, con el propósito, de que esta información sirva de sustento y guía para la perfectibilidad del sistema, adecuando los elementos que inciden en la calidad y garantizando los niveles de servicio que demanda el cliente /usuario.
- Mejorar la calidad de las implantaciones de elementos tecnológicos relacionados con la prestación de servicios del PSC, aumentando su eficiencia operativa.
- Mejorar la operatividad de los elementos tecnológicos TIC.
- Operar la plataforma con adecuados niveles de seguridad.
- Operar la plataforma con adecuados niveles de rendimiento.
- Acordar los niveles de servicios, SLA1, SLA2 y SLA3.

#### **2.3.4. Infraestructura de Clave Pública (ICP)**

Hay muchas maneras de definirla: Podría decirse de forma abstracta que es un protocolo para el intercambio seguro de información. O decir que es una infraestructura de red formada por servidores y servicios. O de forma más clara podría decirse que es una tecnología basada en clave pública. Todas son ciertas y se complementan.

La ICP es un protocolo que trata de describir los procesos organizativos necesarios para la gestión de certificados de claves públicas para el intercambio seguro de información, que permite firmar digitalmente un documento electrónico (un e-mail, el código de un programa, una transacción bancaria, unos análisis médicos, etc, etc, etc...), permite identificar a una persona o empresa en Internet y permite acceder a un recinto o servicio restringido. Los usos son innumerables.

Las ICP, son sistemas mixtos hardware/software, basados en diferentes agentes que permiten dotar a máquinas y usuarios de Certificados de Identidad (certificados X509v3).

#### **2.3.4.1 Elementos que componen la ICP**

Como ya introduje, la ICP se basa en el cifrado de clave pública y está formada por:

- Certificados, por ejemplo X509.
- Una estructura jerárquica para la generación y verificación de estos certificados formada por las Autoridad de Certificación (CA) y las Autoridades de Registro (RA) (que cumplen la función de sucursales de las primeras). Donde la AC es una organización independiente y confiable.
- Directorios de certificados, que son el soporte de software adecuado (bases de datos) para el almacenamiento de los certificados. Por ejemplo directorios X.500 o LDAP (simplificación del primero). Aunque no tienen porque estar localizados en un servidor central (modelo de Tercera Parte Confiable) y estar distribuidos entre los usuarios como hace PGP (modelo de Confianza Directa).
- Un sistema de administración de certificados, que es el programa que utiliza la Agencia de Certificación o la empresa donde se ha instalado la PKI para que realice la comprobación, la generación, la revocación de certificados, etc.... Y este es el producto que cada compañía intenta vender en el mercado. Mercado al que se le augura un prometedor crecimiento.

#### **2.3.4.2    Objetivos de la ICP**

La ICP puede ser utilizada en: a) comunicación y transacciones a través de SSL, Ipsec, VPN y HTTPS, b) seguridad en el envío y recepción de documentos y correos electrónicos, c) firma electrónica de bases de datos, y d) identificación “clara” de dominios y usuarios.

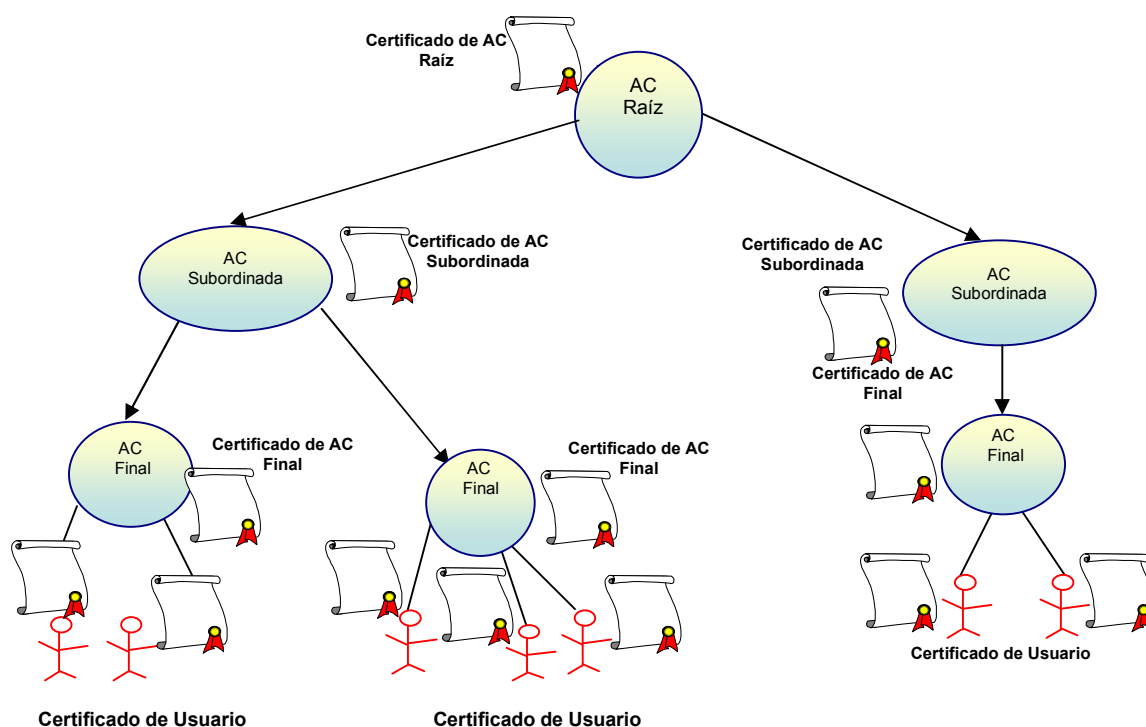
Los objetivos que se persiguen en una PKI, se consiguen gracias a las propiedades de la criptografía de clave pública, y son los siguientes:

- **Autenticación** de usuarios: Asegurar la identidad de un usuario, bien como signatario de documentos o para garantizar el acceso a servicios distribuidos en red, ya que sólo él puede conocer su clave privada, evitando así la suplantación.
- **No repudio:** Impedir que una vez firmado un documento el signatario se retracte o niegue haberlo redactado.
- **Integridad de la información:** Prevenir la modificación deliberada o accidental de los datos firmados, durante su transporte, almacenamiento o manipulación.
- **Auditabilidad:** Identificar y rastrear las operaciones, especialmente cuando se incorporan marcas de tiempo.
- **Acuerdo de claves secretas:** para garantizar la confidencialidad de la información intercambiada, esté firmada o no.

#### **2.3.4.3    Diseño de la Arquitectura de la ICP en Venezuela (INCP)**

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 INCP, donde No existe otra AC 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 SUCERTE, 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).



**Figura 2.2** Estructura jerárquica de la INCP de Venezuela

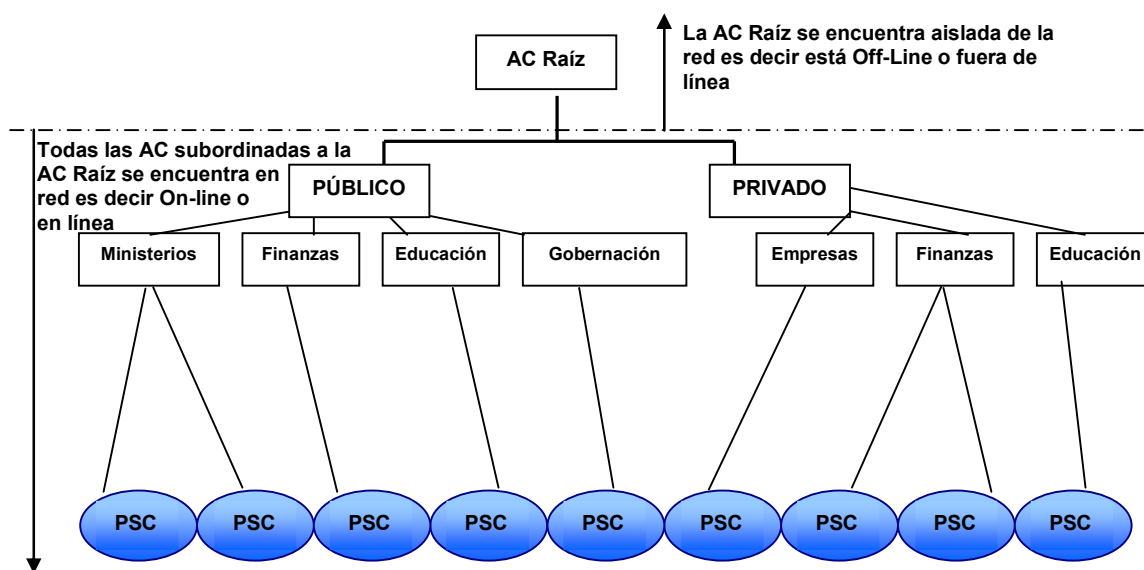
A continuación podemos visualizar que se establecen las relaciones de confianza basadas en el modelo de árbol con una única raíz, punto inicial que deriva toda la confianza del sistema. Este modelo de certificación además de ser simple en su diseño, es fácil de comprender para el usuario común.

En cuanto así 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 INCP.

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 AC Raíz es operada por SUSCERTE en forma “Off-Line<sup>1</sup>”, 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<sup>2</sup>”, porque estos son los que finalmente se encargarán de emitir los certificados electrónicos a los usuarios finales del sistema.



**Figura 2.3** Estructura de (INCP) para los sectores público y privado de Venezuela

<sup>1</sup> Fuera de línea, se mantiene aislada de la red por seguridad.  
<sup>2</sup> En línea, está conectada a la red.

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 2.4, 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 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, ONIDEX, CADIVI, SUDEBAN, 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:** Se 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.

#### **2.3.4.4 Componentes de la Comunidad de Usuarios y Aplicabilidad**

Según la infraestructura del esquema anterior debe contar con los siguientes componentes:

##### **◆ Autoridad de Aprobación de Políticas (AAP) Raíz:**

La Autoridad de Aprobación de Políticas (AAP) creada dentro de SUSCERTE como directorio de la Infraestructura Nacional de Clave Pública (PKI), bajo la autoridad del Ministerio para el Poder Popular y las Telecomunicaciones tiene atribuida la función de elaboración y propuesta de aprobación de la DPC, así como de sus modificaciones. La DPC será aprobada mediante Providencia Administrativa que se publicará en la Gaceta Oficial. La AAP es también la encargada de analizar los informes de las auditorías, totales o parciales, que se hagan de la AC raíz, así como de determinar, en caso necesario, las acciones correctoras a ejecutar.

##### **◆ Autoridad de Certificación AC Raíz:**

La AC Raíz, es la Autoridad de Certificación origen de la jerarquía nacional de certificación electrónica. Este componente de la INCP de Venezuela es responsable por la emisión de los certificados electrónicos que acreditan a los PSC del sector público y privado, según lo establecido en la LSMDFE y su reglamento parcial.

La Autoridad de Certificación de primer nivel sólo emite certificados para sí misma y sus AC Subordinadas. Únicamente estará en funcionamiento durante la realización de las operaciones para las que se establece.

Como parte del modelo comercial del PSC, la AC podrá certificar como AC de tercer nivel (AC3) a las AR que por su volumen de operaciones puedan ser consideradas como AC a pesar de no contar con la infraestructura necesaria para una AC formalmente constituida.

◆ **Autoridad de Registro (AR):**

Las actividades de identificación y registro de los PSC serán realizados por SUSCERTE en conjunto con el proceso de acreditación, no existiendo autoridades de registro adicionales en el ámbito de la autoridad certificación raíz.

◆ **Titulares de Certificados:**

Los certificados emitidos por la AC raíz tienen como titulares a la propia AC raíz, a los PSC acreditados y casos especiales, según lo establecido en la LSMDFE y su reglamento parcial.

✓ **Proveedores de Servicios de Certificados:**

Un Proveedor de Servicios de Certificación corresponde a una entidad emisora de Certificados Digitales de firma electrónica. Desde el punto de vista operativo, comprende un esquema funcional compuesto por una Autoridad de Registro (RA) y Autoridades de Certificación (AC's). Dentro de la dinámica de operación maneja Listas de Revocación de Certificados (CRL), Listas de Certificados Activos, Registro de solicitudes de Certificados, OSCP RESPONDER (Online) y CSR Petición por firma de certificado.

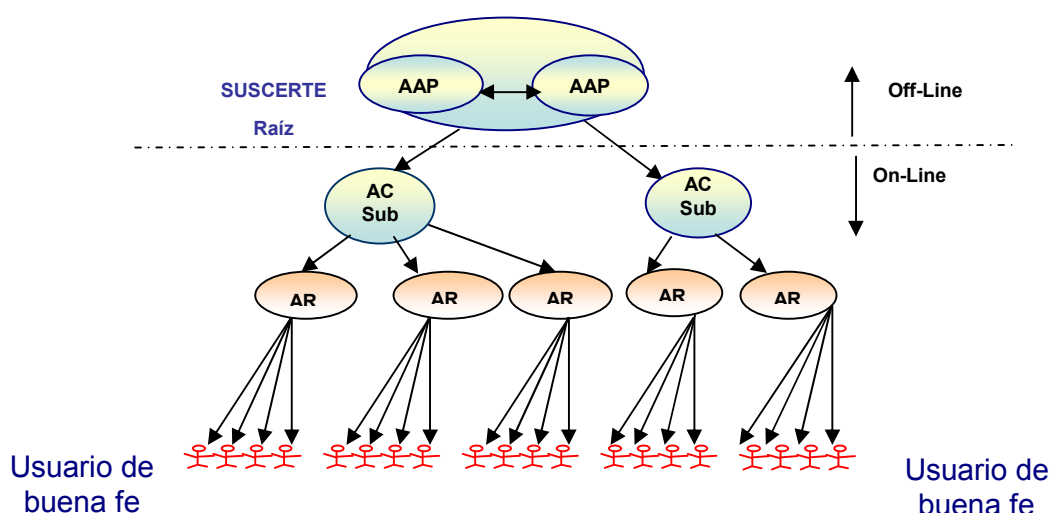
Los PSC operan con una Infraestructura de Clave Pública (ICP) (Public Key Infrastructure X.509: RFC 2459 & 3280), pares de claves y uso de criptografía como elementos de seguridad.

Entre los servicios que ofrece un PSC se incluyen:

- Emisión de Certificados Digitales.
- Generación de claves.
- Distribución de certificados.

- Certificación cruzada.
- Salvaguarda de claves.
- Suspensión y revocación de certificados.

Las AC Subordinadas son llamadas PSC del sector público y privado del país. En el marco legal venezolano, estos son derivados de la jerarquía de 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 INCP 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 la SUSCERTE.



**Figura 2.4** Componentes de la ICP de Venezuela

◆ **Terceros de buena fe:**

Son todas las personas que realicen transacciones utilizando certificados electrónicos provenientes de la INCP y deciden aceptar y confiar en estos certificados.

#### **2.3.4.5 Certificados Digitales**

Los Certificados Digitales son documentos digitales firmados digitalmente por una Autoridad de Certificación, que asocia una Clave Pública con su titular durante el período de vigencia del certificado.

Un Certificado Digital está compuesto de:

- Un Nombre o Pseudónimo del titular.
- Versión del Certificado.
- Un código único que identifica al certificado.
- Un Identificador del PSC que expide el certificado.
- Un período de validez del certificado.
- La Firma Electrónica del PSC que expide el certificado.
- Un dispositivo de verificación de Firma Electrónica que corresponda a un dispositivo de creación de Firma Electrónica bajo control del titular.
- Un Atributo específico del titular.
- Los límites de uso del certificado, si procede.
- Dirección de la Consulta de la Lista de Certificados Revocados.
- Los límites de la responsabilidad del PSC y del valor de las transacciones para las que tiene validez el certificado.

##### **2.3.4.5.1 Tipos de Certificados Digitales**

SUSCERTE establece en las políticas la emisión de dos tipos de certificados. Cada tipo de certificado se identificara por un OID (Object Identifier) único, incluido en el certificado como identificador de política, dentro de la extensión X.509 Certificate Policies.

##### **a) Certificado tipo I – Certificados para AC raíz**

(OID política 2.16.862.1.2.) Este certificado lo genera la Autoridad de Certificación de primer nivel para su identificación. Este es el certificado raíz

autofirmado de la infraestructura de clave pública nacional. El uso de este certificado esta enmarcado en las actividades de la AC raíz.

***b) Certificado tipo II – Certificados de AC para PSC***

(OID política 2.16.862.1.3.) Estos certificados se emitirán al Proveedor de Servicios de Certificación (PSC) acreditados ante SUSCERTE según lo establecido en la LSMDFE y su reglamento parcial. Este tipo de certificado puede emitir otros certificados y tiene privilegio de Autoridad de Certificación intermedia de la ICP nacional.

Las AC's y RA's manejan 4 tipos de Certificados Digitales:

- Certificados para usuarios finales desde 128 bit's SSL.
- Certificados para servidores (correo electrónico, Web, entre otros) desde 256-bit's SSL.
- Certificados para VPN.

Certificados basados en hardware. Como ejemplo de ellos se recomienda el uso de tarjetas inteligentes o Smart Card's.

***2.3.4.5.2 Uso de los Certificados***

***a) Usos permitidos para los certificados***

El certificado electrónico raíz sólo puede utilizarse para la identificación de la propia autoridad certificación raíz y para la distribución de su clave privada de forma segura.

El uso de los certificados emitidos por la AC raíz estará limitado a la firma de certificados electrónicos para entidades subordinadas y la firma de las listas de certificados revocados correspondientes.

***b) Usos no permitidos para los certificados***

El uso no permitido para los certificados emitidos por la AC raíz son todos aquellos que no están explícitamente permitidos en la sección anterior.

### **2.3.4.5.3 Suspensión y Renovación de Certificados**

La Suspensión de Certificados se hará por voluntad del propietario del certificado y deberá tramitarse a través de una solicitud de suspensión requerida a la AR que tramitó la emisión del certificado. Se procesará como un requerimiento en lote correspondiente a las 24 horas posteriores a la última sincronización de repositorios.

A solicitud del propietario, un certificado podrá ser suspendido temporalmente, reactivándose posteriormente a través de una nueva solicitud. La solicitud de suspensión será procesada por la AR de acuerdo a la solicitud del propietario, se realizará el registro correspondiente y se enviará la notificación de suspensión al propietario.

La reactivación de un certificado suspendido será tramitada de forma equivalente a una nueva emisión.

### **2.3.4.5.4 Circunstancias para la renovación del certificado del PSC**

Las circunstancias para la revocación de un certificado del PSC son las siguientes:

- Compromiso de la clave privada de la AC raíz.
- Compromiso o sospecha de la clave privada asociada al certificado del PSC.
- Cuando el PSC solicite a la AC Raíz, la suspensión temporal de su certificado.
- Por resolución judicial o administrativa que lo ordene.
- Por la variación de los datos del certificado.

### **2.3.4.5.5 Entidades que pueden solicitar la renovación del certificado**

Las entidades autorizadas para solicitar la revocación de acreditación de un PSC de la INCP de Venezuela:

- ◆ La autoridad competente a la conformidad con la LSMDFE.
- ◆ El Proveedor de Servicio de Acreditación.
- ◆ La Autoridad de Certificación Raíz.

### 2.3.4.5.6 Procedimiento de Solicitud de Renovación

Los pasos para la revocación de la acreditación de un PSC ante la SUSCERTE, son:

	ACTOR	ACCIÓN
1	DRA	<ul style="list-style-type: none"> <li>● Recibe del Directorio de la SUSCERTE la Resolución donde se determina la suspensión de la Acreditación de un PSC.</li> <li>● Acata la instrucción donde se le solicita participe al PSC de la Resolución tomada.</li> </ul>
2	PSC	<ol style="list-style-type: none"> <li>1. Recibe la notificación de suspensión de la Acreditación como PSC, resuelta por el Directorio de la SUSCERTE.</li> <li>2. Suspende de inmediato la negociación con nuevos usuarios, manteniendo el servicio de los signatarios existentes, hasta nuevo aviso.</li> <li>3. Decide acción para solventar la problemática, en función del razonamiento dado por el Directorio a la suspensión: <ol style="list-style-type: none"> <li>a) Acata medida por estar de acuerdo con la misma.</li> <li>b) U Objeta decreto de suspensión de su Acreditación por el Directorio. Expone el planteamiento ante la SUSCERTE.</li> </ol> </li> </ol>
3	DRA	<ol style="list-style-type: none"> <li>1. Conviene con el PSC, las acciones a llevar a cabo, de acuerdo a su planteamiento: <ol style="list-style-type: none"> <li>a) Acuerdan el mecanismo para activar la suspensión de la que fue objeto, en el lapso de los quince (15) días que tiene para ello.</li> <li>b) O Recibe sus fundamentos en contra de la suspensión de la Acreditación, utilizando los diez (10) días que la Ley Orgánica de Procedimientos Administrativos (LOPA) le asigna para exponer alegatos.</li> </ol> </li> </ol>
4	PSC	<p>Ejecuta las acciones convenidas con la DRA:</p> <ul style="list-style-type: none"> <li>● Envía a la SUSCERTE plan de mejoras para solventar la problemática que originó la suspensión de su Acreditación, si está de acuerdo con la decisión del Directorio.</li> </ul>

		<ul style="list-style-type: none"> <li>• Remite a la SUSCERTE informe justificando las razones de su desacuerdo ante suspensión de la Acreditación.</li> </ul>
5	DRA	<p>Recibe del PSC las comunicaciones y soportes de sus planteamientos, y actúa en consecuencia:</p> <ul style="list-style-type: none"> <li>• Presenta al Directorio el plan de mejoras del PSC interesado en reactivas su Acreditación.</li> <li>• Presenta al Directorio los fundamentos del PSC, donde alega inconformidad con la decisión del Directorio justificando su motivación.</li> </ul>
6	DS	<ol style="list-style-type: none"> <li>1. Admite los documentos del PSC, decidiendo en consonancia con las sustentaciones: <ul style="list-style-type: none"> <li>• 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.</li> <li>• O Analiza reclamo interpuesto por el PSC: <ol style="list-style-type: none"> <li>a) Reafirma la suspensión de la Acreditación, al comprobar nuevamente los incumplimientos que la originaron.</li> <li>b) Reajusta decisión, si los alegatos del PSC tienen fundamento, reactivando la Acreditación por medio de una Resolución.</li> </ol> </li> </ul> </li> <li>2. Participa a la DRA, disposiciones.</li> <li>3. Autoriza a la DRA envío de comunicación informativa al PSC.</li> </ol>
7	DRA	<ol style="list-style-type: none"> <li>1. Comunica al PSC decisión del Directorio: <ul style="list-style-type: none"> <li>• Insta al PSC para que ponga en práctica el plan de mejoras aprobado por el Directorio.</li> <li>• Informa en relación a su reclamo: <ol style="list-style-type: none"> <li>a) 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.</li> <li>b) Da parte de la Resolución emitida por el Directorio, donde reactiva la Acreditación suspendida.</li> </ol> </li> </ul> </li> </ol>



8	PSC	<ol style="list-style-type: none"> <li>1. Recibe notificación de la Dirección de Registro y Acreditación de la SUSCERTE: <ul style="list-style-type: none"> <li>● 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.</li> <li>● Resuelve, con relación a su reclamo: <ol style="list-style-type: none"> <li>a) Elaborar un plan de mejoras, para evitar la revocación de su Acreditación, en el tiempo que le queda para ello. Sigue este procedimiento a partir de la acción 9 A. En caso contrario, continúa con la acción.</li> <li>c) Reiniciar sus actividades ordinarias.</li> </ol> </li> </ul> </li> <li>2. Informa a la DRA resultados de su gestión.</li> </ol>
9	DRA	<ol style="list-style-type: none"> <li>1. 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: <ul style="list-style-type: none"> <li>● 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 SUSCERTE.</li> <li>● Revoca la Acreditación del PSC que incumple con los requisitos y obligaciones exigidos por el Decreto-Ley 1.204, Reglamento Parcial y Normas SUSCERTE.</li> </ul> </li> </ol>

**Tabla N° 2.2** Procedimiento de Solicitud de Renovación

#### **2.3.4.5.7** *Revocación de los Certificados*

La revocación de Certificados Digitales se da como medida de contingencia ante la violación de la seguridad de las AC<sup>3</sup> y la AC o por uso indebido del certificado. En todos los casos, este procedimiento será procesado exclusivamente en la AC.

<sup>3</sup> AC3: Las AC's de nivel 3 que realizan funciones de certificación a través de un conjunto de AR's, reconocidas por un PSC y AR's que atienden solicitudes de Certificados Digitales y Firmas Digitales que serán procesados a través de una AC de cualquiera de los niveles señalados.

Como AR en caso de mal uso de certificados, pérdida o alteración de, o en presencia de auditorias no aprobadas, los propietarios de certificados recibirán una notificación de realización de auditoria con posibilidades de revocación de certificado. Una vez realizada esta auditoria, el certificado podrá ser revocado o liberado de la posible revocación y el propietario recibirá la notificación correspondiente.

### **2.3.5. Tarjetas Inteligentes**

Una de las principales funcionalidades de la aplicación del ROOTVE es el uso de dispositivos criptográficos para el soporte de las operaciones. El uso de estos dispositivos es una práctica común en las aplicaciones de infraestructuras de claves públicas. ROOTVE utiliza 2 tipos de hardware criptográfico: HSM módulos de seguridad en hardware.

El HSM se utiliza para la generación y almacenamiento seguro del par de claves pública/privada de la autoridad de certificación raíz, la firma y revocación de certificados digitales y la generación de listas de revocación de certificados.

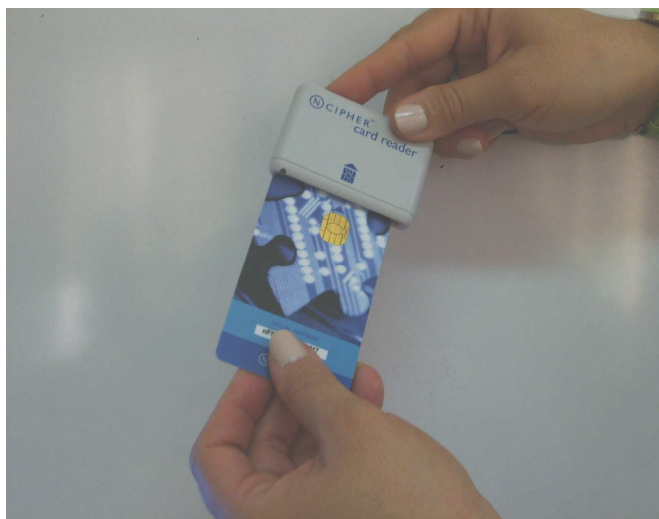
La tarjeta inteligente se utiliza como dispositivo que permite a los usuarios de la ROOTVE<sup>4</sup> autenticarse pues en ellas se generan y almacenan pares de claves públicas/privadas. Como fungen de almacén de la clave privada del usuario, se utilizan cuando un usuario debe firmar digitalmente los datos que modifica durante una sesión en el ROOTVE; de esta forma se garantiza la integridad de la información almacenada. Adicionalmente las tarjetas inteligentes sirven de soporte para exportar certificados digitales en hardware.

---

<sup>4</sup> ROOTVE: Aplicación pensada como una herramienta para gestionar una autoridad de certificación raíz. Se almacenan claves públicas/privadas y se gestionan solicitudes de certificados y listas de revocación de certificados.

### 2.3.5.1 Descripción de HSM soportado por ROOTVE

El módulo HSM nCipher nShield F3 PCI se utiliza como soporte para la generación de pares de claves pública/privada, su respectivo almacenamiento y la generación/revocación de certificados digitales en la aplicación ROOTVE. Se utiliza el concepto “Mundo de seguridad” desarrollado por nCipher, que proporciona una infraestructura de seguridad para administrar el ciclo de vida de las claves generadas y almacenadas en el HSM. Se utiliza el acceso a las claves almacenadas en el HSM a través del esquema umbral límite (K, N) de shamir implementado por nCipher.



**Figura 2.5** HSM nCipher nShield F3 PCI

Entre las características del HSM nCipher nShield F3 PCI se encuentran:

- Algoritmos soportados:
  - Symmetric Ciphers:
    - DES
    - Triples DES
    - CAST
    - AES – Rijndael

- Arc Four (compatible con RC4)
- Public Key Ciphers:
  - RSA
  - DSA
  - ECDSA
  - El Gamal
- Hash and HMAC functions:
  - SHA – 2
  - SHA – 1
  - MD5
  - MD2
  - RIPEMD 160
- Sistemas Operativos:
  - Windows 2000 SP4
  - Windows 2003 and 2003 SP1
  - Solaris 7 (32 y 64 bits), solaris 8, solaris 9.
  - Linux Libc 6.2, kernels 2.4.0 and up
  - AIX 5.1 (32 y 64 bits), AIX 5.2
- Certificaciones y estándares:
  - FIPS 140-2 level 3 and level 2
  - FCC: CFR47, Part 15, subpart B, Class A
  - CE: EN55022, Class A; EN55024-1; EN 60950

En la ICP<sup>5</sup> 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.

---

<sup>5</sup> ICP: siglas en español de PKI, Infraestructura de Clave Pública

### **2.3.6. Contexto Organizacional de Suscerte**

#### **2.3.6.1 Reseña Histórica**

Disponible en <http://www.suscerte.gob.ve> La Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), fue creada a través del Decreto con fuerza de Ley N° 1.204 de fecha 10 de Febrero de 2001, de Mensaje de datos y Firmas Electrónicas, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 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, tal como lo establece la Ley en su artículo 1, 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.

La Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) se convierte en el gran motor del uso de la firma electrónica en el país, pilar fundamental para la existencia y puesta en marcha del gobierno electrónico, gracias al interés del Gobierno Nacional en la modernización del Estado, donde en este momento se encuentran varias iniciativas y proyectos en la administración pública, que van desde la agilización de trámites por vía de medios electrónicos, búsqueda del desarrollo en la incorporación de forma adecuada de esquemas de seguridad de la información y firma electrónica que garanticen la prestación de dichos servicios de forma adecuada y la legalidad de los mismos.

Actualmente, este servicio autónomo continúa examinando de una serie de proyectos pilotos, para expresarle al colectivo el enorme impacto que el uso de certificados y firmas electrónicas proporciona al Estado y al ciudadano, toda vez, que la aplicación y las oportunidades que presenta la aceptación de estos sistemas, van a procurar un impulso definitivo en la implantación de dichas infraestructuras en el país a la luz de la Ley Sobre Mensaje de Datos y Firmas Electrónicas. Es por ello, que la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) ha comenzado a promover toda la materia inherente a las firmas electrónicas mediante la realización y participación de eventos y la suscripción de Convenios de Cooperación Interinstitucional, con el fin de ir consolidando la presencia institucional de tan substancial servicio autónomo para la modernización del Estado.

#### **2.3.6.2 Misión**

“Consolidar el Sistema Nacional de Seguridad de la Información y garantizar el funcionamiento confiable del Sistema Nacional de Certificación Electrónica”.

#### **2.3.6.3 Visión**

“Ser reconocida por la contribución en la aplicación de políticas de inclusión que afiancen la transformación del país y la calidad de vida, mediante el uso masivo de Plataformas Tecnológicas seguras”.

#### **2.3.6.4 Valores**

- Sentido de pertenencia con la organización, expresado en el compromiso para el logro de las metas.
- Ética profesional como expresión de honestidad e integridad.
- Responsabilidad y respeto por el trabajo propio y de los compañeros.
- Sentido de cooperación y confianza para fomentar el trabajo en equipo.
- Proactividad y cultura creativa.

#### **2.3.6.5 *Objetivos Estratégicos de la Organización***

En relación a las competencias de SUSCERTE de acuerdo a lo contemplado en el Decreto con Fuerza de Ley N° 1.204 en el artículo 22 de Mensajes de Datos y Firmas Electrónicas se tiene como objetivos:

- Consolidar la institucionalidad del Sistema Nacional de Seguridad de la Información (SNSI) y del Sistema Nacional de Certificación Electrónica (SNCE).
- Fomentar el desarrollo del capital humano en función de las necesidades y exigencias del SNSI y SNCE.
- Contribuir al desarrollo de la soberanía nacional en materia de seguridad de la información.
- Promover el uso de plataformas tecnológicas seguras que contribuyan a la inclusión.
- Masificar el uso de certificados electrónicos en los servicios de Gobierno Electrónico.
- Fortalecer los procesos de acreditación, supervisión y control de los Proveedores de Servicios de Certificación (PSC).
- Promover la investigación y el desarrollo tecnológico en materia de Certificación Electrónica (CE) y Seguridad de la Información (SI).

#### **2.3.6.6 *Filosofía de Gestión de la Organización***

- La planificación como pilar de la acción.
- Atmósfera agradable que facilite un clima organizacional de cooperación y creatividad.
- La comunicación y el intercambio de información como garantía de calidad en los procesos trabajo.
- Comprometer el éxito de la organización al cumplimiento de las metas



establecidas.

- Se acepta con responsabilidad cualquier tarea requerida para la efectiva operación de la institución.
- Ejercer un liderazgo que promueva la apertura a la crítica y el desarrollo de competencias en el personal.
- Promover el desarrollo de un aprendizaje organizacional continuo.
- Reconocemos la interdependencia entre las demás organizaciones que forman parte del SNSI y SNCE en relación con SUCERTE.
- Reconocer la gerencia por procesos como la vía más efectiva para el éxito de la gestión.
- Orientar la acción hacia una gestión de permanente innovación y promotora del cambio.

#### **2.3.6.7 Macroprocesos de Gestión de la Organización**

##### **a) Certificación Electrónica**

Propósito: Desarrollar los servicios de certificación electrónica en las aplicaciones del Poder Público y el Sector Privado, promoviendo y coordinando el uso masivo de la firma electrónica para la automatización de los procesos, la prestación de servicios en línea y las comunicaciones electrónicas seguras.

##### **b) Promoción y Formación:**

Propósito: Formar capital humano en materias de certificación electrónica, seguridad de la información y derecho en TIC, de acuerdo a las políticas diseñadas por la institución, que permitan generar capacidades y talento nacional.

##### **c) Investigación y Desarrollo Tecnológico:**

Propósito: Potenciar la investigación, desarrollo e innovación en seguridad de la información y certificación electrónica; mediante la integración de los esfuerzos del sector público, privado, académico y científico, a nivel nacional e internacional.

**d) Seguridad de la Información:**

Propósito: Fomentar y consolidar la seguridad de los dispositivos electrónicos y los activos de información que ellos contienen, a fin de que la administración pública pueda fortalecer el correcto funcionamiento de las TIC dentro de sus organizaciones.

**e) Fortalecimiento Institucional:**

Propósito: Garantizar una institución que responda a las necesidades internas y externas de una manera eficaz y eficiente en apoyo a la consecución de una sociedad moderna y de inclusión.

**2.3.6.8 Estructura Organizativa**

La Estructura Organizativa de SUSCERTE se encuentra conformada por las siguientes unidades administrativas:

➤ **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.

## **Superintendencia de Servicios de Certificación Electrónica**

### **(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 N° 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.



**Figura 2.6** Estructura Organizativa actual de SUSCERTE

#### ➤ **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 N° 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 auditoria.

Otro aspecto importante de destacar está contemplado en el artículo 27, Capítulo IV, del Decreto con Fuerza de ley N° 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.

## CAPÍTULO III

### 3. MARCO METODOLÓGICO

#### OBJETIVO

*En este Capítulo, se incluirán los diversos procedimientos que se utilizarán para el proceso de recolección de datos requeridos en la investigación, para ello es necesario situar en detalle, el conjunto de métodos, técnicas e instrumentos empleados, en este diseño de investigación.*

#### 3.1. MODELO DE LA INVESTIGACIÓN

"El Marco Metodológico es la instancia referida a los métodos, las diversas reglas, registros, técnicas y protocolos con los cuales una teoría y su Método calculan las magnitudes de lo real. De allí pues, que se deberá plantear el conjunto de operaciones técnicas que se incorporan en el despliegue de la investigación en el proceso de obtención de los datos" (Balestrini, 1998).

Esta sección cumple un rol importante en esta investigación y en el proceso que señala el conjunto de procedimientos lógicos, técnicas operacionales contenidos en los distintos momentos de la investigación. La finalidad de este Capítulo es poner de manifiesto el análisis y reconstrucción de los datos en estudio.

Este proyecto se refiere a una Metodología Modelo para incorporar la Infraestructura de Clave Pública (ICP) en los Proveedores de Servicios de Certificación (PSC) del Estado Venezolano. En función de los objetivos que se plantearon anteriormente, se tiene una modalidad de proyecto apoyado en un diseño no experimental con un nivel descriptivo por cuanto pretende utilizar criterios sistemáticos para destacar los elementos de la naturaleza del tema que nos ocupa y una investigación de tipo de campo.

### **3.1.1 Nivel de la Investigación**

Como referencia sobre los trabajos de tipo descriptivos podemos citar lo que al respecto dice Méndez (2001) “Los estudios descriptivos acuden a técnicas específicas en la recolección de información, como la observación, las entrevistas y los cuestionarios.”

Tomando en cuenta lo anteriormente mencionado, se puede decir que el nivel de investigación seleccionado para este trabajo es de tipo descriptivo ya que se desea establecer un comportamiento de las variables a estudiar, partiendo de la caracterización de los hechos relacionados con las mismas. Dada la naturaleza de este estudio, se emplearon técnicas específicas de recolección de información como las ya descritas, tomando también como apoyo los informes o documentos existentes 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.

La utilidad de este trabajo es de gran importancia, dada su aplicabilidad, ya que proporcionará referencias claras y detalladas de los pasos a seguir en el diseño de una Infraestructura de Clave Pública, siguiendo las especificaciones solicitadas por SUSCERTE.

### **3.2. DISEÑO DE LA INVESTIGACIÓN**

Según la definición dada por la Universidad Pedagógica Experimental Libertador (2001) la 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 cualquier realidad; en ese sentido se trata de investigaciones a partir de datos originales o primarios”.

Basándonos en esta definición se observó que para dar respuesta a las interrogantes formuladas en este trabajo, la mejor estrategia era plantear el diseño de

investigación de campo, ya que éste proporciona el mejor camino para realizar el análisis, descripción e interpretación del problema planteado.

Vale la pena resaltar que el presente trabajo 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.

### **3.3. POBLACIÓN Y MUESTRA**

En primera instancia se trata el punto de la población; es decir, cuando se está investigado una situación específica, se debe establecer la indagación sobre un conjunto de elementos que comparten características similares (el dato), este conjunto de elementos que brindará la información, que servirá de apoyo en el logro del objetivo del proyecto es llamado universo o población, el cual es definido por Ramírez (1999) como: "...que pertenecen a una misma clase por poseer características similares, pero con la diferencia que se refiere a un conjunto limitado por el ámbito del estudio a realizar..." (p.87)

En el presente trabajo la población corresponde a la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), ente autónomo adscrito al Ministerio del Poder Popular para las Telecomunicaciones y la Informática (MPPTI) de la República Bolivariana de Venezuela y a la Fundación del Instituto de Ingeniería (FII), organismo adscrito al Ministerio Popular para la Ciencia y la Tecnología.

Según Sudman; (cit. Hernández Fernández y Baptista, 2001), la muestra es: "un subgrupo de la población" (p. 204). Entonces se considera como muestra en este trabajo parte del personal de SUSCERTE como lo son cinco (5) especialistas en el área de ingeniería y cinco (5) especialistas de la FII, involucrados en el proceso del diseño de la ICP. 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 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 Administración Pública Nacional.

### **3.4. METODOLOGÍA A UTILIZAR**

Hay diversas maneras de recopilar la información, no obstante la planificación para la recolección de datos se debe ajustar a las necesidades de esta investigación.

La técnica a utilizar para recopilar los datos en este trabajo de investigación se compone básicamente la investigación documental y la aplicación de entrevistas. La combinación de ambas resulta necesaria para acceder a la información de una manera sencilla.

En cuanto al instrumento, cabe destacar que el mismo permite registrar los datos una vez obtenidos a través del empleo de la técnica; según Sabino (2000) que lo define como: “... cualquier recursos de que se vale el investigador para acercarse a los fenómenos y extraer de ellos información.” (p.145).

En este caso el instrumento utilizado es un formato de preguntas, que sirve de apoyo en la realización de la entrevista para la recolección puntual de la información sobre la necesidad de una metodología modelo a seguir para la incorporación de una ICP en los Proveedor de Servicios de Certificación, lo cual generaría más confianza en el proceso de acreditación y un amplio control en el cumplimiento de los recaudos solicitados.

### **3.5. PROCEDIMIENTO DE LA INVESTIGACIÓN**

El desarrollo de este trabajo de investigación se ha basado en las especificaciones de Márquez (2003), quien dice que el trabajo se realiza en 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**

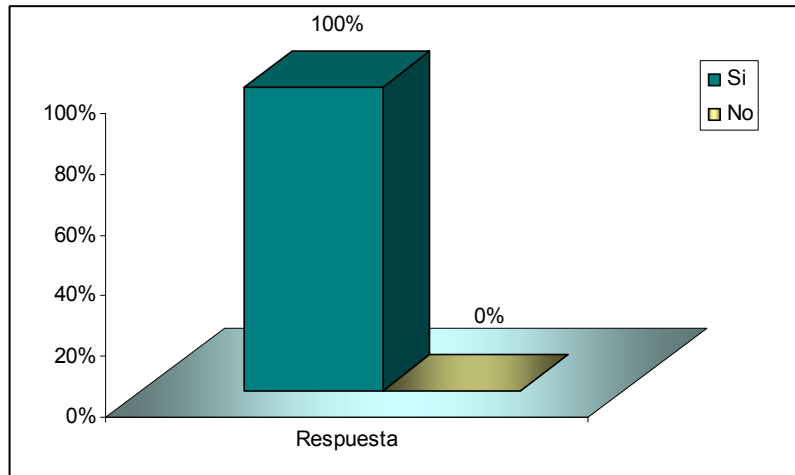
Posteriormente se redacta el borrador del informe del trabajo de grado para el tutor a fin de su revisión y corrección, para finalizar la redacción del trabajo definitivo y luego ser sometido a su evaluación.

## **3.6. 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:**

*¿Existe documentación sobre lo que el solicitante a Proveedor de Servicios de Certificación (PSC) debe saber para acreditarse como tal?*



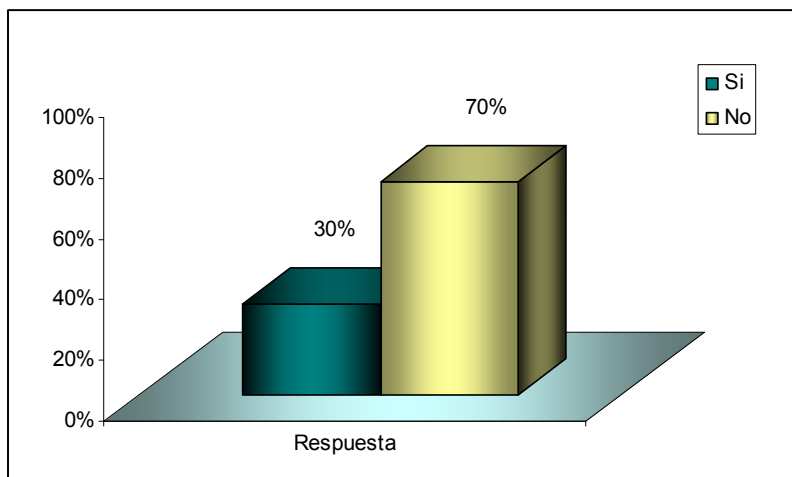
**Gráfico 3.1** Existencia de una documentación

**Resultado:**

De una población de diez 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 documentación sobre los pasos a seguir para acreditarse como Proveedor de Servicios de Certificación.

**Pregunta N° 2:**

*¿La documentación existente es fácil de entender y manipular?*



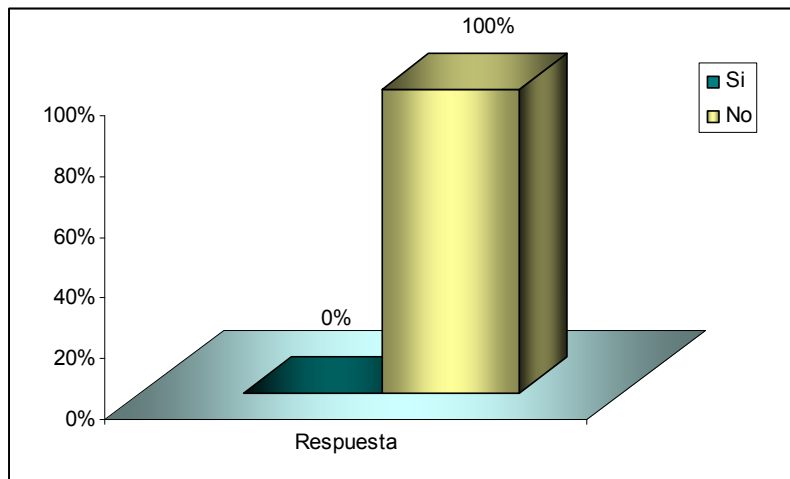
**Gráfico 3.2** Facilidad de la documentación existente.

**Resultado:**

De una población de diez especialistas en el área que conforman el 100% de la muestra, se obtuvo que el 70% considera que la documentación existente no es de fácil de entender y manipular y el 30% restante consideró que si.

**Pregunta N° 3:**

*¿Existe una metodología modelo para incorporar la Infraestructura de Clave Pública (ICP) para que los PSC puedan conocer más fácilmente los elementos mínimos requeridos por SUSCERTE?*



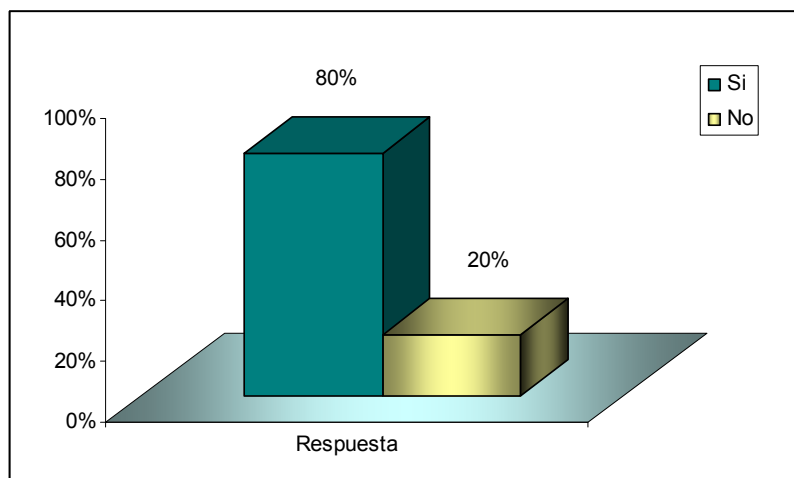
**Gráfico 3.3** Existencia de metodología modelo para incorporar la ICP para los PSC

**Resultado:**

De una población de diez especialistas en el área que conforman el 100% de la muestra, se obtuvo que todos consideran que no existe ninguna metodología modelo para incorporar la Infraestructura de Clave Pública para los PSC puedan conocer más fácilmente los elementos mínimos requeridos por SUSCERTE.

**Pregunta N° 4:**

*¿Existe la necesidad de una metodología modelo a seguir por el PSC?*



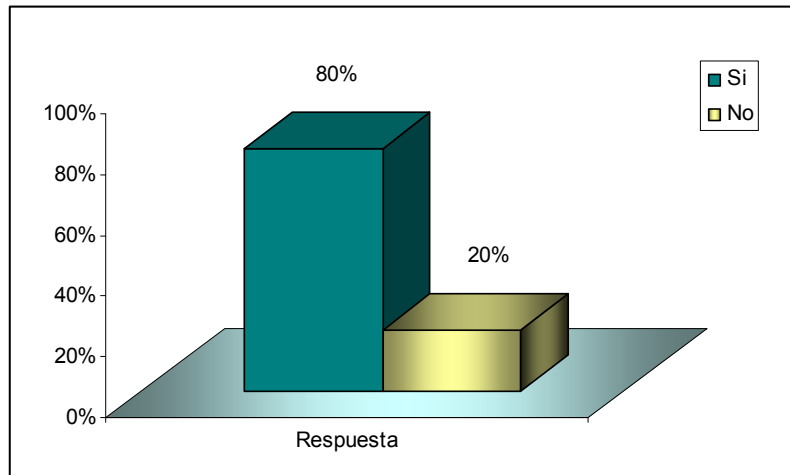
**Gráfico 3.4** Existencia de la necesidad de una metodología modelo a seguir por el PSC

**Resultado:**

De una población de diez especialistas en el área que conforman el 100% de la muestra, se obtuvo que el 80% considera que si existe la necesidad de una metodología modelo a seguir por el PSC para incorporar la Infraestructura de Clave Pública, generando así más confianza en el proceso de acreditación y un amplio control en el cumplimiento de sus recaudos solicitados. En cambio el 20% restante consideró que no existe tal necesidad ya que se encuentran identificados con el proceso actual y cumple con las exigencias mínimas requeridas.

**Pregunta N° 5:**

*¿Facilitaría al PSC su proceso de acreditación y la incorporación de la Infraestructura de Clave Pública, el contar con una metodología modelo?*



**Gráfico 3.5** Facilitaría al PSC su proceso de acreditación y la incorporación de la ICP, el contar con una metodología modelo

**Resultado:**

De una población de diez especialistas en el área, que conforman el 100% de la muestra, se obtuvo que el 80% considera que si facilitaría al PSC su proceso para dar cumplimiento a lo expresado en la LSMDFE, dando así a conocer las mejores prácticas tecnológicas desde el inicio del proceso hasta el cierre del mismo. En cambio el 20% restante considera que el hecho de contar con una metodología modelo no facilitaría el proceso.

•

## CAPÍTULO IV

### 4. PROPUESTA

#### OBJETIVO

*En este capítulo se presenta el Manual sobre una metodología modelo para incorporar la infraestructura de clave pública en los Proveedores de Servicios de Certificación del Estado Venezolano a cumplir con las exigencias ante la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).*

#### 4.1. INTRODUCCIÓN

El desarrollo de la nueva sociedad electrónica es el establecimiento de la confianza por parte de la administración pública nacional, por lo que resulta esencial la utilización de herramientas tecnológicas para aumentar los niveles de transparencia de los actos públicos y dar rápida respuesta a las necesidades y requerimientos de la población.

La necesidad de fomentar la incorporación de las nuevas herramientas de comunicación electrónica a la actividad de las empresas y de las Administraciones Públicas como medio eficaz para incrementar el crecimiento y competitividad de la Economía Venezolana, motivó la aprobación del Decreto-Ley 1.204, de fecha 10 de Febrero de 2.001, sobre Mensaje de Datos y Firmas Electrónica, para ordenar con carácter general, el uso de la firma electrónica y la prestación de los servicios de certificación, destinados a facilitar la confianza de los usuarios en la realización de transacciones en redes abiertas.

La firma electrónica surge con el contexto de un esfuerzo más general que persigue sustituir al tradicional documento impreso por un documento firmado electrónicamente, puesto que el empleo de dichos documentos digitales ha sido tradicionalmente combatido debido a la ausencia de veracidad y seguridad de que adolecen los mismos, donde se pretende acudir a la Firma Electrónica como un

mecanismo que permite superar estas objeciones a través de un Certificado Electrónico, la cual es certificada confiablemente por un Proveedor de Servicios de Certificación que atribuye certeza y validez a la firma.

Es aquí donde interviene la Superintendencia de Servicios de Certificación Electrónica SUSCERTE que es el promotor de la firma electrónica, la cual va a traer grandes beneficios para el desarrollo del país, incrementando de alguna manera las nuevas tecnologías en la sociedad.

Por esta razón se ha impulsado la prioridad de adoptar estas tecnologías de Firmas Electrónicas, y los Servicios de Certificación de la misma, en relación a esto se crea la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), como un servicio autónomo adscrito al Ministerio del Poder Popular para las Telecomunicaciones y la Informática; y cuyo objeto es acreditar, supervisar y controlar, a los proveedores de servicios de certificación (PSC) en los términos previsto en la Ley Sobre Mensaje de Datos y Firmas Electrónicas (LSMDFE) y su Reglamento Parcial. Cabe destacar que el Reglamento (PLSMDFE) tiene entre sus objetivos desarrollar la normativa que regula la acreditación de los Proveedores de Servicios de Certificación ante la Superintendencia de Servicios de Certificación Electrónica.

Por tal motivo, se considera proponer una metodología modelo para incorporar la infraestructura de clave pública (ICP) en los Proveedores de Servicios de Certificación (PSC) del Estado Venezolano a través de las rigurosas normas que exige la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), para ser proveedor acreditado, con el fin de servir como guía para su incorporación progresiva a las transacciones de gobierno electrónico, generalmente.

## **4.2. DEFINICIONES Y TERMINOLOGÍAS**

A los efectos de este documento, se establecen las siguientes definiciones y terminologías:

- ***ACREDITACIÓN***

Es el título que otorga la Superintendencia de Servicios de Certificación Electrónica a los Proveedores de Servicios de Certificación para proporcionar certificados electrónicos. Esta acreditación se otorga una vez cumplidos los requisitos y condiciones establecidos en la DPC de la AC raíz.

- ***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 PRÁCTICAS DE CERTIFICACIÓN***

Documento en el cual la Autoridad de Certificación 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 N° 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.

- ***POLÍTICAS DE CERTIFICADOS***

Documento en el cual la Autoridad de Certificación 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 N° 3.335 de fecha 12 de diciembre de 2004 publicada en Gaceta Oficial de la República Bolivariana de Venezuela, N° 38.086 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 la SUSCERTE, la creación del Registro de Auditores, así como los estándares, planes y procedimientos de seguridad.

- ***ROOTVE***

Es una aplicación desarrollada para crear y administrar certificados X.509 y claves RSA en una Autoridad de Certificación Raíz.

- ***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 la 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 que pertenece al Ministerio del Poder Popular para las Telecomunicaciones y la Informática 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.

### 4.3. SIMBOLOS Y ABREVIATURAS

A los efectos de este documento, se establecerán los siguientes símbolos y abreviaturas:

<b>AC</b>	Autoridad de Certificación
<b>AL</b>	Asesoría Legal
<b>AR</b>	Autoridad d Registro
<b>AAP</b>	Autoridad de Aprobación de Políticas
<b>AV</b>	Autoridad de Validación
<b>DPC</b>	Declaración de Practicas de Certificación
<b>DS</b>	Directorio de la SUSCERTE
<b>DRA</b>	Dirección de Registro y Acreditación
<b>HSM</b>	Modulo de Hardware Criptográfico
<b>INCP</b>	Infraestructura Nacional de Clave Pública
<b>LOAP</b>	Ley Orgánica de Administración Pública
<b>LOPA</b>	Ley Orgánica de Procedimientos Administrativos
<b>LRAC</b>	Lista de Revocación de Autoridades de Certificación
<b>LSMDFE</b>	Iniciales que identifican el Decreto con fuerza de Ley 1.204 Sobre Mensajes de Datos y Firmas Electrónicas.
<b>MCT</b>	Ministerio de Ciencias y Tecnología.
<b>OGA</b>	Oficina de Gestión Administrativa.

---

<b>OCSP</b>	Online Certificate Status Protocol (Protocolo de estado de certificados en línea).
<b>PSC</b>	Proveedor de Servicios de Certificación
<b>PC</b>	Políticas de Certificados
<b>ITSEC</b>	Information Technology Security Evaluation Criteria

#### **4.4. INFRAESTRUCTURA NACIONAL DE CLAVES PÚBLICAS (INCP)**

Es un protocolo que trata de describir los procesos organizativos necesarios para la gestión de certificados digitales de claves públicas para el intercambio seguro de información, que permite firmar digitalmente un documento electrónico (un email, el código de un programa, una transacción bancaria, unos análisis médicos, etc, etc, etc...), o permite identificar a una persona o empresa en Internet, o permite acceder a un recinto o servicio restringido. Los usos son innumerables.

Una Infraestructura Nacional de Claves Públicas (INCP) le permite a una compañía contar con sistemas de autenticación, controles de acceso, confidencialidad y no repudiabilidad para sus aplicaciones en redes, usando tecnología avanzada, tal como firmas digitales, criptografía y certificados digitales.

Las ICP's<sup>6</sup>, son sistemas mixtos hardware/software, basados en diferentes agentes que permiten dotar a máquinas y usuarios de Certificados Digitales de Identidad.

##### ***4.4.1 Elementos que la Componen en General***

Como ya introduce, la ICP se basa en el cifrado de clave pública y está formada por:

- Certificados Digitales, por ejemplo X509.

---

<sup>6</sup> ICP's Infraestructuras de Clave Pública siglas en español, PKI Siglas en Inglés.

- Una estructura jerárquica para la generación y verificado de estos certificados formada por las Autoridad de Certificación (CA) y las Autoridades de Registro (RA) (que cumplen la función de sucursales de las primeras). Donde la CA es una organización independiente y confiable.
- Directorios de certificados, que son el soporte software adecuado (bases de datos) para el almacenamiento de los certificados. Por ejemplo directorios X.500 o LDAP (simplificación del primero). Aunque no tienen porque estar localizados en un servidor central (modelo de Tercera Parte Confiable) y estar distribuidos entre los usuarios como hace PGP (modelo de Confianza Directa).
- Un sistema de administración de certificados, que es el programa que utiliza la Agencia de Certificación o la empresa donde se ha instalado la ICP para que realice la comprobación, la generación, la revocación de certificados, etc. Y éste es el producto que cada compañía intenta vender en el mercado. Mercado al que se le augura un prometedor crecimiento.

#### **4.4.2. Objetivos de la ICP**

La ICP puede ser utilizada en: a) comunicación y transacciones a través de SSL, Ipv6, VPN y HTTPS, b) seguridad en el envío y recepción de documentos y correos electrónicos, c) firma electrónica de bases de datos, y d) identificación “clara” de dominios y usuarios.

Los objetivos que se persigue en una ICP, se consigue gracias a las propiedades de la criptografía de clave pública, y son los siguientes:

- **Autenticación** de usuarios: Asegurar la identidad de un usuario, bien como signatario de documentos o para garantizar el acceso a servicios distribuidos en red, ya que sólo él puede conocer su clave privada, evitando así la suplantación.

- **No repudio:** Impedir que una vez firmado un documento el signatario se retracte o niegue haberlo redactado.
- **Integridad de la información:** Prevenir la modificación deliberada o accidental de los datos firmados, durante su transporte, almacenamiento o manipulación.
- **Auditabilidad:** Identificar y rastrear las operaciones, especialmente cuando se incorporan marcas de tiempo.
- **Acuerdo de claves secretas:** para garantizar la confidencialidad de la información intercambiada, esté firmada o no.

#### ***4.4.3. Selección del Modelo de Confianza de Infraestructura Nacional de Clave Pública***

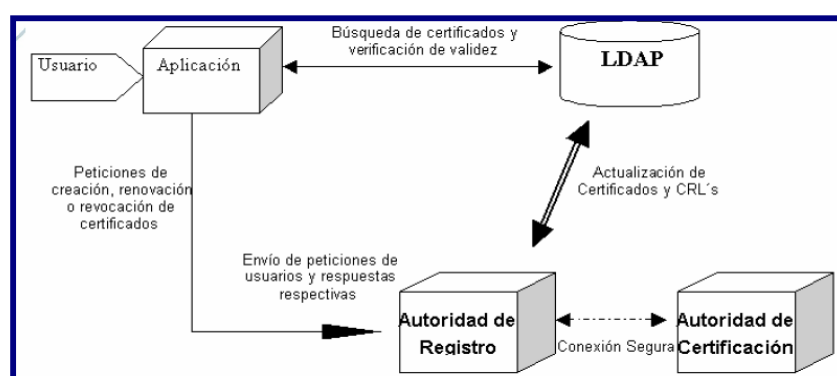
La AC Raíz es la autoridad de certificación Raíz de la Infraestructura de Clave Pública de Venezuela cuya función principal es emitir los certificados digitales a los PSC. Donde un certificado digital es un documento digital que asocia la identidad de un sujeto (entidad, individuo, dispositivo, etc.) 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 posee 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.

La relación de confianza basada en el uso de ICP requiere contar con: a) un nodo de manejo de Bases de Datos repositorios (LDAP) que registran los Certificados Digitales y demás datos sobre su solicitud, vigencia, revocación, etc., b) AC's y AR's que realizan operaciones asociadas al manejo de los Certificados Digitales, c) Elementos públicos para interactuar con los usuarios de ICP, d) Entidades o Usuarios

finales que interactúan con la ICP. Todos estos elementos hacen posible la relación de confianza a través de su interrelación como se muestra en el siguiente esquema, donde las entidades finales son aquellos que poseen un par de claves (pública y privada) y un certificado asociado a su clave pública.

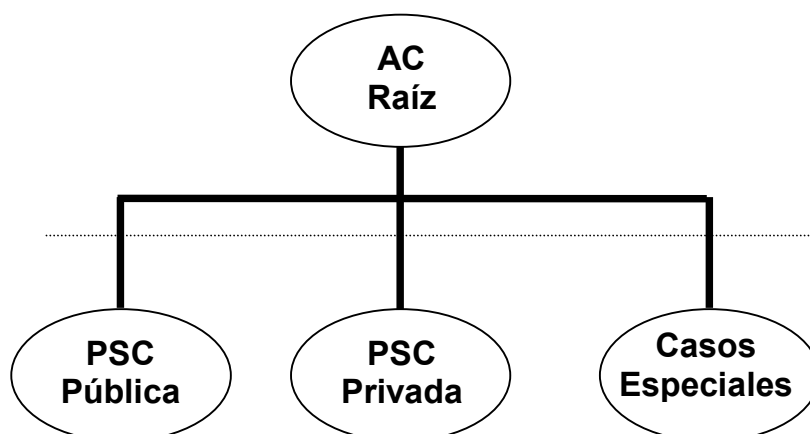
La AC raíz toma como significado en particular en el modelo de la **jerarquía subordinada**, permitiendo de esta manera relaciones de confianza bidireccionales y que los usuarios de certificados seleccionaran las anclas de confianza según se ajustaran (*ver figura 412*).



**Figura 4.1** Relación de Confianza

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



**Figura 4.2** Arquitectura Jerárquico General de la INCP

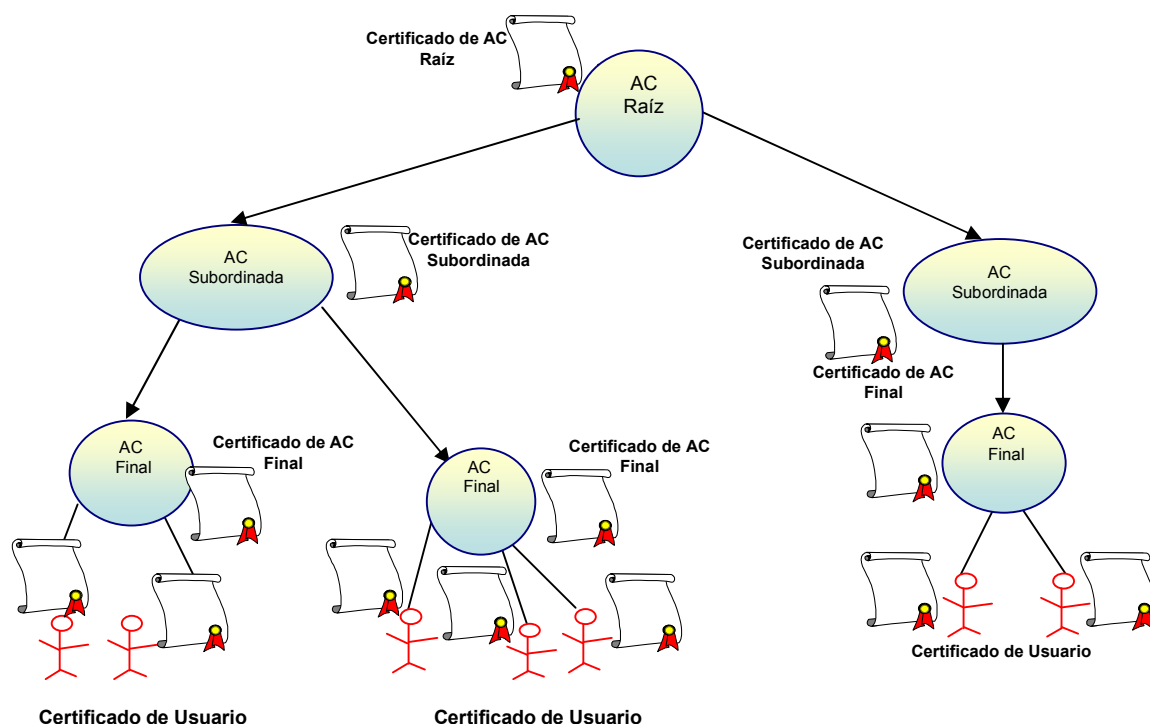
Este modelo es también adoptado para el Proveedor de Servicios de Certificación (PSC) de carácter público que prestará servicios de certificación a la Administración Pública Nacional (APN) porque forma parte del Sistema Nacional de Certificación Electrónica.

#### ***4.4.4. Diseño de la Arquitectura de la INCP en Venezuela***

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 INCP, donde No existe otra AC 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 la SUCERTE, 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).

A continuación podemos visualizar en la figura 4.3 que 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.



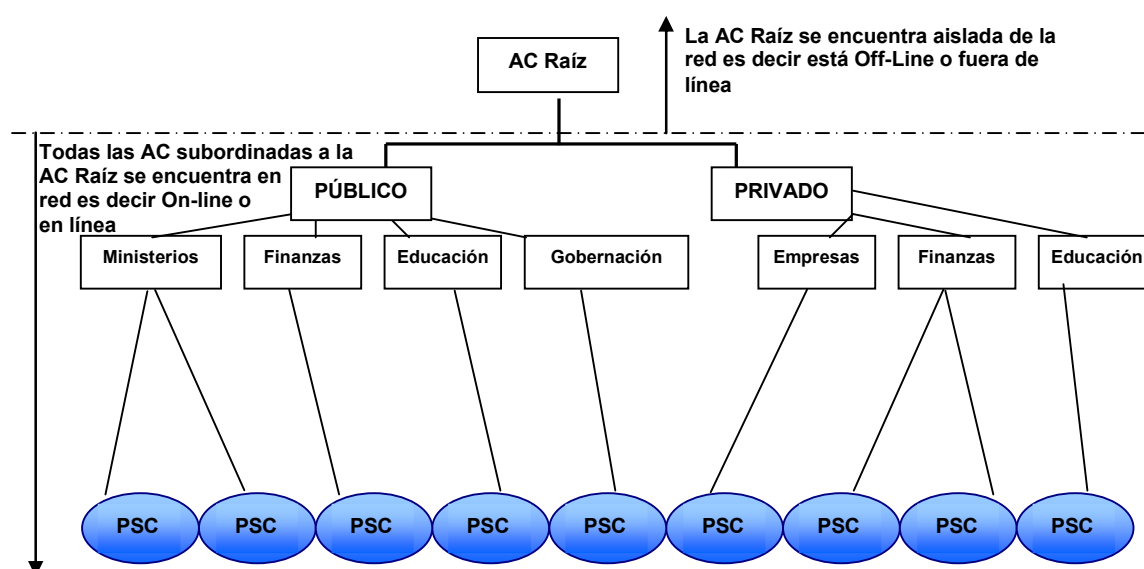
**Figura 4.3** Estructura jerárquica de la INCP de Venezuela

En cuanto así la 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 INCP.

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 4.4** Estructura de (INCP) para los sectores público y privado de Venezuela

La AC Raíz es operada por SUSCERTE en forma “Off-Line<sup>7</sup>”, 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<sup>8</sup>”, 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

<sup>7</sup> Fuera de línea, se mantiene aislada de la red por seguridad.

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 4.4, 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:

- a) **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 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, ONIDEX, CADIVI, SUDEBAN, SENIAT, entre los principales. Se debe garantizar la interoperabilidad con las Autoridades de Certificación (AC) que ya se encuentran operativas en algunos organismos públicos.
- b) **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.
- c) **Sector Finanzas:** Se 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.

---

<sup>8</sup> En línea, está conectada a la red.

- d) **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.

#### ***4.4.5. Crear Autoridades de Certificación y/o Autoridades de Registro***

La Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) podrá, de manera excepcional y a través de una Providencia Administrativa, crear Autoridades de Certificación y/o Autoridades de Registro para casos especiales en proyectos de interés nacional, y permitir los certificados electrónicos para estas Autoridades de Certificación, según corresponda.

En el siguiente paso se encuentra las AC Subordinadas de la AC Raíz llamados PSC una vez acreditados ante la SUCERTE según la LSMDFE, emitirán los certificados según el propósito de los certificados electrónicos especificados en su propia DPC<sup>9</sup> y PC<sup>10</sup>. Además de la LSMDFE existe el Reglamento parcial de la Ley sobre Mensajes de Datos y Firmas Electrónicas.

Solo se podrán crear Autoridades de Certificación y/o Autoridades de Registro para casos especiales en proyectos de interés nacional, cuando:

- a) No exista un Proveedor de Servicios Acreditado.
- b) Los certificados electrónicos requeridos en virtud del caso especial, no puedan ser emitidos por ningún Proveedor de Servicios de Certificación Acreditado.
- c) Los sistemas de información asociados a ese caso especial no se adapten al modelo jerárquico de la Infraestructura Nacional de Certificación Electrónica.
- d) En cumplimiento de normativas técnicas y/o legales internacionales adoptadas por el Estado Venezolano, no pueda utilizarse la infraestructura de los Proveedores de Servicios de Certificación Acreditados.

---

<sup>9</sup> DPC Declaración de Prácticas de Certificación

<sup>10</sup> PC Políticas de Certificación

Es importante resaltar que el personal de cada PSC es responsable de elaborar y su directiva de aprobar la DPC y PC, así como sus actualizaciones. Si se considera necesario modificar la estructura implementada por la SUSCERTE entonces la elegida será el modelo a seguir por todos los que soliciten ser PSC acreditados. Además de que la misma debe evaluar la elaboración de la DPC de cada PSC de la INCP de Venezuela.

En necesario que se encuentre documentado 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) 3647. La RFC 3647<sup>11</sup> con título “Internet x.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” proviene del Grupo de trabajo de la Red IETF<sup>12</sup> donde enumera las partes y requisitos necesarios para una DPC y Políticas de Certificados (PC).

#### ***4.4.6. Componentes de la Comunidad de Usuarios y Aplicabilidad***

La Autoridad de Aprobación de Políticas (AAP) creada dentro de la SUSCERTE como directorio de la Infraestructura Nacional de Clave Pública (INCP), bajo la autoridad del Ministerio para el Poder Popular y las Telecomunicaciones tiene atribuida la función de elaboración y propuesta de aprobación de la DPC, así como de sus modificaciones. La DPC será aprobada mediante Providencia Administrativa que se publicará en la Gaceta Oficial.

La AAP es también la encargada de analizar los informes de las auditorías, totales o parciales, que se hagan de la AC raíz, así como de determinar, en caso necesario, las acciones correctoras a ejecutar.

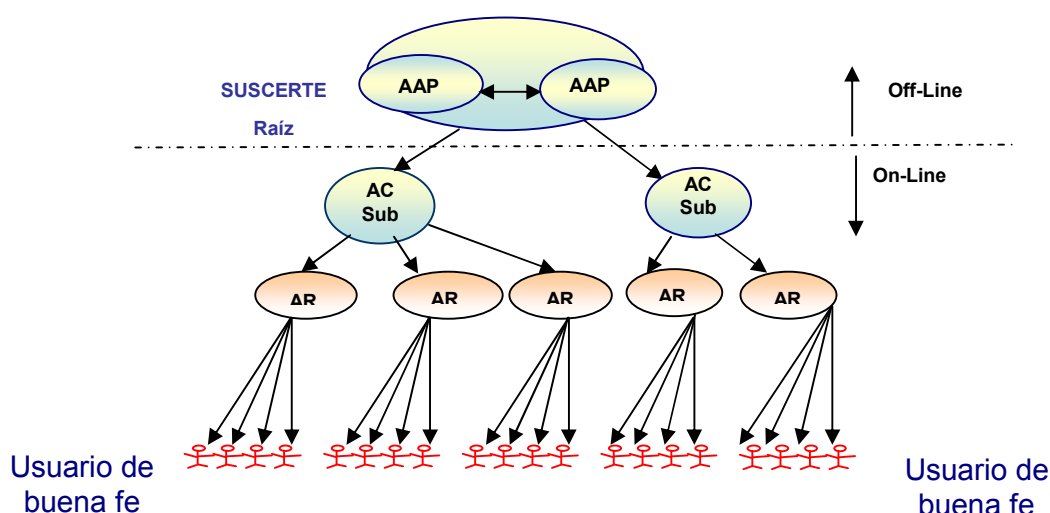
Según la infraestructura basada en el esquema anterior debe contar con los siguientes componentes:

---

<sup>11</sup> Se encuentra en la dirección electrónica <http://www.ietf.org/rfc/rfc3647.txt>

<sup>12</sup> 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.

- a) **Autoridad de Aprobación de Políticas (AAP) Raíz.**
- b) **Autoridad de Certificación AC Raíz.**
- c) **Autoridad de Registro (AR).**
- d) **Titulares de Certificados.**
- e) **Proveedores de Servicios de Certificados.**
- f) **Titulares de Certificados.**
- g) **Terceros de buena fe.**



**Figura 4.5** Componentes de la ICP de Venezuela

#### **a. Autoridad de Aprobación 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.

#### **b. Autoridad de Certificación AC**

La AC Raíz, es la Autoridad de Certificación origen de la jerarquía nacional de certificación electrónica. Este componente de la INCP de Venezuela es responsable por la emisión de los certificados electrónicos que acreditan a los PSC del sector público y privado, según lo establecido en la LSMDFE y su reglamento

parcial.

La Autoridad de Certificación de primer nivel sólo emite certificados para sí misma y sus AC Subordinadas. Únicamente estará en funcionamiento durante la realización de las operaciones para las que se establece.

La estructura de sus datos es:

<b>Campo del Certificado Raíz</b>	<b>Valor del Certificado Raíz</b>
<i>Versión</i>	V3
<i>Serial</i>	<i>Identificador único del certificado. Menor de 32 caracteres hexadecimales.</i>
<i>Algoritmo de firma del certificado</i>	<i>SHA256withRSAEncryption</i>
<b>Datos del emisor (DN)</b>	
<i>CN</i>	<i>Autoridad de Certificación Raíz del Estado Venezolano</i>
<i>C</i>	<i>VE (País)</i>
<i>L</i>	<i>(Dirección)</i>
<i>ST</i>	<i>(Estado)</i>
<i>O</i>	<i>Sistema Nacional de Certificación Electrónica</i>
<i>OU</i>	<i>Superintendencia de Servicios de Certificación Electrónica</i>
<i>E</i>	<i>Correo electrónico <a href="mailto:acraiz@suscerte.gob.ve">acraiz@suscerte.gob.ve</a></i>
<b>Datos del Titular</b>	
<i>CN</i>	<i>Autoridad de Certificación Raíz del Estado Venezolano</i>
<i>C</i>	<i>VE (País)</i>
<i>L</i>	<i>(Dirección)</i>
<i>ST</i>	<i>(Estado)</i>
<i>O</i>	<i>Sistema Nacional de Certificación Electrónica</i>
<i>OU</i>	<i>Superintendencia de Servicios de Certificación Electrónica</i>
<i>E</i>	<i><a href="mailto:acraiz@suscerte.gob.ve">acraiz@suscerte.gob.ve</a></i>
<b>Información de la Clave Pública (SUBJECT PUBLIC KEY INFO)</b>	
<i>Algoritmo de clave pública</i>	<i>Algoritmo con que se generó la Clave Pública (RSA)</i>
<i>Tamaño de clave pública</i>	<i>4096bits</i>
<b>Extensiones</b>	
<i>Restricciones básicas</i>	<i>CA: True y longitud del path = 2</i>
<i>Identificador de clave</i>	<i>SubjectKeyIdentifier = hash AuthorityKeyIdentifier =keyid, issuer, serial</i>
<b>Nombre alternativo del titular</b>	

<i>dNSName</i>	<i>suscerte.gob.ve</i>
<b><i>otherName</i></b>	
<i>OID 2.16.862.2.2</i>	<i>RIF-G-20004036-0</i>
<b><i>Nombre alternativo del emisor</i></b>	
<i>dNSName</i>	<i>suscerte.gob.ve</i>
<b><i>otherName</i></b>	
<i>OID 2.16.862.2.2</i>	<i>RIF-G-20004036-0</i>
<i>Uso de clave (Key usage)</i>	<i>Define el propósito de la clave del certif. Se debe definir como valor crítico: Firma electrónica del certificado y firma de LCR</i>
<i>Punto de distribución de CRL</i>	<i>URI: <a href="http://www.suscerte.gob.ve/lcr">http://www.suscerte.gob.ve/lcr</a> URI: <a href="ldap://acraiz.suscerte.gob.ve">ldap://acraiz.suscerte.gob.ve</a></i>
<i>OCSP</i>	<i>URI: <a href="http://ocsp.suscerte.gob.ve">http://ocsp.suscerte.gob.ve</a></i>

**Tabla N° 4.1** Estructura de los datos del certificado de la AC Raíz

#### **c. Autoridad de Registro (AR)**

Las actividades de identificación y registro de los PSC serán realizados por la SUSCERTE en conjunto con el proceso de acreditación, no existiendo autoridades de registro adicionales en el ámbito de la autoridad certificación raíz.

#### **d. Titulares de Certificados**

Los certificados emitidos por la AC raíz tienen como titulares a la propia AC raíz, a los PSC acreditados y casos especiales, según lo establecido en la LSMDFE y su reglamento parcial.

#### **e. Proveedores de Servicios de Certificados PSC**

Un Proveedor de Servicios de Certificación corresponde a una entidad emisora de Certificados Digitales de firma electrónica. Desde el punto de vista operativo, comprende un esquema funcional compuesto por una Autoridad de Registro (RA) y Autoridades de Certificación (AC's). Dentro de la dinámica de operación maneja Listas de Revocación de Certificados (CRL), Listas de Certificados Activos, Registro de solicitudes de Certificados, OSCP RESPONDER (Online) y CSR Petición por firma de certificado.

Los PSC operan con una Infraestructura de Clave Pública (ICP) (Public Key Infrastructure X.509: RFC 2459 & 3280), pares de claves y uso de criptografía como elementos de seguridad.

La estructura de los datos del Certificado para los PSC es:

<b>Campo del Certificado del PSC</b>	<b>Valor del Certificado Raíz</b>
<i>Versión</i>	V3
<i>Serial</i>	<i>Identificador único del certificado. Menor de 32 caracteres hexadecimales.</i>
<i>Algoritmo de firma del certificado</i>	SHA256withRSAEncryption
<b>Datos del emisor</b>	
<i>CN</i>	<i>Autoridad de Certificación Raíz del Estado Venezolano</i>
<i>O</i>	<i>Sistema Nacional de Certificación Electrónica</i>
<i>OU</i>	<i>Superintendencia de Servicios de Certificación Electrónica</i>
<i>C</i>	VE (País)
<i>E</i>	acraiz@suscerte.gob.ve
<b>Datos del Titular</b>	
<i>CN</i>	<i>Proveedor de Servicios de Certificación [identificación del proveedor]</i>
<i>O</i>	<i>Sistema Nacional de Certificación Electrónica. El campo O se define Sistema Nacional de Certificación Electrónica para que el proveedor se adhiera a la PKI Venezolana</i>
<i>OU</i>	<i>Nombre o razón social tal cual aparezca en el documento constitutivo</i>
<i>C</i>	País
<i>E</i>	Email
<i>Periodo de validez</i>	15 años
<i>Algoritmo de firma del certificado</i>	SHA256withRSAEncryption
<b>Extensiones</b>	
<i>Restricciones básicas</i>	CA: True y longitud del path =1
<i>Políticas de certificados</i>	Lugar en Internet desde donde se descargue las políticas de certificado
<i>Identificador de clave</i>	Dejarlas ambas
<b>Extensiones de información de titular y emisor</b>	



<i>Nombre alternativo del titular</i>	
<b>alternativeName</b>	
<i>dNSName</i>	[nombre de dominio del PSC registrado en nic.ve]
<b>otherName</b>	
<i>OID 2.16.862.2.1</i>	[Código de identificación del PSC acreditado asignado por SUSCERTE]
<i>OID 2.16.862.2.2</i>	RIF-[RIF del PSC]
<i>Nombre alternativo del emisor</i>	
<b>alternativeName</b>	
<i>dNSName</i>	suscerte.gob.ve
<b>otherName</b>	
<i>OID 2.16.862.2.2</i>	RIF-G-20004036-0
<i>Uso de clave</i>	Solo firma de certificado, firma de CRL, ambos críticos
<i>Punto de distribución de CRL</i>	Definidos por el proveedor
<b>OCSP</b>	<a href="http://ocsp.suscerte.gob.ve">URL://http://ocsp.suscerte.gob.ve</a>

**Tabla N° 4.2** Estructura de los datos del certificado del PSC

Entre los servicios que ofrece un PSC se incluyen:

- Emisión de Certificados Digitales.
- Generación de claves.
- Distribución de certificados.
- Certificación cruzada.
- Salvaguarda de claves.
- Suspensión y revocación de certificados.

Las AC Subordinadas son llamadas PSC del sector público y privado del país. En el marco legal venezolano, estos son derivados de la jerarquía de 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 INCP 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 la SUSCERTE.

**f. Terceros de buena fe**

Son todas las personas que realicen transacciones utilizando certificados electrónicos provenientes de la INCP y deciden aceptar y confiar en estos certificados.

#### **4.5. CERTIFICADOS DIGITALES**

Los Certificados Digitales son documentos firmados digitalmente por una Autoridad de Certificación, que asocia una Clave Pública con su titular durante el período de vigencia del certificado.

Un Certificado Digital está compuesto de:

- Un Nombre o Pseudónimo del titular.
- Versión del Certificado.
- Un código único que identifica al certificado.
- Un Identificador del PSC que expide el certificado.
- Un período de validez del certificado.
- La Firma Electrónica del PSC que expide el certificado.
- Un dispositivo de verificación de Firma Electrónica que corresponda a un dispositivo de creación de Firma Electrónica bajo control del titular.
- Un Atributo específico del titular.
- Los límites de uso del certificado, si procede.
- Dirección de la Consulta de la Lista de Certificados Revocados (LCR).

- Los límites de la responsabilidad del PSC y del valor de las transacciones para las que tiene validez el certificado.

#### **4.5.1 Tipos de Certificados Digitales**

SUSCERTE establece en las políticas la emisión de dos tipos de certificados. Cada tipo de certificado se identificara por un OID (Object Identifier) único, incluido en el certificado como identificador de política, dentro de la extensión X.509 Certificate Policies.

##### **a) Certificado tipo I – Certificados para AC raíz**

(OID política 2.16.862.1.2.) Este certificado lo genera la Autoridad de Certificación de primer nivel para su identificación. Éste es el certificado raíz autofirmado de la Infraestructura de Clave Pública Nacional. El uso de este certificado está enmarcado en las actividades de la AC raíz.

##### **b) Certificado tipo II – Certificados de AC para PSC**

(OID política 2.16.862.1.3.) Estos certificados se emitirán al Proveedor de Servicios de Certificación (PSC) acreditados ante SUSCERTE según lo establecido en la LSMDFE y su reglamento parcial. Este tipo de certificado puede emitir otros certificados y tiene privilegio de Autoridad de Certificación intermedia de la ICP nacional.

Las AC's y AR's manejan 4 tipos de Certificados Digitales:

- Certificados para usuarios finales desde 128 bits SSL.
- Certificados para servidores (correo electrónico, Web, entre otros) desde 256-bits SSL.
- Certificados para VPN.
- Certificados basados en hardware. Como ejemplo de ellos se recomienda el uso de tarjetas inteligentes o Smart Cards.

#### **4.5.2. Análisis de los Gestión de los Certificados Electrónicos**

Describe los elementos y variables a considerar en el proceso de evaluación de todos los aspectos técnicos involucrados en la creación, registro y control de los certificados para firmas electrónicas, los cuales serán emitidos por un Proveedor de Servicios de Certificación (PSC).

Para la valoración de los elementos técnicos relacionados con el manejo de los certificados, se tomará en cuenta el resultado del informe presentado por el Auditor registrado en el Sistema de Acreditación de SUSCERTE.

Se constatará que el certificado que presente contenga los siguientes campos:

- Nombre del certificado.
- Versión del certificado.
- Estado del certificado.
- Fecha de emisión.
- Fecha de expiración.
- Localización.
- Identificador único de objeto (OID)

En relación a las Políticas de Certificados, se evaluará la observancia de:

- Indicación de a quien se le puede otorgar un certificado.
- Política de registro del signatario donde se establezca la forma de autenticación y verificación de la identidad del signatario.
- Clara indicación de los propósitos para los cuales se emite el certificado y cuales son sus limitaciones.
- Descripción detallada de las obligaciones de las entidades involucradas en la emisión y utilización del certificado.

- Existencia de clara concordancia entre las prácticas de certificación y Políticas de Certificados con los procedimientos operacionales.
- Políticas definidas para garantizar la privacidad y protección de datos.
- Circunstancias bajo las cuales se suspende o revoca un certificado.

#### **4.5.3 *Uso de los Certificados***

##### **4.5.3.1 Usos permitidos para los certificados**

El certificado electrónico raíz sólo puede utilizarse para la identificación de la propia Autoridad Certificación Raíz y para la distribución de su clave privada de forma segura.

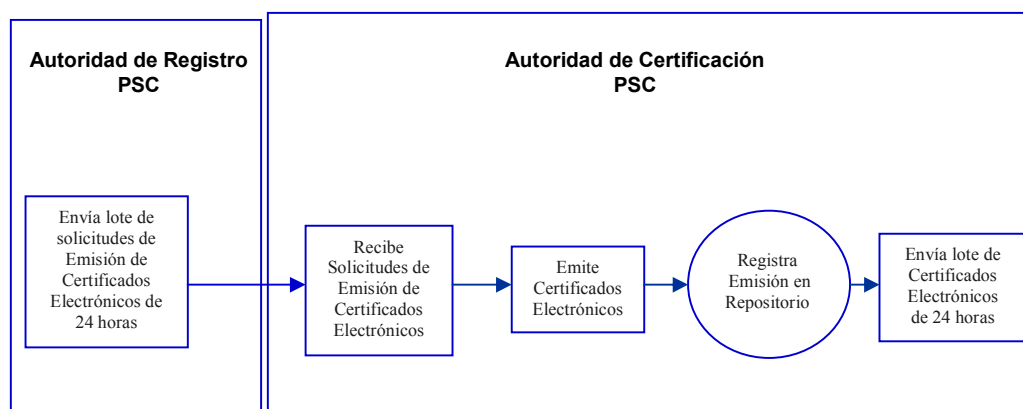
El uso de los certificados emitidos por la AC raíz estará limitado a la firma de certificados electrónicos para entidades subordinadas y la firma de las listas de certificados revocados correspondientes.

##### **4.5.3.2 Usos no permitidos para los certificados**

El uso no permitido para los certificados emitidos por la AC raíz son todos aquellos que no están explícitamente permitidos en la sección anterior.

#### **4.5.4 *Emisión de Certificados***

La emisión de certificados de los PSC es un proceso en lote en el cual se considerarán todas las solicitudes que las AR hayan procesado en las 24 horas anteriores a la sincronización de repositorios. Los certificados emitidos serán almacenados en el repositorio de la AC y se enviarán a la AR durante la próxima sincronización.



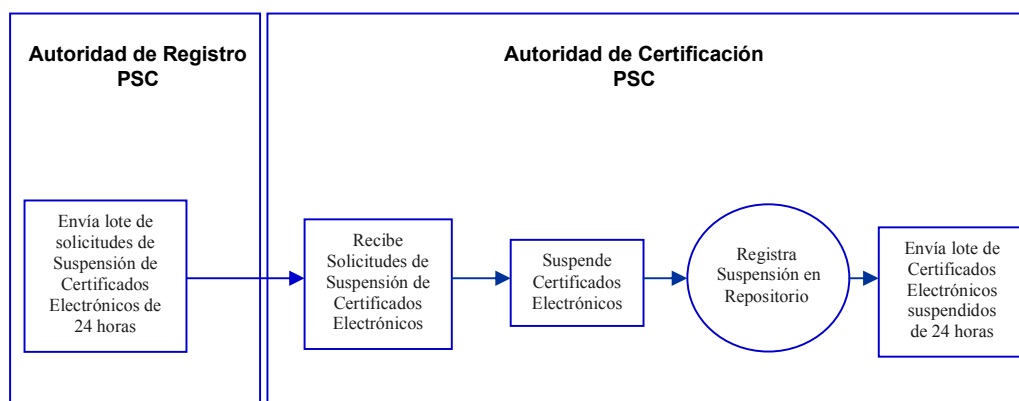
**Figura 4.6** Proceso de Emisión de Certificados

#### **4.5.5 Suspensión y Renovación de Certificados**

La Suspensión de Certificados se hará por voluntad del propietario del certificado y deberá tramitarse a través de una solicitud de suspensión requerida a la AR que tramitó la emisión del certificado. Se procesará como un requerimiento en lote correspondiente a las 24 horas posteriores a la última sincronización de repositorios.

A solicitud del propietario, un certificado podrá ser suspendido temporalmente, reactivándose posteriormente a través de una nueva solicitud. La solicitud de suspensión será procesada por la AR de acuerdo a la solicitud del propietario, se realizará el registro correspondiente y se enviará la notificación de suspensión al propietario.

La reactivación de un certificado suspendido será tramitada de forma equivalente a una nueva emisión.



**Figura 4.7** Proceso de Suspensión de Certificados

#### 4.5.5.1 Circunstancias para la renovación del certificado del PSC

Las circunstancias para la revocación de un certificado del PSC son las siguientes:

- Compromiso de la clave privada de la AC raíz.
- Compromiso o sospecha de compromiso de la clave privada asociada al certificado del PSC.
- Cuando el PSC solicite a la AC Raíz la suspensión temporal de su certificado.
- Por resolución judicial o administrativa que lo ordene.
- Por la variación de los datos del certificado.

#### 4.5.5.2 Entidad que puede solicitar la Renovación

Las entidades autorizadas para solicitar la revocación de acreditación de un PSC de la INCP de Venezuela:

- ◆ La autoridad competente a la conformidad con la LSMDFE.
- ◆ El Proveedor de Servicio de Acreditación.
- ◆ La Autoridad de Certificación Raíz

#### 4.5.5.3 Procedimiento de Solicitud de Renovación

Los pasos para la revocación de la acreditación de un PSC ante la SUSCERTE, son:

	ACTOR	ACCIÓN
1	DRA	<ol style="list-style-type: none"> <li>1. Recibe del Directorio de la SUSCERTE la Resolución donde se determina la suspensión de la Acreditación de un PSC.</li> <li>2. Acata la instrucción donde se le solicita participe al PSC de la Resolución tomada.</li> </ol>
2	PSC	<ul style="list-style-type: none"> <li>➤ Recibe la notificación de suspensión de la Acreditación como PSC, resuelta por el Directorio de la SUSCERTE.</li> <li>➤ Suspende de inmediato la negociación con nuevos usuarios, manteniendo el servicio de los signatarios existentes, hasta nuevo aviso.</li> <li>➤ Decide acción para solventar la problemática, en función del razonamiento dado por el Directorio a la suspensión: <ol style="list-style-type: none"> <li>a. Acata medida por estar de acuerdo con la misma.</li> <li>b. U Objeta decreto de suspensión de su Acreditación por el Directorio. Expone el planteamiento ante la SUSCERTE.</li> </ol> </li> </ul>
3	DRA	<ol style="list-style-type: none"> <li>1. Conviene con el PSC, las acciones a llevar a cabo, de acuerdo a su planteamiento: <ol style="list-style-type: none"> <li>c) Acuerdan el mecanismo para activar la suspensión de la que fue objeto, en el lapso de los quince (15) días que tiene para ello.</li> <li>d) O Recibe sus fundamentos en contra de la suspensión de la Acreditación, utilizando los diez (10) días que la Ley Orgánica de Procedimientos Administrativos (LOPA) le asigna para exponer alegatos.</li> </ol> </li> </ol>
4	PSC	<p>Ejecuta las acciones convenidas con la DRA:</p> <ul style="list-style-type: none"> <li>• Envía a la SUSCERTE plan de mejoras para solventar la problemática que originó la suspensión de su Acreditación, si está de acuerdo con la decisión del Directorio.</li> <li>• Remite a la SUSCERTE informe justificando las razones de su desacuerdo ante suspensión de la Acreditación.</li> </ul>
5	DRA	<p>Recibe del PSC las comunicaciones y soportes de sus planteamientos, y actúa en consecuencia:</p> <ol style="list-style-type: none"> <li>c) Presenta al Directorio el plan de mejoras del PSC interesado en reactivar su Acreditación.</li> <li>d) Presenta al Directorio los fundamentos del PSC, donde alega inconformidad con la decisión del Directorio justificando su motivación.</li> </ol>
6	DS	<ul style="list-style-type: none"> <li>➤ Admite los documentos del PSC, decidiendo en consonancia con las sustentaciones: <ul style="list-style-type: none"> <li>➤ 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.</li> <li>➤ O Analiza reclamo interpuesto por el PSC: <ol style="list-style-type: none"> <li>a) Reafirma la suspensión de la Acreditación, al comprobar nuevamente los incumplimientos que la originaron.</li> <li>b) Reajusta decisión, si los alegatos del PSC tienen fundamento, reactivando la Acreditación por medio de una Resolución.</li> </ol> </li> </ul> </li> </ul>



		<ul style="list-style-type: none"> <li>➤ Participa a la DRA, disposiciones.</li> <li>➤ Autoriza a la DRA envío de comunicación informativa al PSC.</li> </ul>
7	DRA	<ul style="list-style-type: none"> <li>● Comunica al PSC decisión del Directorio: <ul style="list-style-type: none"> <li>➤ Insta al PSC para que ponga en práctica el plan de mejoras aprobado por el Directorio.</li> <li>➤ Informa en relación a su reclamo: <ul style="list-style-type: none"> <li>a) 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.</li> <li>b) O Da parte de la Resolución emitida por el Directorio, donde reactiva la Acreditación suspendida.</li> </ul> </li> </ul> </li> </ul>
8	PSC	<p>2. Recibe notificación de la Dirección de Registro y Acreditación de la SUSCERTE:</p> <ul style="list-style-type: none"> <li>➤ 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.</li> <li>➤ Resuelve, con relación a su reclamo: <ul style="list-style-type: none"> <li>a) Elaborar un plan de mejoras, para evitar la revocación de su Acreditación, en el tiempo que le queda para ello. Sigue este procedimiento a partir de la acción 9 A. En caso contrario, continúa con la acción.</li> <li>b) Reiniciar sus actividades ordinarias.</li> </ul> </li> </ul> <ul style="list-style-type: none"> <li>● Informa a la DRA resultados de su gestión.</li> </ul>
9	DRA	<ul style="list-style-type: none"> <li>● 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: <ul style="list-style-type: none"> <li>➤ 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 SUSCERTE.</li> <li>➤ Revoca la Acreditación del PSC que incumple con los requisitos y obligaciones exigidos por el Decreto-Ley 1.204, Reglamento Parcial y Normas SUSCERTE.</li> </ul> </li> </ul>

**Tabla N° 4.3** Procedimiento de Solicitud de Renovación

#### 4.5.5.4 Circunstancias para la suspensión

Las circunstancias para la suspensión de un certificado de PSC son las siguientes:

- Compromiso de la clave privada de la AC Raíz.

- Compromiso o sospecha de compromiso la clave privada asociada al certificado del PSC.
- Cuando el PSC solicite a la AC Raíz, la suspensión temporal de su certificado.
- Cuando el PSC tenga conocimiento del uso indebido de la Firma Electrónica.
- Por resolución judicial o administrativa que lo ordene.
- Por la variación de los datos del certificado.

#### 4.5.5.5 Entidad que puede solicitar la suspensión

Las entidades autorizadas para solicitar la revocación de acreditación de un PSC de la INCP de Venezuela:

- La autoridad competente a la conformidad con la LSMDFE.
- El Proveedor de Servicio de Acreditación.
- La Autoridad de Certificación Raíz.

#### 4.5.5.6 Procedimiento para la solicitud de suspensión

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

	ACTOR	ACCIÓN
1	DRA	<ol style="list-style-type: none"> <li>4. Recibe del PSC, con la antelación prevista, el plan de mantenimiento y/o mejoras a sus instalaciones, equipos y sistemas, con el cronograma de suspensión temporal del servicio por tales actividades anexo.</li> <li>5. 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.</li> <li>6. Solicita al PSC ajuste la planificación y el cronograma, de no estar conforme.</li> <li>7. Aprueba el plan y el cronograma, cuando estos se adecuen a las disposiciones del Decreto-Ley 1.204 y a las normativas internas de la SUSCERTE.</li> <li>8. 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 aceptado.</li> </ol>
2	PSC	<ul style="list-style-type: none"> <li>• Recibe de la SUSCERTE el plan y el cronograma de suspensión del</li> </ul>

		<p>servicio aprobado.</p> <ul style="list-style-type: none"> <li>● Envía a sus signatarios el cronograma de suspensión del servicio, aprobado por la SUSCERTE.</li> <li>● Remite a la SUSCERTE ejemplar de la notificación con la cual informó a sus signatarios del cronograma de suspensión del servicio.</li> </ul>
3	DRA	<ul style="list-style-type: none"> <li>● Recibe un ejemplar de la notificación donde los signatarios del PSC son informados del cronograma de suspensión temporal del servicio.</li> <li>● Queda pendiente de controlar las acciones a realizar por el PSC para suspender el servicio, en la fecha y hora aprobadas.</li> </ul>
4	PSC	<ul style="list-style-type: none"> <li>● Envía comunicación a sus signatarios donde les recuerda de la fecha y hora de la suspensión del servicio.</li> <li>● Remite ejemplar a la SUSCERTE de la notificación enviada a sus signatarios.</li> <li>● Suspende el servicio en su oportunidad, en la fecha y hora establecidas.</li> <li>● Reinicia el servicio, cumpliendo con el lapso aprobado para la suspensión.</li> <li>● Informa a sus signatarios del reinicio del servicio.</li> <li>● Despacha a la SUSCERTE un ejemplar de la notificación del reinicio del servicio que le enviara a sus signatarios.</li> </ul>
5	DRA	<ol style="list-style-type: none"> <li>3. Recibe del PSC copia de la notificación del reinicio del servicio.</li> <li>● Constata cumplimiento de la programación establecida.</li> <li>● Participa al PSC la adecuada aplicación de las disposiciones legales y normativas de la SUSCERTE.</li> <li>● Queda a la espera de la próxima programación de la suspensión del servicio por parte del PSC.</li> </ol>

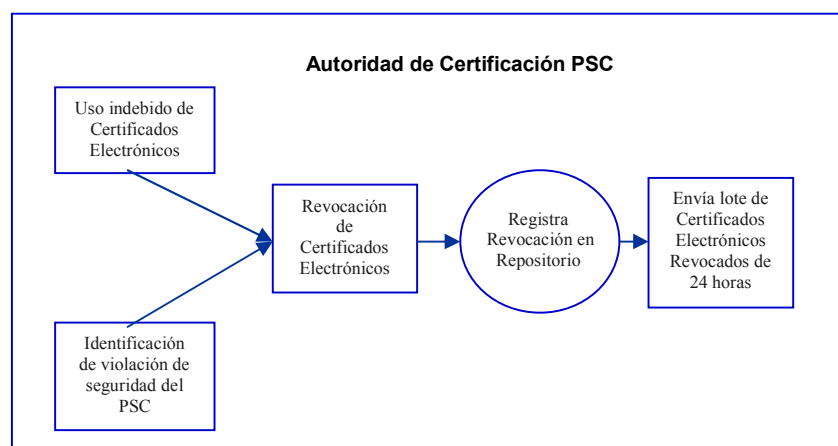
**Tabla N° 4.3** Procedimiento de Solicitud de Suspensión

#### **4.5.6 Revocación de los Certificados**

La revocación de Certificados Digitales se da como medida de contingencia ante la violación de la seguridad de las AC3<sup>13</sup> y la AC o por uso indebido del certificado. En todos los casos, este procedimiento será procesado exclusivamente en la AC.

Como AR en caso de mal uso de certificados, pérdida o alteración de, o en presencia de auditorias no aprobadas, los propietarios de certificados recibirán una notificación de realización de auditoria con posibilidades de revocación de certificado.

<sup>13</sup> AC3: Las AC's de nivel 3 que realizan funciones de certificación a través de un conjunto de AR's, reconocidas por un PSC y AR's que atienden solicitudes de Certificados Digitales y Firmas Digitales que serán procesados a través de una AC de cualquiera de los niveles señalados.



**Figura 4.8** Proceso de Revocación de Certificados

Una vez realizada esta auditoria, el certificado podrá ser revocado o liberado de la posible revocación y el propietario recibirá la notificación correspondiente.

#### **4.5.7 Actualización y Sincronización de los Repositorios**

Los repositorios son las estructuras encargadas de almacenar la información relativa a la ICP. Los dos repositorios más importantes son el Repositorio de Certificados y el Repositorio de Listas de Revocación de Certificados (LRC).

La actualización y sincronización de repositorios es un proceso de mantenimiento de repositorios que se da diariamente como consecuencia de la sincronización de los repositorios de certificados y como garantía a la operación del PSC. Este procedimiento generará los registros históricos requeridos como garantía de operación del PSC.

#### **4.5.8 Publicación**

Es obligación para la AC raíz y los PSC pertenecientes a la jerarquía de confianza publicar la información relativa a sus prácticas, sus certificados y el estado actualizado de dichos certificados.

Las publicaciones que realice la SUSCERTE y el PSC, de toda información clasificada como pública, se anunciará en su respectivas páginas Web de la siguiente manera:

- La lista de Certificados Revocados (LCR), se encuentra disponible en formato CRL V2.
- Las Políticas de Certificados de la AC, se podrán ubicar en formato PDF y Open Document firmado.
- Los certificados emitidos se encuentran disponibles en el repositorio público, en formato X.509 v3.

#### **4.5.9 Frecuencia de la Publicación**

##### **4.5.9.1 Certificados de la AC Raíz**

La publicación del certificado se realizará con anterioridad a su puesta en vigencia a través de la Gaceta Oficial. El periodo de validez es de veinte años.

##### **4.5.9.2 Certificados de PSC**

La publicación del certificado se realizará con anterioridad a su puesta en vigencia a través de la Gaceta Oficial. El periodo de validez es de quince años.

##### **4.5.9.3 Lista de Certificados Revocados (LCR)**

Se realizarán dos tipos de publicaciones para la lista de Certificados Revocados (LCR):

✓ ***Periódicamente:***

- Cada 6 meses a menos que suceda una acreditación o una revocación de un certificado dentro de la ICP nacional. Cuando suceda uno de estos eventos, el periodo de 6 meses comenzará nuevamente desde cero.

✓ ***Eventualmente:***

- Cada vez que se acredite o revoque un certificado dentro de la ICP nacional.

- Cada vez que se comprometa una clave privada de un PSC acreditado.

#### **4.5.9.4 Declaración de Prácticas de Certificación**

La AC Raíz, publicará en el repositorio, las nuevas versiones de este Documento, inmediatamente tras la aprobación de las mismas.

#### **4.5.10 Ciclo de Vida de los Certificados Para PSC**

##### **4.5.10.1 Solicitud de los Certificados**

Los procedimientos operativos establecidos por la SUSCERTE para la acreditación es responsabilidad de los PSC aspirantes a la acreditación. Este proceso se puede llevar a cabo de forma manual dirigiéndose ante las oficinas de la SUSCERTE o a través del sistema automatizado<sup>14</sup>.

Una vez aprobada la solicitud por la directiva de la SUSCERTE, el PSC presenta las garantías necesarias para obtener la acreditación como PSC de la INCP de Venezuela, en la cadena de confianza y 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 la SUSCERTE.

##### **4.5.10.2 Entidades que pueden solicitar Acreditación**

Todas las entidades públicas y privadas del estado venezolano que cumplan con los requisitos solicitados por la SUSCERTE podrán solicitar la acreditación a la cadena de confianza. Los lineamientos exigidos por la ley sobre mensajes de datos y firmas electrónicas son:

- ✓ Capacidad económica y financiera suficiente para prestar los servicios autorizados como PSC. En el caso de organismos públicos, éstos deberán contar con un presupuesto de gastos y de ingresos que permitan el desarrollo de esta actividad.

---

<sup>14</sup> Visitando la dirección electrónica <http://www.suscerte.gob.ve/acreditacion>

- ✓ Capacidad y elementos técnicos necesarios para proveer Certificados Electrónicos.
- ✓ Garantizar un servicio de revocación o cancelación, rápido y seguro, de los Certificados Electrónicos que proporcione.
- ✓ Un sistema de publicación de información de acceso libre, permanente, actualizado y eficiente. En este sistema se publicarán las políticas y procedimientos aplicados para la prestación de sus servicios, así como los Certificados Electrónicos que hubiere proporcionado, revocado, 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.

#### ***4.5.11 Tramitación de Solicitud de un Certificado***

##### **4.5.11.1 Realización de las funciones de identificación y autenticación**

Las funciones de identificación y autenticación las realizan los funcionarios y personal encargado de la operación de los sistemas de acreditación de la SUSCERTE.

Estos funcionarios desempeñan el rol de operador de registro, disponiendo de un dispositivo seguro de creación de firma (tarjeta de funcionario) para el control de acceso a la aplicación de expedición y control de integridad y no repudio de las operaciones y transacciones realizadas.

#### **4.5.11.2 Aprobación o denegación de certificado**

Se aprobará las solicitudes de certificación a aquellos proveedores que cumplan con todos los requisitos y lineamientos técnicos, económicos y jurídicos exigidos por la SUSCERTE en el presente DPC. El sistema garantiza que el certificado emitido este dentro de la cadena de confianza de la ICP nacional.

#### **4.5.11.3 Plazo para la tramitación de un certificado**

La Superintendencia de Servicios de Certificación Electrónica, previa verificación de los documentos de solicitud para la acreditación 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.

#### **4.5.12 Emisión de Certificado**

Luego de verificar y aprobar las exigencias establecidas en la LSMDFE el sistema de la AC procederá a realizar la emisión del certificado al PSC mediante la publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

##### **4.5.12.1 Acciones de la AC durante la Emisión del Certificado**

La emisión de los certificados implica la autorización de la solicitud por parte del sistema de la AC raíz. Después de la aprobación de la solicitud se procederá a la emisión de los certificados de forma segura y se pondrán los certificados a disposición del PSC.

En la emisión de los certificados la AC:

- ✓ Utiliza un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- ✓ Protege la confidencialidad e integridad de los datos de registro.

Todos los certificados iniciarán su vigencia en el momento que se indica en el propio certificado. Se utilizará el campo de “not before” con este fin. Ningún certificado será emitido con un periodo de validez que se inicie con anterioridad de la fecha actual. Sin embargo, si se podrán emitir certificados cuyo periodo de validez se inicie en el futuro o una fecha posterior a la actual.



#### **4.5.12.2 Notificación al solicitante por parte de la AC Raíz acerca de la Emisión de su Certificado**

El PSC sabrá sobre la emisión efectiva del certificado por medio de una carta al representante legal emitido por el directorio de la SUSCERTE. Así mismo, se publica en el diario de mayor circulación nacional, la autorización para que el solicitante comience actuar como PSC.

#### **4.5.13 Aceptación de Certificados**

##### **4.5.13.1 Forma en la que se Acepta el Certificado**

El certificado emitido por la AC Raíz al PSC se considera aceptado luego de su publicación en el repositorio de la INCP.

##### **4.5.13.2 Publicación del Certificado por la AC**

SUSCERTE proveerá diversos tipos de comunicación como correos electrónicos, comunicaciones escritas, repositorio LDAP, repositorio Web, OCSP, Gaceta Oficial y los que considere pertinentes para publicar la aceptación de un certificado.

##### **4.5.13.3 Notificación de la Emisión del Certificado por la AC a otras Autoridades**

La SUSCERTE notificará a las entidades, organismos del gobierno y empresas privadas la emisión de un certificado por medio de la página Web de la SUSCERTE, el diario de mayor circulación nacional y por la Gaceta Oficial de la República Bolivariana de Venezuela.

#### **4.5.14 Uso del par de Claves y del Certificado**

El uso de los certificados emitidos por la AC raíz de Venezuela son los previstos en la LSMEFD y en sus reglamentos.

##### **4.5.14.1 Uso de la clave privada del certificado por el PSC**

El titular sólo puede utilizar la clave privada y el certificado para los usos autorizados en esta DPC. La SUSCERTE emite certificados con los campos de uso de clave privada limitados a firma de certificados y firma de LCR.

#### **4.5.14.2 Uso de la clave pública y del certificado por los terceros de buena fe**

Los terceros de buena fe sólo pueden depositar su confianza en los certificados para aquello que establece esta DPC.

Los terceros de buena fe pueden realizar operaciones de clave pública de manera satisfactoria confiando en el certificado emitido por la cadena de confianza. Así mismo, deben asumir la responsabilidad de verificar el estado del certificado utilizando los medios que se establecen en esta DPC.

#### **4.5.15 Renovación De Certificado Con Cambio De Clave**

##### **4.5.15.1 Causas para la renovación de un certificado**

La causa de la renovación de un certificado por parte del PSC es por la caducidad.

##### **4.5.15.2 Entidad que puede solicitar la renovación del certificado**

Las entidades autorizadas para solicitar la renovación de un certificado con cambio de clave de un PSC de la INCP de Venezuela:

- El Proveedor de Servicio de Acreditación.
- La Autoridad de Certificación Raíz

##### **4.5.15.3 Notificación de la emisión de un nuevo certificado al PSC**

SUSCERTE notificará al PSC sobre la emisión efectiva de un nuevo certificado por medio de una carta al representante legal emitido por el directorio de la SUSCERTE. Así mismo, se publica en el diario de mayor circulación nacional.

##### **4.5.15.4 Publicación del certificado renovado por la AC**

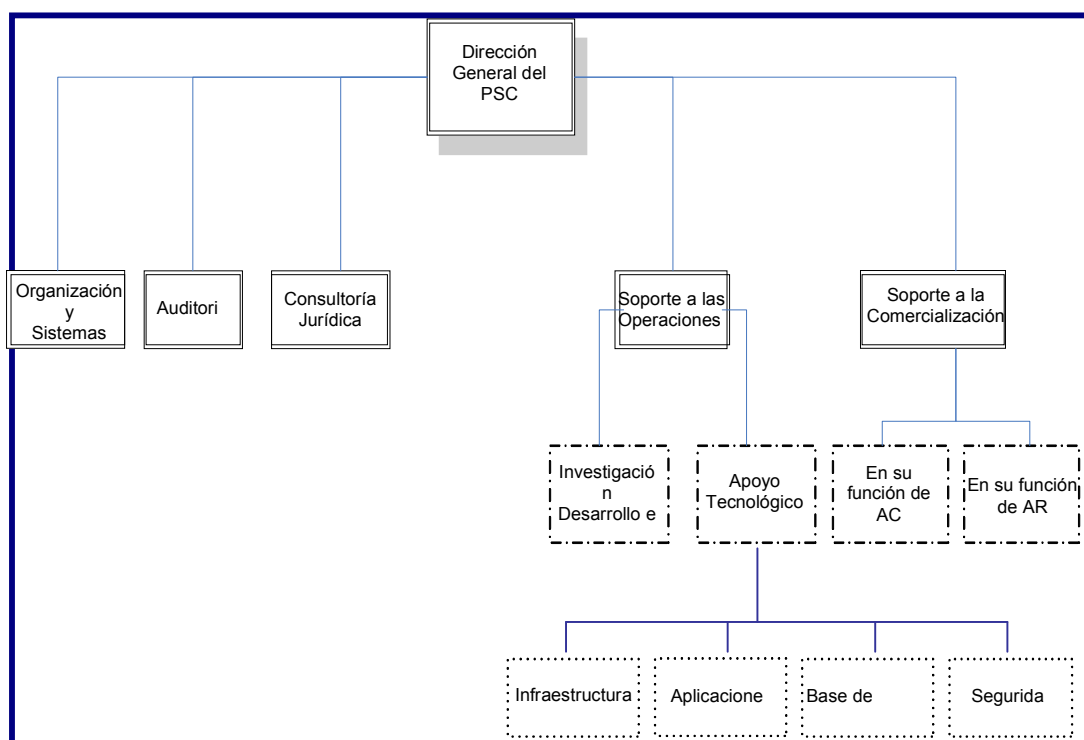
SUSCERTE proveerá diversos tipos de comunicación como correos electrónicos, comunicaciones escritas, repositorio LDAP, repositorio Web, OCSP, Gaceta Oficial y los que considere pertinentes para publicar la renovación de un certificado.

##### **4.5.15.5 Notificación de la emisión del certificado por la AC a otras entidades**

SUSCERTE notificará a las entidades, organismos del gobierno y empresas privadas la renovación de un certificado por medio de la página Web de la SUSCERTE, el diario de mayor circulación nacional y por la Gaceta Oficial de la República Bolivariana de Venezuela.

#### 4.6. UNIDADES ORGANIZACIONALES REQUERIDAS PARA LA OPERACIÓN DEL PSC

Para la operación del PSC se requiere contar con un conjunto de unidades organizacionales o su equivalente en personas responsables según determine el volumen de servicios que se presente. Estas unidades se pueden agrupar en dos grupos operativos y un ente rector tal como se describen a continuación:



**Figura 4.10** Unidades Organizacionales del PSC

#### **4.6.1 Dirección General del PSC**

Es el ente rector del PSC. Sirve de enlace con la SUSCERTE como AC Raíz de Venezuela.

#### **4.6.2 Unidad de Organización de Sistemas**

Asiste a las demás unidades organizacionales en cuanto a la definición de la estructura organizacional, de las normas y procedimientos que lo rigen y el desarrollo de las aplicaciones. Entre sus funciones generales tenemos:

- Analizar los procesos administrativos, con el objeto de reducir tiempos y costos.
- Estudiar, analizar y proponer cambios en la estructura organizativa, así como reestructurar unidades que así lo requieran.
- Elaborar informes técnicos, efectuando las recomendaciones pertinentes a la optimización de procesos.
- Elaborar y mantener los manuales de las diferentes áreas administrativas y los manuales de usuarios.
- Canalizar las solicitudes de diseño y/o actualización de las aplicaciones.
- Formación del usuario en cuanto a la aplicación de sistemas y procedimientos.
- Elaborar, verificar y controlar los diseños de impresos que son necesarios para el PSC.
- Establecer reuniones de trabajo con las distintas unidades, cuando así sea requerido.
- Brindar apoyo necesario a las distintas unidades, en cuanto a la evaluación y definición de nuevas herramientas de trabajo.

#### **4.6.3 Unidad de Auditoría**

Esta unidad es responsable de emplear procedimientos, técnicas y metodologías, a fin de prever y verificar la integridad de los datos, la confiabilidad de los controles internos, información financiera y la seguridad de los activos de la información que se encuentran almacenados en los medios informáticos del PSC.

#### **4.6.4      *Unidad de Consultoría Jurídica***

Esta unidad se encarga de asesorar en todo lo relacionado a los asuntos jurídicos, atiende y representa al PSC en todas las acciones de carácter legal, y de organizar, dirigir y coordinar las actividades relacionadas con la tramitación de los documentos legales.

#### **4.6.5      *Unidad de Soportes a las Operaciones y Tecnología***

Corresponde a esta unidad garantizar, planificar, dirigir y controlar la evaluación y concepción de la plataforma tecnológica y sistémica existente en el PSC. Vendrá inmerso el diagnóstico, concepción, configuración y perfeccionamiento del factor tecnológico requerido para lograr el buen desempeño y aumento del índice de productividad.

En este sentido, será la encargada de mantener permanentemente la disponibilidad de hardware y software en condiciones para permitir la operatividad de las unidades usuarias que reciben el servicio.

#### **4.6.6      *Departamento de Investigación, Desarrollo e Innovación***

Es el encargado de la actualización permanente de las tecnologías de apoyo, los servicios ofrecidos y las operaciones realizadas en el PSC. Igualmente formulará y dirigirá las tareas que permitirán la evaluación de insumos de software y hardware indispensables en los procesos básicos, y que posteriormente serán presentados a nivel gerencial para la toma de decisiones pertinente en cuanto a su adquisición futura.

#### **4.6.7      *Departamento del Apoyo Tecnológico***

Este departamento es responsable del correcto funcionamiento de la plataforma de equipos y aplicaciones que sirven de apoyo a la operación del PSC.

#### **4.6.7.1. Área de Infraestructura**

Esta área se encarga de todo lo relacionado con las comunicaciones y redes existentes en el PSC. Entre las funciones generales tenemos:

- Implementar, administrar y mantener el funcionamiento de las redes existentes.
- Definir funciones de administración general, controlar y verificar el funcionamiento, de las redes.
- Establecer políticas de instalación, configuración, mantenimiento, actualización, tolerancia a fallos, y cualquier tarea que involucre un desarrollo normal en el funcionamiento de las redes.
- Definir y realizar auditorías necesarias para corroborar el estado de funcionamiento y control de las redes.
- Definir, mantener y controlar las políticas de administración preventiva para las redes.
- Definir las especificaciones técnicas, en el área de redes.
- Administrar e implementar las políticas de seguridad perimetral. Mantener o hacer mantener el equipamiento que presta servicios de conectividad.

#### **4.6.7.2. Área de Aplicaciones**

Esta área se encarga de formular, dirigir y llevar a cabo desarrollos que permitan la implementación de diversas aplicaciones que cumplan con los requerimientos del PSC y los usuarios.

#### **4.6.7.3. Área de Base de Datos**

Esta área desarrolla eficientemente actividades concernientes a la concepción, estructuración y administración de las Bases de Datos existentes.

#### **4.6.7.4. Área de Seguridad**

Esta área lleva a cabo actividades concernientes a la aplicación de los diversos controles para mantener la seguridad de los activos de la información, así como

también de verificar el cumplimiento de las políticas de seguridad y planes de contingencia establecidos.

#### **4.6.8 Unidades de Soporte de Comercialización**

##### **4.6.8.1. En su Función de la AC**

El PSC como AC de nivel 2 debe realizar operaciones características de una AC. En tal sentido, esta unidad se encargará de la emisión y revocación de Certificados Digitales, así mismo, se encargará de la acreditación y control de operaciones de las denominadas AC de nivel 3 vinculadas al PSC.

##### **4.6.8.2. En su Función de la AR**

Aún cuando no es función prioritaria del PSC-FII el atender solicitudes de usuarios finales, esta unidad se encargará de realizar la función de AR, atendiendo las solicitudes que se presenten para su tramitación a través de la función de AC.

### **4.7. OPERACIONES DEL PSC**

Las actividades operativas del PSC se dividen en tres grandes grupos descritos en las próximas secciones de este manual. El primer grupo está dirigido a la atención de comercial propia del PSC, el segundo grupo está dirigido a la atención de las operaciones propias del soporte que hace posible la labor comercial, y el tercer grupo se centra en el cumplimiento de las obligaciones operativas del personal, que deberán estar orientados en el cumplimiento de la presente Declaración de Políticas.

#### **4.7.1 Operaciones Comerciales**

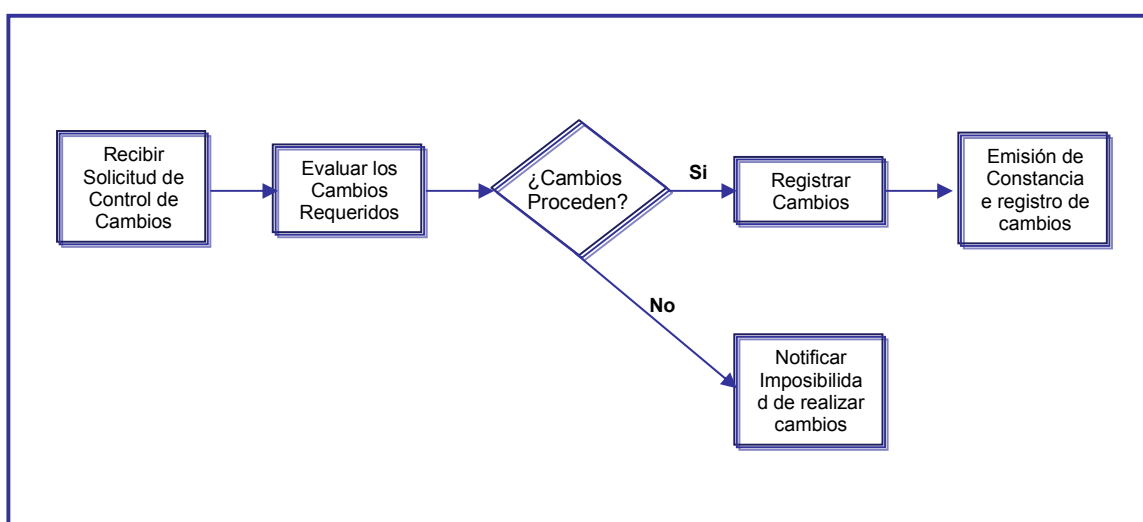
El PSC en su rol de servicio, realizará las operaciones que se vinculen a su modelo comercial. Estas operaciones se dividirán en 2 grandes grupos, según se trate de funciones vinculadas a su rol de AR, AC o AC de tercer nivel (AC3). En el caso de las AC3 se realizarán funciones idénticas a las AR excepto por su posibilidad de crear Certificados Digitales y la obligación de notificar sus creaciones a la AC de orden superior.

#### 4.8. ATENCIÓN A LA GARANTÍA DE CERTIFICADOS DIGITALES Y FIRMAS ELECTRÓNICAS

En atención al artículo 18 del Decreto con rango y fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas, el PSC ofrece el servicio de garantía de Certificados Digitales y Firmas Electrónicas por solicitud de terceros a fin de certificar las Firmas Electrónicas otorgándoles validez legal.

##### 4.8.1. Atención a las Solicitudes de Cambio

Con el fin de garantizar el uso de los Certificados Digitales y Firmas Electrónicas, el PSC requiere que le sean notificados todos los cambios que un propietario de Certificado Digital deba hacer sobre los atributos que componen dicho certificado. La atención a solicitudes de cambios deberá incluir la evaluación de los cambios por parte del PSC, pudiendo otorgarse o negarse la aplicación de los cambios solicitados.



**Figura 4.11** Proceso de Atención de Solicitudes de Cambio



#### **4.8.1.1. De Seguridad y Soporte**

Para el aseguramiento de las operaciones del PSC, se deberán realizar actividades orientadas a la implantación de diversos controles de seguridad que abarcarán el nivel físico de la infraestructura, información, procesos y personal.

#### **4.8.1.2. Acceso Físico**

El acceso a las instalaciones del PSC está restringido sólo al personal autorizado. En el manual de procedimiento de seguridad se encuentra especificado la manera en la que deberá solicitarse y otorgarse el acceso a los sistemas y servicios del PSC.

Han sido establecidos con el fin de reducir el riesgo de accesos no autorizados o de daños a los equipos informáticos. Es importante señalar, que deberán existir revisiones periódicas de la seguridad física del equipamiento a fin de verificar su estado y respectivas fechas de vencimiento.

#### **4.8.1.3. Electricidad y Aire Acondicionado**

El centro de cómputo cuenta con sistemas de aire acondicionado funcionando de manera simultánea y redundante, asegurando la estabilidad de la temperatura en el lugar. Esto contribuye al funcionamiento óptimo y fiable de los equipos que se encuentran dispuestos allí.

#### **4.8.1.4. Respaldos**

Como medida preventiva ante fallas que pongan en riesgo los repositorios, se realizarán operaciones de respaldos periódicos, y estos se almacenarán en un lugar seguro. En este sentido, el PSC manejará la siguiente metodología:

- a) Se realizará respaldos diarios que abarcarán los logs y la información que se encuentre almacenada en la Base de Datos, para ese momento.
- b) Se realizarán respaldos semanales los cuales contendrán tanto la información almacenada como la estructura de la Base de Datos.

De esta manera, los respaldos diarios y semanales en un principio serán dispuestos en el disco duro, y cada dos semanas serán pasados a otros medios de almacenamiento (CD's), para que posteriormente sean colocados en la caja fuerte del PSC, la cual estará ubicada en un lugar ajeno a la sala principal de operaciones.

En este sentido, se resumen las siguientes consideraciones al respecto:

- ✓ Deberán ser almacenados en armarios ignífugos.
- ✓ Solamente personas autorizadas disponen de acceso a los backups.
- ✓ Las copias deberán estar identificadas.
- ✓ Si un material ha contenido backups (disquetes, dvd's...) y se quieren reutilizar nos
- ✓ aseguraremos que los datos que ha contenido hayan sido totalmente borrados haciendo imposible su recuperación.
- ✓ Se autoriza expresamente la extracción de los backups fuera de la Entidad, rellenando una ficha al respecto y anotando el correspondiente detalle en un libro de registro.

#### **4.8.1.5. Auditorias**

A fin de garantizar el correcto desempeño de la relación comercial del PSC con cualquiera de los usuarios del sistema de claves públicas del estado venezolano antes descritos, se realizarán auditorias periódicas sobre cada uno de los actores involucrados, las cuales incluirán:

- ✓ Verificación de los aspectos relacionados con la emisión y gerencia de Certificados Digitales.
- ✓ Controles de los procesos de solicitud, identificación, autenticación, gerencia, publicación, distribución, renovación y revocación de certificados.

Auditoria en cada una de las siguientes áreas:

- a) Políticas de seguridad.

- b) Seguridad física.
- c) Administración de servicios.
- d) Investigación de personal.
- e) DPC utilizadas.
- f) Contratos.

La realización de estas auditorías es de carácter obligatorio y se realizarán de manera interna y externa. Las auditorías internas persiguen garantizar la aprobación de las auditorías externas. Las auditorías externas son medidas de control para el mantenimiento de las certificaciones del PSC y de sus AR y AC3 asociadas. Estas podrán ser realizadas a nivel de documentación, procedimientos y registros de eventos. En este sentido, el PSC, registra y almacena todas las acciones llevadas a cabo que incluyen entre otros, gestión del ciclo de vida de los certificados (solicitud, emisión, revocación, etc.) e intentos de acceso a los sistemas publicación de información en los directorios.

Las auditorías internas en el PSC en cada uno de sus modos operativos serán realizadas trimestralmente (4 por año). Mientras que en las RA asociadas deberán realizarse al menos 2 auditorías por año.

#### **4.9. PROCEDIMIENTO PARA LA EVALUACIÓN DE AUDITORIA AL PSC**

El proceso de auditoría, debe ser efectuada por personal debidamente certificado de alta calificación profesional, a los fines de garantizar que cuentan con el conocimiento, habilidades, destrezas, experiencia, pericia y experticia, traducidas como competencias conductuales, laborales y profesionales, requeridas para el adecuado desempeño de la actividad en concordancia con lo establecido en el Artículo 2 del Reglamento Parcial de la Ley Sobre Mensajes de Datos y Firmas Electrónica, donde, se define a los Auditores como los expertos técnicos inscritos en el Registro de Auditores de SUSCERTE, los cuales son los únicos facultados para emitir los informes de auditoría de conformidad con lo establecido en el artículo 29

del mencionado Reglamento. El auditor es un tercero que puede ser una persona natural o jurídica de carácter unipersonal al cual se le emite una certificación para prestar servicios como auditor a PSC dicha certificación se expedirá por SUSCERTE.

#### ***4.9.1. Evaluación de Auditoría al PSC***

Esta evaluación es un conjunto de procedimientos que deben llevarse a cabo para la evaluación de la Auditoría realizada al Proveedor de Servicios de Certificación, que manifiesta su futura intención de solicitar una Acreditación ante SUSCERTE.

El solicitante entregará entre los recaudos el informe de auditoría que le elaborará un Auditor, previamente seleccionado del Registro de Auditores de SUSCERTE, el cual escogió, entre otros aspectos, conforme a la normativa de independencia del Auditor y de su no vinculación con el Organismo.

A los efectos de lo establecido en el artículo 26 de la LSMDFE, las Auditorías a las que se refiere la mencionada Ley y su Reglamento Parcial, serán realizadas por Auditores debidamente inscritos ante la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).

Los Informes de los Auditores inscritos ante la Superintendencia podrán hacerse valer como parte de los requisitos de Acreditación exigidos ó en cualquier otro caso en que se requiera de conformidad con la RPLSMDFE.

La Superintendencia, así como el personal que actúe bajo su dependencia o terceros por cuenta de ellos y los Auditores Inscritos en el Registro, deberán mantener la confidencialidad de la información y documentos entregados por los PSC, cuando dicha información revista tal carácter en virtud de alguna Norma Legal.

SUSCERTE verificará que el PSC aspirante a ser acreditado, cuente con los elementos técnicos, tecnológicos, de seguridad, que permitan establecer los adecuados controles, a los fines de generar un medio seguro y confiable para la emisión de los certificados.

En el caso que el Proveedor de Servicios de Certificación Electrónica tenga un Plan de Acciones correctivas por ejecutar deberá, corregir los aspectos relativos al mismo, a los fines de ser considerada posteriormente en una revisión para la emisión de un dictamen favorable. Se efectuarán revisiones de seguimiento a fin de determinar el cumplimiento de los aspectos pendientes y se establecerá un plazo para la rectificación de los hallazgos encontrado.

El criterio para aprobar o desaprobar los planes de medidas correctivas presentados por el solicitante con la finalidad de subsanar los requisitos incumplidos, y con el interés de continuar optando por la Acreditación, dependerá de la viabilidad del plan y el tiempo que haya dispuesto para llevarlo a cabo, siendo esta decisión del Auditor.

#### ***4.9.2. Tipos de Auditorias***

El proceso de auditoria es cíclico, que se inicia desde la solicitud de acreditación del PSC y durante toda la auditoria y por el periodo de vigencia de su ejercicio. A tal efecto, se realizarán:

##### **a) Auditoria Inicial**

Será efectuada, a los fines de determinar si el solicitante a PSC se encuentra en condiciones necesarias para que le sea otorgada la acreditación por parte de SUSCERTE.

##### **b) Auditoria Ordinaria**

Es aquella que se realiza el PSC; a los fines de realizar seguimiento a su gestión, mediante la evaluación de los elementos de control establecidos, los elementos de seguridad, los criterios de garantías de calidad y niveles de servicios y los parámetros de confianza, para verificar que estos operan adecuadamente en sus instalaciones y equipos con los que se presta el servicio para el uso de firmas electrónicas y datos certificados. La auditoria ordinaria se realizará semestralmente.

##### **c) Auditoria Extraordinaria**

Es aquella que se realiza de manera eventual y a solicitud de SUSCERTE, a

los fines de dar seguimiento y verificar las condiciones del servicio prestado por el PSC, motivadas por reclamos, quejas o denuncias efectuadas por los signatarios o terceros o decisiones de la gestión de SUSCERTE.

#### **4.9.3. Procedimiento para la Realización de la Auditoría**

Procedimiento es definir la secuencia de acciones y responsabilidades involucradas en el proceso de Auditoría a ser realizada al PSC, a los fines de verificar que se cumplan con todas las políticas, normas, procedimientos, declaración de prácticas de certificación y políticas de certificados para ofrecer un servicio eficaz a sus usuarios.

	<b>ACTOR</b>	<b>ACCIÓN</b>
<b>1</b>	<b>SOLICITANTE PSC</b>	<ol style="list-style-type: none"> <li>1. Ingresa a la página Web de SUSCERTE sección Registro de Auditores.</li> <li>2. Revisa listado de Auditores Registrados y contacta el de su preferencia.</li> </ol>
<b>2</b>	<b>AUDITOR REGISTRADO</b>	<ol style="list-style-type: none"> <li>3. Recibe solicitud por parte del PSC para la realización de la Auditoría.</li> <li>4. Notifica a SUSCERTE la solicitud para la realización de la Auditoría.</li> <li>5. Elabora el Plan de Auditoría.</li> <li>6. Realiza reunión con el PSC: Resume los métodos y procedimientos que van a ser utilizados en la Auditoría y se clarifican los puntos dudosos sobre el Plan de Auditoría a ejecutarse.</li> <li>7. Envía al PSC el Plan de Auditoría, para su aprobación.</li> </ol>
<b>3</b>	<b>SOLICITANTE PSC</b>	<ol style="list-style-type: none"> <li>8. Recibe el Plan de Auditoría y lo aprueba en conformidad.</li> <li>9. Envía al Auditor Plan de Auditoría aprobado.</li> </ol>
<b>4</b>	<b>AUDITOR REGISTRADO</b>	<ol style="list-style-type: none"> <li>10. Recibe el Plan de Auditoría aprobado y envía copia a SUSCERTE.</li> <li>11. Inicia la Auditoría basándose en procesos sistemáticos, independientes, que le permitan verificar: la existencia, el cumplimiento y la eficacia de normas, políticas, planes y procedimientos de seguridad relacionados con Tecnología de Información y Comunicación (TIC), para minimizar los riesgos y determinar el cumplimiento de las garantías de calidad y sus niveles de servicios asociados, siguiendo la lista de chequeo establecida en la Norma SUSCERTE N° 044-11/06.</li> <li>12. Determina y describe las observaciones analíticas realizadas durante el proceso de Auditoría.</li> <li>13. Realiza reunión con el responsable del PSC, informando las evidencias y/o hallazgos encontrados en la auditoría.</li> </ol>

		<p>Encuentran evidencias y/o hallazgos:</p> <p>A. Si se encuentran evidencias y/o hallazgos indica las detecciones y llena el registro de detección de evidencias ó mejora. Espera tiempo solicitado y cierra auditoria.</p> <p>B. Si no se encuentran evidencias y/o hallazgos se procede al cierre de la Auditoria.</p> <p>14. Realiza reunión de cierre: El objetivo de esta reunión es presentar las observaciones de la auditoria y manifestar el comportamiento del desarrollo de la auditoria e informar a los responsables de las áreas auditadas las evidencias y/o hallazgos encontrados.</p> <p>15. Culminado el proceso de auditoria, emite Informe preliminar de auditoria al PSC con los lineamientos establecidos en la Norma SUSCERTE N° 045-11/06, dejando claramente indicado un dictamen sobre la revisión efectuada.</p>
5	<b>SOLICITANTE PSC</b>	<p>16. Recibe el Informe preliminar de Auditoria:</p> <p>A. Si hay evidencias y/o hallazgos elabora plan de acciones correctivas para subsanar las evidencias y/o hallazgos encontrados y envía plan de acciones correctivas al Auditor.</p> <p>B. Si no hay evidencias y/o hallazgos se procede a realizar el cierre de la auditoria.</p>
6	<b>AUDITOR REGISTRADO</b>	<p>17. Hay evidencia y/o hallazgos:</p> <p>A. Si hay evidencias y/o hallazgos recibe plan de acciones correctivas y ejecuta el correctivo.</p> <p>B. Si no hay evidencias y/o hallazgos elabora Informe de Auditoria y entrega dos (2) originales, uno para el Solicitante a PSC y otro para ser consignado ante SUSCERTE. El tiempo para consignar el original del Informe de Auditoria ante SUSCERTE no podrá exceder en cinco (5) días hábiles.</p>

**Tabla N° 4.4** Procedimiento para la realización de la Auditoria

#### 4.9.4. Responsabilidades

##### a. Auditores:

- ✓ Realizar aquellas pruebas sustantivas y de desempeño que le permitan verificar la existencia, el cumplimiento y la eficacia de los procedimientos de control implantados, las normas y procedimientos de seguridad.

- ✓ Revisar las políticas y los manuales del PSC y asegurarse que los mismos son conocidos y aplicados por el personal correspondiente, además de ser conocidos por los signatarios y terceros particularmente en aquellas informaciones que se requieran para garantizar la calidad, los niveles de servicio y el modelo de confianza.
- ✓ Las pruebas deben incluir revisiones de la documentación, utilización de software específico de auditoría, de programas utilitarios adecuados para la revisión, así como inspecciones oculares y entrevistas al personal, además de todo otro procedimiento e información que se juzgue conveniente, las normativas que al respecto establezca ó otra información que determine explícitamente SUSCERTE.

**b. PSC:**

- ✓ Elaborar carta compromiso, en donde se compromete a entregar al auditor toda la información necesaria para efectuar el proceso de auditoría; además de indicar el o los puntos focales de enlace para facilitar el proceso de auditoría, indicando la persona, cargo y ubicación por área de la organización que será revisada.

**4.9.5. Criterios para realizar la auditoría**

- A.** Administración de Certificados y Llaves.
- B.** Seguridad y Ambiente Operacional.
- C.** Calidad, Confianza y Servicios.



<b>Área 1</b>	<b>Administración de Certificaciones y Llaves Electrónicas</b>
<b>Fin:</b>	Comprobar que existan y se cumplan razonablemente las condiciones básicas de control sobre los criterios correspondientes a políticas, normas, procesos y procedimientos de Certificación, Certificados y Llaves Electrónicas que conforman el ambiente organizacional de un PSC.
<b>Criterio 1.1</b>	<b>Contenido del Marco Normativo de Certificación, Certificados y Llaves Electrónicas</b>
<b>Finalidad:</b>	Comprobar que existan y se cumplan razonablemente las condiciones básicas de control sobre los atributos correspondientes a políticas, normas y procedimientos que conforman el ambiente organizacional de un PSC.
	<b>Atributos</b>
<b>1.1.1</b>	<b>Política de Certificación de Firmas Electrónicas (PC)</b> Constar que el PSC cuenta con las estructuras y funciones requeridas para manejar la definición y al ambiente organizacional y de servicios
<b>1.1.2</b>	<b>Manual de Política de Certificado de Firmas Electrónicas (MPC)</b> Verificar que el PSC ha diseñado un Manual de la política de certificados, incluyendo todos los elementos mínimos necesarios, contemplados en el marco legal vigente y los estándares internacionales.
<b>1.1.3</b>	<b>Declaración de Prácticas de Certificación (CPS)</b> Verificar que El PSC ha diseñado y mantiene actualizada la Declaración de Prácticas de Certificación, así como los procesos y procedimientos de operación inherentes para otorgar certificados, en concordancia con el marco legal vigente.
<b>1.1.4</b>	<b>Instrumentos Operacionales para la AC, la AR, y el PSC</b> Verificar que los Instrumentos operacionales de la AC cumplen con los requisitos establecidos en el marco legal vigente en relación con operatividad y confidencialidad, para la prestación de los SCDFE.
<b>1.1.5</b>	<b>Validez de la Política de Certificación de Firmas Electrónicas (PC)</b> Constar que el PSC cuenta correctamente con las estructuras y funciones requeridas para manejar la definición y al ambiente organizacional y de servicios
<b>1.1.6</b>	<b>Validez del Manual de Política de Certificado de Firmas Electrónicas (MPC)</b> Verificar que el PSC ha diseñado correctamente un Manual de la Política de Certificados, incluyendo todos los elementos mínimos necesarios, contemplados en el marco legal vigente y los estándares internacionales.

- 1.1.5 Validez de la Declaración de Prácticas de Certificación (CPS)**  
 Verificar que El PSC correctamente ha diseñado y mantiene actualizada la Declaración de Prácticas de Certificación, así como los procesos y procedimientos de operación inherentes al otorgamiento de certificados, en concordancia con el marco legal vigente.
- 1.1.6 Validez de los Instrumentos Operacionales para la AC, la AR, y el PSC**  
 Verificar que los Instrumentos operacionales de la AC cumplen correctamente con los requisitos establecidos en el marco legal vigente en relación con operatividad y confidencialidad, para la prestación de los SCDFE.
- 1.1.7 Validez de los Planes para la AC, la AR, y el PSC**  
 Verificar que los Instrumentos operacionales de la AC cumplen correctamente con los requisitos establecidos en el marco legal vigente en relación con operatividad y confidencialidad, para la prestación de los SCDFE.

## **Criterio 1.2 Operacionalidad de la Administración de las Claves y Certificados**

**Finalidad:** Comprobar que existan y se cumplan razonablemente las condiciones básicas de control sobre los atributos que conforman la Administración de las Claves criptográficas y de los Certificados que emite el PSC en concordancia con lo establecido en la Ley, sus reglamentos y estándares internacionales, de forma tal que permita mantener un nivel de confianza hacia los signatarios y terceros. Estos atributos o áreas de control general son: a) Ciclo de Vida de las Claves del PSC, b) Administración del Ciclo de Vida de los dispositivos criptográficos y c) Administración del Ciclo de Vida de las Claves de los Signatarios Provistas por los PSC.

### **Atributos**

- 1.2.1 Operacionalidad del Ciclo de vida de las Claves del PSC**  
 Constatar que el PSC mantiene controles básicos que aseguren la razonabilidad sobre la administración del ciclo de vida de las claves, de forma tal de garantizar su nivel de confiabilidad, sustentado en estándares internacionales reconocidos y que están contenidos en la Infraestructura de Claves Públicas de la República Bolivariana de Venezuela (ICPRBV).
- 1.2.2 Operacionalidad de la Administración del Ciclo de Vida de los Dispositivos Criptográficos**  
 Constatar que el PSC posee controles básicos que aseguren razonablemente que el acceso al hardware criptográfico de la Entidad de Certificación se limita al personal autorizado y que el hardware criptográfico funciona adecuadamente.

- 1.2.3 Operacionalidad de la Administración del Ciclo de Vida de las Claves de los Signatarios Provistas por el PSC**
- Constatar que el PSC mantiene controles básicos que aseguren razonablemente que el ciclo de vida de las Claves del signatario provistas por el PSC, se administra de acuerdo con lo establecido en los estándares internacionales adoptados por la Infraestructura de Claves Públicas de la República Bolivariana de Venezuela (ICPRBV).
- 1.2.4 Operacionalidad de la Estructura e Información del Certificado**
- Constatar que la estructura e información del certificado cumpla con los criterios mínimos establecidos por la ley de Mensajes de Datos y Firmas Electrónicas, además de contemplar otros parámetros definidos en los estándares internacionales.
- 1.2.5 Operacionalidad de la Administración del Ciclo de Vida de Dispositivos Externos de Circuitos Integrados**
- Posee controles que proveen razonabilidad sobre una adecuada y segura gestión del ciclo de vida de los dispositivos externos de circuito integrado.
- 1.2.6 Operatividad Activa del Ciclo de vida de las Claves del PSC**
- Constatar que el PSC mantiene controles básicos que aseguren la razonabilidad sobre la administración del ciclo de vida de las claves, de forma tal de garantizar su nivel de confiabilidad, sustentado en estándares internacionales reconocidos y que están contenidos en la Infraestructura de Claves Públicas de la República Bolivariana de Venezuela (ICPRBV).
- 1.2.7 Operatividad Activa de la Administración del Ciclo de Vida de los Dispositivos Criptográficos**
- Constatar que el PSC posee controles básicos que aseguren razonablemente que el acceso al hardware criptográfico de la Entidad de Certificación se limita al personal autorizado y que el hardware criptográfico funciona adecuadamente.
- 1.2.8 Operatividad Activa de la Estructura e Información del Certificado**
- Constatar que la estructura e información del certificado cumpla con los criterios mínimos establecidos por la ley de Mensajes de Datos y Firmas Electrónicas, además de contemplar otros parámetros definidos en los estándares internacionales.
- 1.2.9 Operatividad Activa de la Administración del Ciclo de Vida de Dispositivos Externos de Circuitos Integrados**

Posee controles que proveen razonabilidad sobre una adecuada y segura gestión del ciclo de vida de los dispositivos externos de circuito integrado.

### **Criterio 1.3 Funcionalidad de la Administración de las Claves**

#### **Finalidad:**

Comprobar que existan y se cumplan razonablemente las condiciones básicas de control sobre los atributos que conforman la Administración de las Claves criptográficas en concordancia con lo establecido en la Ley, sus reglamentos y estándares internacionales, de forma tal que permita mantener un nivel de confianza hacia los signatarios y terceros. Estos atributos o áreas de control general son: a) Ciclo de Vida de las Claves del PSC, b) Administración del Ciclo de Vida de los dispositivos criptográficos y c) Administración del Ciclo de Vida de las Claves de los Signatarios Provistas por los PSC.

#### **Atributos**

##### **1.3.1 Funcionalidad del Ciclo de vida de las Claves del PSC**

Constatar que el PSC mantiene controles básicos que aseguren la razonabilidad sobre la administración del ciclo de vida de las claves, de forma tal de garantizar su nivel de confiabilidad, sustentado en estándares internacionales reconocidos y que están contenidos en la Infraestructura de Claves Públicas de la República Bolivariana de Venezuela (ICPRBV).

##### **1.3.2 Funcionalidad de la Administración del Ciclo de Vida de los Dispositivos Criptográficos**

Constatar que el PSC posee controles básicos que aseguren razonablemente que el acceso al hardware criptográfico de la Entidad de Certificación se limita al personal autorizado y que el hardware criptográfico funciona adecuadamente.

##### **1.3.3 Funcionalidad de la Estructura e Información del Certificado**

Constatar que la estructura e información del certificado cumpla con los criterios mínimos establecidos por la ley de Mensajes de Datos y Firmas Electrónicas, además de contemplar otros parámetros definidos en los estándares internacionales.

##### **1.3.4 Funcionalidad de la Administración del Ciclo de Vida de Dispositivos Externos de Circuitos Integrados**

Constatar que el PSC cuenta con las estructuras y funciones requeridas para manejar la definición y al ambiente organizacional y de servicios.

### **Área 2**

#### **Seguridad y control del ambiente operacional.**

<b>Finalidad:</b>	Comprobar que existan y se cumplan razonablemente las condiciones de seguridad y control sobre el ambiente operacional, en cuanto a: Organización de la seguridad, evaluación del riesgo y clasificación de activos, seguridad del personal, seguridad física y ambiental, administración de las operaciones y las comunicaciones, control de acceso a los sistemas, y administración de la continuidad del negocio.
<b>Criterio 2.1</b>	<b>Contenido del marco normativo aplicable a la seguridad y control del ambiente operacional.</b>
<b>Finalidad:</b>	Comprobar que el manual de la seguridad contenga los elementos de seguridad y control aplicables al ambiente operacional del PSC y que se definen en el marco legal vigente y las mejores prácticas internacionales.
<b>Atributos</b>	
2.1.1	<b>Política de Seguridad</b> Constatar que la política de seguridad del ambiente operacional del PSC, contiene los elementos que se establecen en el marco legal vigente y las mejores prácticas internacionales.
2.1.2	<b>Planes específicos de seguridad y control del ambiente operacional</b> Constatar que los planes específicos de: Seguridad de Información, Continuidad del Negocio y Recuperación de Operaciones, Capacidades y Respaldo, Custodia y Resguardo de Información del PSC, contienen los elementos que se establecen en el marco legal vigente y la política de seguridad de la información.
<b>Criterio 2.2</b>	<b>Validez en el contenido del marco normativo aplicable a la seguridad y control del ambiente operacional.</b>
<b>Finalidad:</b>	Comprobar que el manual de la seguridad contenga los elementos de seguridad y control aplicables al ambiente operacional del PSC y que se definen en el marco legal vigente y las mejores prácticas internacionales
<b>Atributos</b>	
2.2.1	<b>Política de Seguridad</b> Constatar que el contenido de la política de seguridad del ambiente operacional del PSC, se ajusta con el marco legal vigente y las mejores prácticas internacionales.
2.2.2	<b>Planes específicos de seguridad y control del ambiente operacional</b> Constatar la validez en el contenido de los planes de Seguridad, de Continuidad del Negocio y Recuperación de Desastres, De Capacidades y de Respaldo, Resguardo y Custodia de Información del PSC, verificando que se ajusten al marco legal vigente y la política de seguridad de la información.

<b>Criterio: 2.3</b>	<b>Evaluación funcional de la seguridad y el control del ambiente operacional del PSC</b>
<b>Finalidad:</b>	Comprobar que existan y se cumplan razonablemente las condiciones básicas de seguridad y control sobre el ambiente operacional, en cuanto a: Organización de la seguridad, evaluación del riesgo y clasificación de activos, seguridad del personal, seguridad física y ambiental, administración de las operaciones y las comunicaciones, control de acceso a los sistemas, y administración de la continuidad del negocio.
<b>Atributos</b>	
2.3.1	<p><b>Organización de la Seguridad</b></p> <p>Constatar que el PSC mantiene una adecuada organización de la política de seguridad de la información requerida para requerida para proveer un adecuado nivel de confianza sobre los servicios que presta a signatarios y terceros.</p>
2.3.2	<p><b>Clasificación y Evaluación de Riesgo de los activos los activos de información</b></p> <p>Constatar que El PSC mantiene una adecuada gestión sobre la clasificación y la evaluación de riesgo de los activos de información, a los fines que se consideren todas las amenazas y vulnerabilidades a los que están expuestos, así como el establecimiento de una adecuada clasificación en función del valor e importancia que tienen los activos de información para el PSC, los signatarios y terceros.</p>
2.3.3	<p><b>Requerimientos de seguridad en la administración de recursos humanos</b></p> <p>Constatar que El PSC posee una adecuada gestión en las prácticas de contratación y administración del personal, de forma tal que respalden y aumenten la confiabilidad de sus operaciones, para minimizar o reducir los riesgos por la ocurrencia de errores humanos o delitos electrónicos.</p>
2.3.4	<p><b>Seguridad Física y Ambiental</b></p> <p>Constatar que se mantiene una adecuada gestión en las prácticas y procedimientos que permitan asegurar razonablemente que el acceso físico a las instalaciones y el equipamiento en tecnología de información comunicaciones, garantiza la operacionalización del servicio de certificación de firmas electrónicas del PSC.</p>
2.3.5	<p><b>Administración de las Operaciones y las comunicaciones</b></p>

Constatar que El PSC administra adecuadamente las prácticas y procedimientos que aseguren razonablemente que: a) Se mantiene un correcto y seguro funcionamiento de sus servicios de procesamiento de información; b) Se minimizan los riesgos de fallas en los sistemas; c) La integridad de los sistemas y datos se encuentra protegidos contra virus y software malicioso; d) Los daños ocasionados por incidentes de seguridad y funcionamiento deficiente son minimizados a través del uso de reportes de incidentes y procedimientos de respuesta, y e) Los medios y soportes son administrados en forma segura para protegerlos de daños, robo y accesos no autorizado.

#### **2.3.6 Administración del control de acceso**

Constatar que El PSC mantiene una adecuada gestión en el control de acceso a los sistemas, de forma tal que se encuentra limitado sólo a personas debidamente autorizadas.

#### **2.3.7 Administración de los registro de eventos del servicio de certificación de firmas electrónicas**

Constatar que el PSC posee una adecuada administración en cuanto a: se registran eventos normales y significativos, tanto manuales como de procesos automatizados del SCFE; se mantiene la confidencialidad e integridad de los registros de eventos actuales e históricos; los registros de eventos se archivan en forma completa y confidencial de acuerdo con las prácticas del negocio, y los registros de eventos son revisados periódicamente por personal autorizado.

#### **2.3.8 Desarrollo y mantenimiento de los sistemas**

Constatar que el PSC mantiene una adecuada gestión en el desarrollo y mantenimientos de sus sistemas de aplicación desde el punto de vistas de incluir en todo el proceso los elementos de seguridad y control necesarios para garantizar la integridad, confidencialidad, disponibilidad, privacidad de la información y sus procesos relacionados que soportaran el servicio de certificación de firmas electrónicas.

#### **2.3.9 Administración de la Continuidad del Negocio**

Constatar que El PSC mantiene adecuados controles que aseguren razonablemente: a) La continuidad de las operaciones en caso de desastre; b) La continuidad de las operaciones en caso de la vulneración de su clave privada, y c) Minimizar potenciales interrupciones en el servicio a los signatarios y terceros, como resultado del cese de sus operaciones.

**Finalidad:** Constatar que El PSC cuenta con todos los elementos mínimos necesarios y maneja apropiadamente el área de calidad, confianza y servicios.

**Criterio 3.1 Contenido del Marco Normativo de Calidad, Confianza y Servicios**

**Finalidad:** Constatar que El PSC cuenta con una política que regule los mecanismos relativos a los elementos de calidad, servicios, confianza, y como mecanismos asociado a la los servicios y la confianza, lo relativo al registro de acceso público.

**Atributos**

**3.1.1 Contenido de la Política de Calidad, Confianza y Servicios**

Constatar que la política de calidad, confianza y servicios del PSC contiene los elementos mínimos relativos al registro y acceso público requerido por los signatarios; así como con los mecanismos, instrumentos y sistemas apropiados para la custodia y resguardo de la información que cumpla con lo establecido en el marco legal vigente.

**3.1.2 Contenido Modelo de Garantías de Calidad y Niveles de Servicios**

Constatar que la política de calidad, confianza y servicios del PSC contiene los elementos mínimos relativos al registro y acceso público requerido por los signatarios; así como con los mecanismos, instrumentos y sistemas apropiados para la custodia y resguardo de la información que cumpla con lo establecido en el marco legal vigente.

**3.1.3 Contenido del Modelo de Confianza**

Constatar que la política de calidad, confianza y servicios del PSC contiene los elementos mínimos relativos al Modelo de Confianza y Servicios.

**Criterio 3.2 Validez del Contenido del Marco Normativo de Calidad, Confianza y Servicios**

**Finalidad:** Constatar que la política de calidad, confianza y servicios del PSC cuenta con un contenido correcto, que se ajuste a las disposiciones legales vigentes, mejores prácticas, lineamiento, normativas, en lo relativo a la política que regule los mecanismos relativos a los elementos de calidad, servicios, confianza, y como mecanismos asociado a la los servicios y la confianza, lo relativo al registro de acceso público.

**Atributos**

**3.2.1 Validez del Contenido de la Política de Calidad, Confianza y Servicios**



Constar que la política de calidad, confianza y servicios del PSC cuenta con un contenido del manual que es correcto y se ajusta a las disposiciones legales vigentes, mejores, prácticas, estándares, lineamientos y normativas, en lo relativo a los elementos mínimos relativos al registro y acceso público requerido por los signatarios; así como con los mecanismos, instrumentos y sistemas apropiados para la custodia y resguardo de la información que cumpla con lo establecido en el marco legal vigente.

### 3.2.2 **Validez del Contenido Modelo de Garantías de Calidad y Niveles de Servicios**

Constar que la política de calidad, confianza y servicios del PSC cuenta un contenido del manual que es correcto y se ajusta a las disposiciones legales vigentes, mejores, prácticas, estándares, lineamientos y normativas, en lo relativo a los elementos mínimos relativos al registro y acceso público requerido por los signatarios; así como con los mecanismos, instrumentos y sistemas apropiados para la custodia y resguardo de la información que cumpla con lo establecido en el marco legal vigente.

### 3.2.3 **Validez del Contenido del Modelo de Confianza**

Constar que la política de calidad, confianza y servicios del PSC contiene los elementos mínimos relativos al Modelo de Confianza y Servicios.

## **Criterio 3.3 Elementos Operativos de Calidad, Confianza y Servicios**

**Finalidad:** Constar que El PSC cuenta con los elementos operativos para manejar el modelo de calidad, confianza y servicios.

### **Atributos**

#### 3.3.1 **Elementos Operativos del Registro de Acceso Público como Mecanismo para la Confianza**

Constar que el PSC cuenta con los mecanismos operativos mínimos para el registro y acceso público requerido por los signatarios; para la custodia y resguardo de la información que cumpla con lo establecido en el marco legal vigente.

#### 3.3.2 **Elementos Operativos del Sistema de Garantías de Calidad y Niveles de Servicios como elementos de Soporte a la Confianza**

Constar que el PSC cuenta con los elementos operativos mínimos necesarios para el sistema de garantías de calidad y niveles de servicio.

#### 3.3.3 **Elementos Operativos del Modelo de Confianza**

Constar que el PSC cuenta con los elementos operativos mínimos necesarios para el sistema de garantías de calidad y niveles de servicio.

#### 3.3.4 **Elementos Operativos del Riesgo de Reputación como Elemento Fundamental de la Confianza**

	<p>Constar que el PSC cuenta con los elementos operativos mínimos necesarios para el sistema de garantías de calidad y niveles de servicio.</p>
<b>3.3.5</b>	<p><b>Operatividad del Registro de Acceso Público como Mecanismo para la Confianza</b></p> <p>Constar que el PSC cuenta tiene operativos los elementos de registro y acceso público requerido por los signatarios; para la custodia y resguardo de la información que cumpla con lo establecido en el marco legal vigente.</p>
<b>3.3.6</b>	<p><b>Elementos Operativos del Sistema de Garantías de Calidad y Niveles de Servicios como elementos de Soporte a la Confianza</b></p> <p>Constar que el PSC cuenta con los elementos operativos mínimos necesarios para el sistema de garantías de calidad y niveles de servicio.</p>
<b>3.3.7</b>	<p><b>Elementos Operativos del Modelo de Confianza</b></p> <p>Constar que el PSC cuenta con los elementos operativos mínimos necesarios para el sistema de garantías de calidad y niveles de servicio.</p>
<b>3.3.8</b>	<p><b>Elementos Operativos del Riesgo de Reputación como Elemento Fundamental de la Confianza</b></p> <p>Constar que el PSC cuenta con los elementos operativos mínimos necesarios para el sistema de garantías de calidad y niveles de servicio.</p>
<b>Criterio 3.4</b>	<p><b>Funcionalidad de los Elementos de Calidad, Confianza y Servicios</b></p>
<b>Finalidad:</b>	<p>Constar que El PSC cuenta con los elementos funcionales para manejar el modelo de calidad, confianza y servicios.</p>
<b>Atributo</b>	
<b>3.4.1</b>	<p><b>Funcionalidad del Registro de Acceso Público como Mecanismo para la Confianza</b></p> <p>Constar que el PSC mantiene en forma funcional los elementos de registro y acceso público requerido por los signatarios; para la custodia y resguardo de la información que cumpla con lo establecido en el marco legal vigente.</p>
<b>3.4.2</b>	<p><b>Funcionalidad del Sistema de Garantías de Calidad y Niveles de Servicios como elementos de Soporte a la Confianza.</b></p> <p>Constar que el PSC cuenta con los elementos operativos mínimos necesarios para el sistema de garantías de calidad y niveles de servicio.</p>
<b>3.4.3</b>	<p><b>Modelo de Confianza y Servicios</b></p> <p>Constar que el PSC mantiene funcionalmente los elementos que manejan apropiadamente las condiciones técnicas y de servicio que otorgan confianza al signatario desde el punto de vista del manejo del SCDPE, así como desde la perspectiva del servicio recibido por parte de los signatarios y terceros.</p>
<b>3.4.4</b>	<p><b>Riesgo de Reputación como Elemento de la Confianza</b></p>

Constatar que el PSC mantiene funcionalmente los elementos que manejan apropiadamente la reputación del servicio que otorguen confianza al signatario desde el punto de vista del manejo del SCDFE, así como desde la perspectiva del servicio recibido; a través de sus clientes eficaces (los que disponen y Utilizan los medios de detección, notificación y publicación), o terceros.

**Tabla N° 4.5** Clasificación de criterios por áreas a ser evaluados a los Solicitante a PSC

## CONCLUSIONES

El impacto de las nuevas tecnologías, genera la posibilidad de que las comunicaciones internas de las organizaciones se extiendan. De esta manera contando así con una plataforma tecnológica común para todos los usuarios finales y disponiendo de un medio de comunicación ampliamente distribuido, y de accesos flexibles, se debe incorporar la Infraestructura de Clave Pública (ICP).

Una vez que se empezó a desarrollar el trabajo se hizo necesario una metodología con la cuál guiarse. Debido a que el tema ICP es tan reciente, que no existe metodología modelo de diseño y desarrollo que estén claramente definidas, las cuales describan una secuencia lógica de los procesos que involucren la incorporación de la ICP a los Proveedores de Servicios de Certificación (PSC).

Como el presente trabajo esta dirigido a establecer un marco de referencia por el cuál guiarse en la incorporación de ICP en los PSC, se desarrolló una metodología dirigida no solamente como guía a seguir durante el desarrollo del trabajo, sino también se creó la más completa posible que establezca y describa los pasos a seguir para el PSC a la hora de diseñar e implementar la Infraestructura, y que de por si fuese un importante producto resultante.

El uso de las Infraestructuras de Clave Pública es una condición previa para el funcionamiento de los servicios integrados. Mientras no se establezcan soluciones concretas de la identificación a seguir para incorporar dicha infraestructura, está claro que no se podrán realizar mejoras significativas, seguras y asequibles en la prestación de sus servicios.

Sin integración o colaboración no se podrá desplegar el verdadero potencial de los servicios en cuanto al proceso de acreditación, sin embargo, la integración intensifica la necesidad de que la identificación en los procesos sea muy segura para todos los actores involucrados.

Para finalizar, podemos concluir que esta investigación resalta la importancia que tiene para la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) la realización e implementación de esta propuesta, ya que facilita las herramientas necesarias para el fin deseado, dando respuesta a todos los solicitante a PSC, con la finalidad de aclarar las dudas que puedan surgir en el cumplimiento de los requisitos solicitados por el ente regulador, centralizando y unificando todo los alcances, responsabilidades, obligaciones y elementos que deben componer la ICP, describiendo así los procesos Legales, Económicos – Financieros, Técnicos y de Auditoria.

## RECOMENDACIONES

1. Se recomienda a SUSCERTE supervisar a los Solicitantes a Proveedores de Servicios de Certificación en la aplicación correcta de la Metodología Modelo propuesta.
2. Se recomienda a SUSCERTE evaluar anualmente el resultado de la aplicación de la Metodología Modelo y mantenerla actualizada.
3. La Metodología Modelo propuesta determina las reglas y pasos que deben seguir los Solicitantes a Proveedores de Servicios de Certificación a la hora de cumplir con los requisitos para incorporar una ICP.
4. Se recomienda a SUSCERTE difundir y publicar en su página Web [www.suscerte.gob.ve](http://www.suscerte.gob.ve) la Metodología Modelo propuesto, para así dar a conocer abiertamente los lineamientos y pasos que se debe seguir para incorporar una ICP en los Proveedores de Servicios de Certificación.
5. Considerar las recomendaciones 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.
6. Capacitar al personal técnico en el uso de esta nueva tecnología para darle mantenimiento y continuidad a la ICP de la organización y asistencia a los futuros Proveedores de Servicios de Certificación.
7. 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.
8. Continuar con la divulgación de las ventajas y beneficios proporcionados al incorporar en las aplicaciones la firma electrónica y los certificados electrónicos.

9. Mantener en SUSCERTE los conocimientos constantes acerca de las nuevas tecnologías que brindan seguridad de la Información en las transacciones electrónicas a nivel Internacional.
10. Continuar con las mesas de trabajos con otros países para establecer alianzas para aplicar la certificación electrónica, a través del uso de las tecnologías que garantice la autenticidad, confiabilidad, integridad y la aceptación del mismo.

## LISTA DE REFERENCIAS

- Ley de Mensaje de Datos y Firmas Electrónicas, Decreto con Fuerza de Ley N° 1.204 de fecha 10 de Febrero de 2001, publicado en Gaceta Oficial N° 37.148 de fecha 28.02.2001.
- Reglamento Parcial del Decreto Ley Sobre Mensaje de Datos y Firmas Electrónicas de fecha 12 de Diciembre de 2004, publicado en Gaceta Oficial N° 38.086.
- Constitución de la República Bolivariana de Venezuela extraordinario del viernes de Marzo de 2000, publicada en Gaceta Oficial N° 5.453.
- Ley Especial Contra Delitos Informáticos del 30 de Octubre de 2001, publicada en Gaceta Oficial N° 37.313.
- British Standard. Information technology - Code of practice for information security management. Technical Report BS ISO/IEC 17799:2000, British Standard Publishing Limited, December 2000
- Méndez, C. (2001). Metodología Diseño y Desarrollo del Proceso de Investigación. Colombia: Editorial Mc Graw Hill.
- Falcón, Marifrancly. (2005). “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. Trabajo de grado, Ingeniería Informática, Universidad Alejandro de Humboldt.
- Ramírez, T. (1992). Como Hacer un Proyecto de Investigación. Caracas: Editorial Panapo.
- VV.AA. (2004). PKI Infraestructura de Claves Públicas. Colombia. Editorial MCGRAW-HILL / Interamericana de Colombia..



- ISO/IEC 17799:2000 Information Technology - Code for information security management.
- Kaliski, B. and Staddon, J.. PKCS #1: RSA Cryptography Specifications. Internet drafts, Internet Engineering Task Force, Sept 1998. Versión 2.0.
- Liendo, María del Carmen. (2006). “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”.
- National Institute of Standards and Technology (NIST). *FIPS 186-2 Digital Signature Standard*, federal information processing standards publication edition, 1999.
- Holmes D. (2001). Estrategias de negocio electrónico para el gobierno. E-gobierno.

## FUENTES ELECTRÓNICAS

- <http://www.suscerte.gob.ve>[Página en Línea]. [Consulta: 2004, Junio 08].
- [http://www.htmlweb.net/seguridad/cripto/cripto\\_3.html](http://www.htmlweb.net/seguridad/cripto/cripto_3.html) [Documento en Línea]. [Consulta: 2005, Enero].
- [http://www.htmlweb.net/seguridad/cripto/cripto\\_5.html](http://www.htmlweb.net/seguridad/cripto/cripto_5.html) [Documento en Línea]. [Consulta: 2006, Agosto].
- <http://www.eurollogic.es/soluciones/que-es-pki.html>[Documento en Línea]. [Consulta: 2004, Agosto].
- <http://www.enterate.unam.mx/articulos/dos/septiembre/firmas.html> [Documento en Línea]. [Consulta: 2004, Septiembre].
- <http://www.unav.es/cti/ca/cadocs.html> [Documento en Línea] [Consulta: 2004, Noviembre].

- [http://www.eurologic.es/soluciones/que\\_es\\_pki.htm](http://www.eurologic.es/soluciones/que_es_pki.htm) [Documento en Línea] [Consulta: 2004, Noviembre].
- <http://www.pki.gva.es> [Documento en Línea] [Consulta: 2004, Diciembre].
- <http://www.greenfacts.org/es/glosario/mno/modelo.html> [Documento en Línea] [Consulta: 2004, Diciembre].
- : Disponible en <http://www.certcamara.com> Certicamara.
- Cámara de Comercio de Chile. Disponible en: : <http://www.e-certchile.cl/>
- Cámara de Argentina de Comercio. Disponible en: <http://www.e-certchile.cl/http://www.cace.org.ar/Content.aspx?Id=1891>
- CERES (Autoridad Pública de Certificación Electrónica). Disponible en: <http://www.cert.fnmt.es>
- FNMT (Fábrica Nacional de Moneda y Timbre). Disponible en: <http://www.fnmt.es>
- Firma Digital República de Argentina. Disponible en: <http://www.pki.gov.ar/index.php?option=content&task=view&id=54&Itemid=55>
- XCA. Disponible es: <http://www.hohnstaedt.de/xca.html>
- OPENCA. Disponible en: <http://www.openca.org>
- Openssl. Disponible en: <http://www.openssl.org/>
- PKCS (*Public Key Cryptography Standards*) Disponible en: <http://dat.etsit.upm.es/~mmonjas/cripto/16.html#1>
- Moline, G. (2006). Modelo funcional del PSC del Estado Nacional. Disponible en: <http://pki.fii.org>

## **ANEXOS**

## ANEXO A. 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:

1. **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).
2. **PKCS#2** y **PKCS#4** han sido incorporadas a PKCS#1.
3. **PKCS#3** (*Diffie-Hellman Key-Agreement Standard*) describe un método para implementar el intercambio de claves Diffie-Hellman.

4. **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.
  
5. **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.
  
6. **PKCS#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.
  
7. **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.
  
8. **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.

9. **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.
  
10. **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.
  
11. **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.
  
12. **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.
  
13. **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 B. 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 N° 37.148 de fecha 28 de febrero de 2001

**Decreto N° 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 a 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:

- 1 Que la información que contengan pueda ser consultada posteriormente.
- 2 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 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:

- El propio Emisor.
- Persona autorizada para actuar en nombre del Emisor respecto de ese mensaje.
- 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:

1. Toda comunicación del Destinatario, automatizada o no, que señale la recepción del Mensaje de Datos.
2. 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:

- Garantizar que los datos utilizados para su generación puedan producirse sólo una vez, y asegurar, razonablemente, su confidencialidad.
- Ofrecer seguridad suficiente de que no pueda ser falsificada con la tecnología existente en cada momento.
- 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 crítica.**

**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:

- 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.
- Revocar o suspender la acreditación otorgada cuando se incumplan las condiciones, requisitos y obligaciones que se establecen en el presente Decreto-Ley.
- Mantener, procesar, clasificar, resguardar y custodiar el Registro de los Proveedores de Servicios de Certificación públicos o privados.
- Verificar que los Proveedores de Servicios de Certificación cumplan con los requisitos contenidos en el presente Decreto-Ley y sus reglamentos.
- 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.
- Liquidar, recaudar y administrar las tasas establecidas en el artículo 24 de este Decreto-Ley.
- Liquidar y recaudar las multas establecidas en el presente Decreto-Ley.
- Administrar los recursos que se le asignen y los que obtenga en el desempeño de sus funciones.
- Coordinar con los organismos nacionales o internacionales cualquier aspecto relacionado con el objeto de este Decreto-Ley.
- Inspeccionar y fiscalizar la instalación, operación y prestación de servicios realizados por los Proveedores de Servicios de Certificación.
- Abrir, de oficio o a instancia de parte, sustanciar y decidir los procedimientos administrativos relativos a presuntas infracciones a este Decreto-Ley.

- 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.
- 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.
- Seleccionar los expertos técnicos o legales que considere necesarios para facilitar el ejercicio de sus funciones.
- Presentar un informe anual sobre su gestión al Ministerio de adscripción.
- Tomar las medidas preventivas o correctivas que considere necesarias conforme a lo previsto en este Decreto-Ley.
- Imponer las sanciones establecidas en este Decreto-Ley.
- Determinar la forma y alcance de los requisitos establecidos en los artículos 31 y 32 del presente Decreto-Ley.
- 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:

1. Los recursos que le sean asignados en la Ley de Presupuesto a través del Ministerio de Ciencia y Tecnología.
2. Los provenientes de su gestión conforme a lo establecido en esta Ley.
3. Cualquier otro ingreso permitido por ley.

#### **De las tasas.**

**Artículo 24.-** La Superintendencia de Servicios de Certificación Electrónica cobrará las siguientes tasas:

- 4.3.1** Por la acreditación de los Proveedores de Servicios de Certificación se cobrará una tasa de un mil unidades tributarias (1.000 U.T.).
- 4.4.1** Por la renovación de la acreditación de los Proveedores de Servicios de Certificación se cobrará una tasa de quinientas unidades tributarias (500 U.T.).

**4.5.1** Por la cancelación de la acreditación de los Proveedores de Servicios de Certificación se cobrará una tasa de quinientas unidades tributarias (500 U.T.).

**4.6.1** 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:

1. Ser venezolano.
2. 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:

- Ser expedidas por una entidad aseguradora o bancaria autorizada para operar en el país, conforme a las disposiciones que rigen la materia.
- 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 página 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:

- No haber tenido la intención de causar el hecho imputado de tanta gravedad.
- 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 C. 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 Artículo 87 de la Ley Orgánica de la administración Pública

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.

**Audidores:** 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:

1. Identificación completa del solicitante.
2. Información económica y financiera con la cual se demuestre la capacidad suficiente para prestar servicios como Proveedor de Servicios de Certificación.
3. Copia de los contratos correspondientes a aquellos servicios que sean prestados por terceros en caso de haberlos.
4. Proyecto de contrato a ser suscrito con los Signatarios.
5. Políticas de Certificados y Declaración de Prácticas de Certificación.
6. Estados financieros auditados y declaraciones del impuesto sobre la renta de los dos últimos ejercicios fiscales.
7. 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.

8. 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 Auditoría**

**Artículo 5:** El informe de auditoría deberá contener al menos:

- Nombre e identificación de los auditores.
- Fecha de inicio y terminación de la auditoría.
- 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.
- Manifestación del cumplimiento de los estándares indicados en el Capítulo VII de este reglamento.
- 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 artículo 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:

2. 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.
3. 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.
4. Cumplir cabalmente con las Políticas de Certificados y la Declaración de Prácticas de Certificación vigente.
5. Informar en la forma establecida en el numeral 4° del artículo 31 y 6° 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.
6. 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.
7. Garantizar de manera fácil y permanente el acceso de los Signatarios y terceros al repositorio.
8. Informar a la Superintendencia de Servicios de Certificación Electrónica de manera inmediata la ocurrencia de cualquier evento que comprometa la prestación del servicio.
9. 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.
10. Mantener actualizado el registro de los Certificados Electrónicos revocados.



11. Informar al signatario dentro de las 24 horas siguientes de la suspensión o revocatoria de su Certificado Electrónico.
12. 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:

1. 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.
2. 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.
3. 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 párrafo 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 SERVICIOS 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**

**Artículo 31:** 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 32:** 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 33:** 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 34:** 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 35:** 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 36:** 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 37:** 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:

- Políticas y procedimientos de seguridad de las instalaciones físicas y los equipos.

- Políticas de acceso a los sistemas e instalaciones del proveedor y monitoreo constante de los mismos.
- Planes y procedimientos de actualización de hardware y software, utilizados para la operación de Proveedores de Servicios de Certificación.
- 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.
- Plan de manejo, control y prevención de virus informático.

### **Cumplimiento de los Requisitos Técnicos**

**Artículo 38:** 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 39:** 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 40:** 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 41:** Cualquiera de los requisitos establecidos en este reglamento deberán presentarse en idioma castellano o traducido al castellano por intérprete público.

**Artículo 42:** La Superintendencia de Servicios de Certificación Electrónica será el órgano encargado de la ejecución del presente Decreto.

**Artículo 43:** 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 193° de la Independencia y 144° 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 D. Entidades Reguladoras en Firmas y Certificados Digitales en el Mundo**

	<b>País</b>	<b>Entidad Reguladora</b>
	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
	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 d'Information
	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 E. 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 Advancement 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.

**AUTENTICACIÓN SIMPLE:** Procedimiento para autenticar a una entidad haciendo uso de una clave.

**AUTENTICACIÓN FUERTE:** Autenticación 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 **Massachusetts Institute of Technology**), 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 autenticar 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 F. Conceptos Definidos por Suscerte en sus Normas 017, 018, 019, 020, 021, 023, 024 Y 025**

<b>ACREDITACIÓN</b>	Es el título que otorga la Superintendencia de servicios de Certificación Electrónica a los Proveedores de Servicios de Certificación para proporcionar Certificados Digitales, una vez cumplidos los requisitos y condiciones establecidos en el Decreto-Ley 1.204.
<b>ACREDITACIÓN RENOVADA</b>	Resolución emitida por la SUSCERTE, que informa al PSC que el periodo de validez de su Acreditación ha sido renovado, por lo que está autorizado para actuar como Proveedor de Servicios de Certificación (PSC) durante el lapso de vigencia.
<b>ACREDITACIÓN SUSPENDIDA</b>	Resolución emitida por la SUSCERTE, que informa al PSC que su Acreditación ha sido suspendida temporalmente y, a partir de ese momento, no puede actuar como Proveedor de Servicios de Certificación hasta tanto no cesen las causales de la suspensión.
<b>AUTORIDAD DE CERTIFICACIÓN</b>	Entidad, dentro del PSC, responsable de la emisión de los certificados.
<b>AUTORIDAD DE REGISTRO</b>	Entidad, dentro del PSC, responsable del registro de los Suscritores, y registro y control de los certificados.
<b>CERTIFICADO RAÍZ</b>	Certificado emitido por la Autoridad de Certificación para si misma. En este certificado consta la clave pública de la Autoridad de Certificación y por tanto será necesario para comprobar la autenticidad de cualquier certificado emitido por ella. Es el origen de la cadena de confianza.
<b>CERTIFICADO DE ACREDITACIÓN</b>	Instrumento que otorga la SUSCERTE, tanto como Providencia Administrativa como en forma electrónica, a los Proveedores de Servicios de Certificación Electrónica (PSC) los cuales le permiten prestar el servicio de emisión de Certificados Digitales.

<b>CERTIFICADO DE FIRMA ELECTRÓNICA</b>	Instrumento electrónico que autentica el vínculo entre el firmante o titular del Certificado Electrónico y la Firma Electrónica.
<b>CLAVE PÚBLICA</b>	Una de las dos claves usadas para el cifrado y firmado de mensajes de datos. Es publicada, como parte de un certificado, para que la conozcan todos aquellos que quieran comunicarse de modo seguro con el propietario de la clave privada.
<b>CÓDIGO DEL PSC</b>	Un código de identificación único del Título de Acreditación dado a un Proveedor de Servicios de Certificación el cual queda registrado en el Sistema de Acreditación de la SUSCERTE. Este código permite reconocer a los solicitantes acreditados.
<b>CREDCENCIAL</b>	Número de asignado por la SUSCERTE al solicitante, para poder tramitar la Solicitud de Acreditación.
<b>DESTINATARIO</b>	Persona a quien va dirigido el Mensaje de Datos enviado por medios electrónicos por el signatario de la Firma Electrónica.
<b>DIRECCIÓN DE CORREO ELECTRÓNICO</b>	Dirección basada en dominios o en UUCP con que se identifica un usuario de Internet. Para las comunicaciones ente la SUSCERTE y los solicitantes y PSCs, esta dirección tendrá un vínculo para establecer el domicilio electrónico. Para los solicitantes, el domicilio electrónico se conectará por medio del número que tendrá el certificado que proporciona la SUSCERTE para iniciar el proceso y para los PSCs el contacto será con el código del título de Acreditación.
<b>DOMICILIO ELECTRÓNICO</b>	Será el medio electrónico de comunicación con la SUSCERTE. Para los solicitantes, el domicilio será dado por el número asignado a la Solicitud de Acreditación el cual se vinculará al correo electrónico o a un Sistema de Información programado por el solicitante, mientras que para el Proveedor de Servicios de Certificación, se utilizará el código dado al Certificado de Acreditación.

<b>DOMICILIO FÍSICO</b>	Lugar de dirección suministrado por el Solicitante o PSC, donde funcionará la infraestructura física y de servicios necesaria para la emisión de los Certificados Digitales.
<b>EMISOR</b>	Persona que origina un Mensaje de Datos por sí mismo, o a través de terceros autorizados.
<b>EVALUACIÓN AL SOLICITANTE</b>	Evaluación pormenorizada de los aspectos técnicos, legales, económicos-financieros y tecnológicos del solicitante realizada por las unidades internas de la SUSCERTE, de acuerdo a su área de competencia.
<b>FIRMA ELECTRÓNICA</b>	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 y de acuerdo a lo establecido en el decreto con fuerza de Ley 1.204.
<b>FUNCIONES HASH</b>	Funciones matemática que realizan un resumen del documento a firmar, transformando un texto de longitud variable en uno de longitud fija, son irreversibles, es decir, que a partir de un bloque comprimido no se puede obtener el bloque sin comprimir y son de dominio público.
<b>INSPECCIÓN EXTRAORDINARIA</b>	Visita específica, no programada, que realizará la SUSCERTE a las instalaciones del PSC, con la finalidad de evaluar el desarrollo de sus actividades motivada por oficio o denuncia.
<b>INSPECCIÓN ORDINARIA</b>	Visita anual que realizará el personal propio o designado por la SUSCERTE al domicilio físico del PSC para evaluar el desarrollo de sus actividades de manera programada.

<b>LEY 1.204 SOBRE MENSAJE DE DATOS Y FIRMAS ELECTRONICAS</b>	Decreto con fuerza de Ley, de fecha 10 de febrero de 2001, publicado en Gaceta Oficial de la República Bolivariana de Venezuela N° 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 Digitales.
<b>LEY 1.204 SOBRE MENSAJE DE DATOS Y FORMAS ELECTRONICAS</b>	Decreto con fuerza de Ley, de fecha 10 de febrero de 2001, publicado en Gaceta Oficial de la República Bolivariana de Venezuela N° 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 Digitales.
<b>LEY SOBRE MENSAJES DE DATOS Y FIRMAS ELECTRÓNICAS</b>	Decreto con fuerza de Ley, de fecha 10 de febrero de 2001, publicado en Gaceta Oficial de la República Bolivariana de Venezuela N° 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 Digitales.
<b>MENSAJES DE DATOS</b>	Toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio.
<b>NÚMERO DE CERTIFICADO</b>	Número asignado al Solicitante cuando es acreditado y se le hace entrega del Certificado

<b>PLAN DE MEJORAS</b>	Proyecto y cronograma requerido por la SUSCERTE al solicitante en referencia a las debilidades técnicas detectadas durante el proceso de evaluación, que involucran medidas correctivas para subsanar las deficiencias encontradas y poder así continuar con el proceso de Acreditación.
<b>PROCEDIMIENTO DE ACREDITACIÓN</b>	Forma de actuación de la SUSCERTE, para la valoración a realizar a una persona jurídica interesada en prestar servicios de certificación de firmas electrónicas, utilizando para ello criterios y estándares previamente establecidos y expuestos en las Normas SUSCERTE, a las cuales se ceñirán los PSC para garantizar la seguridad en su uso.
<b>PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN</b>	Persona dedicada a proporcionar Certificados Digitales y demás actividades previstas en la Ley 1.204.
<b>PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA (PSC)</b>	Persona jurídica prestadora de servicios de certificación de firmas electrónicas, dedicada a proporcionar Certificados Digitales y demás actividades previstas en la Ley 1.204.
<b>REGISTRO DE LA SUSCERTE</b>	Base de datos diseñada y mantenida por la SUSCERTE para llevar a cabo la Acreditación, supervisión y control de los Proveedores de Servicios de Certificación Electrónica.
<b>REGLAMENTO PARCIAL DEL DECRETO- LEY 1.204</b>	Decreto N° 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 la SUSCERTE, la creación del Registro de Auditores, así como los estándares, planes y procedimientos de seguridad.
<b>SIGNATARIO</b>	Persona titular de una Firma Electrónica la cual se encuentra ampara por un Certificado Electrónico emitido por un PSC.

<b>SOLICITANTE</b>	Persona (Natural o Jurídica) que llenó y remitió a la SUSCERTE la Solicitud de Acreditación con todos los recaudos necesarios para optar a ser PSC.
<b>SOLICITUD DE ACREDITACIÓN</b>	Petición dirigida a la SUSCERTE y que tiene por objeto obtener la Acreditación para proporcionar Certificados Digitales y demás actividades previstas en el Decreto-Ley 1.204.
<b>SOLICITUD DE ACREDITACIÓN ADMITIDA</b>	Calificación que se da a aquella Solicitud que ha sido aceptada para su evaluación, por cumplir con todos los extremos exigidos por el Decreto-Ley 1.204 y su Reglamento Parcial.
<b>SOLICITUD DE ACREDITACIÓN DESISTIDA</b>	Calificación que se da a aquella Solicitud en la que el solicitante manifestó su voluntad de desistir del procedimiento de Acreditación, aunque la SUSCERTE le otorgara tiempo para que fuera corregida o subsanado el incumplimiento detectado.
<b>SOLICITUD DE ACREDITACIÓN DIMITIDA</b>	Calificación que se da a aquella Solicitud que no ha sido admitida por no haber cumplido con todos los recaudos exigidos, pese a que se le informó al solicitante y se le dio el plazo para subsanar, pero éste no lo hizo en el tiempo establecido a tal efecto, ni manifestó su voluntad de continuar con el procedimiento de Acreditación.
<b>SOLICITUD DE ACREDITACIÓN OBJETADA</b>	Calificación que se da a aquella Solicitud que debe ser subsanada o corregida por el solicitante, conforme a las indicaciones de la SUSCERTE, para que luego sea admitida.
<b>SOLICITUD DE ACREDITACIÓN APROBADA</b>	Calificación que se da a aquella Solicitud que ha sido evaluada y que cumple con todos los requisitos exigidos por el Decreto-Ley 1.204 y que, por lo tanto, le da derecho a la Acreditación.
<b>SOLICITUD DE ACREDITACIÓN RECHAZADA</b>	Calificación que se da a aquella Solicitud que ha sido evaluada y no ha cumplido con los requisitos exigidos por el Decreto-Ley 1.204 y su Reglamento.

- SUPERINTENDENCIA DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA** Servicio Autónomo, adscrito al Ministerio de Ciencia y Tecnología, que tiene por objeto 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, a los Auditores Registrados para la evaluación de los PSC y a los signatarios de firmas electrónicas.
- 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.

**ANEXO G. Identificación de Acrónimos que Considera lo Expuesto en las Normas 017, 018, 019, 020, 021,023, 024 y 025 Emitidas por Suscerte.**

<b>AC</b>	Autoridad de Certificación
<b>AL</b>	Asesoría Legal
<b>AR</b>	Autoridad de Registro
<b>CRL</b>	Lista de Certificados Revocados
<b>DIF</b>	Dirección de Inspección y Fiscalización de la SUSCERTE
<b>DPC</b>	Declaración de Prácticas y Políticas de Certificación
<b>DRA</b>	Dirección de Registro y Acreditación
<b>LOAP</b>	Ley Orgánica de Administración Pública
<b>LOPA</b>	Ley Orgánica de Procedimientos Administrativos
<b>LSMDFE</b>	Iniciales que identifican el Decreto con fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas (1.204).
<b>OGA</b>	Oficina de Gestión Administrativa.
<b>PSC</b>	Siglas para identificar a los Proveedores de Servicios de Acreditación como las personas prestadoras de servicios de certificación de firmas, que proporcionan los Certificados Digitales correspondientes.
<b>PSC-FII</b>	Proveedor de Servicios de Certificación de la Fundación Instituto de Ingeniería.
<b>SUSCERTE</b>	Siglas con que se abrevia el nombre de la Superintendencia de Servicios de Certificación Electrónica.



## **ANEXO H. Requerimientos Generales de Hardware y Software para el Otorgamiento de Certificados Digitales**

### **SISTEMA DE CIRCUITO CERRADO DE TELEVISIÓN (CCTV)**

El Datacenter posee un sistema de grabación digital de video con mínimo cuatro entradas para cámara y dispositivos de alarma, capacidad mínima del disco duro 240GB y conexión a la red con tarjeta Ethernet. Posee un software para programación y visualización de las cámaras con búsqueda de eventos por alarmas, día, hora y/o cámara a través del protocolo TCP/IP, preferiblemente a través de una interfaz WEB. Además tiene la capacidad de programarse en grabación por detección de movimiento por software independientemente.

Se consta de cuatro cámaras de alta resolución con lente varifocal 3-6 mm, auto-iris para montaje en pared.

### **SISTEMA DE CONTROL DE ACCESO**

Se posee dentro de la estructura operativa del PSC FII, un controlador del sistema, administrado por TCP/IP con tarjeta Ethernet, en ambiente Web con sus respectivos módulos de control para las lectoras, cerraduras y pulsadores manuales.

Se consideran tres (3) lectoras integradas de proximidad (magnética), huella digital (biométrica) y teclado numérico. Compatibles con tarjetas INDALA.

Se considera la configuración de la apertura de las puertas con la presencia concurrente de al menos 2 de las personas autorizadas (autenticación N de M con N=2).

Ajustado al acceso de la Sala Cofre, se presenta una cerradura para puerta de bóveda con bloqueo y desbloqueo programable y teclado numérico.

Todas estas actividades son monitoreadas mediante una aplicación para el registro, control, supervisión, creación de gráficos y estadísticas por pantalla en tiempo real. La interfaz de la aplicación debe ser preferiblemente con interfaz Web.

### **SISTEMA DE DETECCIÓN Y EXTINCIÓN DE INCENDIOS**

Se presenta un sistema de detección y extinción de incendio basado en gas FM-200, con descarga aérea y bajo piso falso, el cual contiene una central de control para sistema de detección y extinción inteligente y alarma contra incendio, fuente de alimentación y

gabinete para empotrar. Este incluye además una interfaz Ethernet (TCP/IP) para administración, configuración y monitoreo del sistema.

El sistema de detección consta de un respaldo de baterías, cuatro (4) detectores fotoeléctricos inteligentes, dos (2) detectores térmicos inteligentes. Estos incluyen módulos de control, supervisión, relés y aislamiento de lazo.

Se cuenta con una sirena electrónica con señal visual estroboscópica de 15 candelas para instalación en pared, una estación manual de descarga con cajetín superficial color rojo y una estación manual de aborto con cajetín superficial color amarillo.

Dentro de la infraestructura de detección, se cuenta con los siguientes atributos:

- Cilindro contenedor de FM-200 en estado líquido,
- Presurizado con nitrógeno líquido @ 25 bar, de 52 lts de capacidad, con cabezales de descarga y discos de seguridad
- Agente extintor FM-200 para llenado del cilindro
- Activador eléctrico con control manual, compatible con el cabezal de los cilindros contenedores de FM-200
- Armaduras soportes para arreglo de cilindros contenedores de FM-200, con anclajes para fijar a la pared, herrajes, suministrada por el mismo fabricante de los cilindros
- Activador manual, compatible con el cabezal de los cilindros contenedores de FM-200, listado por UL y/o aprobado por FM
- Tobera de 360° de descarga horizontal, de bronce

### **SISTEMA DE FUENTE DE ALIMENTACIÓN ININTERRUMPIDA (UPS)**

En los sistemas de fuente de alimentación, se han considerados tres niveles de división del detalle que se describen a continuación:

#### **Salida**

- Capacidad de Potencia de Salida de 6400 Vatios / 8000 VA
- Máxima potencia configurable de 12800 Vatios / 16000 VA
- Tensión de salida nominal de 120V/208V
- Configurable para una tensión de salida de 120/208 o 120/240

- Eficiencia con carga completa de al menos 90%
- Distorsión de tensión de salida menor del 5% con carga completa
- Frecuencia de salida (sincronizada a red eléctrica principal) 47 - 63 Hz
- Factor de cresta de hasta 5:1
- Onda sinusoidal
- Conexiones de salida
- (1) Hard Wire 4-wire (2PH + N +G)

#### **Entrada**

- Desviación interna (automática y manual)
- Entrada de voltaje de 208V
- Frecuencia de entrada entre 45 y 65 Hz (con detección automática)

#### **Baterías y autonomía**

- Baterías selladas de plomo
- Tiempo típico de recarga no mayor de 3 hora(s)
- Duración típica de reserva a media carga de 17.0 minutos (3200 Vatios)
- Duración típica de reserva con carga completa de 5.9 minutos (6400 Vatios)

### **SISTEMA DE AIRE ACONDICIONADO DE PRECISIÓN PARA CONTROL DE TEMPERATURA Y HUMEDAD**

Dentro del ambiente controlado que debe tener el DataCenter, se puede precisar las siguientes características:

- La potencia de entrada y salida de 480 V, tres fases y tierra.
- Control de parámetros de la sala:
  - Setpoint de temperatura (18 – 29 °C)
  - Sensibilidad de Temperatura (+/-0.6 - 5.6 °C)
  - Setpoint de Humedad (20 – 80 % HR)
  - Sensitividad de Humedad (1 – 30 % HR)
  - Alarma de Alta temperatura (2 – 32 °C)

- Alarma de baja temperatura (2 – 32 °C)
- Alarma de Alta Humedad (15 – 85 % HR)
- Alarma de baja humedad (15 – 85 % HR)

El sistema de aire acondicionado contempla un display de panel frontal que permite visualizar temperatura de retorno (en °C ó °F), Humedad Relativa (%RH) y estado de operación del sistema (Enfriando, Calentando, Humidificando y Deshumidificando)

- Diagnóstico

Se permite la visualización de porcentajes de operación de trabajo de cada uno de los componentes: Compresor, Resistencias de calentamiento y Humidificador.

Se posee la capacidad de diagnosticar funcionamiento de los componentes del sistema de aire acondicionado, tales como: Motor de unidad manejadora de aire, compresores, válvula solenoide de línea de líquido, resistencias, humidificador y alarma común.

- Registros

El microprocesador posee la capacidad de registrar al menos los últimos 10 eventos que hayan implicado la activación de alarmas. Estos, deben quedar registrados con el día, hora y minutos, en tiempo real en el cual ocurrió.

Se puede apreciar los tiempos de operación de cada uno de los componentes: Compresores, resistencias, motor de manejadora, humidificador y deshumidificador.

- Sistema de control interno:

- Controlar ciclos cortos en los sistemas de refrigeración
- Posee secuencia automática de funcionamiento de los compresores
- Arranque automático del equipo cuando exista corte de fluido eléctrico
- Permitir la programación de retardo de encendido con un tiempo aproximado de 1 a 3 minutos
- Sistema autoflush que permita desalojar los sólidos de la superficie de la bandeja humidificadora, para humidificador tipo infrarrojo

- Calibración de los sensores de humedad y temperatura
- Desactivación de alarmas y sistemas de operación
- El refrigerante utilizado para el equipo será refrigerante Freón 22. Se puede ofrecer como alternativa equipos con refrigerante ecológico como el 407C
- Dos compresores para maximizar la eficiencia de operación y facilitar el mantenimiento que deben estar instalados sobre amortiguadores con protección contra sobrecarga, mira de vidrio para el nivel de aceite, interruptor de alta presión de rearme manual, interruptor de baja presión, línea de succión, bombas reversibles de aceite para lubricación forzada y control de desconexión
- Humidificador de tipo infrarrojo o canister, que garantice el suministro de la humedad necesaria cuando el ambiente lo requiera
- Condensador remoto enfriado por aire construido en lámina de aluminio de alta resistencia a la corrosión, con tubería de cobre de alta presión
- Detector de líquido, detector de fuego, detector de humo, tarjetas de comunicaciones NIC (Network Interface Card) con el software respectivo

## ANEXO I. Estructura de los Certificados Digitales

### 1.1. Campos para los certificados de Personas Naturales

En la Tabla 1 se indican los campos que forman parte de los certificados de personas naturales:

Descripción del atributo	Ubicación	Nombre del atributo		
Versión del certificado	Certificado	Versión		
ID del certificado	Certificado	Serial Number		
Algoritmo de Firma	Certificado	Signature Algorithm		
Emisor	Certificado	DN	<b>Issuer (DN)</b>	
			emailAddress	
			CN	
			OU	
			O	
Validez del certificado	Certificado	Validity	Not Before = fecha de inicio	
			Not After = fecha de fin	
Asunto del certificado	Certificado	DN	<b>Subject (DN)</b>	
			SerialNumber = ID del certificado	
			L = Dirección	
			CN = Nombre de la persona	
			OU = RA Emisora	
			O = CA Emisora	
Algoritmo de clave pública	Certificado	Public Key Algorithm		
		RSA Public Key		
Clave pública RSA	Certificado	RSA Public Key		
Uso de la clave	Extensiones	X509v3 Key Usage		
Uso de la clave extendido	Extensiones	X509v3 Extended Key Usage		
Identificador de la clave del asunto	Extensiones	X509v3 Subject Key Identifier		
Identificador de la clave de la autoridad	Extensiones	X509v3 Authority Key Identifier		
Nombre Alternativo	Extensiones	X509v3 Subject Alternative Name		
		<b>Nombre</b>	<b>OID</b>	<b>Campo</b>
		Identificador PSC	2.16.862.2.1	otherName
		Documento de Identificación	2.16.862.2.2	otherName
		Rol	2.16.862.2.3	otherName
		Dirección Web de la RA	2.16.862.2.4	otherName
		Dirección Web de la CA	2.16.862.2.5	otherName
Correo electrónico		email		
Nombre Alternativo del emisor	Extensiones	X509v3 Issuer Alternative Name		
Teléfono	HEADER			
Teléfono celular	HEADER			
OCSF	Extensiones	Authority Information Access		
Políticas de seguridad	Extensiones	X509v3 Certificate Policies		
CRL	Extensiones	X509v3 CRL Distribution Points		

Tabla 1. Campos del certificado de persona natural

## 1.2. Campos para los certificados de Personas Jurídicas

En la Tabla 2 se indican los campos que forman parte de los certificados de personas jurídicas:

Descripción del atributo	Ubicación	Nombre del atributo		
Versión del certificado	Certificado	Version		
ID del certificado	Certificado	Serial Number		
Algoritmo de Firma	Certificado	Signature Algorithm		
Emisor	Certificado	<b>Issuer (DN)</b>		
		DN	emailAddress	
			CN	
			OU	
			O	
		C		
Validez del certificado	Certificado	Validity	Not Before = fecha de inicio	
			Not After = fecha de fin	
Asunto del certificado	Certificado	<b>Subject (DN)</b>		
		DN	SerialNumber = ID del certificado	
			L = Dirección	
			CN = Nombre de la persona jurídica	
			OU = RA Emisora	
			O = CA Emisora	
	C = País (VE)			
Algoritmo de clave pública	Certificado	Public Key Algorithm		
Clave pública RSA	Certificado	RSA Public Key		
Uso de la clave	Extensiones	X509v3 Key Usage		
Uso de la clave extendido	Extensiones	X509v3 Extended Key Usage		
Identificador de la clave del asunto	Extensiones	X509v3 Subject Key Identifier		
Identificador de la clave de la autoridad	Extensiones	X509v3 Authority Key Identifier		
Nombre Alternativo	Extensiones	X509v3 Subject Alternative Name		
		<b>Nombre</b>	<b>OID</b>	<b>Campo</b>
		Identificador PSC	2.16.862.2.1	otherName
		Documento de Identificación	2.16.862.2.2	otherName
		Rol	2.16.862.2.3	otherName
		Dirección Web de la RA	2.16.862.2.4	otherName
		Dirección Web de la CA	2.16.862.2.5	otherName
Correo electrónico persona jurídica		email		
Nombre Alternativo del emisor	Extensiones	X509v3 Issuer Alternative Name		
Teléfono	HEADER			
Teléfono opcional	HEADER			
NIT	HEADER			
Nombre de persona responsable	HEADER			
Correo electrónico persona responsable	HEADER			

OCSP	Extensiones	Authority Information Access
Políticas de seguridad	Extensiones	X509v3 Certificate Policies
CRL	Extensiones	X509v3 CRL Distribution Points

**Tabla 2. Campos del certificado de persona jurídica**

#### 1.4. Campos para los certificados de Servidores

En la Tabla 3 se indican los campos que forman parte de los certificados de servidores:

Descripción del atributo	Ubicación	Nombre del atributo		
Versión del certificado	Certificado	Version		
ID del certificado	Certificado	Serial Number		
Algoritmo de Firma	Certificado	Signature Algorithm		
Emisor	Certificado	<b>Issuer (DN)</b>		
		DN	emailAddress	
			CN	
			OU	
			O	
C				
Validez del certificado	Certificado	Validity	Not Before = fecha de inicio	
			Not After = fecha de fin	
Asunto del certificado	Certificado	<b>Subject (DN)</b>		
		DN	SerialNumber = ID del certificado	
			L = Dirección	
			CN = Nombre de la persona responsable	
			OU = RA Emisora	
			O = CA Emisora	
C = País (VE)				
Algoritmo de clave pública	Certificado	Public Key Algorithm		
Clave pública RSA	Certificado	RSA Public Key		
Uso de la clave	Extensiones	X509v3 Key Usage		
Uso de la clave extendido	Extensiones	X509v3 Extended Key Usage		
Identificador de la clave del asunto	Extensiones	X509v3 Subject Key Identifier		
Identificador de la clave de la autoridad	Extensiones	X509v3 Authority Key Identifier		
Nombre Alternativo	Extensiones	X509v3 Subject Alternative Name		
		<b>Nombre</b>	<b>OID</b>	<b>Campo</b>
		Identificador PSC	2.16.862.2.1	otherName
		Documento de Identificación	2.16.862.2.2	otherName
		Rol	2.16.862.2.3	otherName
		Dirección Web de la RA	2.16.862.2.4	otherName
		Dirección Web de la CA	2.16.862.2.5	otherName
		Correo electrónico persona responsable		email
		Dirección IP		IP
		DNS primario		DNS
DNS secundario		DNS		
Nombre Alternativo del emisor	Extensiones	X509v3 Issuer Alternative Name		



Teléfono	HEADER	
OCSP	Extensiones	Authority Information Access
Políticas de seguridad	Extensiones	X509v3 Certificate Policies
CRL	Extensiones	X509v3 CRL Distribution Points

**Tabla 3. Campos del certificado de servidor**

### 1.5. Campos para los certificados de operadores (RA/CA)

En la Tabla 4 se indican los campos que forman parte de los certificados de los operadores de la RA y la CA:

Descripción del atributo	Ubicación	Nombre del atributo		
Versión del certificado	Certificado	Version		
ID del certificado	Certificado	Serial Number		
Algoritmo de Firma	Certificado	Signature Algorithm		
Emisor	Certificado	DN	<b>Issuer (DN)</b>	
			emailAddress	
			CN	
			OU	
			C	
Validez del certificado	Certificado	Validity	Not Before = fecha de inicio Not After = fecha de fin	
Asunto del certificado	Certificado	DN	<b>Subject (DN)</b>	
			SerialNumber = ID del certificado	
			L = Dirección	
			CN = Nombre de la persona responsable	
			O = RA Emisora	
O = CA Emisora				
C = País (VE)				
Algoritmo de clave pública	Certificado	Public Key Algorithm		
Clave pública RSA	Certificado	RSA Public Key		
Uso de la clave	Extensiones	X509v3 Key Usage		
Uso de la clave extendido	Extensiones	X509v3 Extended Key Usage		
Identificador de la clave del asunto	Extensiones	X509v3 Subject Key Identifier		
Identificador de la clave de la autoridad	Extensiones	X509v3 Authority Key Identifier		
Nombre Alternativo	Extensiones	X509v3 Subject Alternative Name		
		<b>Nombre</b>	<b>OID</b>	<b>Campo</b>
		Identificador PSC	2.16.862.2.1	otherName
		Documento de Identificación	2.16.862.2.2	otherName
		Rol	2.16.862.2.3	otherName
		Dirección Web de la RA	2.16.862.2.4	otherName
		Dirección Web de la CA	2.16.862.2.5	otherName
		Correo electrónico persona responsable		email
		Dirección IP		IP
		DNS primario		DNS
DNS secundario		DNS		
Nombre Alternativo del emisor	Extensiones	X509v3 Issuer Alternative Name		
Teléfono	HEADER			
Teléfono opcional	HEADER			
OCSP	Extensiones	Authority Information Access		
Políticas de seguridad	Extensiones	X509v3 Certificate Policies		
CRL	Extensiones	X509v3 CRL Distribution Points		

**Tabla 4. Campos del certificado de operador (RA y CA)**

## ANEXO J. Formulario de Solicitud de Acreditación

Ministerio del Poder Popular  
para las **Telecomunicaciones y la Informática**

**SUSCERTE**  
Superintendencia de Servicios de Certificación Electrónica



## SOLICITUD DE ACREDITACIÓN

- 
- **PREVIO AL LLENADO DE ESTA SOLICITUD, CONSULTE Y VERIFIQUE LOS DOCUMENTOS QUE ESTABLECEN LOS REQUISITOS DE ACREDITACIÓN (DECRETO-LEY 1.204, REGLAMENTO, PROCEDIMIENTO DE ACREDITACIÓN Y LEY ORGÁNICA DE PROCEDIMIENTOS ADMINISTRATIVOS)**
  - **LA INFORMACIÓN PUEDE SER RECADADA DEL PORTAL WEB DE SUSCERTE [www.suscerte.gob.ve](http://www.suscerte.gob.ve)**
- 

**DATOS DEL SOLICITANTE**

TIPO DE PERSONA: De Derecho Privado  De Derecho Público

Nombre o Razón Social: \_\_\_\_\_ Teléfono: \_\_\_\_\_

Domicilio Fiscal: \_\_\_\_\_ Ciudad / Estado: \_\_\_\_\_

Nº RIF: \_\_\_\_\_ Correo Electrónico: \_\_\_\_\_

**DATOS DEL REPRESENTANTE LEGAL:**

Cedula de Identidad : \_\_\_\_\_ Nº de Credencial: \_\_\_\_\_

Nombre: \_\_\_\_\_ Apellido: \_\_\_\_\_

Dirección: \_\_\_\_\_ Ciudad / Estado: \_\_\_\_\_

Teléfono: \_\_\_\_\_ Correo Electrónico: \_\_\_\_\_

**TIPO DE SOLICITUD:** Acreditación  Renovación

Solicito a la Superintendencia de Servicios de Certificación Electrónica sírvase proceder al análisis de la documentación anexa, la cual expreso como verdadera y ajustada a los requisitos de Acreditación. Así mismo, manifiesto conocer las obligaciones que conllevan la obtención de la Acreditación.

En tal sentido, me comprometo a cumplir con los procedimientos de Acreditación establecidos por SUSCERTE y estoy en disposición de dar facilidades al personal designado para llevar a cabo el proceso de evaluación de la documentación consignada.

Fecha: \_\_\_\_\_

Firma: \_\_\_\_\_

## ANEXO K . Formato de Evaluación de Recaudos para el PSC

Ministerio del Poder Popular  
para las Telecomunicaciones y la Informática

**SUSCERTE**  
Superintendencia de Servicios de Certificación Electrónica



### FORMATO DE EVALUACIÓN DE RECAUDOS PARA EL PSC F01-014

- I. Formato para uso exclusivo del personal autorizado por SUSCERTE para la evaluación de los recaudos de los solicitantes a Proveedores de Servicios de Certificación (PSC).

#### DATOS DEL SOLICITANTE

Nombre o Razón Social: \_\_\_\_\_ N° de RIF: \_\_\_\_\_

#### DATOS DEL EVALUADOR

**Dirección de adscripción:**  Registro y Acreditación  Inspección y Fiscalización

Asesoría Legal  Gestión Administrativa  Otra: \_\_\_\_\_

Nombre y Apellido: \_\_\_\_\_ N° Cédula Identidad: \_\_\_\_\_

Cargo: \_\_\_\_\_

#### DATOS DEL DOCUMENTO A EVALUAR

Código: \_\_\_\_\_ Aprobado:  Si  No

Observaciones:

Fecha: \_\_\_\_\_

Firma: \_\_\_\_\_

Sello: \_\_\_\_\_

## ANEXO L. Formato de Registro del Expediente del PSC

Ministerio del Poder Popular  
para las Telecomunicaciones y la Informática

**SUSCERTE**  
Superintendencia de Servicios de Certificación Electrónica



### FORMATO DE REGISTRO DEL EXPEDIENTE DEL PSC F01-026

- Este formato es para uso exclusivo del personal autorizado por SUSCERTE para apertura y control del expediente del solicitante a PSC.

#### DATOS DEL SOLICITANTE O PSC

Nombre o Razón Social: \_\_\_\_\_ N° de RIF: \_\_\_\_\_

N° de Teléfono: \_\_\_\_\_ Correo-electrónico: \_\_\_\_\_

#### DATOS DE RECEPCIÓN

Fecha de Recepción: \_\_\_\_\_ Hora: \_\_\_\_\_

Entregado por (Nombre y Apellido): \_\_\_\_\_ Cargo: \_\_\_\_\_

Recibido por (Nombre y Apellido): \_\_\_\_\_ Cargo: \_\_\_\_\_

#### DATOS DEL DOCUMENTO

Código del Expediente: \_\_\_\_\_ Versión del Expediente: \_\_\_\_\_

Código del Certificado de Acreditación (en caso de ser PSC Acreditado): \_\_\_\_\_

Firma recibido: \_\_\_\_\_

Sello: \_\_\_\_\_

**ANEXO M. Lista de Recaudos Legales, Económicos - Financieros y Técnicos**

<b>LEGALES</b>		
<b>No.</b>	<b>NOMBRE DEL RECAUDO</b>	<b>OBSERVACIÓN</b>
<b>L01</b>	<b>PARA PERSONA DE DERECHO PRIVADO</b>	
L01.1	Registro de Información Fiscal (RIF) actualizado	Copia fotostática
L01.2	Solvencia Laboral	Copia fotostática
L01.3	Inscripción en el Servicio Nacional de Contratistas (SNC) actualizada	Copia fotostática
L01.4	Identificación y datos de ubicación de los Representantes Legales	Incluye: Cédula de Identidad o Pasaporte, domicilio, números telefónicos, fax y correo electrónico
L01.5	Documento donde conste la designación del o los representantes legales y la legitimidad para actuar en nombre del solicitante	Copia Certificada
L01.6	Documento Constitutivo o Estatutos del Solicitante.	Copia Certificada
L01.7	Actas de Asambleas Ordinarias y/o Extraordinarias, celebradas por el solicitante	Copia Certificada
<b>L02</b>	<b>PARA PERSONA DE DERECHO PÚBLICO</b>	
L02.1	Gaceta Oficial de la publicación del decreto de creación	Copia fotostática, si se trata de un organismo, órgano o ente de la administración pública central, descentralizada o desconcentrada funcionalmente
L02.2	Gaceta Oficial donde conste el acto administrativo que confiera las atribuciones del representante legal del solicitante o documento en el que conste la capacidad para actuar en nombre y representación del solicitante	Copia fotostática
L02.3	Identificación y datos de ubicación de los Representantes Legales	Incluye: Cédula de identidad o pasaporte, domicilio, números telefónicos, fax y correo electrónico
L02.4	Registro de Información Fiscal (RIF) actualizada	Copia fotostática, en caso de ser contribuyente
<b>L05</b>	<b>DOCUMENTOS COMUNES PARA TODOS LOS SOLICITANTES</b>	
L05.1	Modelo de Garantías necesarias para su acreditación	De conformidad con la LSMDFE y su Reglamento Parcial
L05.2	Contratos de servicios suscritos con terceras personas que guarden relación con alguno de los servicios a ser acreditados en virtud de la acreditación	Copia fotostática
L05.3	Modelos de contratos a ser suscritos con los signatarios	Copia fotostática
L05.4	Documento de la Declaración de Prácticas de Certificación y Políticas de Certificados	Copia fotostática

**Tabla No. 1 Recaudos Legales**

<b>ECONÓMICOS-FINANCIEROS</b>		
<b>No.</b>	<b>NOMBRE DEL RECAUDO</b>	<b>OBSERVACIÓN</b>
<b>E01</b>	<b>PARA PERSONA DE DERECHO PRIVADO</b>	
E01.1	Estados Financieros (Balance General, Estado de Ganancias y Pérdidas)	Con sus respectivas notas, debidamente certificado por un contador público colegiado y visado por el colegio de contadores públicos de Venezuela, correspondiente a los dos (02) últimos años
E01.2	Declaración auditada del Impuesto sobre la Renta	De los últimos tres (3) años
E01.3	Proyecto Económico	Para un período mínimo de tres (3) años, presentado en forma anual y en moneda oficial de la República Bolivariana de Venezuela y firmado por un economista colegiado.  Debe contener: <ul style="list-style-type: none"> <li>● Análisis de Mercado, que incluya localización y sectorización, demanda y oferta</li> <li>● Explicación detallada de los ingresos</li> <li>● Fuente de Financiamiento de la inversión</li> <li>● Cronograma de inversión, indicando la inversión inicial y total</li> <li>● Costos Fijos desglosados</li> <li>● Costos variables desglosados</li> <li>● Gastos de Personal desglosados</li> <li>● Punto de Equilibrio</li> <li>● Flujo de Caja Proyectado</li> <li>● Estado de Ganancias y Pérdidas proyectado</li> <li>● Amortización de Financiamiento</li> <li>● Listado de Equipos a adquirir, especificado en Bolívares</li> </ul>
E01.4	Balance de Apertura	Solo para empresas recién constituidas o sin giro, con sus respectivas notas de los estados financieros, expresado en valores constantes y en bolívares, debidamente certificado por un contador público colegiado y visado por el colegio de contadores públicos de Venezuela
E01.5	Referencias bancarias	Con vigencia de tres (3) meses. Si la empresa es de reciente constitución, serán sus accionistas quienes deberán consignar dichas referencias
E01.6	Carta de intención para financiamiento (cuando se requiera) por parte de una institución financiera reconocida	Destacando: monto del financiamiento, condiciones y términos de respaldo, dirección, teléfonos y dirección del sitio web o e-mail.  Si es emitida en el exterior, deberá estar traducida al castellano y legalizada por el Consulado Venezolano
E01.7	Documento autenticado de intención de financiamiento, si	Acompañado de los estados financieros debidamente firmados por un contador público colegiado y visado por el colegio de

	el financiamiento es a través de terceros (persona natural o jurídica)	contadores públicos de Venezuela. Destacando: monto del financiamiento, condiciones y términos de respaldo, dirección, teléfonos y dirección del sitio web o e-mail.
E01.8	<b>SI EL O LOS ACCIONISTAS SON PERSONAS JURÍDICAS DEBE PRESENTAR ADICIONALMENTE</b>	
E01.8.1	Balance General Estado de ganancias y pérdidas, Flujo de efectivo y movimiento de patrimonio	Con sus notas explicativas de las partidas que integran dicho balance con una vigencia no mayor de seis (6) meses y en moneda oficial de la República Bolivariana de Venezuela, firmada por un contador público colegiado y visado por el colegio de contadores públicos de Venezuela
E01.9	<b>SI EL O LOS ACCIONISTAS SON PERSONAS NATURALES DEBE PRESENTAR ADICIONALMENTE</b>	
E01.9.1	Balance personal actualizado	Con sus notas explicativas de las partidas que integran dicho balance con una vigencia no mayor de seis (6) meses y en moneda oficial de la República Bolivariana de Venezuela, firmada por un contador público colegiado y visado por el colegio de contadores públicos de Venezuela
<b>E03</b>	<b>PARA PERSONA DE DERECHO PÚBLICO</b>	
E03.1	Proyecto económico	Para un período mínimo de tres (3) años, presentado en forma anual y en moneda oficial de la República Bolivariana de Venezuela y firmado por un economista colegiado.  Debe contener:  1. Análisis de Mercado, que incluya localización y sectorización, demanda y oferta 2. Explicación detallada de los ingresos 3. Fuente de Financiamiento de la inversión 4. Cronograma de inversión, indicando la inversión inicial y total 5. Costos Fijos desglosados 6. Costos variables desglosados 7. Gastos de Personal desglosados 8. Punto de Equilibrio 9. Flujo de Caja Proyectado 10. Estado de Ganancias y Pérdidas proyectado 11. Amortización de Financiamiento 12. Listado de Equipos a adquirir, especificado en Bolívares
E03.2	Apartado presupuestario	Presupuesto de ingreso Presupuesto de gasto

**Tabla No. 2** Recaudos Económico-Financieros



<b>TÉCNICOS</b>		
<b>No.</b>	<b>NOMBRE DEL RECAUDO</b>	<b>OBSERVACIÓN</b>
<b>T01</b>	<b>INFRAESTRUCTURA DE CLAVE PÚBLICA</b>	
T01.1	Estructura del certificado de firma electrónica	Modelo de Certificado tipo de firma electrónica y Modelo de la solicitud de firma del certificado (CSR)
T01.2	Estructura e información de la lista de Certificados de firma electrónica revocados (LCR)	Lista de Certificados Revocados (LCR) Certificado de firma electrónica de la AC que la emite
T01.3	Registro de acceso público	Documento descriptivo que contenga al menos: detalle del sitio web donde se publicará la información, descripción de la tecnología, disponibilidad, accesibilidad, conexión, esquemas y diagramas de funcionamiento, medidas de seguridad y sitio web con funcionalidades requeridas
T01.4	Modelo de confianza	O alternativamente la DPC y PC, si describe el modelo de confianza utilizado por el PSC para lograr el objetivo
<b>T02</b>	<b>SEGURIDAD</b>	
T02.1	Evaluación de riesgos	Debe incluir el reporte de la valoración de riesgos y la estructura del proceso de valoración de riesgos
T02.2	Política de seguridad de la información	Debe estar basada en las recomendaciones del estándar ISO 17799 y en los anexos No. 4 y 6, presentados en la Norma SUSCERTE No. 040.
T02.3	Plan de continuidad del negocio y recuperación ante desastres	Debe estar basada en las recomendaciones del estándar ISO 17799 sección 14 y en los anexos No. 4 y 7 de la Norma SUSCERTE No. 040
T02.4	Plan de Seguridad de la información	Debe basarse en las recomendaciones del estándar ISO 17799 y en el anexo 8 y 11 de la Norma SUSCERTE No. 040.
T02.5	Plan de Administración de Claves Criptográficas	Debe estar basada en las recomendaciones del estándar ETSI TS 102 042 y FIPS 140-2
T02.6	Documento de la Implementación de seguridad física y ambiental	Debe seguirse las recomendaciones del apartado de Seguridad física y ambiental de la Norma ISO 17799 (contemplado en la sección 9 del anexo 4 en la norma SUSCERTE 040).
<b>T03</b>	<b>PLATAFORMA TECNOLÓGICA</b>	
T03.1	Evaluación de la plataforma Tecnológica	Debe contemplar lo especificado en el Pto. 5.3.11 de la Norma SUSCERTE No. 040
<b>T04</b>	<b>POLÍTICAS DE CERTIFICACIÓN</b>	
T04.1	Declaración de Prácticas de Certificación y Política de Certificados	Debe seguirse las recomendaciones del estándar RFC 3647 y ETSI TS 102 042.
T04.2	Modelo de Operación de la Autoridad de Certificación (AC) del PSC	Debe contemplar lo especificado en el Anexo No. 9 de la Norma SUSCERTE No. 040
T04.3	Modelo de Operación de la Autoridad de Registro (AR)	Debe contemplar lo especificado en el Anexo No. 10 de la Norma SUSCERTE No. 040

<b>T05 ADMINISTRACIÓN DE LOS SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA</b>		
T05.1	Manual de Operación de la Autoridad de Certificación del PSC	Debe seguir las recomendaciones del estándar RFC 3647 y ETSI TS 102 042 y contemplar lo especificado en el apartado 5.3.17 de la Norma SUSCERTE No. 040
T05.2	Manual de Operación de la Autoridad de Registro	Debe seguir las recomendaciones del estándar RFC 3647 y contemplar lo especificado en el apartado 5.3.18 de la Norma SUSCERTE No. 040
<b>T06 MODELO ORGANIZACIONAL</b>		
T06.1	Estructura organizativa	Debe presentar la estructura organizativa del PSC, describiendo las unidades y cantidad de personas dedicadas a las labores relacionadas a la acreditación solicitada
T06.2	Evaluación del personal	<p>Debe seguir las recomendaciones del estándar ISO 17799 y ETSI TS 102 042 y contemplar lo especificado en el apartado 5.3.19 de la Norma SUSCERTE No. 040 y presentar:</p> <ul style="list-style-type: none"> <li>- Perfiles de los cargos que manejan información o sistemas sensibles</li> <li>- Currícula de las personas que ocupan los cargos y funciones sensibles</li> <li>- Procedimientos de seguridad aplicados en la contratación</li> <li>- Identificación del personal calificado como crítico, durante la visita del experto designado por SUSCERTE, en la forma que el experto lo solicite (cv, foto, etc)</li> </ul>

**Tabla No. 3** Recaudos Técnicos

<b>AUDITORÍA</b>		
A01	Informe de Auditoría Técnica	Elaborado por un Auditor inscrito en el Registro de auditores de SUSCERTE y de conformidad con lo establecido en la Norma SUSCERTE No. 045. Guía modelo de informe de auditoría

**Tabla No. 4** Recaudos de Auditoría Técnica