MODELO PARA LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN Y POLÍTICAS DE CERTIFICADOS DE LOS PROVEEDORES DE SERVICIOS DE CERTIFICACIÒN (PSC)

CONTROL DE VERSIONES

VERSIÒN (EDICIÒN)	MOTIVO DE CAMBIO	PUBLICACIÒN
01	Creación	Julio 2005
02	Actualización General	Septiembre 2007
03	Actualización General	Abril 2008
04	Clasificación de la norma	Enero 2011

ÍNDICE

TRÁMITE					
1. AUTORIDADES					
NOMBRE		CARGO SUSCERTE			
2. GRUPO DE TRABAJO:			3. COMISIÓN ESPECIAL:		
MIEMBROS PERMANENTES:			CARGO:		
NOMBRE	UNIDAD	CARGO			
			4. ESPECIALISTA(S) INVITADO(S):		
			NOMBRE	ENTIDAD	CARGO
OBSERVACIONES			RESPONSABLE DE LA EDICIÓN		
			COORDINADOR: FECHA: FIRMA:		
			SUPERINTENDENTE: FECHA: FIRMA:		
			APROBACIÓN APLICACIÓN EN: FECHA: FIRMA:		

1.OBJETO Y CAMPO DE APLICACIÓN

Esta norma tiene por finalidad presentar el Modelo de Declaración de Prácticas de Certificación y Políticas de Certificados que los Proveedores de Servicios de Certificación (PSC) deben consignar ante la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) como requisito parcial para la Acreditación, según lo establecido en el Decreto 1.204 con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas (LSMDFE) y su Reglamento Parcial (RPLSMDFE), definiendo las responsabilidades y obligaciones de los PSC como emisores y de los signatarios como titulares de la firma electrónica.

2.REFERENCIAS NORMATIVAS

1.1 Decreto 1.204 con Fuerza de Ley 1.204 Sobre Mensajes de Datos y Firmas Electrónicas (LSMDFE)

1.2 Reglamento Parcial de la Ley 1.204 Sobre Mensajes de Datos y Firmas Electrónicas (RPLSMDFE)

1.3 Norma SUSCERTE Nº 040. Guía de Estándares Tecnológicos y Lineamientos de Seguridad para la Acreditación como Proveedor de Servicios de Certificación Electrónica.

1.4 Norma RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, del Internet Engineering Task Force (IETF)

3.DEFINICIONES Y TERMINOLOGÍAS

A los efectos de esta norma, se establecen las siguientes definiciones y terminologías:

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

ALGORITMO CRIPTOGRÀFICO	Transformación matemática que partiendo de un texto plano lo cambia a datos ilegibles cifrados.
AUDITORÍA	Procedimiento usado para verificar que se están llevando a cabo controles en un sistema de información y que estos son adecuados para los objetivos que se persiguen. Incluye el análisis de las actividades para detectar intrusiones o abusos dentro del sistema informático.
AUTENTICIDAD	Característica por la que se garantiza la identidad del usuario que origina un mensaje o transacción, es decir, conocer con certeza quién envía algo.
AUTENTIFICACIÓN	Proceso utilizado para confirmar la identidad y autenticidad de una persona o probar la integridad de información específica.
AUTENTIFICACIÓN DE MENSAJES	Proceso de autentificación que incluye la identificación de la fuente del mensaje.
AUTORIDAD CERTIFICADORA (AC)	Tercera parte de confianza que acredita la conexión entre una determinada clave pública y su propietario. La confianza en la AC supone la confianza en los certificados que emite.
AUTORIDAD DE REGISTRO (RA)	Entidad autorizada por la AC para registrar a los usuarios de la infraestructura asignándoles un identificador único de usuario.
CERTIFICADO RAÍZ	Certificado emitido por la Autoridad de Certificación para si misma. Es el origen de la cadena de confianza.
CERTIFICADO RAÍZ (CONT..)	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.
CERTIFICADO DE FIRMA ELECTRÓNICA	Instrumento electrónico que autentica el vínculo entre el firmante o titular del Certificado Electrónico y la Firma Electrónica.
CERTIFICADO ELECTRÓNICO	Mensaje de Datos proporcionado por un Proveedor de Servicios de Certificación que le atribuye certeza y validez a la Firma Electrónica.

CIFRADO	Transformación de un mensaje en otro, utilizando una clave para impedir que el mensaje transformado pueda ser interpretado por aquellos que no conocen la clave.
CLAVE	Valor numérico que participa en un algoritmo para cifrar información. Una clave también puede verse como una secuencia de caracteres empleada para cifrar y/o descifrar un mensaje.
CLAVE PRIVADA	Clave personal que no es conocida por el resto de los usuarios y que es utilizada para crear firmas digitales y para descifrar mensajes cifrados con la correspondiente clave pública.
CLAVE PÚBLICA	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 o validar las firmas electrónicas generados por estos.
CONFIABILIDAD	Parte que asegura que la información sólo puede ser vista y utilizada por las partes que están autorizadas. La comunicación entre partes confiables se establece una vez que se ha realizado el proceso de autentificación.
CONTROL DE ACCESO	Significa que cada usuario tiene un registro de los accesos a una red o sistema, de manera que se pueda monitorear la información a la que se ingresa y las aplicaciones que son empleadas.
CONTROL N DE M	Mecanismo de control de acceso, en el cual se requiere un mínimo N de personas, del conjunto total M para acceder a un determinado recurso donde N ≤ M.
CRIPTOGRAFÍA	Rama de las matemáticas aplicadas que se ocupa de transformar mensajes en formas aparentemente ininteligibles y devolverlas a su forma original.
DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN	Documento en el cual el Proveedor de Servicios de Certificación (PSC), define los procedimientos relacionados con el manejo de los certificados electrónicos que emite.

DESTINATARIO	Persona a quien va dirigido el Mensaje de Datos enviado por medios electrónicos por el signatario de la Firma Electrónica.
DISPONIBILIDAD	Característica técnica y administrativa que previene contra la denegación no autorizada de acceso a la información.
DOCUMENTO ELECTRÓNICO	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.
DOMICILIO FÍSICO DEL PSC	Lugar de dirección suministrado por PSC, donde funcionará la infraestructura física y de servicios necesaria para la emisión de los certificados electrónicos.
EMISOR	Persona que origina un Mensaje de Datos por sí mismo, o a través de terceros autorizados.
EVALUACIÓN AL PSC	Evaluación pormenorizada de los aspectos técnicos, legales, económicos-financieros y tecnológicos del PSC realizada por las unidades internas de SUSCERTE, de acuerdo a su área de competencia.
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
FUNCIÓN HASH	Funciones matemáticas 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.
INTEGRIDAD	Garantía de la exactitud de la información.

LEY 1.204 SOBRE MENSAJE DE DATOS Y FIRMAS ELECTRÓNICAS	Decreto con fuerza de Ley, de fecha 10 de febrero de 2001, publicado en Gaceta Oficial de la República Bolivariana de Venezuela Nº 37.148, de fecha 28 de febrero de 2001, que tiene por objeto otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y a los Certificados Electrónicos.
LISTA DE REVOCACIÓN DE CERTIFICADOS (LCR)	Documento mantenido y publicado por una Autoridad de Certificación (AC) que enumera los certificados revocados por la entidad emisora.
MENSAJE DE DATOS	Toda información inteligible en formato electrónico o similar que pueda ser intercambiada por cualquier medio.
PAR DE CLAVES	Combinación de las claves de cifrado privada y pública que proporciona comprobación del origen de los datos enviados a través de la red.
PLAN DE MEJORAS	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
POLÍTICA DE CERTIFICADOS	Documento en el cual el Proveedor de Servicios de Certificación, define las reglas a seguir para el uso de un Certificado Electrónico en una comunidad de usuarios o aplicación determinada y sus requerimientos de seguridad.
POLÍTICA DE CERTIFICADOS	Documento en el cual el Proveedor de Servicios de Certificación, define las reglas a seguir para el uso de un Certificado Electrónico en una comunidad de usuarios o aplicación determinada y sus requerimientos de seguridad.

POLÍTICA DE SEGURIDAD	Documento que recoge todos los requisitos y prácticas de seguridad para asegurar el funcionamiento de la infraestructura de una forma fiable.
PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN	Personas dedicada a proporcionar Certificados Electrónicos y demás actividades previstas en este Decreto-Ley
PRIVACIDAD	Característica que garantiza que nadie salvo el destinatario puede acceder al contenido de un mensaje.
REGLAMENTO PARCIAL DEL DECRETO-LEY SOBRE MNSAJES DE DATOS Y FIRMAS ELECTRONICAS	Decreto Nº 3.335 de fecha 12 de diciembre de 2004 publicado en Gaceta Oficial de la República Bolivariana de Venezuela, Nº 38.086 de fecha14 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 PSC ante la SUSCERTE, la creación del Registro de Auditores, así como los estándares, planes y procedimientos de seguridad.
REPOSITORIO	Sistema de información utilizado para el almacenamiento y acceso de los certificados electrónicos y la información asociada a los mismos
REPUDIO	Negación o intento de negación de haber participado en una comunicación.
REVOCACIÓN DE CERTIFICADOS	Anulación de la validez de un certificado de clave pública antes del fin del periodo de validez.
RSA	Desarrollado por (Rivest, Shamir, Adleman. Algoritmo criptográfico de cifrado de clave asimétrica, utiliza una clave para cifrar y otra para descifrar.
SIGNATARIO	Persona titular de una Firma Electrónica la cual se encuentra amparado por un Certificado Electrónico emitido por un PSC.
SOLICITANTE	Persona que presenta ante la SUSCERTE la Solicitud de Acreditación con todos los recaudos necesarios para optar a ser PSC.

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 CERTIFICACIÒN ELECTRÒNICA	Servicio Autónomo que pertenece al Ministerio del Poder Popular para las Telecomunicaciones y la Informática cuyo objeto es acreditar, supervisar y controlar, en los términos previstos en el Decreto-Ley 1.2004 (LSMDFE) y su Reglamento Parcial, a los Proveedores de Servicios de Certificación públicos o privados.

4.SÍMBOLOS Y ABREVIATURAS

AC	Autoridad de Certificación
AR	Autoridad de Registro
DPC	Declaración de Prácticas de Certificación
DRA	Dirección de Registro y Acreditación
ICP	Infraestructura de Clave Pública
ISO/IEC	Organización Internacional de Normalización.
LDAP	Protocolo de Acceso de Servicio de Directorio
LCR	Lista de Certificados Revocados
LSMDFE	Decreto con fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas (1.204).
OCSP	On-Line Certificate Status Protocol (Protocolo de estado de certificados en línea)
OID	Identificador único de objeto.
PC	Política de Certificados
PSC	Proveedor de Servicios de Certificación
SUSCERTE	Superintendencia de Servicios de Certificación Electrónica.

5.PROCEDIMIENTO

5.1 Principio Básico

Establecer el Modelo de Declaración de Prácticas de Certificación (DPC) y Políticas de Certificados (PC) que el Proveedor de Servicios de Certificación (PSC) acreditado debe utilizar para regular todo lo concerniente a la solicitud, emisión, aceptación, renovación, suspensión, revocación, responsabilidades y obligaciones del uso de los certificados, lo que permitirá llevar un control exhaustivo del PSC en la provisión de servicios de certificación y asegurar la confiabilidad de la Infraestructura Nacional de Certificación Electrónica.

5.2 Unidades Involucradas

5.2.1 Dirección de Registro y Acreditación (DRA).

5.3 Interrelación con otros Sistemas y Procedimientos

5.3.1 Norma SUSCERTE Nº 017. Procedimiento para el Análisis de los Recaudos Técnicos del Solicitante.

5.3.2 Norma SUSCERTE Nº 028. Procedimiento para la Autorización de Modificación de Políticas de Certificados por el Proveedor de Servicios de Certificación.

5.3.3 Norma SUSCERTE Nº 029. Procedimiento para la Autorización de Modificación de Prácticas de Certificación por el Proveedor de Servicios de Certificación.

5.4 Consideraciones Generales

5.4.1 La Declaración de Prácticas de Certificación es el documento donde se definirán los procedimientos relacionados con el manejo de los certificados electrónicos que emite el PSC, estableciendo los lineamientos que debe cumplir obligatoriamente, tanto en sus funciones de Autoridad de Certificación como de Autoridad de Registro, mientras que la Política de Certificados es un documento que detalla las condiciones y reglas específicas para un tipo de certificado, según lo establecido en el Reglamento Parcial del Decreto Ley Sobre Mensajes de Datos y Firmas Electrónicas.

5.4.2 De igual manera, la Declaración de Prácticas de Certificación describe las medidas técnicas y de seguridad que se emplearan para la generación de los certificados electrónicos.

5.5 Consideraciones Específicas

5.5.1 La Declaración de Prácticas de Certificación y Políticas de Certificados deberán estar redactada en idioma castellano y no podrán utilizarse siglas o términos que no puedan ser interpretados por usuarios finales; en caso de ser éstos necesarios deben explicarse en un glosario.

5.5.2 La Declaración de Prácticas de Certificación y Políticas de Certificados debe estar conformada con los siguientes elementos:

1. DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN Y POLÍTICAS DE CERTIFICADOS DEL PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN

1.1PRESENTACIÓN

Está sección contemplará una introducción general del documento.

1.2 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

Se identificara el documento de la siguiente manera:

CAMPOS	CONTENIDO
Nombre del Documento	Declaración de Practicas de Certificación (DPC) y Política de Certificados (PC) del PSC
Versión del Documento	Permite identificar la cantidad de actualizaciones de la DPC y PC del PSC
Estado del Documento	Para identificar la aprobación o no de la DPC y PC del PSC
Fecha de Emisión	Fecha en que se emite el documento de la DPC y PC del PSC
Fecha de Expiración	Fecha en que expira el documento de la DPC y PC del PSC
Localización	Lugar en Internet desde donde se descarga la DPC y PC del PSC
Identificador único de objeto (OID)	Identificador único de la DPC y PC del PSC

1.3 COMUNIDAD DE USUARIOS Y APLICABILIDAD

Está sección incluirá las distintas entidades que cumplen roles con relación al certificado y cuya integración se encuentre prevista para el cumplimiento de la actividad de certificación.

1.3.1 Proveedor de Servicios de Certificación

Se identificara el Proveedor de Servicios de Certificación que

presente éste documento de Declaración de Prácticas de Certificación y Política de Certificados.

1.3.2 Autoridades de Registro (AR)

Se identificaran a las Autoridades de Registro utilizadas por el Proveedor de Servicios de Certificación en el proceso de recepción de solicitudes de emisión de certificados, identificación y autenticación de los solicitantes de certificados y recepción y validación de solicitudes de revocación.

1.3.3 Signatario

Se identificaran las personas físicas o jurídicas, equipamientos u aplicaciones que recibirán certificados emitidos por el Proveedor de Servicios de Certificación.

1.3.4 Terceros de buena fe

Se identificaran las personas que realicen transacciones utilizando certificados electrónicos provenientes del Proveedor de Servicios de Certificación y deciden aceptar y confiar en estos certificados.

1.4 USO DE LOS CERTIFICADOS

1.4.1 Usos permitidos

El PSC especificará los usos permitidos para los certificados que emite a sus signatarios

1.4.2 Usos no permitidos

Deberá especificar los usos no permitido de los certificados emitidos por el PSC.

1.5 POLÍTICAS DE ADMINISTRACIÓN DEL PSC

1.5.1 Especificaciones de la organización administrativa

Esta sección incluye información correspondiente a la organización responsable por el registro, mantenimiento y actualización de la DPC y PC, como son:

- Nombre de la Organización del PSC
- Correo electrónico
- Dirección de la organización
- Número telefónico

- Número de Fax
- Sitio Web de la organización

1.5.2 Persona Contacto

En está sección se incluirá el nombre de la autoridad responsable para el registro, mantenimiento de los Certificados Electrónicos e incluye lo siguiente:

- Nombre del Contacto
- Teléfonos
- Correo Electrónico
- Domicilio
- Fax
- Sitio de Internet

1.5.3 Competencia para determinar la adecuación de la DPC a las políticas.

El PSC especificara quién dentro de su organización es el responsable de la aplicabilidad de la DPC y PC.

2. PUBLICACIÓN DE INFORMACIÓN DEL PSC Y REPOSITORIOS DE LOS CERTIFICADOS

2.1 REPOSITORIOS

Se indicara la entidad o entidades que son responsables de los repositorios, indicando si el servicio es propio del certificado o está administrado por un proveedor independiente del mismo.

2.2 PUBLICACION

Debe indicar la información a ser publicada por el PSC en el repositorio, la forma, condiciones de accesibilidad y modalidades en que la misma se podrá a disposición de terceros.

2.3 FRECUENCIA DE PUBLICACIÓN

La publicación del certificado se realizará con anterioridad a su puesta en vigencia en el repositorio público del PSC.

Se debe garantizar su actualización inmediata después que la información a incluir se encuentre disponible. El periodo de validez es de quince (15) años. El PSC debe especificar la frecuencia de actualización del repositorio para:

2.3.1 Certificados del PSC

Determinar la frecuencia de publicación de:

- Sus propios certificados electrónicos.
- Información del estado de los certificados emitidos.
- Versiones anteriores y actualizadas de su DPC y PC
- Los datos de contacto del PSC
- Toda otra información considerada relevante referida a los certificados emitidos.

2.3.1Lista de Certificados Revocados (LCR)

Se debe establecer la periodicidad de la lista actualizada de los certificados revocados, que se encuentran en el repositorio del PSC.

2.3.2Declaración de Prácticas de Certificación y Políticas de Certificados

El PSC debe presentar la PC para cada tipo de certificado. El PSC debe publicar en el repositorio, las nuevas versiones de esta DPC y PC, en forma inmediata luego de su aprobación.

Se debe establecer la frecuencia de las versiones anteriores y actualidades de las Prácticas de Certificación y Política de Certificados que respalden la emisión de los certificados.

2.4 CONTROLES DE ACCESO AL REPOSITORIO DE CERTIFICADOS

Se deben incluir los controles y eventuales restricciones que se impondrán al acceso a la información publicada por el PSC.

Se debe garantizar la no imposición de restricciones al certificado del certificador, a la lista de certificados revocados, a la Política de Certificados correspondiente y a su manual de procedimientos, en sus versiones anteriores y actualizadas.

3. IDENTIFICACION Y AUTENTICACIÓN

Se describirán los procedimientos a utilizar para autenticar, como paso previo a la emisión de un certificado, la identidad y demás atributos del solicitante. Se deben establecer los medios admitidos para recibir los requerimientos de certificados y para comunicar su aceptación.

3.1 REGISTRO DE NOMBRES

3.1.1 Tipo de nombres

Se deben describir los tipos de nombres admitidos para los titulares de certificados emitidos en función de la Política de Certificados.

3.1.2 Necesidad de que los nombres sean significativos

Se deben describir las distintas denominaciones que se utilicen para cada tipo de certificado, debiendo utilizarse como mínimo los parámetros establecidos en la normativa especifica establecida por SUSCERTE para tal fin (Norma SUSCERTE N° 032)

3.1.3 Interpretación de formatos de nombres

Se incluirán las reglas para interpretar las distintas clases de nombres admitidas por la Política de Certificados.

3.1.4 Unicidad de nombres

Deben especificarse que el nombre distintivo debe ser único a cada suscriptor (puede haber más de un certificado con igual nombre distintivo si corresponde al mismo suscriptor).

3.1.5 Resolución de Conflictos relativos a nombres

En está sección el Proveedor de Servicios de Certificación puede reservarse el derecho de tomar todas las decisiones referidas a posibles conflictos sobre la utilización de nombres entre sus suscriptores conforme su normativa al respecto. En caso de conflicto, la parte que solicite debe demostrar su interés legítimo y su derecho a la utilización de un nombre en particular.

3.2 VALIDACION INICIAL DE LA IDENTIDAD

3.2.1 Método de prueba de posesión de la clave privada

Se indican los procedimientos que implementará el Proveedor de Servicios de Certificación para asegurar que el solicitante se encuentra en posesión de la clave privada correspondiente a la clave pública remitida con el requerimiento del certificado electrónico, de acuerdo a protocolos de seguridad adecuados y que dicha clave privada es para firmar un documento electrónico.

3.2.2 Autenticación de la identidad de la organización

Se deben describir los procedimientos de autenticación de la identidad de los titulares o responsables de los certificados de personas jurídicas, debiendo indicarse:

1.El requerimiento debe efectuarse únicamente por intermedio de un representante autorizado a actuar en nombre del signatario.

2. EL Proveedor de Servicios de Certificación debe verificar la identidad del representante del suscriptor y su autorización para utilizar las claves criptográficas en su nombre. La verificación se efectuará, mediante la revisión de los siguientes documentos que deben ser presentados por el signatario:

a.Copia Certificada del Acta Constitutiva o Estatutos del solicitante para el caso de personas jurídicas.

b.Copias Certificadas de Actas de Asambleas Ordinarias y extraordinarias celebradas por el solicitante o Poderes en los que conste la designación del o los representantes legales y la legitimidad para actuar en nombre del solicitante.

3. Se requiere información de registros oficiales o contratar los servicios de terceros a fin de efectuar la verificación mencionada.

3.2.3 Autenticación de la identidad de Personas Naturales

Se especifican los procedimientos de autenticación de la identidad de los titulares de los certificados de personas naturales, debiendo indicarse como mínimo:

- De poseer nacionalidad venezolana, se requerirá Cedula de Identidad.
- De tratarse de extranjeros, se solicitará Pasaporte válido, en caso de no poseer Cedula de Identidad.

En todos los casos, se establecerá la obligatoriedad de la conservación de la documentación que respalda el proceso de autenticación por parte del PSC.

3.2.4 Comprobación de las facultades de representación

La comprobación de la representación ante el PSC se debe realizar mediante la comprobación de un documento legal, que lo califique como representante legal.

3.3 IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE RENOVACIÓN DE LA CLAVE

3.3.1 Generación de nuevo Par de Claves (Re Key)

Especificar los procedimientos de identificación y autenticación a seguir para la generación de un nuevo par de claves y su correspondiente certificado previo a la expiración del certificado vigente. Este método de renovación requiere que la clave privada no este ni vencida ni revocada.

3.3.2 Generación de Nuevo Certificado (Posterior a Revocación)

Establecer los procedimientos a seguir para validar la identidad del solicitante del nuevo certificado cuando el anterior hubiera sido renovado.

La solicitud de un nuevo certificado exige el cumplimiento de idénticos procedimientos a lo previstos para el proceso de registro inicial.

El certificado debe controlar la existencia y validez del certificado y que la información utilizada para verificar la identidad y atributos del titular.

Si algunos de los términos y condiciones del certificado han cambiado, deben ser comunicados al suscriptor y esté debe expresar su consentimiento a los mismos.

Si alguna información relativa al suscriptor ha sido cambiada debe ser verificar, registrada y acordada con el mismo.

El Proveedor de Servicios de Certificación sólo debe emitir un nuevo certificado utilizado una clave pública existente si no hay evidencia de que la correspondiente clave privada ha sido comprometida y el período de vida del par de claves no ha sido expirado.

3.4 IDENTIFICACIÓN Y AUTENTICACIÓN DE LAS SOLICITUDES DE REVOCACIÓN DE LA CLAVE

Incluyen los procedimientos a seguir para validar la identidad del solicitante de la revocación de un certificado, incluyendo la documentación del proceso.

La AC del PSC puede solicitar de oficio la revocación de un certificado si tiene el conocimiento o sospecha del compromiso de la

clave privada del suscriptor o cualquier otro hecho que recomiende emprender dicha acción.

4. EL CICLO DE VIDA DE LOS CERTIFICADOS (REQUERIMIENTOS OPERATIVOS)

4.1 SOLICITUD DE CERTIFICADOS

Incluyen los requerimientos y procedimientos operativos establecidos por la Autoridad de Certificación para recibir los requerimientos de certificados. Estos procedimientos deben ser cumplidos por los Proveedores de Servicios de Certificación y por los solicitantes de certificados.

Adicionalmente, en está sección deben incluirse una descripción de los procedimientos utilizados para comprobar que el suscriptor se encuentra en poder de la clave privada correspondiente a la clave pública presentada para la generación del certificado.

Los procedimientos deben establecer que los requerimientos solo podrán ser iniciados por el suscriptor o por el representante autorizado de la persona jurídica solicitante.

4.1.1 Proceso de generación de la solicitud de certificados y responsabilidades

Se deberán establecer los requerimientos y procedimientos referidos a la generación de solicitud de certificados y sus responsables

4.1.2 Proceso de firma del certificado

Se deberán describir los procedimientos operativos establecidos por el PSC para efectuar la firma del certificado

4.1.3 Proceso de generación de la solicitud de renovación de las claves del certificado

Se deberán incluir los procedimientos a seguir por el PSC para la generación de una solicitud de renovación de las claves del certificado

4.1.4 Procedimiento para realizar una solicitud de renovación de un certificado

Se deberán especificar los procedimientos del PSC para realizar una solicitud de renovación de un certificado

4.1.5 Procedimiento para realizar una solicitud de suspensión de un certificado

Se deberán definir los procedimientos del PSC para realizar la solicitud de suspensión de un certificado

4.2 TRAMITACIÓN DE SOLICITUD DE UN CERTIFICADO

4.2.1 Realización de las funciones de identificación y autenticación

Se deberán especificar las funciones de identificación y autenticación que realizan los funcionarios y personal encargado de las Autoridades de Registro.

Estos funcionarios que desempeñan el rol de operador de registro, deben disponer 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.

4.2.2 Aprobación o denegación de un certificado

Se deberán determinar los procesos de aprobación o denegación de las solicitudes de certificación para aquellos solicitantes que cumplan con todos los requisitos y lineamientos económicos y legales exigidos.

4.2.3 Plazo para la tramitación de un certificado

Se deberán definir el tiempo máximo del PSC para la expedición de un certificado electrónico.

4.3 EMISIÓN DE CERTIFICADOS

Se deberán establecer los requerimientos y procedimientos establecidos por los Proveedores de Servicios de Certificación para la emisión del certificado y para la notificación de dicha emisión al solicitante.

4.3.1 Acciones del PSC durante la emisión de un certificado

Se deberán incluir los procedimientos a efectuar durante la emisión de un certificado electrónico.

4.3.2 Notificación al solicitante por parte del PSC acerca de la emisión de su certificado electrónico.

Se deberán definir los procedimientos del PSC para notificar al solicitante sobre la emisión de su certificado.

4.4 ACEPTACIÓN DE CERTIFICADOS

Se deberán establecer los requerimientos y procedimientos referidos a la publicación del certificado y a la aceptación del mismo por su titular.

4.4.1 Forma en la que se acepta el certificado

Se deberán definir los procedimientos establecidos para la aceptación del certificado por el solicitante

4.4.2 Publicación del certificado

Se deberán determinar los diversos medios que se utilizan para publicar un certificado

4.4.3 Notificación de la emisión del certificado a otras autoridades

Se deberán incluir los procedimientos establecidos para notificar a las entidades, organismos del gobierno, personas naturales y empresas privadas de la emisión del certificado en caso que aplique.

4.5 USO DE PAR DE CLAVES Y DEL CERTIFICADO

Se deberán establecer los procedimientos referidos al uso de los certificados emitidos del PSC

4.5.1 Uso de la clave privada del certificado

Se describirá la responsabilidad de usar apropiadamente la clave privada y el certificado, autorizados en esta DPC y en consistencia con el contenido aplicable del certificado. El uso del certificado deben estar conforme a los términos acordados por el suscriptor

4.5.2 Uso de la clave pública y del certificado por los terceros de buena fe

Se describirá la responsabilidad de los terceros de buena fe para el uso de los certificados.

4.6 RENOVACIÓN DEL CERTIFICADO

Se describirán los elementos relacionados con la renovación del certificado. La renovación del certificado significa la emisión de un nuevo certificado al suscriptor sin modificar el suscriptor, o ninguna otra información en el certificado

4.6.1 Causas para la renovación

Se determinarán las circunstancias bajo las cuales ocurre la renovación del certificado

4.6.2 Entidad que puede solicitar la renovación de un certificado

Se definirá que entidad esta autorizada para renovar un certificado del usuario

4.6.3 Procedimiento de solicitud para la renovación de un certificado

Se establecerán los procedimientos de las entidades autorizadas para efectuar la solicitud de renovación de un certificado

4.6.4 Notificación de la emisión de un nuevo certificado

Se determinará el proceso para notificar al suscriptor la emisión del nuevo certificado

4.6.5 Publicación del certificado renovado por el PSC

Se determinara el proceso del PSC para publicar el nuevo certificado

4.6.6 Notificación de la emisión del certificado a otras entidades

Se establecerá el procedimiento del PSC para notificar a otras entidades sobre la emisión del certificado nuevo en caso que aplique.

4.7 NUEVA CLAVE DEL CERTIFICADO

Se describirán los elementos relacionados con el suscriptor que genera un nuevo par de claves y solicita la emisión de un nuevo certificado para esta clave pública

4.8 MODIFICACIÓN DE CERTIFICADOS

Establecer los procesos relacionados con la emisión de un nuevo certificado por motivo de cambios en la información del certificado con excepción de la clave pública del suscriptor, como son:

- Causas por las cuales la modificación puede ocurrir
- Quién puede solicitar la modificación del certificado
- Notificación del certificado nuevo al suscriptor
- Conducta que constituye la aceptación del certificado
- Publicación del certificado por parte del AC del PSC
- Notificación de la emisión del certificado por parte del AC del PSC a

otras entidades

4.9 REVOCACIÓN Y SUSPENSIÓN DE UN CERTIFICADO

En está sección se especificarán los procedimientos del PSC para asegurar que los certificados sean revocados de una manera oportuna, basadas en una solicitud de revocación de certificado autorizada y validada.

4.9.1 Circunstancias para la Revocación del certificado del signatario.

Se indicarán las circunstancias bajo las cuales un certificado podrá ser revocado y aquellos casos en los cuales la revocación deberá ser obligatoria, conteniendo como mínimo una descripción detallada de:

- Las obligaciones establecidas en el artículo 11 del Reglamento Parcial del Decreto Ley Sobre Mensaje de Datos y Firmas Electrónicas.

Así mismo se especificará el plazo en que un Proveedor de Servicios de Certificación deberá revocar, todo certificado que deje de cumplir con las Políticas y Normas y el Decreto-Ley Sobre Mensaje de Datos y Firmas Electrónicas.

4.9.2 Entidad que puede solicitar la Revocación

Se especifican quienes son las personas autorizadas para solicitar la revocación de un certificado, debiendo admitirse como mínimo:

1. Al titular del certificado.
2. Al responsable autorizado que efectuar el requerimiento, en el caso de certificados de personas jurídicas.
3. A la persona jurídica titular del certificado a través de un funcionario debidamente autorizado.
4. A aquellas personas habilitadas por el titular de certificado a tal fin.
5. A la autoridad judicial competente.

4.9.3 Procedimientos de Solicitud de la Revocación

Se describirán los procedimientos establecidos por los Proveedores de Servicios de Certificación para la revocación de los certificados que emita. Se garantizara que los

procedimientos de revocación se encontrarán disponibles en su correspondiente Política de Certificados, a disposición de los autorizados en el apartado anterior.

Se debe garantizar lo siguiente:

1.El solicitante de la revocación será debidamente identificado

2.Las solicitudes de revocación, así como toda acción efectuada por los Proveedores de Servicios de Certificación, serán documentadas y conservadas en sus archivos.

3.La documentación y el archivo de las justificaciones de las revocaciones aprobadas.

4.Una vez efectuada la revocación, se actualizará el estado del certificado en el repositorio y se generara y publicará la nueva lista de certificados revocados.

5.El suscriptor del certificado revocado debe ser informado del cambio de estado de su certificado.

Deberán indicarse las vías de contacto disponible para la realización de la solicitud de revocación.

4.9.4 Límites del período de la Solicitud de Revocación

Se especificará que la solicitud de revocación debe efectuarse en forma inmediata cuando se presente alguna de las circunstancias previstas en el apartado 4.4.1. Para los plazos de revocación de los certificados, luego de recibida la solicitud, puede elegirse entre éstas dos opciones, en función del tipo de certificado y el modelo adoptado por el Proveedor de Servicios de Certificación.

Opción 1: El párrafo siguiente puede variar entre políticas de certificados.

El plazo máximo entre la recepción de la solicitud y el cambio de la información de estado del certificado, indicando la revocación, puesta a disposición de los terceros usuarios debe ser a lo sumo de cuatro (4) horas.

Opción 2: El párrafo siguiente puede variar entre políticas de certificados.

El plazo máximo entre la recepción de la solicitud y el cambio de la información de estado del certificado, indicando la revocación, puesta a disposición de los terceros usuarios debe ser a lo sumo de ocho (8) horas.

Se establecerán en éste documento que los Proveedores de Servicios de Certificación serán responsables de la Política de Certificados y deberán responder plenamente por los daños causados por el uso de un certificado en el periodo transcurrido entre la recepción de la solicitud de revocación y la publicación de la lista de certificados revocados.

4.9.5 Circunstancias para la Suspensión

Se especificarán los motivos para solicitar la suspensión de un certificado, de ser aplicable.

4.9.6 Entidad que puede solicitar la Suspensión

Se definen quienes son las personas autorizadas para solicitar la suspensión de un certificado, de ser aplicable.

4.9.7 Procedimientos para la Solicitud de Suspensión

Se especifican los procedimientos necesarios para solicitar la suspensión de un certificado, de ser aplicable.

4.9.8 Límites del Período de Suspensión de un Certificado

Se especificará el límite máximo de tiempo durante el cual un certificado podrá estar suspendido, de ser aplicable.

4.9.9 Frecuencia de Emisión de Listas de Certificados Revocados

Se definirá la frecuencia con que se emitirá la lista de certificados revocados con relación a la Política de Certificados. Para los plazos de emisión de lista de certificados luego de recibida la solicitud puede elegirse entre éstas dos opciones, en función del tipo de certificado y el modelo adoptado por el Proveedor de Servicios de Certificación.

Los siguientes plazos deben ser respetados por los Certificadores:

Opción 1: El párrafo siguiente puede variar entre políticas de certificados.

Para aquellas políticas de certificación correspondientes a certificados de personas físicas, personas jurídicas u Organismos Públicos las Listas de Certificados Revocados deben emitirse como mínimo cada cuatro (4) Horas.

Opción 2: El párrafo siguiente puede variar entre políticas de certificados.

Para aquellas políticas de certificación correspondientes a certificados de personas físicas, personas jurídicas u Organismos Públicos las Listas de Certificados Revocados deben emitirse como mínimo cada ocho (8) Horas.

4.9.10 Requisitos para la comprobación de la Lista de Certificados Revocados

Se establecerán los mecanismos ofrecidos para validar el estado de los certificados, mediante el control de la lista de certificados revocados, a menos que utilicen otro sistema con características de seguridad y confiabilidad al menos equivalente.

Así mismo, se especificarán los mecanismos para verificar la autenticidad y validez de la lista de certificados revocados.

Para aquellas políticas de certificación correspondientes a los certificados de AC, las Listas de Certificados Revocados deben emitirse como mínimo cada treinta (30) días.

4.9.11 Disponibilidad de comprobación en Línea del Servicio de Revocación del Estado del Certificado

Se establecerá si los Proveedores de Servicios de Certificación poseen disponible un servicio de revocación de certificados en línea y de verificación de su estado. La verificación del estado de un certificado podrá efectuarse directamente ante los Proveedores de Servicios de Certificación por medio del acceso a la lista de certificados revocados o de otros medios de verificación de estado en línea.

Los Proveedores de Servicios de Certificación deben poner a disposición de los terceros usuarios:

1. La información relativa a las características operacionales de los servicios de verificación de estado.
2. La disponibilidad de tales servicios y cualquier políticas aplicable en caso de no disponibilidad.
3. Cualquier característica opcional de tales servicios.

4.9.12 Requisitos de comprobación en Línea del Estado de Revocación

Se definirán los requisitos para la verificación en línea de la información de revocación de certificados por parte de los

terceros.

4.9.13 Otras Formas Disponibles para la Divulgación de la Revocación

Se definirá, de existir, otras formas utilizadas por los Proveedores de Servicios de Certificación para divulgar la información sobre revocación de certificados.

4.9.14 Requisitos para la Verificación de Otras Formas de Divulgación de Revocación

Se definirán los requisitos para la verificación por parte de los terceros, de las formas de divulgación de revocación de certificados prevista en el apartado anterior.

4.9.15 Requisitos Específicos para Casos de Compromiso de Claves

Se establecerán los requisitos específicos aplicables a la revocación de certificados provocada por el compromiso de la correspondiente clave privada. En tal caso, se exige que el titular del certificado comunique de inmediato tal circunstancia al Proveedor de Servicios de Certificación.

4.10 SERVICIO DE COMPROBACIÓN DE ESTADO DE CERTIFICADOS

4.10.1 Características operativas

Determinar las características operativas de los servicios de comprobación de los certificados

4.10.2 Disponibilidad del servicio

Establecer los compromisos de disponibilidad del servicio de comprobación del estado de los certificados

4.10.3 Características adicionales

Establecer otras características adicionales sobre el servicio de comprobación del estado de los certificados

4.11 FINALIZACIÓN DE LA SUSCRIPCIÓN

Describir los casos en que finaliza la suscripción de un certificado

4.12 CUSTODIA Y RECUPERACIÒN DE LA CLAVE

4.12.1 Prácticas y políticas de recuperación de la clave

Describir las prácticas y políticas establecidas para el servicio

de custodia y recuperación de la clave privada

5. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES

Se describirán brevemente los procedimientos referidos a los controles de seguridad física, funcionales y de personal implementados por los Proveedores de Servicios de Certificación.

5.1 CONTROLES DE SEGURIDAD FÍSICA

Se incluirán en está sección los siguientes aspectos:

5.1.1 Construcción y localización de instalaciones.

Determinar los procedimientos sobre las medidas de seguridad de protección de las instalaciones.

5.1.2 Acceso Físico.

Se determinarán los procedimientos de control para acceder a las instalaciones del PSC

5.1.3 Alimentación Eléctrica y Aire Acondicionado.

Se establecerán los mecanismos para asegurar el suministro de energía eléctrica y el correcto funcionamiento y mantenimiento de los sistemas de aire acondicionado.

5.1.4 Exposición al agua.

Se establecerán los mecanismos instalados en la AC del PSC para evitar las exposiciones al agua de las instalaciones

5.1.5 Prevención y protección contra incendios.

Se definirán los mecanismos con que cuenta la AC del PSC para la protección y prevención de incendios

5.1.6 Sistemas de almacenamiento.

Se establecerán los mecanismos de almacenamiento de información relacionada con la AC del PSC

5.1.7 Eliminación de residuos.

Se establecerán los mecanismos de la AC del PSC para verificar todos los materiales desechables donde se almacena información sensible.

5.1.8 Almacenamiento de copias de seguridad

Se establecerá el procedimiento de almacenamiento de copias de seguridad en sitios externos.

5.2 CONTROLES DE PROCEDIMIENTOS

5.2.1 Definición de roles confiables

Se definirá la descripción del personal que por sus responsabilidades son sometidos a procedimientos de control en la AC del PSC

5.2.2 Separación de funciones

Se determinará la separación de funciones en cuanto a los roles que no pueden ser ejecutados por la misma persona

5.2.3 Número de personas requeridas por rol

Se determinarán las responsabilidades compartidas entre los distintos roles y personas

5.2.4 Identificación y autenticación para cada rol

Se determinará el proceso de identificación y autenticación de cada rol

5.3 CONTROLES DE SEGURIDAD PERSONAL

Se especificarán los controles implementados sobre los siguientes aspectos:

5.3.1 Requerimientos de antecedentes, calificación, experiencia y acreditación

Se describirán los antecedentes laborales, calificaciones, experiencia e idoneidad del personal tanto de aquellos que cumplen funciones críticas como de aquellos que cumplen funciones administrativas, seguridad, limpieza, etc.

5.3.2 Requerimientos de formación

Se describirá el entrenamiento y capacitación inicial requerida para el cargo del personal calificado

5.3.3 Requerimientos y frecuencia de actualización de la formación

Se describirá la frecuencia de los procesos de actualización técnica o profesional

5.3.4 Frecuencia y secuencia de rotación de tareas

Se describirá la frecuencia y secuencia con que se rotan las tareas de cada uno de los cargos

5.3.5 Sanciones por acciones no autorizadas

Se definirá el procedimiento sancionador para los empleados que incumplen un acción no autorizada

5.3.6 Documentación proporcionada al personal

Se determinará la documentación proporcionada a los empleados para el desempeño de sus tareas

5.4 PROCEDIMIENTOS DE CONTROL DE SEGURIDAD

Se incluye en esta sección temas vinculantes a los PSC

5.4.1 Tipos de eventos registrados

Se establecerán los tipos y procesos por las cuales se registran los logs de auditoria

5.4.2 Frecuencia de procesamiento de los registros de los logs de auditoria

Se determinará la frecuencia de procesamiento y archivo de los logs de auditoria

5.4.3 Períodos de retención de los logs de auditoria

Se establecerá el período de conservación de los logs de auditoria

5.4.4 Protección de los logs de auditora

Se describirán los métodos de protección contra borrado o modificación de los logs de auditoria

5.4.5 Procedimiento de Backup de los logs de auditoria

Se determinará el procedimiento de resguardo de los logs de auditoria

5.4.6 Sistema de recopilación de información de auditoria

Se definirá el sistema de recolección de datos de auditoria

5.4.7 Notificación de eventos significativos

Se establecerán el procesos de notificación de los eventos significativos

5.4.8 Análisis de vulnerabilidades

Se determinarán los procesos de análisis y gestión de las vulnerabilidades registradas

5.5 ARCHIVO DE INFORMACIONES Y REGISTROS

Se incluirán información referida a los siguientes procedimientos de resguardo de archivos

5.5.1 Tipos de registros archivados

Se determinarán los diferentes tipos de registros archivados

5.5.2 Período de retención de un archivo

Se establecerá el período de conservación de los archivos y registros

5.5.3 Método de protección del archivo

Se establecerá el método por el cual se protegen los archivos contra borrado o modificación y quién puede ver el archivo, obsolescencia de hardware, deterioro del medio por el cual el archivo es almacenado

5.5.4 Requerimiento para el sellado de tiempo de archivos

Se definirán los requisitos para la incorporación del sellado electrónico en los archivos de registros

5.5.5 Procedimientos de backup del archivo

Se establecerán el procedimiento de resguardo de los archivos

5.5.6 Sistema de repositorios de archivos (interno y externo)

Se definirán los medios por las cuales se realiza el repositorio de los archivos

5.5.7 Procedimiento para obtener y verificar información de archivos

Se establecerá el proceso requerido para obtener información de archivos de datos para llevar a cabo verificaciones de integridad.

5.6 CAMBIO DE CLAVE

Se incluirán los procedimientos a seguir para distribuir una nueva clave pública a los usuarios de un certificado luego de un cambio de la misma. Dichos procedimientos pueden ser los mismos que fueron utilizados para distribuir la clave que se reemplaza. La nueva clave puede ser incluida en un certificado firmado electrónicamente con la clave reemplazada.

5.7 PLAN DE RECUPERACIÓN EN CASO DE DESASTRES

Se describirán los requisitos y procedimientos relativos a la recuperación de recursos de los PSC en caso de compromiso de la clave privada o desastres

5.7.1 Procedimientos de gestión de incidentes y vulnerabilidades

Se describirán los procedimientos para establecer un Plan de Continuidad que defina las acciones a realizar, recursos a utilizar y personal a emplear en caso de ocurrir un acontecimiento intencionado o accidental que utilice o degrade los recursos y servicios de certificación prestados por la AC del PSC

5.7.2 Alteración de los recursos hardware, software y/o datos

Se establecerán los procedimientos de recuperación ante compromiso o sospecha de alteración de los recursos de hardware, software y datos

5.7.3 Procedimiento de actuación ante la vulnerabilidad de la clave privada del PSC

Se establecerá el procedimiento de recuperación ante compromiso o sospecha de compromiso de la clave privada del PSC

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

Se incluirá el procedimiento de continuidad de las operaciones en un entorno seguro luego de ocurrir un desastre natural o de otra naturaleza

5.8 CESE DE LAS ACTIVIDADES DEL PSC

Se describen los procedimientos a ser adoptados en caso de finalización de servicios de los Proveedores de Servicios de Certificación.

Se especifican los procedimientos referidos a:

a) Notificación a SUSCERETE, los titulares, terceros usuarios, otros Proveedores de Servicios de Certificación y otros usuarios vinculados.

b) Revocación del certificado de Proveedor de Servicios de Certificación y de los certificados emitidos a otras AC y signatarios.

c)Transferencia de la custodia de archivos y documentación.

Se establecerá que el responsable de la custodia de archivos y documentación cumplirá con idénticas exigencias de seguridad que las revistas para los Proveedores de Servicios de Certificación discontinuado.

6. CONTROLES DE SEGURIDAD TÉCNICA

Se describirán las medidas de seguridad implementada por los Proveedores de Servicios de Certificación para proteger sus claves criptográficas y otros parámetros de seguridad críticos. Además se incluirá los controles técnicos que se implementaran sobre las funciones operativas de la Autoridad de Certificación, Autoridades de Registro, repositorios, suscriptores, etc.

6.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

La generación e instalación del par de claves debe ser considerado desde la perspectiva de la Autoridad de Certificación, de los repositorios, de las Autoridades de Registro y de los suscriptores. Para cada una de estas entidades deberán abordarse los siguientes temas:

a)Responsables de la generación de claves.

b)Métodos de generación de claves, indicando si las mismas se efectuaran por software o por hardware.

c)Métodos de distribución de la clave pública del Proveedor de Servicios de Certificación en forma segura.

d)Características y tamaño de las claves y controles efectuados sobre las mismas.

e)Propósitos para los cuales pueden ser utilizadas las claves y restricciones para dicha utilización.

6.1.1 Generación del par de claves

Se definirán todos los aspectos relativos a la generación del par de claves de los certificado definidos en las Políticas de Certificados, del par de claves de los responsables de las Autoridades de Registro, de los servicios de información de estado de certificados, suscriptores, etc.

Deben considerarse los siguientes requerimientos mínimos:

a) El par de claves debe ser generado únicamente por el titular del certificado, permaneciendo su clave privada en todo momento bajo su absoluto y exclusivo control.

b) El medio de generación y almacenamiento de la clave privada debe asegurar que: La clave privada sea única y su confidencialidad se encuentre debidamente garantizada.

6.1.2 Entrega de la Clave Privada al suscriptor

Deben considerarse obligatoriamente las exigencias reglamentarias impuestas por la obligación de abstenerse de generar, exigir o por cualquier otro medio tomar conocimientos o acceder a la clave privada de los subscriptores.

6.1.3 Entrega de la Clave Pública al emisor del certificado

Se establecen los procedimientos utilizados para la entrega de la clave pública del titular del certificado al Proveedor de Servicios de Certificación responsable de la emisión del certificado.

6.1.4 Disponibilidad de la Claves Pública del PSC para los usuarios

Se definirán los medios adoptados para poner el certificado del Proveedor de Servicios de Certificación, y el resto de los certificados que compongan su cadena de certificación, a disposición de todos los suscriptores y tercera partes interesadas.

6.1.5 Tamaño de las Claves

Se definirán los tamaños mínimos de las claves criptográficas asociadas con los certificados emitidos según la Política de Certificados.

Deben respetarse las siguientes longitudes mínimas de claves:

a) Para certificados de los Proveedores de Servicios de Certificación o de información de estado de certificados: 4096 bits.

b) Para certificados utilizados en servicios relacionados a la firma electrónica (certificación de hora digital, almacenamiento seguro de documentos electrónicos, etc.): 2048 bits.

c) Para certificados de responsables de Autoridades de Registro que sean utilizados para aprobar solicitudes,

renovaciones, revocaciones, etc.:2048 bits.

d) Para certificados de usuario (personas físicas o jurídicas): 1024 bits en software y 2048 bits en hardware.

6.1.6 Parámetros de generación de la clave pública y verificación de la calidad

Se deben describir los parámetros de generación de claves asimétricas y los procedimientos de verificación utilizados respecto de la calidad de los parámetros de generación de claves

6.1.7 Generación de claves por hardware y software

Se deberá describir el tipo de soporte utilizado para la generación de claves.

Deben respetarse las siguientes exigencias mínimas:

a) Las claves criptográficas de la Autoridad de Certificación deben ser generadas por dispositivos homologados FIPS 140-2 nivel 3 ó equivalentes.

b) Las claves criptográficas utilizadas para la firma de información de estado de certificados o servicios relacionados a la firma electrónica deben ser generadas en dispositivos FIPS 140-2 nivel 3 o equivalente.

c) Las claves criptográficas que los usuarios responsables de la Autoridad de Registro utilicen para aprobar solicitudes, renovaciones, revocación, etc., deben ser generadas en dispositivos FIPS 140-2 nivel 2 o equivalente.

6.1.8 Propósito de utilización de la clave privada

Se establecerán los propósitos para los cuales se utilizaran las claves criptográficas de los titulares de los certificados (por ejemplo autenticación, integridad, no repudio) y las posibles restricciones en su uso.

6.2 PROTECCIÓN DE LA CLAVE PRIVADA

En está sección la protección de la clave privada debe ser considerada desde la perspectiva de la Autoridad de Certificación, de lo repositorios, de las Autoridades de Registro y de los suscriptores. Para cada una de estas entidades deberán abordarse los siguientes temas:

a) Estándares utilizados para la generación del par de claves.

b) Número de personas involucradas en el control de la clave

privada.

c) De existir copias de resguardo de la clave privada, controles de seguridad establecidos sobre las misma.

d) De encontrarse archivada la clave privada en un módulo criptográfico.

e) Responsable de activación de la clave privada y acciones a realizar para su activación.

f) Duración del período de activación de la clave privada y procedimientos a utilizar para su desactivación.

g) Procedimiento de destrucción de la clave privada.

6.2.1 Estándares para Módulos Criptográficos

Se describen los estándares utilizados para los módulos de generación y almacenamiento de claves criptográficas.

Deben respetarse las siguientes exigencias mínimas:

a) Las claves criptográficas de la Autoridad de Certificación deben ser generadas y almacenadas en dispositivos homólogos FIPS 140-2 nivel 3 equivalentes.

b) Las claves criptográficas utilizadas para la firma de información de estado de certificados o servicios relacionados a la firma electrónica deben ser generadas y almacenadas en dispositivo FIPS 140-2 nivel 3 o equivalentes.

c) Las claves criptográficas que los usuarios responsables de la Autoridad de Registro utilicen para aprobar solicitudes, renovación, revocaciones, etc. Deben ser generadas y almacenadas en dispositivos FIPS 140-2 nivel 2 ó equivalentes.

6.2.2. Control de “N de M” de la Clave Privada

Se describen los controles empleados para la actividad de las claves, indicando cuantas personas están involucradas en el control de dicha clave.

Deben respetarse las siguientes exigencias mínimas:

- El control de la utilización de las claves criptográficas de la Autoridad de Certificación debe estar dividido de forma tal que sea necesaria la presencia de al menos 2 personas distintas (o N distintas de un total de M posibles, con N≥2).

Por ejemplo puede requerirse la presencia de al menos dos administradores de un grupo de tres para utilizar la clave de la AC.

6.2.3 Custodia de la Clave Privada

Se describen los procedimientos empleados por los PSC para la recuperación de sus propias claves.

6.2.4 Copia de seguridad de la Clave Privada

Se describirán en está sección los procedimientos y controles de seguridad empleados para la realización de copias de seguridad de las claves

En todos los casos deben establecerse procedimientos que garanticen que los niveles de seguridad de las claves no disminuyan por la creación de copias de resguardo. La Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) no se hará responsable del resguardo de las claves.

6.2.5 Archivo de la Clave Privada

Se describirán en está sección los procedimientos y controles de seguridad empleados para el archivo de las claves privadas de los Proveedores de Servicios de Certificación.

En todos los casos deben establecerse procedimientos que garanticen que los niveles de seguridad de las claves no disminuyan por le proceso de archivo.

6.2.6 Inserción de claves privadas en módulos criptográficos

Se establecerán los requisitos para la inserción o extracción de la clave privada del titular en el modulo criptográfico, describiendo bajo que circunstancia se puede realizar la operación, a quienes les esta permitido realizar la operación y cual es el formato de la clave privada utilizado durante la transferencia.

6.2.7 Método de activación de la Clave Privada

Se describirán los requisitos y procedimientos necesarios para la activación de la clave privada del Proveedor de Servicios de Certificación.

Se exigirá la autenticación de los responsables a través de métodos adecuados.

6.2.8 Método de desactivación de la Clave Privada

Se describirán los requisitos y procedimientos necesarios para la desactivación de la clave privada del Proveedor de Servicios de Certificación.

Se exigirá la autenticación de los responsables a través de métodos adecuados.

6.2.9 Método de Destrucción de la Clave Privada

Se especificarán en está sección los procedimientos a seguir para la destrucción de la clave privada y de sus copias de seguridad ante cualquier hecho que motivara el final de la vida útil de un certificado, tales como su revocación o expiración.

Se definirán los responsables de la destrucción, formas de autenticación, y acciones a desarrollar.

6.3 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

6.3.1 Archivo de la clave pública

Se describen en está sección los procedimientos y controles de seguridad implementados para el sistema de archivo de la clave pública, el software y hardware necesarios a preservar como parte de dicho archivo para permitir la utilización de la clave pública en el tiempo y la duración en el tiempo que se mantendrá archivada la información.

Está sección no se delimita a describir la utilización de firmas electrónicas con el archivo de datos, si no que debe dirigirse, además, a los controles de integridad utilizados para impedir la adulteración de datos (no para verificar su adulteración).

6.3.2 Períodos operativos de los certificados y periodos de Uso para el par de Claves Pública y Privada

Se debe determinar que las claves privadas correspondientes a los certificados emitidos por el Proveedores de Servicios de Certificación podrán ser utilizadas por su titular únicamente durante el periodo de validez de los mismos. Las correspondientes claves públicas podrán ser utilizadas durante el periodo por las normas legales vigentes, a fin de posibilitar

la verificación de las firmas generadas durante su periodo de validez, según se establece en el apartado anterior.

6.4 DATOS DE ACTIVACIÓN

Se establecerán medidas de seguridad para proteger los datos de activación requeridos para la operación de los módulos criptográficos para todos los usuarios de certificados.

6.4.1 Generación e Instalación de Datos de Activación

Se especificará en está sección el resguardo de los datos de activación de la clave privada de los titulares de certificados sean únicos y aleatorios.

6.4.2 Protección de Datos de Activación

Se especificarán en está sección los procedimientos a seguir para la adecuada protección de activación de la clave privada de los titulares de certificados contra usos no autorizados.

6.4.3 Otros Aspectos Referidos a los Datos de Activación

Se incluirá otros aspectos relativos a los controles sobre los datos de activación, tales como los referidos a las claves incluidos en los apartados 6.1 a 6.3.

6.5 CONTROLES DE SEGURIDAD DEL COMPUTADOR

6.5.1 Requisitos técnicos específicos

Se establecerán los requisitos de seguridad referidos al equipamiento de los Proveedores de Servicios de Certificación.

Los requisitos mínimos serán:

a) Control de acceso a los servicios y roles de certificación.

b) Separación de funciones para los roles de certificación.

c) Identificación y autenticación de los roles de certificación.

d)Re-utilización o separación para memoria de acceso aleatorio.

e)Utilización de criptografía para las sesiones de comunicación y bases de datos.

f) Archivo de datos históricos y de auditoria del Proveedor de Servicios de Certificación y usuarios.

g) Auditoria de eventos de seguridad.

h)Auto-testing de seguridad relativa a servicios de certificación.

i)Caminos confiables para identificación de roles de certificación.

a)Mecanismos de recuperación para claves y sistemas de certificación

Las funcionalidades mencionadas pueden ser provistas por el sistema operativo, o bien a través de una combinación del sistema operativo, software de certificación y controles físico.

6.5.2 Calificaciones de Seguridad Informática

Se describirán en está sección los resultados de evaluaciones realizadas por terceros respecto a la seguridad informática.

6.6 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

Se especificará en está sección el software específico para la utilización de los certificados emitidos, se describirán los controles de seguridad implementados sobre dicho software.

6.6.1 Controles de Desarrollo de Sistemas

Desarrollo de Software: Se especificará en esta sección la metodología para el diseño y desarrollo del software. El software de certificación debe ser objeto de verificación por un tercero.

Adquisición de Software: Se especificará en esta sección el diseño de los módulos y partes del software.

Software a la medida: Se especificara en esta sección el diseño y desarro0llo del mismo.

6.6.2 Controles de Administración de Seguridad

Se establecerá la configuración del sistema de certificación, así como toda modificación o actualización que debe ser documentada y controlada. El PSC garantizará la existencia de un método de detección de modificaciones no autorizadas al software o a su configuración.

6.6.3 Calificaciones de Seguridad del Ciclo de Vida

Se describirán los resultados de evaluaciones realizadas por terceros del ciclo de vida.

6.7 CONTROLES DE SEGURIDAD DE LA RED

En está sección se establecerán como los servidores de la Autoridad de Certificación estarán protegidos ante cualquier ataque a través de redes abiertas a las que se encuentren conectados.

6.8 SELLADO DE TIEMPO

Se indicarán en esta sección los requisitos o prácticas referente al uso de sellado de tiempo en los datos y si el sellado de tiempo utiliza una fuente confiable del tiempo

7. PERFILES DE CERTIFICADOS, LCR/OCSP

Se especificarán en está sección los formatos de certificados y de listas de certificados revocados generados según la Política de Certificados.

7.1 PERFIL DEL CERTIFICADO

Todos los certificados correspondientes a la presente Política de Certificados serán emitidos conforme con lo establecido en el estándar ITU X.509 y la normativa específica de SUSCERTE para tal fin (Norma 032), ya que así lo establece el documento de lineamientos de seguridad para la acreditación de los Proveedores de Servicios de Certificación de la SUSCERTE.

7.2 PERFILES DE LA LISTA DE CERTIFICADOS REVOCADOS (LCR)

Las listas de certificados revocados correspondientes a la presente Política de Certificados deberán ser emitidas conforme con lo establecido en el estándar ITU X.509 y la normativa específica de SUSCERTE para tal fin (Norma 032).

7.3 PERFIL DEL PROTOCOLO DE ESTADO DE CERTIFICADOS EN LÍNEA (OCSP)

Esta sección trata los asuntos tales como:

7.3.1 Número de versión

Versión de OCSP que se esta utilizando como la base para establecer un sistema OCSP

7.3.2 Extensiones de la OCSP

Definir las extensiones de la OCSP utilizadas en los certificados.

8. AUDITORIA DE CONFORMIDAD

En este componente se indican los aspectos específicos del proceso de auditoria, como son:

- Temas principales a evaluar en las auditorias.

  Establecer la lista de los tópicos cubiertos en la auditoria o la metodología de la evaluación realizada

- Frecuencia de realización de auditorias

  Definir la frecuencia de la evaluación conforme a la política de certificación de PSC

- Identidad del auditor

  Determinar la identidad y calificación del personal que realiza la auditoria.

- Relación entre el auditor y la entidad auditada

  Definir la relación funcional del auditor con el área objeto de la auditoria

- Medidas a adoptar en caso de dictámenes no favorables.

  Definir las acciones tomadas como resultado de las deficiencias encontradas durante la evaluación

- Modalidad de comunicación de informes de auditoria.

  Definir quién tiene derecho de ver los resultados de la auditoria.

9. REQUISITOS COMERCIALES Y LEGALES

9.1 ARANCELES

En esta sección se especifican las tasas de registro vigentes para la extensión. Renovación y revocación de certificados además de las promociones y ofertas de las tarifas a pagar por concepto de aranceles

9.2 RESPONSABILIDAD FINANCIERA DEL PSC

En esta sección se especifica la responsabilidad de recursos disponibles de manera de apoyar el funcionamiento de sus responsabilidades operacionales.

9.3 POLITICAS DE CONFIDENCIALIDAD

9.3.1 Información Confidencial

Se especificará la información considerada confidencial por el Proveedor de Servicios de Certificación tanto de la Autoridad de Certificación como por las Autoridades de Registro vinculadas.

9.3.2 Información No Confidencial

Se especificará cuál es la información no considerada confidencial por el Proveedor de Servicios de Certificación operativamente vinculadas. Entre otros aspectos comprenderá:

- Contenido de los certificados y de las listas de certificados revocados.
- Información sobre personas físicas o jurídicas que se encuentre disponible en certificados o en directorios de acceso público.
- Políticas de Certificación y Manual de Procedimientos del Proveedor de Servicios de Certificación.
- Versiones públicas de las Políticas de Seguridad del Proveedor de Servicios de Certificación.

9.3.3 Publicación de Información sobre la Revocación o Suspensión de un Certificado

Se deberá considerar la información sobre la revocación o suspensión de un certificado como información no confidencial.

9.3.4 Divulgación de Información a Autoridades Judiciales

Se describirán las condiciones bajo las cuales los Proveedores de Servicios de Certificación deberán revelar información confidencial a autoridades judiciales.

9.4 PROTECCIÓN DE LA INFORMACIÓN PRIVADA/SECRETA

9.4.1 Información considerada privada .

Establecer los procesos de protección de la información personalmente identificable como privada.

9.4.2 Información considerada no privada.

Establecer los procesos de protección de la información considerada como no privada.

9.4.3 Responsabilidad de proteger la información privada/secreta.

Establecer las obligaciones legales como PSC.

9.4.4 Consentimiento previo para el uso de información privada/secreta.

9.4.5 Comunicación de la información a autoridades administrativas y/o judiciales.

9.5 DERECHO DE PROPIEDAD INTELECTUAL

Se incluirá especificaciones acerca de los derechos de propiedad intelectual, derechos de autor y patentes relacionadas a los documentos elaborados por los Proveedores de Servicios de Certificación, así como de nombres o claves criptográficas y otras herramientas, de acuerdo con la legislación vigente.

9.6 REPRESENTACIONES Y GARANTIAS

Determinar los requisitos de las representaciones y garantías que aparecen en ciertos acuerdos, tales como el suscriptor o acuerdos entre las partes en que confían.

9.7 LIMITACIONES DE RESPONSABILIDAD

9.7.1 Deslinde de Responsabilidad

Definir la responsabilidad de cubrir los tipos de daños y perjuicios recuperables.

9.7.2 Limitaciones de Pérdidas.

Definir las limitaciones sobre la cobertura por certificado o por transacción.

9.8 PLAZO Y FINALIZACIÓN.

9.8.1 Plazo.

Determinar el periodo de tiempo en que una DPC y PC permanecen vigentes.

9.8.2 Terminación.

Definir las circunstancias en las cuales la DPC y PC, las partes o su aplicabilidad dejan de ser permanecer en vigor.

9.10 MODIFICACIONES

Se establecerán en está sección los procedimientos para el

mantenimiento y administración de la Política de Certificados.

9.10.1 Procedimientos de Cambio de Especificaciones.

Se establecerán en está sección los procedimientos utilizados para efectuar modificaciones en la Política de Certificados. Toda modificación deberá ser aprobada previamente por la SUSCERTE.

9.10.2 Procedimientos de Publicación y Notificación.

Se describirán los mecanismos utilizados para notificar a los suscriptores acerca de la Política de Certificados y de sus modificaciones.

9.10.3 Procedimientos de Aprobación.

En está sección todas las Políticas de Certificados deberán ser sometida a aprobación de la SUSCERTE durante el proceso de Acreditación.

Toda modificación de la Política de Certificados deberá ser comunicada y aprobada por la SUSCERTE.

9.11 RESOLUCIÓN DE CONFLICTOS.

Se especifican todas las diferencias, desavenencias y/o controversias que se produzcan entre las partes y además se identificara el ente que solucionara el conflicto y se establecerá la Ley para esté tipo de casos, así mismo la Superintendencia de Servicios de Certificación Electrónica puede ser un mediador entre las partes en conflicto.

9.12 LEGISLACIÓN APLICABLE

Se establecerá la legislación que respalda la interpretación, aplicación y validez de la Declaración de Prácticas de Certificación y Política de Certificados, debiendo indicar la Ley Sobre Mensaje de Datos y Firma Electrónica, y otras norma complementarias dictada por la Superintendencia de Servicios de Certificación Electrónica.

10. OBLIGACIONES Y RESPONSABILIDAD CIVIL

10.1 OBLIGACIONES DEL PSC

Se especifican las obligaciones que debe tener el PSC ante el titular del Certificado Electrónico, para garantizar la validez del certificado. Como por ejemplo: Adoptar las medidas necesarias para determinar la exactitud de los Certificados Electrónicos que identifiquen al

signatario o garantizar la validez, vigencia y legalidad del Certificado Electrónico que proporcione.

Estas obligaciones se encuentran en el artículo 35 de la Ley Sobre Mensajes de Datos y Firmas Electrónicas y otras que establezca la Superintendencia de Servicios de Certificación Electrónica.

Se especifican las obligaciones que tiene el PSC ante el titular del Certificado Electrónico, para resguardar su identidad y se compromete a cumplirlas. Por ejemplo: Almacenar de forma segura y por un periodo razonable la documentación aportada en el proceso de emisión del certificado y en el proceso de suspensión/revocación del mismo.

10.2 OBLIGACIONES DEL SIGNATARIO

En esta sección se enumeran detalladamente las obligaciones que debe cumplir como titular de la firma electrónica, por ejemplo: Almacenar y garantizar la seguridad de las claves criptográficas de firmas electrónicas .

10.3 OBLIGACIONES DE TERCEROS INTERESADOS

Se informarán las obligaciones de los terceros usuarios, incluyendo como mínimo:

a)La obligatoriedad de aceptar los términos de este documento.

b)La obligatoriedad de rechazar la utilización del certificado para fines distintos a los preventivos en este documento.

c)La obligatoriedad de verificar la validez, revocación o suspensión del certificado utilizando la información de estado de revocación adecuada.

La falta de cumplimiento de estas obligaciones por parte del tercero parte no exime las responsabilidades del certificado y del signatario que pudieran resultar.

10.4 RESPONSABILIDAD DEL PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN

En está sección se especifica de una manera sistemática las responsabilidades que tendrá el Proveedor de Servicios de Certificación ante el titular del Certificado y además establecer algunas limitaciones.

10.5 RESPONSABILIDAD DEL SIGNATARIO

Se especificará en esta sección la responsabilidad que tendrá el signatario con respecto a la seguridad de las claves privadas y el uso

de los certificados.

10.6 RESPONSABILIDAD DE TERCEROS AUTORIZADOS

Se especifican las responsabilidades del usuario y riesgos derivados de la aceptación de un certificado sin haber realizado previamente la preceptiva verificación de su validez.