Decreto Nº 33018 -MICIT

EL PRESIDENTE DE LA REPÚBLICA

Y EL MINISTRO DE CIENCIA Y TECNOLOGÍA

Con fundamento en lo dispuesto en los artículos 140, incisos 3) y 18) y 146 de la Constitución Política; y el artículo 33 de la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, número 8454 del 30 de agosto del 2005,

CONSIDERANDO:

1º— Que la sociedad de la información y del conocimiento se debe construir sobre la base de la confianza de los ciudadanos y sobre la garantía de la utilización de las tecnologías de la información y las comunicaciones en un doble plano: la protección y confidencialidad de los datos de carácter personal y la seguridad de las transacciones electrónicas.

2º— Que la Ley Nº 8454, Ley de Certificados, Firmas Digitales y Documentos Electrónicos, establece el marco jurídico general para la utilización transparente, confiable y segura en nuestro medio de los documentos electrónicos y la firma digital en las entidades públicas y privadas.

3º— Que el artículo 33 de dicha ley establece que el Poder Ejecutivo deberá reglamentarla ley en un plazo de 6 meses, regulación que debe servir para garantizar la disponibilidad de los sistemas e infraestructuras telemáticas, la seguridad y autenticidad de las transacciones, así como la confidencialidad e integridad de la información.

Por tanto

DECRETAN:

Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos

Capítulo Primero – Disposiciones Generales

Artículo 1.- **Propósito.** El presente texto servirá para reglamentar y dar cumplida ejecución a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, número 8454 del 30 de agosto del 2005. Tendrá el carácter y la jerarquía de reglamento general, en los términos del artículo 6.1.d) de la Ley

General de la Administración Pública, frente a los demás reglamentos particulares o autónomos en la materia.

Artículo 2.- **Definiciones.** Para los efectos del presente Reglamento, se entenderá por:

1) AUTENTICACIÓN: Verificación de la identidad de un individuo.

a.- En el proceso de registro, es el acto de evaluar las credenciales de la entidad final (por ejemplo, un suscriptor) como evidencia de que realmente es quien dice ser.

b.- Durante el uso, es el acto de comparar electrónicamente las credenciales y la identidad enviada (Ej., código de usuario y contraseña, certificado digital, etc.) con valores previamente almacenados para comprobar la identidad.

2) AUTENTICACIÓN MUTUA: Proceso mediante el cual dos entidades verifican su identidad en forma recíproca.

3) AUTENTICIDAD: La veracidad, técnicamente constatable, de la identidad del autor de un documento o comunicación. La autenticidad técnica no excluye el cumplimiento de los requisitos de autenticación o certificación que desde el punto de vista jurídico exija la ley para determinados actos o negocios.

4) AUTORIDAD DE REGISTRO (AR): Entidad delegada por el certificador registrado para la verificación de la identidad de los solicitantes y otras funciones dentro del proceso de expedición y manejo de certificados digitales. Representa el punto de contacto entre el usuario y el certificador registrado.

5) BITÁCORAS DE AUDITORIA: Registro cronológico de las actividades del sistema, que son suficientes para habilitar la reconstrucción, revisión, y la inspección de la secuencia del entorno y las actividades secundarias o primarias para cada evento en la ruta de una transacción desde su inicio hasta la salida del resultado final.

6) CERTIFICACIÓN: Proceso de creación de un certificado de llave pública para un suscriptor.

7) CERTIFICADO DIGITAL: Una estructura de datos creada y firmada digitalmente por un certificador, del modo y con las características que señalan este Reglamento y su anexo, cuyo propósito primordial es posibilitar a sus suscriptores la creación de firmas digitales, así como la identificación personal en transacciones electrónicas. Sin perjuicio del concepto anterior, la DCFD podrá autorizar a los certificadores registrados la generación de certificados con propósitos diferentes o adicionales a los indicados.

8) CERTIFICADO SUSPENDIDO: Cesación temporal o interrupción de la validez de un certificado.

9) CERTIFICADO VÁLIDO: Se refiere a aquel certificado que se encuentra activo, que ha sido emitido por un certificador registrado.

10) CERTIFICADOR: La persona jurídica pública o privada, nacional o extranjera, prestadora del servicio de creación, emisión y operación de certificados digitales.

11) CERTIFICADOR RAÍZ: El nodo superior autocertificante de la jerarquía nacional de certificadores registrados.

12) CERTIFICADOR REGISTRADO: El certificador inscrito y autorizado por la Dirección de Certificadores de Firma Digital.

13) CERTIFICADOR PADRE: Certificador registrado que se encuentra en la posición inmediata superior con respecto a otro certificador registrado, en la jerarquía de certificadores.

14) CERTIFICADOR SUBORDINADO: Certificador registrado que se encuentra en la posición inmediata inferior con respecto a otro certificador registrado, en la jerarquía de certificadores.

15) COMPROMISO: Violación de la seguridad de un sistema, por haber ocurrido una divulgación no autorizada de información sensible.

16) CONTROL MÚLTIPLE: Condición mediante la cual dos o más partes, separada y confidencialmente, tienen la custodia de los componentes de una llave particular, pero que individualmente no tienen conocimiento de la llave resultante.

17) DATOS DE ACTIVACIÓN: Valores de datos (que no son las llaves), que son requeridos para operar los módulos criptográficos y que necesitan ser protegidos(ejemplo: PINs, frase clave, biométricos o llaves distribuidas manualmente).

18) DECLARACIÓN DE LAS PRÁCTICAS DE CERTIFICACIÓN (DPC): Declaración de las prácticas que utiliza el certificador para la emisión de los certificados (define el equipo, las políticas y los procedimientos que el certificador utiliza para satisfacer los requerimientos especificados en las políticas del certificado que son soportados por él).

19) DIRECCIÓN DE CERTIFICADORES DE FIRMA DIGITAL (DCFD): Dependencia del Ministerio de Ciencia y Tecnología, encargada de la administración y supervisión del sistema de certificación digital.

20) DISPOSITIVO O MODULO SEGURO DE CREACION DE FIRMAS (MSCF): Dispositivo que resguarda las claves y el certificado de un suscriptor, utilizado para generar su firma digital y que, al menos, garantiza:

a.- Que los datos utilizados para la generación de la firma solo pueden producirse una vez en la práctica y se garantiza razonablemente su confidencialidad;

b.- Que existe una expectativa razonable de que los datos utilizados para la generación de la firma no pueden ser descubiertos por deducción y la firma está protegida contra falsificación por medio de la tecnología disponible a la fecha, siendo posible detectar cualquier alteración posterior; y,

c.- Que los datos empleados en la generación de la firma pueden ser protegidos de modo fiable por el firmante legítimo, contra su utilización por cualesquiera terceros.

21) DOCUMENTO ELECTRÓNICO: Cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático.

22) ENTE COSTARRICENSE DE ACREDITACIÓN (ECA): La dependencia pública a que se refiere la "Ley del Sistema Nacional para la Calidad", número 8279 de 2 de mayo del 2002.

23) ENTIDAD FINAL: Suscriptor del certificado.

24) FIRMA DIGITAL: Conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento.

25) FIRMA DIGITAL CERTIFICADA: Una firma digital que haya sido emitida al amparo de un certificado digital válido y vigente, expedido por un certificador registrado.

26) INFRAESTRUCTURA DE LLAVE PÚBLICA (PKI por sus siglas en inglés): Se refiere a una estructura de *hardware*, *software*, personas, procesos y políticas que emplean tecnología de firma digital para proveer una asociación verificable entre una llave pública y un suscriptor específico que posee la llave privada correspondiente.

27) INTEGRIDAD: Propiedad de un documento electrónico que denota que su contenido y características de identificación han permanecido inalterables desde el momento de su emisión, o bien que -habiendo sido alterados posteriormente- lo fueron con el consentimiento de todas las partes legitimadas.

28) LEY: La Ley de Certificados, Firmas Digitales y Documentos electrónicos, Ley número 8454 del 30 de agosto del 2005.

29) LGAP: La Ley General de la Administración Pública.

30) LINEAMIENTOS TÉCNICOS: El conjunto de definiciones, requisitos y regulaciones de carácter técnico-informático, contenido en el anexo de este Reglamento.

31) LRC: Lista de revocación de certificados.

32) MECANISMO EN LÍNEA PARA VERIFICAR EL ESTADO DEL CERTIFICADO: Mecanismo mediante el cual se permite a las partes que confían, consultar y obtener, la información del estado de un certificado sin requerir para ello el uso de una LRC.

33) OFICINA DE TARJETAS (*card bureau*): Agente del certificador registrado o de la autoridad de registro que personaliza la tarjeta de circuito integrado (o tarjeta inteligente), que contiene la llave privada del suscriptor (como mínimo).

34) PARTE CONFIANTE: Se refiere a las personas físicas, equipos, servicios o cualquier otro ente que confía en la validez de un certificado emitido por un certificador específico.

35) POLÍTICAS DEL CERTIFICADO (PC): Conjunto de reglas que indican la aplicabilidad del certificado a una comunidad particular y/o clase de aplicaciones con los requerimientos comunes de seguridad.

36) PROTOCOLO EN LÍNEA PARA DETERMINAR EL ESTADO DEL CERTIFICADO (OCSP POR SUS SIGLAS EN INGLÉS): Protocolo suplementario para determinar el estado actual de un certificado.

37) RECUPERACIÓN DE LLAVES: Capacidad de restaurar la llave privada de una entidad a partir de un almacenamiento seguro, en el caso de que se pierda, corrompa o que por cualquier otra razón se convierta en no utilizable.

38) RE-EMISIÓN DE LLAVES DEL CERTIFICADO: Proceso por medio del cual una entidad con un par de llaves y un certificado previamente emitidos, luego de la generación de un nuevo par de llaves, recibe un nuevo certificado y una nueva llave pública.

39) REGLAMENTO: Este Reglamento.

40) RENOVACIÓN DEL CERTIFICADO: Proceso donde una entidad emite una nueva instancia de un certificado existente, con un nuevo período de validez.

41) REPOSITORIO: Sistema de almacenamiento y distribución de certificados e información relacionada (Ej., almacenamiento y distribución de certificados, almacenamiento y recuperación de políticas de certificación, estado del certificado, etc.).

42) ROL DE CONFIANZA: Función de trabajo que permite ejecutar labores críticas. Si dichas labores se ejecutan de una forma insatisfactoria puede ocurrir

un impacto adverso, que dará como resultado una degradación en la confianza que provee el certificador.

43) SELLO DE GARANTÍA (*tamper evident*): Características de un dispositivo que proveen evidencia de que existió un intento de ataque sobre él.

44) SERVICIOS DE VALIDACIÓN DE CERTIFICADOS: Servicios provistos por el certificador registrado o sus agentes que ejecutan la tarea de confirmar la validez del certificado a una tercera parte que confía.

45) SUSCRIPTOR: La persona física a cuyo favor se emite un certificado digital y que lo emplea para los propósitos señalados en el inciso 7) anterior, en conjunto con las claves, contraseñas y/o dispositivos necesarios al efecto y de cuya custodia es responsable.

46) VERIFICACIÓN DE FIRMA: Con relación a la firma digital, significa determinar con precisión: (1) que la firma ha sido creada durante el período operacional de un certificado válido, utilizando la llave pública listada en el certificado; y, (2) que el mensaje no ha sido alterado desde que la firma fue creada.

Artículo 3.- **Aplicación al Estado.** A los efectos del párrafo segundo del artículo 1 de la Ley, los Supremos Poderes, el Tribunal Supremo de Elecciones, los demás órganos constitucionales y todas las entidades públicas podrán adoptar separadamente las disposiciones particulares que requiera su ámbito específico de competencia o la prestación del servicio público, incluyendo la posibilidad de fungir como certificador respecto de sus funcionarios.

Artículo 4.- **Incentivo de los mecanismos de gobierno electrónico.** Con excepción de aquellos trámites que necesariamente requieran la presencia física del ciudadano, o que éste opte por realizarlos de ese modo, el Estado y todas las dependencias públicas incentivarán el uso de documentos electrónicos, certificados y firmas digitales para la prestación directa de servicios a los administrados, así como para facilitar la recepción, tramitación y resolución electrónica de sus gestiones y la comunicación del resultado correspondiente.

En la emisión de los reglamentos particulares a que se refieren los artículos 2, inciso c) y 33 de la Ley, todas las dependencias públicas procurarán ajustar sus disposiciones a los principios de neutralidad tecnológica e interoperatividad. En ningún caso se impondrán exigencias técnicas o jurídicas que impidan o dificulten injustificadamente la interacción con las oficinas públicas por medio de firmas o certificados digitales emitidos por un certificador registrado.

En lo relativo a la conservación de los documentos electrónicos, así como la migración de documentos de soporte físico a electrónico, se aplicará lo dispuesto en el artículo 6 de la Ley.

Capítulo Segundo – Certificados Digitales

Artículo 5.- **Contenido y características.** El contenido, condiciones de emisión, suspensión, revocación y expiración de los certificados digitales, serán los que se señala en el anexo de este Reglamento y en las políticas que al efecto emita la DCFD.

Artículo 6.- **Tipos de certificados.** El DFCD establecerá los tipos de certificados que podrán emitir los certificadores, con estricto apego a las normas técnicas y estándares internacionales aplicables que promuevan la interoperabilidad con otros sistemas.

En el caso de los certificados digitales que vayan a ser utilizados en procesos de firma digital y de autenticación de la identidad, los certificadores necesariamente deberán utilizar al menos:

1) Un proceso de verificación y registro presencial (cara a cara) de sus suscriptores.

2) Guardar copia de la documentación utilizada para verificar la identidad de la persona.

3) Registrar de forma biométrica (fotografía, huellas digitales, etc.) al suscriptor a quién le será emitido un certificado.

4) Requerir el uso de módulos seguros de creación de firma, con certificación de seguridad FIPS 140-1 nivel 2 o mejor.

5) Establecer un contrato de suscripción detallando el nivel de servicio que ofrece y los deberes y responsabilidades de las partes.

6) La DCFD podrá establecer cualquier otro requisito que considere pertinente, en tanto emisor y gestor de políticas del sistema de firma digital.

Artículo 7.- **Obligaciones de los usuarios.** Para los efectos de los artículos 14, inciso d) y 15 de la Ley, todos los suscriptores del sistema de certificados y firmas digitales estarán obligados a:

1) Suministrar a los certificadores la información veraz, completa y actualizada que éstos requieran para la prestación de sus servicios.

2) Resgardar estrictamente la confidencialidad de la clave, contraseña o mecanismo de identificación que se les haya asignado con ese carácter, informando inmediatamente al certificador en caso de que dicha confidencialidad se vea o se sospeche que haya sido comprometida.

3) Acatar las recomendaciones técnicas y de seguridad que le señale el correspondiente certificador.

Artículo 8.- **Plazo de suspensión de certificados.** La suspensión de un certificado digital, en aplicación del artículo 14 de la Ley, se mantendrá por todo el plazo en que subsista la causal que le dio origen.

Artículo 9.- **Revocación por cese de actividades.** Para los efectos del artículo 16 de la Ley, en el caso del cese de actividades de un certificador, éste mismo –o la DCFD en su defecto- gestionarán el traslado de la cartera de suscriptores que así lo hayan consentido a otro certificador, que expedirá los nuevos certificados.

Capítulo Tercero – Certificadores

Artículo 10.- **Reconocimiento jurídico.** Solo tendrán pleno efecto legal frente a terceros, así como respecto del Estado y sus instituciones, los certificados digitales expedidos por certificadores registrados ante la Dirección de Certificadores de Firma Digital.

Las firmas y certificados emitidos dentro o fuera del país que no cumplan con esa exigencia no surtirán efectos por sí solos, pero podrán ser empleados como elemento de convicción complementario para establecer la existencia y alcances de un determinado acto o negocio.

Artículo 11.- **Comprobación de idoneidad técnica y administrativa.** Para obtener la condición de certificador registrado, se requiere poseer idoneidad técnica y administrativa, que serán valoradas por el ECA de acuerdo con los lineamientos técnicos del anexo de este Reglamento y los restantes requisitos que esa dependencia establezca, de conformidad con su normativa específica.

Artículo 12.- **Formalidades de la solicitud.** La solicitud de inscripción del certificador se presentará debidamente autenticada y deberá incluir la información siguiente:

1) Nombre o razón social de la solicitante, número de cédula de persona jurídica, domicilio y dirección postal, así como los correspondientes números telefónicos y de fax (si lo tuviera), su sitio web en Internet y al menos una dirección de correo electrónico para la recepción de comunicaciones de la DCFD y/o el ECA.

2) Identificación completa de la persona o personas que fungirán como responsables administrativos del certificador ante la DCFD y el ECA. Ésta o éstas necesariamente serán los firmantes de la gestión y ostentarán la representación legal u oficial de la solicitante.

3) Identificación completa de la persona o personas que fungirán como responsables técnicos del certificador, si no fueren las mismas del punto anterior. Se entenderá por tales a la persona o personas que recibirán y custodiarán las claves, contraseñas y/o mecanismos de identificación

asignados al certificador y que podrán firmar digitalmente en su nombre.

4) La dirección física precisa del establecimiento o local desde el cual se realizará la actividad de certificación digital.

5) Certificación de personería, en el caso de los sujetos privados, o de nombramiento, para los funcionarios públicos. Dicho documento deberá acreditar, en el primer supuesto, que la persona jurídica se encuentra debidamente constituida de acuerdo con la ley y en pleno ejercicio de su capacidad jurídica.

6) Certificación de composición y propiedad del capital social, si la solicitante fuera una sociedad mercantil.

7) En el caso de los sujetos privados, comprobación de haber rendido la caución necesaria para responder por las eventuales consecuencias civiles, contractuales y extracontractuales, de su actividad.

Artículo 13.- **Caución.** La caución a que se refiere el artículo anterior será rendida preferiblemente por medio de póliza de fidelidad expedida por el Instituto Nacional de Seguros. El monto –de acuerdo con la Ley- será fijado por la DCFD en consulta con el INS, tomando en consideración los riesgos y responsabilidades inherentes en la labor de certificación digital.

Cuando la caución esté sujeta a vencimiento, necesariamente deberá ser renovada por el interesado al menos dos meses antes de la fecha de expiración.

Artículo 14.- **Trámite de la solicitud.** Recibida la solicitud de inscripción, la DCFD procederá a:

1) Apercibir al interesado en un plazo no mayor de diez días y por una única vez, sobre cualquier falta u omisión que deba ser subsanada para dar inicio a su trámite. Al efecto, se aplicará lo dispuesto en la "Ley de protección al ciudadano del exceso de requisitos y trámites administrativos", número 8220 de 4 de marzo del 2002; y –en cuanto fuere necesario- lo dispuesto en el artículo 340 de la LGAP.

2) Remitir la solicitud al ECA una vez cumplido lo indicado en el inciso 1), para efectos de analizar la idoneidad técnica y administrativa del gestionante.

Artículo 15.- **Oposiciones.** Recibida en orden la solicitud y obtenida la acreditación correspondiente por parte del ECA, el solicitante publicará en el diario oficial La Gaceta" un resumen que le entregará la DCFD, sin perjuicio de que ésta lo haga también en los medios electrónicos establecidos en la Ley y este Reglamento.

Dentro de los cinco días hábiles siguientes a la publicación impresa, quien se sintiere legítimamente perjudicado por la solicitud planteada o que dispusiera de alguna información que pueda contribuir a calificarla, deberá hacerlo presentando las pruebas pertinentes a la DCFD, la cual conferirá audiencia al interesado por un plazo de cinco días hábiles.

No se aplicará lo dispuesto en este artículo cuando la gestión corresponda a una dependencia pública.

Artículo 16.- **Resolución.** Cumplido lo dispuesto en el artículo anterior, la DCFD resolverá lo que corresponda –incluyendo las oposiciones formuladas, si las hubiere- en un plazo no mayor de quince días, por medio de resolución fundada que notificará a los interesados. Si el acuerdo fuera favorable, se publicará a través de los medios electrónicos previstos en la Ley y este Reglamento.

Artículo 17.- **Silencio positivo.** La gestión que no haya sido resuelta dentro del plazo que señala el artículo precedente se entenderá aprobada.

Artículo 18.- **Recursos.** Contra lo resuelto por la DCFD, se admitirá el recurso de reposición, aplicándose al efecto lo dispuesto en los artículos 346, siguientes y concordantes, de la LGAP.

Artículo 19.- **Funciones.** Los certificadores registrados tendrán las siguientes atribuciones y responsabilidades:

1) Expedir las claves, contraseñas o dispositivos de identificación a sus suscriptores, en condiciones seguras y previa verificación fehaciente de su identidad. Lo mismo hará respecto de sus certificadores subordinados cuando los hubiere, los cuales también deberán registrarse ante la DCFD.

El certificador no podrá copiar o conservar información relativa a la clave privada de firma digital de un suscriptor y deberá abstenerse de tomar conocimiento o acceder a ella bajo ninguna circunstancia.

2) Llevar un registro completo y actualizado de todos sus suscriptores, para lo cual les requerirá la información necesaria. En el caso de los certificadores, comerciales, no se solicitará de sus clientes más información personal que la que sea estrictamente necesaria, quedando obligados a mantenerla bajo estricta confidencialidad, con la salvedad prevista en el inciso último de este artículo.

3) Expedir el certificado digital que respalde la firma digital de los suscriptores de sus servicios y de sus certificadores subordinados, así como suspenderlo o revocarlo bajo las condiciones previstas en la Ley y este Reglamento.

4) Prestar los servicios ofrecidos a sus suscriptores, en estricta conformidad con las políticas de certificación que haya comunicado al público y que hayan sido aprobados por la DFCD.

5) Conservar la información y registros relativos a los certificados que emitan, durante no menos de diez años contados a partir de su expiración o revocación. En caso de cese de actividades, la información y registros respectivos deberán ser remitidos a la DCFD, quien dispondrá lo relativo a su adecuada conservación y consulta.

6) Mantener un repositorio electrónico, permanentemente accesible en línea y publicado en internet para posibilitar la consulta de la información pública relativa a los certificados digitales que haya expedido y de su estado actual, de la manera que se indique en el anexo de este Reglamento y en los lineamientos que sobre el particular dicte la DCFD.

7) Suministrar, con arreglo a las disposiciones constitucionales y legales pertinentes, la información que las autoridades competentes soliciten con relación a sus suscriptores y a los certificados que les hayan sido expedidos.

8) Impartir lineamientos técnicos y de seguridad a los suscriptores y certificadores subordinados, con base en los que a su vez dicte la DCFD.

9) Acatar las instrucciones y directrices que emita la DCFD para una mayor seguridad o confiabilidad del sistema de firma electrónica.

10) Rendir a la DCFD los informes y datos que ésta requiera para el adecuado desempeño de sus funciones y comunicarle a la mayor brevedad cualquier otra circunstancia relevante que pueda impedir o comprometer su actividad.

Artículo 20.- **Divulgación de datos.** En adición al repositorio en línea a que se refiere el artículo previo, todo certificador registrado deberá mantener un sitio o página electrónica en Internet, de alta disponibilidad y protegida con esquemas de seguridad razonables para impedir su subplantación, por medio del cual suministre permanentemente al público al menos los datos siguientes, empleando un lenguaje fácilmente comprensible y en idioma español:

1) Su nombre, dirección física y postal, número(s) telefónico(s) y de fax (si lo tuviera), así como un mecanismo de contacto por medio de correo electrónico.

2) Los datos de inscripción ante la DCFD y su estado actual (activo o suspendido).

3) Las políticas de certificación que aplica y que son respaldados y aprobados por la DCFD

4) El resultado final más reciente de evaluación o auditoría de sus servicios, efectuada por el Ente Costarricense de Acreditación.

5) Cualesquiera restricciones establecidas por la DCFD.

6) Cualquier otro dato de interés general que disponga la Ley, este Reglamento o la DCFD.

Artículo 21.- **Corresponsalías.** Al informar a la DCFD sobre el establecimiento de relaciones de corresponsalía conforme al artículo 20 de la Ley, se deberá especificar si la homologación de certificados expedidos por certificadores extranjeros está o no sujeta a alguna clase de restricción o salvedad y, caso afirmativo, en qué consiste. Lo mismo se hará al momento de ofrecer este servicio al público.

Artículo 22.- **Actualización permanente de datos.** Los certificadores deberán mantener permanentemente actualizada la información que requieran la DCFD y el ECA para el cumplimiento de sus funciones. Cualquier cambio de domicilio físico o electrónico, o de cualquier otro dato relevante, deberá ser comunicado de inmediato al ECA, que a su vez lo notificará a la DCFD.

Capítulo Cuarto – Dirección de Certificadores de Firma Digital

Artículo 23.- **Responsabilidad.** La Dirección de Certificadores de Firma Digital -perteneciente al Ministerio de Ciencia y Tecnología- será el órgano administrador y supervisor del sistema de certificación digital. Las resoluciones dictadas en los asuntos de su competencia agotarán la vía administrativa.

La DCFD tendrá, de pleno derecho, el carácter de certificador raíz. No obstante, para garantizar una óptima efectividad en el cumplimiento de esta función, podrá gestionar el apoyo de otro órgano, entidad o empresa del Estado, a los efectos de que supla la infraestructura material y el personal idóneo necesarios para operar la raíz, debiendo satisfacer los mismos requisitos de acreditación y evaluaciones periódicas por parte del ECA que debe cumplir todo certificador.

Artículo 24.- **Funciones.** La Dirección de Certificadores de Firma Digital (DCFD tendrá las funciones que señala la Ley. El registro de certificados digitales a que se refiere el inciso b) del artículo 24 de la Ley tendrá un contenido y propósitos puramente cuantitativos y estadísticos.

La DCFD tendrá la responsabilidad de definir políticas y requerimientos para el uso de certificados digitales que deberán ser especificados en una Política de

Certificados o acuerdos complementarios: en especial la DCFD será el emisor y el gestor de las políticas para el sistema de certificadores de firma digital.

Dentro de sus actividades, la DCFD procurará realizar programas de capacitación y actualización profesional en esta materia, así como establecer enlaces de cooperación con organismos o programas internacionales relacionados.

Artículo 25.- **Cooperación interinstitucional.** Se autoriza a las instituciones del Estado para presupuestar y girar recursos, en la medida de sus posibilidades jurídicas y materiales, a fin de contribuir a lograr los objetivos de la DCFD.

Artículo 26.- **Jefatura.** El superior administrativo de la DCFD será el director, quien será nombrado por el ministro de Ciencia y Tecnología y será un funcionario de confianza, de conformidad con el inciso g) del artículo 4, del Estatuto de Servicio Civil. El director deberá declarar sus bienes oportunamente, de acuerdo con la Ley contra el enriquecimiento ilícito de los servidores públicos.

Quien sea designado Director deberá reunir los siguientes requisitos:

1) Poseer un título universitario pertinente al cargo, con grado mínimo de licenciatura.

2) Tener experiencia profesional demostrable en el tema.

3) Estar incorporado al respectivo colegio profesional y al día en sus obligaciones con éste.

4) Los demás que establezca el manual de clasificación y puestos del Ministerio de Ciencia y Tecnología.

Artículo 27.- **Régimen interior.** El régimen de servicio al que estará sujeto el personal de la DCFD será el establecido en el reglamento autónomo de servicio del Ministerio de Ciencia y Tecnología, que se aplicará también al Director en lo que legalmente sea procedente.

Artículo 28.- **Comité Asesor de Políticas.** El Director de la DCFD contará con la asesoría de un comité de políticas, integrado por representantes de los siguientes órganos y entidades:

1) Banco Central de Costa Rica;

2) Tribunal Supremo de Elecciones;

3) Poder Ejecutivo;

4) Poder Judicial;

5) Consejo Nacional de Rectores (CONARE), en representación del sector académico; y,

6) Asociación Cámara Costarricense de Tecnologías de la Información y Comunicaciones (CAMTIC), en representación del sector privado.

Cada una de esas dependencias designará a un representante propietario y otro suplente, por períodos de dos años, reelegibles indefinidamente. Deberá tratarse en todos los casos de profesionales con grado mínimo de licenciatura, graduados en materias afines y con experiencia demostrable en el tema. El cargo será desempeñado en forma *ad honorem*.

El Comité asesor será presidido por el Director de la DCFD. Se reunirá ordinariamente al menos una vez cada dos meses y extraordinariamente cada vez que lo convoque el Director de la DCFD o lo soliciten por escrito al menos cuatro de los integrantes. Las reuniones se realizarán en la sede de la Dirección.

En lo demás, el Comité ajustará su funcionamiento al régimen de los órganos colegiados previsto en la LGAP.

Artículo 29.- **Funciones del Comité Asesor de Políticas.** El Comité Asesor tendrá las siguientes funciones:

1) Recomendar a la DCFD las políticas generales de operación del sistema nacional de certificación digital, observando los estándares y buenas prácticas internacionales de la materia;

2) Interpretar, aclarar o adicionar esas políticas ante las dudas o consultas de cualquier operador del sistema;

3) Evaluar y actualizar periódicamente las políticas de operación, formulando -en caso necesario- las recomendaciones pertinentes a la DCFD; y,

4) Aconsejar a la DCFD en cualquier otro aspecto que ésta someta a su consideración.

Salvo caso de urgencia, la adopción o modificación de políticas que afecten la operación del sistema nacional de certificación digital se hará previa consulta pública, en la que se invitará a las entidades públicas y privadas, organizaciones representativas y público en general a ofrecer comentarios y sugerencias pertinentes; todo conforme a los artículos 361 y 362 de la LGAP.

Capítulo Quinto – Sanciones

Artículo 30.- **Aplicación de mecanismos alternativos de solución de conflictos**. Tanto antes como durante la tramitación de los procedimientos disciplinarios por quejas o denuncias planteadas contra un certificador, la DCFD procurará aplicar mecanismos alternativos de resolución de conflictos para

encontrar salidas que permitan tutelar los derechos legítimos de las partes, así como la continuidad y confiabilidad del sistema, todo conforme a la legislación aplicable.

Artículo 31.- Multas. El pago de las multas impuestas conforme al artículo 28 de la Ley se realizará por medio de Entero de Gobierno, dentro de los diez días hábiles siguientes a la firmeza de la resolución que las imponga.

El cobro de multas no canceladas oportunamente se realizará conforme a lo dispuesto en el artículo 36 siguiente.

Artículo 32.- **Suspensión.** La suspensión que se aplique de acuerdo con el artículo 29 de la Ley implicará la imposibilidad para el certificador sancionado de expedir nuevos certificados digitales o de renovar los que expiren durante el plazo de la suspensión. No afectará en nada los emitidos previamente.

En los casos del inciso a) del referido artículo, si al cabo del plazo de suspensión el certificador persiste en no renovar debidamente la caución a pesar de la prevención que en ese sentido se le hará, se procederá conforme al artículo 30, inciso c) de la Ley, a efectos de declarar la revocatoria de la inscripción.

Artículo 33.- **Revocatoria de la inscripción.** Para los efectos del artículo 30, inciso a) de la Ley, se entenderá por "certificado falso" aquel que no esté respaldado por una solicitud previa demostrable del correspondiente suscriptor o cuyo trámite no haya seguido los procedimientos de seguridad establecidos para la clase de certificado de que se trate.

Artículo 34.- **Publicidad de las sanciones.** Para los propósitos del artículo 32 párrafo segundo de la Ley, la publicación electrónica de las sanciones impuestas se mantendrá:

1) En el caso de multa, por todo el lapso en que ésta permanezca sin cancelar y posteriormente por dos años a partir del pago.

2) En el caso de suspensión o revocatoria de la inscripción, durante cinco años desde la firmeza de la resolución sancionatoria.

Artículo 35.- **Determinación de responsabilidades adicionales**. Si corresponde, lo relativo a la responsabilidad civil en que pueda haber incurrido un certificador se examinará y resolverá en el mismo procedimiento en que se discuta la responsabilidad disciplinaria. Caso de estimarse que ha lugar al pago de una indemnización, el acto final prevendrá al certificador su oportuno pago, dentro del plazo que al efecto se señalará y que no excederá de un mes.

De llegarse a considerar además que los hechos investigados suponen la posible comisión de un ilícito penal, la Dirección ordenará testimoniar las piezas correspondientes y pondrá los hechos en conocimiento del Ministerio Público.

Artículo 36.- **Medios de ejecución.** Si el certificador sancionado no realiza oportunamente el pago a que estuviere obligado, se procederá a ejecutar la caución por el monto respectivo. En tal caso (así como para el reclamo de cualquier saldo en descubierto que pudiera subsistir) se aplicará en lo pertinente lo dispuesto en los artículos 149 y 150 de la LGAP. La DCFD será el órgano competente para realizar las intimaciones de ley, así como para expedir el título ejecutivo, si corresponde.

Capítulo Sexto – Disposiciones Finales

Artículo 37.- **Vigencia**. Rige a partir de su publicación.

Dado en la Presidencia de la República, a las nueve horas del día veinte, del mes de marzo, del año dos mil seis.

Publíquese

ABEL PACHECO DE LA ESPRIELLA

Fernando Gutiérrez Ortiz

MINISTRO DE CIENCIA Y TECNOLOGÍA

Anexo único – Lineamientos técnicos

La operación de todos los certificadores registrados del sistema nacional de certificación digital deberá apegarse necesariamente a los siguientes lineamientos técnicos.

Tabla de abreviaturas

AR	Autoridad de registro
DPC	Declaración de prácticas de certificación
LRC	Lista de revocación de certificados
PC	Política de certificados
MSCF	Modulo seguro de Creación de Firma
EGP	Emisor y gestor de políticas

1. Controles ambientales

1.1. De la administración de la PC y de la DPC

La EGP tendrá la responsabilidad de definir las políticas y requerimientos de negocio para el uso de los certificados digitales, que deberán ser especificados en una PC o acuerdos complementarios. El Certificador deberá mantener los controles para brindar una seguridad razonable de que los procesos de administración establecidos en la PC y la DPC sean efectivos.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

1.1.1. Gestión de la EGP

La EGP tiene la responsabilidad de garantizar que los procesos de control del Certificador, estipulados en la DPC, cumplen totalmente con los requerimientos de la PC.

La EGP tiene la responsabilidad y autoridad final para especificar y aprobar las PC.

La EGP tiene la responsabilidad y autoridad suficiente para aprobar la DPC del Certificador.

La EGP debe verificar que exista una DPC, que describa al menos lo siguiente:

1) Los controles ambientales del Certificador;

2) Los controles de administración del ciclo de vida de las llaves;

3) Los controles de administración del ciclo de vida del certificado.

La EGP debe garantizar que las aplicaciones de servicio están cumpliendo con la PC apropiada.

La EGP debe tener un procedimiento para el caso en que una PC se actualice o deje de ser válida y debe notificar a las partes afectadas. La EGP debe notificar, en primera instancia, a aquellos certificadores que utilizan esa PC, para tomar las acciones apropiadas en forma expedita.

La EGP debe tener un procedimiento para el cese de sus funciones. En el caso de este evento, todas las partes afectadas deben ser notificadas y deberá existir un procedimiento para la transferencia de los registros archivados que sean relevantes, a un custodio.

1.1.2. Administración de las PC

Las PC deben ser aprobadas por la EGP, de acuerdo con un proceso de revisión definido que incluya las responsabilidades para darles mantenimiento.

El proceso de revisión definido debe garantizar además, que las políticas establecidas en la PC pueden ser soportadas o implementadas por los controles especificados en la DPC.

La EGP debe asegurar que las PC utilizadas por el Certificador, estén disponibles para todos sus subscriptores y partes confiantes.

La DPC debe contener una explicación de los controles que garanticen el cumplimiento de:

1) Requerimientos legales;

2) Requerimientos contractuales;

3) Requerimientos educativos y de notificación;

4) Prevención y detección de virus y otros programas maliciosos;

5) Requerimientos de continuidad del negocio; y

6) Requerimientos de escalamiento como consecuencia de violaciones a políticas de seguridad o incidentes de seguridad.

La EGP debe realizar evaluaciones periódicas para determinar la adecuación de la PC para gestionar los riegos de negocio.

1.1.3. Administración de la DPC por parte del Certificador

La DPC del Certificador debe ser aprobada por la EGP y modificada de conformidad con un procedimiento de revisión definido que incluya las responsabilidades para darle mantenimiento.

El Certificador debe asegurar que su DPC este disponible a todas las partes legítimamente interesadas.

Las nuevas versiones de la DPC del Certificador deben estar disponibles a todas las partes legítimamente interesadas.

1.1.4. Administración del Certificador

Los controles del Certificador deben estar descritos en la DPC.

1.2. De la administración de la seguridad

El Certificador debe mantener controles para asegurar razonablemente que:

- La seguridad es planificada, administrada y apoyada por la organización;
- Los riesgos identificados son administrados efectivamente;
- Se mantiene la seguridad de las instalaciones, los sistemas y los activos de información del Certificador, en especial los que son accedidos por terceros; y,
- Se mantiene la seguridad de la información cuando funciones del Certificador y sus correspondientes responsabilidades, hayan sido transferidas a otra organización o entidad.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

1.2.1. Políticas de seguridad de información

La Gerencia del Certificador debe aprobar, publicar y comunicar a todos los empleados, un documento de políticas de seguridad de información, que incluya controles para los aspectos de infraestructura física, de personal, de procedimientos y de los elementos técnicos

La política de seguridad de información debe incluir lo siguiente:

1) Una definición de seguridad de la información, sus objetivos generales y su alcance, y la importancia de la seguridad como un mecanismo que permite compartir información;
2) Una declaración de propósito gerencial, apoyando las metas y los principios de la seguridad de la información;

3) Una explicación de las políticas de seguridad, sus principios, estándares y requerimientos de cumplimiento, que sean de especial importancia para la organización;

4) Una definición de las responsabilidades generales y específicas para la administración de la seguridad de la información, incluyendo el reporte de incidentes de seguridad; y,

5) Las referencias a la documentación que apoya las políticas de seguridad.

Debe existir un proceso de revisión definido para darle mantenimiento a las políticas de seguridad de información, que incluya responsabilidades y fechas periódicas de revisión.

1.2.2. Infraestructura de seguridad de información

Las gerencias de más alto rango y/o un comité de alto nivel de administración de seguridad de información, tienen la responsabilidad de asegurar que existe una dirección clara y apoyo administrativo para manejar los riesgos efectivamente.

Debe existir un grupo de control o un comité de seguridad para coordinar la implementación de la seguridad de la información y la administración de los riesgos.

Deben definirse claramente, las responsabilidades para la protección de los activos individuales y para llevar a cabo procesos específicos de seguridad de información.

Debe existir y seguirse un proceso de autorización administrativa para el uso de nuevas instalaciones y equipos de procesamiento de la información.

1.2.3. Seguridad de acceso para terceras partes

Deben existir y seguirse procedimientos para controlar el acceso físico y lógico de terceras partes, a las instalaciones y a los sistemas del Certificador (Ej., contratistas actuando en el sitio, socios comerciales, proveedores y aliados.)

Si hubiese una necesidad comercial para el Certificador de permitir el acceso a un tercero a sus instalaciones y sistemas, debe ejecutarse una evaluación de riesgos para determinar las implicaciones de seguridad y los requerimientos de control específicos.

Los arreglos que comprendan el acceso de un tercero a las instalaciones y sistemas del Certificador, deben basarse en un contrato formal, que contenga todos los requerimientos de seguridad necesarios.

1.2.4. Servicios o funciones contratados a terceros (outsourcing)

En el caso que el Certificador transfiera a otra organización, vía *"outsourcing"*, la administración y/o el control de todos o algunos componentes de tecnología de información (sistemas de información, redes de datos, ambientes o estaciones de trabajo, etc.), los requerimientos de seguridad del Certificador deben ser consignados en un contrato previamente acordado entre las partes.

En el caso que el Certificador escoja delegar una parte de sus roles y las respectivas funciones a otra organización, el Certificador debe ser, en definitiva, el responsable por el cumplimiento de las funciones transferidas y por la definición y mantenimiento de lo estipulado en su DPC.

1.3. De la clasificación y administración de activos

El Certificador debe mantener controles para brindar una seguridad razonable de que sus activos e información reciben un nivel apropiado de protección, basado en los requerimientos de todas las PC en uso y en el análisis de riesgos.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

1) Todos los activos del Certificador deben tener un encargado/dueño debidamente identificado, con responsabilidades asignadas para el mantenimiento de los controles aplicables.

2) Deben mantenerse inventarios de los activos del Certificador.

3) El Certificador debe implementar un esquema para la clasificación de la información y los controles de protección aplicables a esta información, basados en las necesidades de negocio e impactos comerciales asociados con tales necesidades.

4) Se deben definir procedimientos para asegurar que el etiquetado y la manipulación de información, se lleven a cabo de acuerdo con el esquema de clasificación del Certificador.

1.4. De la seguridad del personal

El Certificador debe mantener controles para brindar una seguridad razonable de que las prácticas de personal y de reclutamiento incrementan y apoyan la confianza de sus operaciones.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

1) El Certificador debe emplear personal que posea las habilidades, conocimiento y experiencia relevantes y apropiados para las funciones del trabajo.

2) El Certificador debe documentar en las descripciones de puestos, los roles de seguridad y las responsabilidades, tal como se especifican en las políticas de seguridad de la organización. Los puestos de confianza sobre los que depende la seguridad del Certificador, deben ser claramente identificados.

La definición de los puestos de confianza debe incluir, al menos las siguientes funciones:

1) Responsabilidad general de administrar la implementación de las prácticas de seguridad del Certificador;

2) Aprobación de la generación, revocación y suspensión de los certificados;

3) Instalación, configuración y mantenimiento de los sistemas del Certificador;

4) Operación diaria de los sistemas del Certificador, respaldo y recuperación de sistemas;

5) Inspección y mantenimiento de las bitácoras del sistema del Certificador y de los registros de auditoría;

6) Funciones de administración del ciclo de vida de llaves criptográficas (Ej. custodios de componentes de llaves); y,

7) Desarrollo de sistemas del Certificador.

Las políticas y procedimientos del Certificador deben especificar los procedimientos de comprobación y aprobación de antecedentes de los candidatos (currículo, referencias, etc.), requeridos para roles de confianza y otros roles. Como mínimo, la verificación de los antecedentes de los empleados debe ejecutarse al momento de la aplicación para el puesto y periódicamente para aquellas personas que ejecutan roles de confianza.

El rol de confianza de un individuo debe ser aprobado antes de otorgar el acceso a los sistemas, instalaciones o ejecutar acciones que requieran de dicho rol.

El Certificador debe asegurar la no divulgación de información sensible, por parte de su personal y los que ocupan roles de confianza, utilizando mecanismos de control (Ej., acuerdos de confidencialidad).

Los contratistas que ejecutan roles de confianza, deben estar sujetos, al menos, al mismo control de contratación y a los mismos procedimientos de manejo de personal, que los funcionarios del Certificador.

Cualquier arreglo contractual entre contratistas y el Certificador, debe admitir una cláusula de contrato de personal temporal, que explícitamente permita a la organización tomar medidas en el caso de que el personal contratado viole las políticas de seguridad de la organización. Las medidas protectoras pueden incluir:

1) Requerimientos de garantía en contrato de personal;

2) Indemnización por daños debido a acciones perjudiciales premeditadas del personal contratado; y,

3) Multas financieras.

Debe existir y seguirse un proceso disciplinario formal para empleados que hayan violado las políticas y procedimientos de seguridad de la organización.

Cuando un contrato de trabajo es concluido, deben ejecutarse acciones apropiadas y oportunas, de manera que los controles (Ej. controles de acceso), no sean perjudicados.

Al personal que podría ser blanco de coerción, debe proporcionársele una alarma contra coacción, amenaza o violencia.

Todos los empleados de la organización, y cuando sea pertinente, de los contratistas como terceras partes, deben recibir un entrenamiento apropiado en procedimientos y políticas organizacionales, especialmente en materia de seguridad, marco legal y controles de la organización.

1.5. De la seguridad física y ambiental

El Certificador debe mantener controles para brindar una seguridad razonable de que:

- El acceso físico a las instalaciones del Certificador está limitado a personal autorizado.

- Las instalaciones estén protegidas de peligros ambientales.

- Se previenen posibles pérdidas y daños o compromisos de los bienes del Certificador y se previene la posible interrupción de sus actividades normales.

- Se previene el compromiso de la información y de la infraestructura que procesa esa información.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

1.5.1. Seguridad física de las instalaciones del Certificador

La protección física debe lograrse por medio de la creación de un perímetro de seguridad restringido (Ej., barreras físicas y lógicas). Las instalaciones donde se generan y entregan los certificados del Certificador deben protegerse con su propio y único perímetro físico.

El perímetro del edificio o sitio donde se encuentran las instalaciones de producción de certificados del Certificador, deben tener el mínimo de puntos de acceso y estos deben ser debidamente controlados.

Debe existir un área de recepción debidamente controlada y atendida por personal de seguridad, y barreras físicas, para restringir el acceso al edificio y al sitio de operaciones del Certificador, únicamente para el personal debidamente autorizado.

Se deben colocar barreras físicas (Ej., paredes sólidas que se extiendan desde el piso "real" al cielo raso "real") para prevenir el ingreso no autorizado y la contaminación ambiental a las instalaciones de producción de certificados del Certificador.

Se deben colocar barreras para prevenir emisiones de radiación electromagnética en las operaciones del certificador raíz registrado, (Ej., generación de llaves y de certificados de Certificador raíz y Certificador subordinado) y donde la PC lo requieran.

Las puertas contra incendio que se ubiquen en el perímetro de seguridad alrededor de las instalaciones operacionales del Certificador, deben tener alarmas y cumplir con las regulaciones locales contra incendios.

Se debe instalar y probar regularmente, un sistema de detección de intrusos, que cubra todas las puertas externas del edificio donde se encuentran las instalaciones operacionales del Certificador.

Cuando las instalaciones operacionales del Certificador estén desocupadas, deben estar cerradas con llave y con las alarmas debidamente activadas.

Todo el personal debe portar una identificación visible. Los empleados deben ser instados a confrontar a cualquiera que no tenga la identificación visible.

El acceso a las instalaciones operacionales del Certificador debe ser controlado y restringido a personas autorizadas, utilizando controles de autenticación.

Todo el personal que entra y sale de las instalaciones operacionales debe registrarse (es decir, se mantiene en forma segura un registro de auditoría de todos los accesos).

Los visitantes a las instalaciones operacionales del Certificador deben ser escoltados y registrarse la fecha y hora de entrada y salida.

Al personal de soporte (provisto por terceros) se les puede conceder acceso restringido a las instalaciones operacionales del Certificador, solamente cuando sea requerido y dicho acceso debe ser autorizado y escoltado.

Los derechos de acceso a las instalaciones del Certificador deben revisarse y actualizarse regularmente.

1.5.2. Seguridad de los equipos

El Certificador debe de mantener un inventario de sus equipos.

El equipo debe ubicarse o protegerse de tal forma que se reduzcan los riesgos de amenazas ambientales y peligros, así como de oportunidades de accesos no autorizados.

El equipo debe estar protegido contra fallas de corriente y otras anomalías eléctricas.

El cableado eléctrico y de telecomunicaciones, que conduce datos o servicios de respaldo del Certificador, debe ser protegido contra interceptaciones o daños.

El equipo debe mantenerse de acuerdo con las instrucciones del fabricante y/u otros procedimientos documentados, para asegurar su disponibilidad e integridad continua.

Todos los equipos que contengan medios de almacenamiento (discos fijos o removibles) deben examinarse, previo a su eliminación, para asegurar que no contienen datos confidenciales o protegidos. Los medios de almacenamiento que contengan datos sensibles debe ser destruidos físicamente o sobrescritos en forma segura, previo a su eliminación o reutilización.

1.5.3. Controles generales

Se debe guardar bajo llave la información de negocio sensible o crítica, cuando no sea requerida y cuando las instalaciones del Certificador estén desocupadas (sin ocupación humana).

Los procedimientos deben requerir que, cuando las computadoras personales y estaciones de trabajo no se estén utilizando, deben cerrarse las sesiones, bloquearse con contraseña o utilizar algún otro control similar.

Los procedimientos deben requerir que el equipo, la información y los programas de cómputo (*software*), pertenecientes a la organización, no pueden ser extraídos de las instalaciones sin autorización.

1.6. De la administración de operaciones

El Certificador debe mantener controles para brindar una seguridad razonable de que:

- Está garantizada la operación correcta y segura de las instalaciones de procesamiento de información del Certificador;

- El riesgo de fallas en los sistemas del Certificador es reducido al mínimo;

- La integridad de los sistemas e información del Certificador está protegida contra virus y programas de cómputo (*software*) maliciosos;

- El daño por incidentes de seguridad y defectos de funcionamiento es reducido al mínimo utilizando reportes de incidentes y procedimientos de respuesta; y

- Los medios de almacenamiento de información son manejados con seguridad para protegerlos de daños, robos y accesos no autorizados.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

1.6.1. Procedimientos operacionales y responsabilidades

Los procedimientos operacionales del Certificador deben estar documentados y deben ser mantenidos por área funcional.

Deben existir procedimientos y responsabilidades formalmente establecidos, para controlar todos los cambios en el equipo, *software* y procedimientos operativos del Certificador.

Las obligaciones de los cargos y áreas de responsabilidad deben estar segregadas para reducir las oportunidades de modificación no autorizada o mal uso de la información o los servicios, por parte de una sola persona.

Las instalaciones para desarrollo y prueba de sistemas deben estar separadas de las instalaciones operacionales.

1.6.2. Planificación y aprobación de nuevos sistemas

Se deben monitorear y evaluar las demandas de capacidad y hacer proyecciones de los requerimientos futuros de capacidad, para asegurar que esté disponible el adecuado poder de procesamiento y de almacenamiento.

Se deben establecer criterios de aprobación de nuevos sistemas de información, de mejoras y nuevas versiones, así como llevar a cabo pruebas de sistemas antes de su aceptación.

1.6.3. Protección contra virus y programas de cómputo maliciosos

Deben implementarse controles de detección y prevención contra virus y *software* malicioso. Deben existir programas de concientización apropiados para los empleados, sobre este problema.

1.6.4. Reporte y respuesta de incidentes

Debe existir un procedimiento formal de reporte de incidentes de seguridad, que detalle las acciones a ser tomadas en caso de reportarse un incidente. Este debe incluir una definición y documentación de responsabilidades asignadas y procedimientos de escalamiento. Cualquier incidente debe ser reportado a la EGP con urgencia.

Los usuarios de los sistemas del Certificador que desempeñan roles de confianza deben anotar y reportar (de acuerdo con lo establecido en la PC) cualquier observación o sospecha de debilidades o amenazas en la seguridad interna de los sistemas o servicios, para asegurar una respuesta apropiada a los incidentes de seguridad.

Debe existir y seguirse un procedimiento para reportar el mal funcionamiento del *hardware* y *software* (equipos, programas de cómputo, etc.)

Debe existir y seguirse un procedimiento para asegurar que las fallas son reportadas y que se toman las acciones correctivas.

Debe existir un proceso formal de manejo de problemas, que permita documentar, cuantificar y monitorear los tipos, cantidad e impacto de incidentes y fallas de funcionamiento.

1.6.5. Manejo y seguridad de los medios de almacenamiento de información

Los procedimientos para el manejo de medios de almacenamiento de información removibles de las computadoras deben requerir lo siguiente:

1) que el contenido anterior de cualquier medio reutilizable de información que vaya a ser removido de la organización, debe borrarse o bien destruir el medio de almacenamiento de la información en forma segura.

2) para toda la información que sea removida de la organización, se requiere una autorización y se conserva un registro de tales remociones para mantener un rastro de auditoría; y

3) que todo medio de información se almacena en un ambiente adecuado y seguro, de acuerdo con las especificaciones del fabricante.

Los equipos que contengan medios de almacenamiento (es decir, discos duros fijos), deben examinarse para determinar si contienen alguna información sensible, antes de su eliminación o reutilización. De ser el caso, estos deben ser destruidos físicamente o sobrescritos en forma segura, antes de su eliminación o re-utilización.

Deben existir y seguirse procedimientos para el manejo y almacenamiento de la información, para protegerla de divulgación no autorizada o mal uso.

La documentación del sistema debe protegerse de accesos no autorizados.

1.7. De la administración de acceso al sistema

El Certificador debe mantener controles para brindar una seguridad razonable que el acceso a sus sistemas se limita a personal autorizado. Tales controles deben proveer una seguridad razonable con respecto a:

- El acceso al sistema operativo, este debe ser restringido a individuos autorizados con privilegios para tareas predeterminadas.

- El acceso a segmentos de red, donde se ubican las sistemas del Certificador está limitado a individuos, aplicaciones y servicios autorizados; y

- El uso de las aplicaciones del Certificador está limitado solamente a individuos autorizados.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

1.7.1. Administración del control de acceso de usuarios

Los requerimientos de negocio para el control de acceso, deben estar definidos y documentados en una política de control de acceso, la cual debe incluir al menos lo siguiente:

1) roles y permisos de acceso correspondientes;

2) procesos de identificación y autenticación para cada usuario;

3) la segregación de deberes;

4) el número de personas (“key share holders”) requeridas para ejecutar operaciones específicas del Certificador (es decir, regla “m de n”, dónde “m” representa el número de partes de la llave requeridos para ejecutar una operación y “n” representa el número total de partes de la llave.)

Debe existir un procedimiento formal para la inscripción y desinscripción de los usuarios con roles de confianza, para otorgar acceso a los servicios y sistemas del Certificador.

La asignación y uso de los privilegios debe ser restringido y se deben ejercer controles dobles.

La asignación de contraseñas u otros mecanismos de autenticación, deben ser controlados a través de un proceso de administración formal.

Los derechos de acceso para usuarios con roles de confianza deben ser revisados regularmente.

1.7.2. Control de acceso a la red

El personal del Certificador debe ser provisto de acceso solamente a aquellos servicios que específicamente le han sido autorizados a utilizar. La ruta de acceso desde la terminal del usuario a los servicios computarizados debe ser controlada.

El acceso remoto a los sistemas del Certificador, realizado por los empleados o por sistemas externos debe tener autenticación mutua.

Las conexiones hechas por los empleados o sistemas del Certificador hacia sistemas computadorizados remotos deben tener autenticación mutua.

El acceso a los puertos utilizados para diagnóstico debe estar controlado en forma segura.

Los controles (Ej., *firewalls*) deben estar instalados en la forma y lugar apropiados para proteger el dominio de la red interna del Certificador de accesos no autorizados desde cualquier otro dominio.

Los controles deben estar instalados en la forma y lugar apropiados para limitar los servicios de la red (Ej. HTTP, FTP, etc.) y mantenerlos disponibles a los usuarios autorizados, de acuerdo con las políticas de control de acceso del Certificador. Las características de seguridad de todos los servicios de la red utilizada por la organización del Certificador deben estar debidamente documentadas.

Los controles de enrutamiento deben asegurar que las conexiones de las computadoras y la circulación de la información, no violen las políticas de control de acceso del Certificador.

El Certificador debe asegurar que los componentes de la red local (Ej. *firewalls*, enrutadores) se mantengan en un ambiente físicamente seguro y sus configuraciones deben ser auditadas periódicamente en cumplimiento con los requerimientos de configuración establecidos por el Certificador.

Los datos sensibles deben estar cifrados (encriptados) cuando se intercambian sobre redes públicas o no confiables.

1.7.3. Control de acceso al sistema operativo

Los sistemas operativos deben estar configurados de acuerdo con los estándares de configuración del sistema operativo establecidos para el Certificador y deben revisarse periódicamente.

Las actualizaciones y parches de los sistemas operativos deben ser aplicados de manera oportuna, cuando sea considerado necesario, basándose en una evaluación de riesgos.

La identificación automática de terminales debe utilizarse para autenticar las conexiones a equipo portátil o a lugares específicos.

El acceso a los sistemas del Certificador requiere de un proceso seguro de autenticación.

Todo el personal del Certificador debe tener un identificador único (ID de usuario), para su uso personal y exclusivo, de modo que las actividades puedan ser rastreadas hasta el individuo responsable. Cuando se requieren cuentas de grupos o compartidas, deben implementarse otros controles de monitoreo para mantener la asignación de responsabilidades en forma individual.

La utilización de programas utilitarios del sistema debe ser restringida al personal autorizado, y debe ser estrictamente controlado.

Las terminales inactivas conectadas a los sistemas del Certificador, deben re-autenticarse antes de utilizarse. El período para la inactivación se regirá por las políticas aplicables.

Deben utilizarse restricciones en los tiempos de conexión, para proporcionar una seguridad adicional, a las aplicaciones de alto riesgo.

La información sensible del sistema debe ser protegida contra la divulgación a usuarios no autorizados.

1.7.4. Control del acceso a las aplicaciones

El acceso a la información y a las funciones del sistema de aplicaciones debe ser restringido, de acuerdo con las políticas de control de acceso del Certificador.

El personal del Certificador debe ser debidamente identificado y autenticado, antes de utilizar las aplicaciones críticas relacionadas con el manejo de los certificados.

Los sistemas sensibles (Ej. Certificador raíz), deben contar con un ambiente informático dedicado (aislado).

1.8. Del desarrollo y mantenimiento de sistemas

El Certificador debe mantener controles que proporcionen una seguridad razonable de que las actividades de desarrollo y mantenimiento en los sistemas son autorizadas, de modo tal que se salvaguarde la integridad de los mismos.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

1) Los requerimientos de negocio para nuevos sistemas o para la expansión de los sistemas existentes, deben especificar los requerimientos de control.

2) Deben existir y seguirse procedimientos de prueba de software y control de cambios para la implementación de software en los sistemas en producción, incluyendo un cronograma para la puesta en marcha de nuevas versiones de software, modificaciones o arreglos de emergencia.

3) Deben existir y seguirse procedimientos de control del cambio para el hardware, los componentes de la red y los cambios de configuración del sistema.

4) Debe existir control sobre el acceso a las bibliotecas de los programas fuentes.

5) Cuando ocurran cambios en el sistema operativo, los sistemas deben ser revisados y probados.

6) Las modificaciones informales a los paquetes de software deben ser desalentadas y todos los cambios estrictamente controlados.

7) La compra, uso y modificación del software debe controlarse e inspeccionarse para protegerse contra posibles canales encubiertos y códigos troyanos. Esto debe incluir la autenticación del código fuente del software. Estos controles deben aplicarse igualmente al desarrollo del software externo. Esto debe incluir la acreditación de Criterios Comunes (“Common Criteria”) según lo definido por el ISO 15408 o la que defina la EGP.

1.9. De la administración de la continuidad del negocio

El Certificador debe mantener controles para proporcionar una seguridad razonable de la continuidad de las operaciones, en caso de un desastre. Tales controles deben incluir como mínimo:

- El desarrollo y prueba de un plan de recuperación de desastres del Certificador;

- El almacenaje del material criptográfico requerido (es decir, dispositivos criptográficos seguros y material de activación), en un sitio alterno;

- El almacenaje de los respaldos de los sistemas, datos e información de la configuración en un sitio alterno; y

- La disponibilidad de un sitio alterno, equipo y conectividad para permitir la recuperación.

El Certificador debe mantener los controles necesarios para proporcionar una seguridad razonable de que; ante la cesación o degradación de sus servicios, las potenciales interrupciones a suscriptores y terceros dependientes sean minimizadas.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

- El Certificador debe contar con un proceso administrativo para desarrollar y mantener los planes de continuidad del negocio. El Certificador debe contar con una estrategia de planeamiento de continuidad del negocio basada en una evaluación de riesgo apropiada.

- El Certificador debe tener un plan de continuidad del negocio para mantener o restaurar sus operaciones de una manera oportuna después de una interrupción, o falla de los procesos críticos. El plan de continuidad del negocio del Certificador debe contemplar lo siguiente:

    1) Las condiciones para la activación de los planes;

    2) Procedimientos administrativos de emergencia;

    3) Procedimientos operativos de emergencia (“fallback procedures”);

    4) Procedimientos de reanudación o recuperación;

    5) Un cronograma de mantenimiento para el plan;

    6) Requerimientos de concientización y educación;

    7) Las responsabilidades de los individuos;

    8) Tiempo de recuperación meta (“recovery time objective”, RTO); y

    9) Pruebas regulares de los planes de contingencia.

Los planes de continuidad del negocio deben incluir procesos de recuperación de desastres para todos los componentes críticos del sistema del Certificador, incluyendo el *hardware*, *software* y llaves, en el caso de falla de uno o más de estos componentes.

Específicamente:

10) los dispositivos criptográficos utilizados para el almacenamiento del respaldo de las llaves privadas del Certificador deben ser guardados de forma segura, en un sitio alterno, para que sean recuperados en el caso de un desastre en el sitio primario;

11) las partes de la clave secreta o los componentes necesarios para usar y manejar los dispositivos criptográficos de recuperación de desastres, deben estar también guardados con seguridad en una ubicación fuera del sitio primario.

Deben realizarse regularmente copias de respaldo de la información de negocio esencial. Los requerimientos de seguridad de estas copias deben ser consistentes con los controles de la información respaldada.

El Certificador debe identificar y acondicionar un sitio alternativo donde el núcleo de las operaciones de la infraestructura de llave pública (PKI, por sus siglas en inglés) pueda ser restaurado en caso de desastre en el sitio primario. El equipo de respaldo (*"fallback equipment"*) y los medios de respaldo deben ubicarse en un lugar que asegure que se evitaran daños por el desastre ocurrido en el sitio principal.

Los planes de continuidad del negocio del Certificador deben incluir los procedimientos para asegurar sus instalaciones, hasta donde sea posible, durante un período aceptable después de un desastre y antes de restaurar en un ambiente seguro, ya sea en el sitio original o en uno remoto.

Los planes de continuidad del negocio del Certificador deben establecer los procedimientos de recuperación a utilizar, si los recursos computacionales, *software*, y/o datos están corruptos o se sospechen que lo están.

Los planes de continuidad del negocio deben probarse regularmente para asegurar que se encuentran actualizados y son efectivos.

1.10.De la supervisión y el cumplimiento

El Certificador debe mantener controles que proporcionen una seguridad razonable de que:

- Está cumpliendo con los requerimientos legales, regulatorios y contractuales relevantes;

- Está asegurado el cumplimiento de las políticas y procedimiento de seguridad del Certificador y

- El uso no autorizado de los sistemas es detectado.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

1.10.1. Cumplimiento de los requisitos legales

El Certificador debe tener procedimientos para asegurar que todos los requerimientos relevantes legales, regulatorios y contractuales son explícitamente definidos y documentados para cada sistema de información.

El Certificador debe tener procedimientos implementados para asegurar el cumplimiento de restricciones legales en el uso de material, con respecto a los derechos de propiedad intelectual, y al uso de productos de *software* patentados.

Los controles deben estar establecidos para asegurar el cumplimiento con acuerdos nacionales, leyes, regulaciones y otros instrumentos para controlar el acceso a, o uso de *hardware* y *software* criptográfico.

Deben existir procedimientos para asegurar que la información personal está protegida de conformidad con la legislación pertinente.

La política de seguridad de la información debe abordar lo siguiente:

1) La información que debe mantenerse confidencial por el Certificador o el Registrador;

2) La información que no es considerada confidencial;

3) La política de entrega de información a las autoridades judiciales;

4) La información que puede ser revelada como parte de un proceso civil,

5) Las condiciones sobre las cuales la información puede ser revelada con el consentimiento del suscriptor; y

6) Cualquier otra circunstancia bajo la cual la información confidencial puede ser revelada.

Los registros importantes del Certificador deben estar protegidos contra pérdida, destrucción y falsificación.

1.10.2. Revisión del cumplimiento de la política de seguridad y el cumplimiento técnico

Los directores del servicio de certificación son responsables de garantizar que los procedimientos de seguridad dentro de su área de responsabilidad, se llevan a cabo correctamente.

Las operaciones del Certificador deben estar sujetas a revisiones periódicas para asegurar el cumplimiento con lo estipulado en su DPC.

Los sistemas del Certificador deben ser inspeccionados periódicamente para asegurar que cumplen con los estándares de seguridad implementados.

1.10.3. Monitoreo del acceso y uso de los sistemas

Se deben establecer procedimientos para monitorear el uso de los sistemas del Certificador, y revisar periódicamente el resultado de esta actividad. Se deben implementar mecanismos de alerta para detectar accesos no autorizados.

1.11.Del registro de auditorías

El Certificador debe mantener controles para brindar una seguridad razonable de que:

- Los eventos relacionados con el ambiente de operación del Certificador, el manejo de las llaves y los certificados, son registrados exacta y apropiadamente;

- Se mantiene la confidencialidad y la integridad de los registros de auditoría, los (vigentes y archivados);

- Los registros de auditoría son archivados completa y confidencialmente, de conformidad con las prácticas de negocio divulgadas; y,

- Los registros de auditoría son revisados periódicamente por personal autorizado.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

1.11.1. Bitácoras de auditoría

El Certificador debe generar bitácoras de auditoría automáticas (electrónicos) o manuales, según lo requerido por la legislación y la DPC.

Todos los registros en la bitácora deben incluir lo siguiente:

1) El día y la hora del registro;

2) El número de serie o de secuencia del registro (para registros de bitácora automáticos);

3) Tipo de registro;

4) La fuente del registro (Ej., terminal, puerto, ubicación, cliente, etc.); y,

5) La identidad de la entidad que hace el registro en la bitácora.

1.11.2. Eventos a registrar

El Certificador debe registrar los siguientes eventos relacionados con la administración del ciclo de vida de su llave y la del suscriptor (si aplica):

1) La generación de llaves del Certificador;

2) La instalación de las llaves criptográfica manuales y su resultado (con la identidad del operador);

3) El respaldo de la llaves del Certificador;

4) El almacenamiento de las llaves del Certificador;

5) La recuperación de la llave del Certificador;

6) Las actividades de custodia de las llaves del Certificador (si aplica);

7) El uso de las llaves del Certificador;

8) El archivado de las llaves del Certificador;

9) El retiro de servicio, del material relacionado con las llaves ("keying material");

10) La destrucción de las llaves del Certificador;

11) La identidad de la entidad que autoriza una operación administrativa de llaves;

12) La identidad de las entidades que manipulan cualquier material relacionado con las llaves ("keying material"), tales como componentes de llave, o llaves almacenadas en dispositivos o medios portátiles;

13) La custodia de llaves y de dispositivos o medios de almacenamiento de llaves; y,

14) El compromiso de una llave privada.

El Certificador debe registrar los siguientes eventos relacionados con la administración del ciclo de vida del dispositivo criptográfico:

1) La recepción e instalación del dispositivo;

2) La colocación o remoción de un dispositivo de su lugar de almacenamiento;

3) La activación y el uso del dispositivo;

4) La desinstalación del dispositivo;

5) La designación de un dispositivo para servicio y reparación; y

6) El retiro permanente del dispositivo.

Si el Certificador proporciona servicios de administración de llaves del suscriptor, este debe registrar los siguientes eventos relacionados con el manejo del ciclo de vida de estas llaves:

1) La generación de la llave;

2) La distribución de la llave (si aplica);

3) El respaldo de la llave (si aplica);

4) La custodia de la llave (si aplica);

5) El almacenamiento de la llave (si aplica);

6) La recuperación de la llave (si aplica);

7) El archivado de la llave (si aplica);

8) La destrucción de la llave;

9) La identidad de la entidad que autoriza una operación administrativa con las llaves; y,

10) El compromiso de la llave.

El Certificador debe registrar (o solicitar que el registrador registre) la siguiente información en la solicitud del certificado:

1) El método de identificación utilizado y la información utilizada para satisfacer los requerimientos de "Conozca a su Cliente" ("Know Your Customer");

2) El expediente con datos de identificación únicos, números o una combinación de estos (Ej. número de cédula de identidad del solicitante), documentos de identificación, si aplica;

3) El lugar de archivo de las copias de solicitudes y copias de los documentos de identificación;

4) La identificación de la entidad que acepta la solicitud;

5) El método utilizado para validar los documentos de identificación, si hay alguno;

6) El nombre del Certificador que recibe o del registrador que envía la solicitud, si aplica;

7) La aceptación del solicitante del contrato de suscriptor; y

8) El consentimiento del suscriptor para permitir que el Certificador mantenga registros con datos personales, traslade esta información a terceros específicos, y publique los certificados. Todo lo anterior cuando se requiera y de conformidad con la legislación aplicable,

El Certificador debe registrar los siguientes eventos relacionados con la administración del ciclo de vida del certificado:

1) El recibo de solicitudes para certificado(s) – incluyendo solicitudes iniciales de certificado, solicitudes de renovación y solicitudes de reemisión;

2) La presentación de llaves públicas para certificación;

3) La afiliación de un suscriptor;

4) La generación de certificados;

5) La distribución de la llave pública del Certificador;

6) Las solicitudes de revocación de certificado;

7) La revocación de certificado;

8) Las solicitudes de suspensión de certificado (si aplica);

9) La suspensión y reactivación del certificado (si aplica); y,

10) La generación y emisión de las LRC.

El Certificador debe registrar los siguientes eventos sensibles de seguridad:

1) Lectura y escritura de registros o archivos sensibles de seguridad, incluyendo las mismas bitácoras de auditoría;

2) Las acciones tomadas contra los datos sensibles de seguridad.

3) Los cambios de perfil de seguridad;

4) El uso de mecanismos de identificación y autenticación, tanto exitosos como infructuosos (incluyendo múltiples intentos de autenticación fallida);

5) Las transacciones no financieras de seguridad sensible (Ej. cambios en la cuenta, nombre, dirección, etc.);

6) Las caídas del sistema, fallas del hardware y otras anomalías;

7) Las acciones tomadas por individuos con roles de confianza, operadores de computadora, administradores del sistema, y oficiales de seguridad de sistemas;

8) La afiliación de un suscriptor;

9) Las decisiones de pasar por alto los procedimientos o procesos de encriptación o autenticación; y,

10) El acceso a los sistemas del Certificador o cualquiera de sus componentes.

Las bitácoras de auditoría no deben registrar las llaves privadas de ninguna forma (Ej. en texto plano o encriptado).

Los relojes del sistema de cómputo del Certificador deben estar sincronizados para un registro exacto, como se define en la PC o la DPC, que especifican la fuente de tiempo aceptada.

1.11.3. Protección de las bitácoras de auditoría

Las bitácoras de auditoría actuales o archivadas, deben mantenerse de forma que prevenga su modificación o destrucción no autorizada.

La llave privada utilizada para firmar las bitácoras de auditoría no debe ser utilizada para ningún otro propósito. Esto debe aplicarse igualmente a una llave secreta simétrica utilizada con un mecanismo "*Message Authentication Code*" (MAC) simétrico.

1.11.4. Archivo de bitácoras de auditoría

El Certificador debe archivar sus bitácoras de auditoría periódicamente.

Además de lo indicado por una posible estipulación regulatoria, debe ejecutarse una evaluación de riesgo, para determinar el período apropiado para la retención de las bitácoras de auditoría.

El Certificador debe mantener las bitácoras de auditoría archivadas en un sitio alterno seguro, por un período determinado, definido por la evaluación de riesgo y los requerimientos legales aplicables.

1.11.5. Revisión de bitácoras de auditoría

Las bitácoras de auditoría actuales y archivadas deben ser recuperadas solamente por personal autorizado, ya sea por razones válidas del negocio o por seguridad.

Las bitácoras de auditoría deben ser revisadas de acuerdo con las prácticas establecidas en la declaración de prácticas de certificación.

La revisión de las bitácoras de auditoría actuales y archivadas debe incluir una validación de la integridad de las mismas, y la identificación y seguimiento de actividades poco comunes, no autorizadas o sospechosas.

Ejemplos de condiciones que requieren análisis y una posible acción, incluyen la saturación inusual de los recursos del sistema, un incremento repentino e inesperado en el volumen y accesos en horarios inusuales o desde lugares inusitados.

2. Controles para la administración del ciclo de vida de la llave del Certificador

2.1. De la generación de las llaves del Certificador

El Certificador debe mantener controles para brindar una seguridad razonable de que los pares de llaves son generados de acuerdo con el protocolo definido para la generación de llaves y con los requerimientos de la DPC.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

2.1.1. Generación de llaves del Certificador, incluyendo las llaves del Certificador raíz

La generación de las llaves del Certificador debe llevarse a cabo de acuerdo con un detallado procedimiento (protocolo) de generación de llaves, que especifique los pasos a ejecutar y las responsabilidades de los participantes.

El documento que registra el procedimiento de generación de llaves del Certificador debe incluir lo siguiente:

1) Definición de roles y responsabilidades;

2) Aprobación para dirigir el protocolo de la generación de llaves;

3) El hardware criptográfico y los materiales de activación requeridos por el protocolo

4) Los pasos específicos ejecutados durante el protocolo de generación de llaves;

5) Procedimientos para el almacenamiento seguro del hardware criptográfico y los materiales de activación, después de terminado el protocolo de generación de llaves;

6) La firma (de cualquier tipo válido) de aprobación de los participantes y testigos indicando si el proceso se ejecutó de acuerdo con el protocolo de generación de llaves;

7) Anotación de cualquier desviación con respecto al procedimiento estipulado en el protocolo de generación de llaves.

La generación de las llaves del Certificador debe producirse dentro de un Módulo Criptográfico que cumpla con los requerimientos del ISO 15782-1 o los que defina la EGP, y los requerimientos de negocio correspondientes estipulados por la DPC. Tal dispositivo criptográfico debe ejecutar la generación de la llave utilizando un generador de números aleatorio (RNG por sus siglas en inglés) o un generador de números seudo-aleatorio (PRNG) como se especifica en ISO 18032 o en las políticas que defina la EGP.

La generación de las llaves del Certificador debe llevarse acabo en un ambiente físicamente seguro, por personal con roles de confianza y bajo los principios de control múltiple y de conocimiento (secreto) dividido.

El Certificador debe generar su propio par de llaves, en el mismo dispositivo criptográfico en el cual será utilizado, o el par de llaves debe ser introducido directamente desde el dispositivo criptográfico donde fue generado al dispositivo criptográfico donde será utilizado.

El proceso de generación de llaves debe producir llaves que:

1) Sean apropiadas para la aplicación o propósito destinado, y que sean proporcionales a los riegos identificados;

2) Usen un algoritmo aprobado, como se especifica en ISO 18033 o en las políticas que defina la EGP;

3) Tengan una longitud de llave (“key length”) que sea apropiada para el algoritmo y para el período de validez del certificado del Certificador;

4) Tomen en cuenta los requerimientos del tamaño de llave del Certificador padre y subordinado; y

5) Sean acordes con la PC.

La generación de llaves del Certificador debe tener por resultado un tamaño de llave de acuerdo con la PC. La longitud de la llave pública que va a ser certificada por el Certificador, debe ser menor o igual que la de su llave privada de firma.

Debe probarse la integridad del *hardware*/*software* utilizados para la generación de llaves y las interfaces al *hardware*/*software*, antes de su uso en producción.

2.2. Almacenamiento, respaldo y recuperación de la llave del Certificador

El Certificador debe mantener controles para proporcionar una seguridad razonable de que:

- Las llaves privadas del Certificador permanecen confidenciales y mantienen su integridad y

- El acceso al *hardware* criptográfico del Certificador está limitado a individuos autorizados.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

Las llaves privadas del Certificador (de firma y confidencialidad) deben guardarse y usarse dentro de un dispositivo criptográfico seguro que al menos cumpla con el perfil de protección apropiado conforme al ISO 15408 o los requerimientos del nivel FIPS 140-1 apropiado, basados en una evaluación de riesgo y en los requerimientos de negocio del Certificador, y de acuerdo con la PC y DPC aplicables del Certificador.

Si las llaves privadas del Certificador no son exportadas del módulo criptográfico seguro, entonces la llave privada del Certificador debe ser generada, guardada y utilizada dentro del mismo módulo criptográfico.

Si las llaves privadas del Certificador son exportadas desde un módulo criptográfico seguro hacia un medio de almacenamiento seguro para propósitos de procesamiento fuera de línea ("*offline*"), o respaldo y recuperación, entonces deben ser exportadas dentro de un esquema de manejo de llaves seguro que incluya alguna de las siguientes formas de exportación:

1) Como un texto cifrado, utilizando una llave que esté asegurada apropiadamente;

2) Como una llave fragmentada cifrada, utilizando controles múltiples y conocimiento/propiedad dividida; o,

3) En otro módulo criptográfico seguro, tal como un dispositivo de transporte de llaves utilizando control múltiple.

Si las llaves privadas del Certificador son respaldadas, deben ser respaldadas, guardadas y recuperadas por personal autorizado con roles de confianza, utilizando controles múltiples en un ambiente físicamente seguro. La cantidad de personal autorizado para llevar a cabo estas funciones debe mantenerse al mínimo.

Si las llaves privadas del Certificador son respaldadas, las copias de respaldo deben estar sujetas al mismo o mayor nivel de control de seguridad que las llaves que actualmente están en uso. La recuperación de las llaves del Certificador debe ser llevada a cabo de una forma tan segura como el proceso de respaldo.

2.2.1. Administración del ciclo de vida del dispositivo criptográfico del Certificador

Las políticas y procedimientos deben requerir que el *hardware* criptográfico del Certificador sea enviado por el fabricante vía correo certificado (o equivalente) utilizando un embalaje con sello de garantía (*"tamper evident"*). Al recibir el Certificador este equipo criptográfico del fabricante, el personal autorizado del Certificador debe inspeccionar el embalaje, para determinar si el sello está intacto.

Al recibir el Certificador el *hardware* criptográfico del fabricante o cuando se le ha dado mantenimiento o ha sido reparado, debe ejecutar pruebas de aceptación y verificación de la configuración del "*firmware*".

Para prevenir alteraciones ("*tampering"*), el *hardware* criptográfico del Certificador, este debe ser guardado y utilizado en un sitio seguro, con acceso limitado a personal autorizado, que tenga las siguientes características:

1) Procesos y procedimientos de control de inventario para administrar el origen, llegada, condición, salida y destino de cada dispositivo;

2) Procesos y procedimientos de control de acceso para limitar el acceso físico a personal autorizado;

3) Grabar en bitácoras de auditoría todos los intentos exitosos y fallidos de acceso a las instalaciones del Certificador y al mecanismo de almacenaje del dispositivo (Ej. caja fuerte);

4) Procesos y procedimientos de manejo de incidentes para tratar eventos irregulares, violaciones de seguridad, investigación y reportes; y

5) Procesos y procedimientos de auditoría para verificar la efectividad de los controles.

Cuando el *hardware* criptográfico del Certificador no esté conectado al sistema, debe ser guardado en un contenedor resistente a violaciones ("*tamper resistant*") y que es guardado en forma segura, bajo múltiples controles (Ej. una caja fuerte).

El manejo del *hardware* criptográfico del Certificador, debe ejecutarse en la presencia de no menos de dos empleados de confianza, incluyendo las siguientes tareas:

1) Instalación del hardware criptográfico del Certificador;

2) Retiro del hardware criptográfico del Certificador de producción;

3) Mantenimiento o reparación del hardware criptográfico del Certificador (incluyendo instalación del nuevo hardware, firmware o software); y,

4) Desmontaje y remoción permanente de uso.

Los dispositivos utilizados para almacenar y recuperar llaves privadas y las interfaces hacia estos dispositivos, deben ser probados antes de su uso para asegurar su integridad (Ej. siguiendo las instrucciones del fabricante).

2.3. Distribución de la llave pública del Certificador

El Certificador debe mantener controles para proporcionar una seguridad razonable de que se mantiene la integridad y la autenticidad de la llave pública del Certificador y cualquier parámetro asociado, durante la distribución inicial y subsiguiente.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

El Certificador debe proporcionar un mecanismo para validar la autenticidad e integridad de las llaves públicas del Certificador. Para el proceso de distribución del Certificador raíz (Ej. utilizando un certificado auto-firmado), debe usarse un mecanismo de notificación fuera de banda ("*out-of-band"*). Cuando un certificado auto-firmado es utilizado por cualquier Certificador, éste debe proporcionar un mecanismo para verificar la autenticidad del certificado (Ej. publicación de la huella del certificado).

Las llaves públicas de los certificadores subsecuentes y/o subordinados deben ser validadas utilizando un método de encadenamiento, o un proceso similar, para así enlazarlos al certificado raíz de confianza. Para un nuevo certificado de la raíz, podría requerirse un proceso fuera de banda (*"out-of-band"*).

El mecanismo inicial de distribución de la llave pública del Certificador, debe controlarse como se documenta en la DPC del Certificador. Las llaves públicas del Certificador deben ser distribuidas inicialmente dentro de un certificado utilizando uno de los siguientes métodos, de conformidad con la DPC del Certificador:

1) Medios digitales (Ej. tarjeta inteligente, CD ROM), desde una fuente autenticada;

2) En un módulo criptográfico de la entidad; o,

3) Otros medios seguros que garanticen autenticidad e integridad.

La llave pública del Certificador debe ser cambiada ("*re-keyed"*) periódicamente, de acuerdo con los requerimientos de la DPC. La comunicación de este cambio debe proporcionarse con anterioridad suficiente para evitar interrupciones en los servicios del Certificador. El mecanismo de distribución

subsiguiente para la llave pública del Certificador debe ser controlado y documentado en su DPC.

En caso de que una entidad tenga ya una copia autenticada de la llave pública del Certificador, cualquier nueva llave pública del Certificador debe ser distribuida utilizando uno de los siguientes métodos de acuerdo con su DPC:

1) Transmisión electrónica directa desde el Certificador;

2) Ubicándola dentro de una reserva ("cache") o directorio remoto;

3) Cargarla dentro de un módulo criptográfico; o

4) Cualquiera de los métodos utilizados para la distribución inicial.

2.4. Del uso de la llave del Certificador

El Certificador debe mantener controles para proporcionar una seguridad razonable de que sus llaves son utilizadas únicamente para las funciones designadas y en las localizaciones predeterminadas.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

La activación de la llave privada de firma del Certificador debe ejecutarse utilizando control de múltiples partes (es decir, "m" de "n") con un valor mínimo de 3 recomendado para "m".

Basándose en una evaluación de riesgo o cuando la PC lo requiera, la activación de la llave privada del Certificador debe efectuarse utilizando autenticación de múltiples factores (Ej. tarjeta inteligente y contraseña, biometría y contraseña, etc.)

Las llaves de firma del Certificador, utilizadas para generar certificados y/o para emitir información del estado de las revocaciones, no deben ser utilizadas para ningún otro propósito.

Las llaves privadas del Certificador deben utilizarse únicamente dentro de un sitio físicamente seguro (refiérase a 1.5).

El Certificador debe suspender el uso de un par de llaves al final de la vida operacional definida para el mismo, o cuando se conoce o sospecha que la llave privada ha sido comprometida.

El funcionamiento correcto del *hardware* criptográfico del Certificador se debe verificar periódicamente.

La EGP debe requerir una revisión anual de la longitud de la llave (*"key length"*) para determinar el período de uso apropiado de la misma. Las recomendaciones deben ser implementadas.

2.5. Del archivado y destrucción de la llave del Certificador

El Certificador debe mantener controles para brindar una seguridad razonable de que:

- Las llaves archivadas del Certificador permanecen confidenciales y seguras en el caso en que sean puestas de nuevo en producción; y,

- Las llaves del Certificador son completamente destruidas al final del ciclo de vida del par de llaves, como lo determina la DPC.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

2.5.1. Archivado de llaves del Certificador

Las llaves archivadas del Certificador deben estar sujetas al mismo o mayor nivel de control de seguridad que las llaves que están en uso actualmente.

La llave privada del Certificador no debe ser destruida hasta que el propósito de negocio o la aplicación hayan dejado de tener valor o hayan expirado las obligaciones legales.

Las llaves archivadas deberán ponerse nuevamente en producción solamente cuando un incidente de seguridad resulte en la pérdida de las llaves de producción o cuando se requiera de validación de evidencia histórica. Se requerirá de procesos de control para asegurar la integridad de los sistemas del Certificador y de los conjuntos de llaves.

Las llaves archivadas deben ser recuperadas en el menor tiempo posible para satisfacer los requerimientos de negocio.

2.5.2. Destrucción de la llave del Certificador

La autorización para destruir la llave privada del Certificador y el procedimiento de destrucción, deben ser regulados de acuerdo con la DPC del Certificador

Todas las copias y fragmentos de la llave privada del Certificador deben ser destruidos de manera tal que la llave privada no pueda ser recuperada.

En caso de que un dispositivo criptográfico del Certificador haya sido permanentemente retirado de servicio, cualquier llave contenida dentro del dispositivo, que se haya utilizado para cualquier propósito criptográfico, debe ser borrada del dispositivo.

2.6. Del compromiso de la llave del Certificador

El Certificador deberá mantener controles para proporcionar una seguridad razonable de que la continuidad de las operaciones se mantenga en caso de que la(s) llave(s) privada(s) del Certificador se comprometa(n).

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

Los planes de continuidad del negocio del Certificador deben referirse al compromiso o sospecha de compromiso de las llaves privadas del mismo, como un desastre.

Deben existir procedimientos de recuperación de desastre que incluyan la revocación y re-emisión de todos los certificados que fueron firmados con la llave privada del Certificador, en el caso de compromiso o sospecha de compromiso de la llave privada de firma del Certificador.

Los procedimientos de recuperación utilizados en el caso de compromiso de la llave privada del Certificador, deben incluir las siguientes acciones:

1) Cómo asegurar el uso de la llave en el ambiente que es restablecida;

2) Cómo se revoca la vieja llave pública del Certificador;

3) Los procedimientos de notificación para las partes afectadas (Ej. certificadores afectados, Repositorios, suscriptores, etc.);

4) Cómo se proporciona la nueva llave pública del Certificador a las entidades finales y partes confiantes, junto con el mecanismo para su autenticación; y

5) Cómo se re-certifican las llaves públicas de los suscriptores.

En el caso que un certificador padre Registrado tenga que reemplazar su llave privada, deben existir los procedimientos para la segura y autenticada revocación de lo siguiente:

1) La llave pública vieja del certificador padre Registrado;

2) El conjunto de todos los certificados (incluyendo cualquiera auto-firmado) emitidos por cualquier Certificador, basándose en la llave privada comprometida; y,

3) Todas las llaves públicas de los certificadores subordinados y los certificados correspondientes que requieran re-certificación.

En caso de compromiso de la llave privada, el plan de continuidad del negocio del Certificador debe establecer quién es notificado y qué acciones deben

tomarse con los sistemas de *hardware* y *software*, llaves simétricas y asimétricas, firmas generadas previamente y datos cifrados

El plan de continuidad del negocio del Certificador debe considerar las técnicas de réplica de llave, tales como las descritas en Anexo J del ISO 15782-1 o en la política que defina la EGP.

3. Controles de administración del ciclo de vida de la llave del suscriptor

3.1. De los servicios de generación de llaves de suscriptor ofrecidos por el Certificador (si se ofrecen)

Si el Certificador proporciona servicios de administración de llaves de suscriptor, el Certificador debe mantener controles para proporcionar una seguridad razonable de que:

- Las llaves de suscriptores generadas por el Certificador (o la AR) son generadas de acuerdo con la PC; y,

- Las llaves de suscriptores generadas por el Certificador (o la AR) son distribuidas en forma segura a los suscriptores por el Certificador (o la AR).

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

3.1.1. Servicios de generación de llaves de suscriptor ofrecidos por el Certificador (o AR)

La generación de llaves de los suscriptores efectuada por el Certificador (o la AR) debe ocurrir dentro de un dispositivo criptográfico seguro, que al menos cumpla con los requerimientos para el nivel apropiado del ISO 15782-1 o los requerimientos del nivel apropiado del FIPS 140-1, basándose en una evaluación de riesgo y en los requerimientos de negocio del Certificador y de acuerdo con la PC y DPC pertinente. Tal dispositivo criptográfico debe efectuar la generación de las llaves de los suscriptores utilizando un generador de números aleatorio (RNG) o un generador de números seudo-aleatorio (PRNG) como se especifica en el estándar ISO/IEC 18032 o en la política que defina la EGP

La generación de llaves de suscriptores efectuada por el Certificador (o la AR) debe:

1) Utilizar un algoritmo de generación de llave tal como lo especifica la PC;

2) Tener como resultado tamaños de llave de acuerdo con la PC; y,

3) Ser efectuada por personal autorizado de acuerdo con la DPC del Certificador.

Cuando el Certificador (o la AR) efectúa la generación de llaves de suscriptores, éste debe entregar al suscriptor el par de llaves que generó, de forma segura (confidencial) de acuerdo con la PC.

3.2. De los servicios de almacenamiento y recuperación de llaves de suscriptores proporcionados por el Certificador (si se ofrecen)

Si el Certificador (o la AR) proporciona almacenamiento de llaves de suscriptores y servicios de recuperación, el Certificador debe mantener controles para proporcionar una seguridad razonable de que:

- Las llaves privadas de suscriptores almacenadas por el Certificador (o AR), permanecen confidenciales y mantienen su integridad;

- Las llaves de suscriptores archivadas por el Certificador (o AR), permanecen confidenciales;

- Las llaves de suscriptores almacenadas por el Certificador (o AR), son destruidas completamente al final de su ciclo de vida; y,

- Que las llaves de suscriptores en custodia por el Certificador (o AR), permanecen confidenciales.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

3.2.1. Almacenamiento, respaldo y recuperación de llaves de los suscriptores ofrecidos por el Certificador

Las llaves privadas de confidencialidad de suscriptores almacenadas por el Certificador (o AR), deben ser guardadas en forma cifrada usando un algoritmo criptográfico y un largo de llave basado en una evaluación de riesgo y en los requerimientos de la PC.

Si el Certificador genera pares de llaves a nombre de un suscriptor, el Certificador (o AR), debe asegurar que las llaves privadas del suscriptor no son reveladas a ninguna otra entidad más que al dueño (es decir, el suscriptor) de las llaves.

Si el Certificador (o AR), genera pares de llaves públicas/privadas de firma, no mantendrá copia de ninguna llave privada de firma una vez que el suscriptor confirme la recepción de la llave.

Si el Certificador (o AR) proporciona almacenamiento, respaldo y recuperación de llaves (de confidencialidad) de suscriptores, estos servicios deben ser ejecutados por personal autorizado.

Si el Certificador (o AR) proporciona almacenamiento, respaldo y recuperación de llaves de suscriptores, deben existir controles que aseguren la integridad de la llave privada (de confidencialidad) durante su ciclo de vida.

3.2.2. Archivo de llaves de suscriptores ofrecido por el Certificador

Las llaves privadas (de confidencialidad) de suscriptores archivadas por el Certificador (o AR), deben almacenarse en forma cifrada usando un algoritmo criptográfico y una longitud de llave, basada en una evaluación de riesgo y de conformidad con los requerimientos de la PC.

Si el Certificador proporciona el servicio de archivado de llaves (de confidencialidad) de suscriptores, entonces todas estas llaves archivadas deben destruirse al final del período de archivo.

3.2.3. Destrucción de llaves de suscriptores, ofrecido por el Certificador

Si el Certificador proporciona almacenamiento de llaves (de confidencialidad) de suscriptores, la autorización para destruir la llave privada de un suscriptor y los medios para hacerlo (Ej., sobre escritura de la llave), deben ser regulados de acuerdo con la PC.

Si el Certificador proporciona almacenamiento de llaves (de confidencialidad) de suscriptores, todas las copias y fragmentos de la llave privada del suscriptor deben ser destruidos al final del ciclo de vida del par de llaves.

3.2.4. Custodia de llaves de suscriptores ofrecida por el Certificador

Las llaves privadas (de confidencialidad) de suscritores, custodiadas por el Certificador con el propósito de ser accedidas, por orden judicial, deben ser guardadas en forma cifrada usando un algoritmo criptográfico y una longitud de llave basada en una evaluación de riesgo y en los requerimientos de la PC.

3.3. De la administración del ciclo de vida del dispositivo o módulo seguro de creación de firma (MSCF)

Si el Certificador (o AR), de acuerdo con las políticas que al efecto emita la EGP o el Certificador raíz, distribuye pares de llaves y certificados a los suscriptores utilizando MSCF, el Certificador (o la AR) debe mantener los controles para brindar una seguridad razonable de que:

- La adquisición, preparación y personalización de los MSCF son controlados en forma segura por el Certificador (o AR);

- El uso de los MSCF es habilitado por el Certificador (o la AR), antes de ser entregado;

- Los MSCF son almacenados y distribuidos en forma segura por el Certificador (o la AR);

- Los MSCF son reemplazados en forma segura por el Certificador (o la AR); y,

- Los MSCF devueltos al Certificador (o a la RA) son inicializados o destruidos en forma segura.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

3.3.1. Adquisición de los MSCF

Los MSCF utilizados por el suscriptor deben satisfacer los perfiles de protección apropiados del estándar ISO 15408 o las políticas que al efecto emita la EGP.

En el caso de dispositivos criptográficos para los que aplica (Ej., *tokens* USB criptográficos), se debe cumplir también con el nivel del FIPS 140-1 apropiado, basado en la evaluación de riesgos y en los requerimientos de la PC.

En el caso de las tarjetas inteligentes (*"smartcards"*), deben ser protegidas durante el transporte entre la oficina de tarjetas del Certificador (si hubiere) y el Certificador (o la AR), a través del uso de correo certificado (o equivalente) utilizando un embalaje con sello de garantía (*"tamper evident"*). Al momento de recibirlas, el personal autorizado del Certificador (o la AR), debe inspeccionar el embalaje, para determinar si el sello está intacto. Además, se debe cumplir también con los estándares ISO de tarjetas (por ejemplo: ISO 7810, 7811 partes 1-5, 7813, 7816, 10202) o los que defina la EGP.

Los certificadores y ARs deben verificar la integridad física de los MSCF apenas se reciban por parte del fabricante.

Los MSCF deben almacenarse en forma segura y bajo un control de inventario, mientras estén bajo el control del Certificador (o el AR).

3.3.2. Preparación y personalización de los MSCF

Deben existir y seguirse procedimientos y procesos de preparación de los MSCF, incluyendo los siguientes:

1) Carga o verificación del sistema operativo del MSCF;

2) Creación de estructuras de datos lógicas (sistema de archivos y dominios de seguridad del MSCF);

3) Carga de aplicaciones;

4) Protección lógica de los MSCF para prevenir modificaciones no autorizadas del sistema operativo, sistema de archivos, dominios de seguridad y aplicaciones; y,

5) Cualquier otro que se especifique en las políticas que al efecto emita la EGP o el Certificador raíz en el PC apropiado.

Deben existir y deben seguirse procesos y procedimientos de personalización de los MSCF, incluyendo lo siguiente:

1) Cargar la información de identificación en el MSCF;

2) Generación del par de llaves del suscriptor, de acuerdo con la PC;

3) Cargar la(s) llave(s) privada(s) del suscriptor en el MSCF, según lo establecido en la PC;

4) Cargar el certificado del suscriptor en el MSCF;

5) Cargar el certificado del Certificador y otros certificados del ambiente contractual en el MSCF;

6) Protección lógica del MSCF contra accesos no autorizados; y,

7) Cualquier otro que se especifique en las políticas que al efecto emita la EGP o el Certificador raíz en la PC apropiada.

El Certificador (o la AR) deben registrar la preparación y personalización de los MSCF en una bitácora de auditoría.

Para el caso de tarjetas inteligentes, éstas no deben entregarse a un suscriptor, a menos que hayan sido preparadas y personalizadas por el Certificador o la AR.

3.3.3. Entrega del MSCF

Deben existir procesos y procedimientos para la entrega segura del MSCF al suscriptor, de acuerdo con las políticas que al efecto emita la EGP o el Certificador raíz en el PC apropiado.

La información de activación inicial del MSCF (Ej., PIN de inicialización), debe ser definida por el suscriptor o bien comunicada en forma segura al suscriptor, usando un método fuera de banda (*"out-of-band"*). En este último caso, el suscriptor debe ser motivado a cambiar la información de activación inicial al recibir el MSCF.

La entrega de los MSCF debe ser registrada por el Certificador (o la AR) en una bitácora de auditoría.

3.3.4. Uso del MSCF por parte del suscriptor

Se debe proveer al suscriptor de mecanismos para proteger el acceso a la información del MSCF, incluyendo las llaves privadas guardadas en el mismo, durante el uso por parte del suscriptor (Ej. mecanismos de control de acceso por medio de PIN, biometría).

Las llaves privadas del suscriptor guardadas en el MSCF no deben ser exportadas a una aplicación para que realice funciones criptográficas (Ej. firma).

El suscriptor esta obligado a utilizar un mecanismo de autenticación mutua para aplicaciones criptográficas y las funciones del MSCF, con el fin de asegurar la integridad del sistema.

El suscriptor estará obligado a usar una aplicación que despliegue el mensaje o el resumen (*"digest"*) del mismo, antes de firmar los datos del mensaje (o transacción). La aplicación del MSCF del suscriptor debe producir bitácoras de auditoría de todos los usos que ha tenido el MSCF. Esto también incluye todos los intentos del proceso de verificación del propietario de la llave privada. (Nota: Esta evidencia puede ser presentada por el suscriptor ante las partes confiantes, para cualquier disputa acerca de la autenticidad y/o integridad de una transacción).

El MSCF debe ser utilizado por el suscriptor de acuerdo con los términos de la PC.

3.3.5. Reemplazo del MSCF

Deben existir y seguirse procesos y procedimientos para el reemplazo de un MSCF dañado o extraviado por el suscriptor.

En el caso de pérdida o daño del MSCF, los certificados del suscriptor deben ser renovados o reemitida su llave, de acuerdo con la PC.

El reemplazo del MSCF debe ser registrado por el Certificador (o la AR) en una bitácora de auditoría.

3.3.6. Devolución del MSCF

Todos los MSCF devueltos al Certificador (o la AR) (si la devolución aplica), deben ser inicializados, desactivados o destruidos (de acuerdo con la PC) en forma segura para prevenir su uso no autorizado.

La devolución de un MSCF y las acciones subsecuentes (Ej. Destrucción, inicialización, etc.) deben ser registradas por el Certificador (o AR) en una bitácora de auditoría.

3.4. De los requerimientos para la administración de la llave del suscriptor

El Certificador debe establecer los mecanismos necesarios para administrar de forma segura las llaves del suscriptor durante el ciclo de vida de las mismas.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

3.4.1. Generación de llaves del suscriptor

La PC debe especificar los requisitos de nivel del ISO 15782-1 o FIPS 140-1 apropiados para módulos criptográficos, utilizados para la generación de la llave del suscriptor.

La PC debe especificar los algoritmos de generación de llave que pueden utilizarse para la generación de la llave del suscriptor.

La PC debe especificar los tamaños aceptables de llave para la generación de llave del suscriptor.

3.4.2. Almacenamiento, respaldo y recuperación de la llave del suscriptor

El Certificador o la AR deben proporcionar o tener disponibles los mecanismos que le permitan a los suscriptores accesar (es decir, un método de verificación del propietario de la llave privada), administrar y controlar el uso de sus llaves privadas.

La PC debe especificar los requerimientos de protección de llaves privadas almacenadas del suscriptor.

La PC debe establecer las circunstancias, la autoridad y los procesos de control cuando la llave privada de confidencialidad del suscriptor sea restaurada.

La PC debe especificar (si aplica) los requerimientos de protección de la llave privada de confidencialidad, para copias de respaldo almacenadas por el suscriptor.

3.4.3. Uso de la llave del suscriptor

El Contrato de suscriptor debe describir los procesos requeridos que deben ser seguidos por el suscriptor para cualquier uso del mecanismo criptográfico (Ej. los MSCF y el *software* de la aplicación)

La PC debe especificar los usos aceptables para el par de llaves del suscriptor.

La PC debe especificar los requerimientos para el uso de la llave del suscriptor.

3.4.4. Almacenamiento de la llave del suscriptor

La PC debe especificar los requisitos de protección para las llaves privadas de confidencialidad del suscriptor archivadas.

La PC debe especificar los requisitos para la destrucción de las llaves de confidencialidad archivadas del suscriptor, al final del período de almacenamiento.

3.4.5. Destrucción de la llave del suscriptor

La PC debe especificar los medios a través de los cuales puede ser ejecutada la destrucción de la llave del suscriptor.

La PC o la DPC deben especificar los requerimientos para la destrucción de todas las copias y fragmentos de la llave privada de confidencialidad del suscriptor al final del ciclo de vida del par de llaves.

3.4.6. Uso remoto del hardware criptográfico del suscriptor

La PC debe especificar los requerimientos para el uso y manejo del *hardware* criptográfico y el proceso de autenticación del suscriptor (y las acciones subsecuentes), cuando el *hardware* criptográfico esta en otros lugares físicos (Ej. Un MSCF conectado a un equipo remoto).

3.4.7. Compromiso de la llave del suscriptor

La PC debe especificar los requerimientos para la notificación al Certificador o la AR, en el caso de que la llave del suscriptor se comprometa.

4. Controles para la administración del ciclo de vida del certificado

4.1. Del registro del suscriptor

El Certificador debe mantener controles para brindar una seguridad razonable de que:

- Los suscriptores son identificados con precisión, de acuerdo con los requerimientos aplicables de “conozca su cliente”; y,

- Las solicitudes de certificado de los suscriptores son precisas, autorizadas y completas.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

4.1.1. Identificación y autenticación

El Certificador debe verificar, o requerir que la AR verifique, las credenciales presentadas por el solicitante o suscriptor como evidencia de identidad o

autoridad para ejecutar un rol específico de acuerdo con la PC y los requisitos legales y regulatorios apropiados.

Para los certificados individuales de suscriptor, el Certificador o la AR deben verificar (como lo determina la PC), la identidad de la persona cuyo nombre será incluido en el campo del "nombre distintivo del suscriptor" del certificado. Un nombre individual no autenticado no debe ser incluido en el "nombre distintivo del suscriptor"

El Certificador o la AR deben verificar la exactitud de la información incluida en la solicitud del certificado, de acuerdo con la PC.

El Certificador o la AR deben revisar la solicitud del Certificado para evitar omisiones o errores de acuerdo con la PC.

Para los certificados de suscriptor el Certificador debe utilizar la llave pública de la AR incluida en la solicitud del certificado, para verificar la firma de la AR en la presentación de la solicitud de certificado.

El Certificador debe verificar la unicidad del "nombre distintivo del suscriptor", dentro de los límites o comunidad definida por la PC.

Deben utilizarse controles de encriptación y de acceso para proteger la confidencialidad e integridad de los datos de registro en tránsito y almacenados.

La AR o el Certificador deben informar al suscriptor, de los términos y condiciones concernientes al uso del certificado.

4.1.2. Solicitud de certificado

El Certificador debe exigir que la entidad solicitante de un certificado, prepare los datos apropiados de la solicitud del certificado y los entregue a la AR (o Certificador) como se especifica en la PC.

El Certificador debe requerir que las entidades solicitantes, remitan sus llaves públicas en un mensaje auto-firmado al Certificador para la certificación. El Certificador debe exigir que las entidades solicitantes firmen digitalmente la solicitud de certificado usando la llave privada que se relaciona con la llave pública contenida en la solicitud de certificado con el fin de:

1) Permitir la detección de errores en el proceso de aplicación del certificado; y,

2) Confirmar la propiedad de la llave privada correspondiente a la llave pública que está siendo registrada.

La solicitud de certificado debe ser considerada como una aceptación por parte del solicitante, de los términos y condiciones para utilizar el certificado, como se describe en el Contrato de suscriptor.

El Certificador debe validar la identidad de la AR autorizada para emitir las solicitudes de c, bajo una PC específica.

El Certificador debe solicitar que las AR envíen la información de solicitud del certificado al Certificador, en un mensaje firmado por la AR. El Certificador debe verificar la firma de la AR en la solicitud de certificado.

El Certificador debe requerir que la AR asegure la parte del proceso de aplicación del certificado por la cual la AR, asume la responsabilidad de acuerdo con la DPC del Certificador.

El Certificador debe requerir que la AR, registre sus acciones en una bitácora de auditoría.

El Certificador debe verificar la autenticidad de los envíos de la AR de acuerdo con la DPC del Certificador.

4.2. De la renovación de certificado (si se ofrece)

Si la renovación del certificado está soportada por la PC, el Certificador debe mantener controles para proporcionar una seguridad razonable de que las solicitudes de renovación de certificado son precisas, autorizadas y completas.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

4.2.1. Solicitud de renovación de certificado

La solicitud de renovación del certificado debe incluir al menos el: "nombre distintivo del suscriptor", el "número de serie del certificado" (u otra información que identifique al certificado), y el período de validez solicitado (el Certificador sólo renovará certificados que él mismo ha emitido).

El Certificador debe requerir que la entidad solicitante firme digitalmente la "Solicitud de renovación del certificado", usando la llave privada que se relaciona con la llave pública, contenida en el certificado de llave pública existente de la entidad solicitante.

El Certificador debe emitir un nuevo certificado usando la llave pública del suscriptor previamente certificado, solamente si su seguridad criptográfica es todavía suficiente para el período de vida previsto para el nuevo certificado y que no existan indicios de que la llave privada del suscriptor haya sido comprometida.

El Certificador o la AR deben procesar la información de renovación del certificado para verificar la identidad de la entidad solicitante e identificar el certificado que va a ser renovado.

El Certificador o la AR deben validar la firma de la entidad solicitante en la "Solicitud de renovación del certificado".

El Certificador debe verificar la existencia y validez del certificado a ser renovado. No se permite ninguna renovación, a menos que el estado del certificado existente sea activo (es decir, que no esté revocado o suspendido).

El Certificador o la AR deben verificar que la solicitud, incluyendo la extensión del período de validez, cumple con los requisitos definidos en la PC

Si se utiliza una AR, el Certificador debe solicitar que las AR envíen los datos de la renovación del certificado al Certificador en un mensaje ("Solicitud de renovación de certificado") firmado por la AR.

Las AR deben asegurar la parte del proceso de renovación del certificado por el cual asumen responsabilidad de acuerdo con la PC.

El Certificador debe requerir que las AR almacenen sus acciones en una bitácora de auditoría.

El Certificador debe verificar la autenticidad del envío de la AR.

El Certificador debe verificar la firma de la AR en la "Solicitud de renovación del certificado"

El Certificador debe verificar errores u omisiones de la "Solicitud de renovación del certificado". Esta función puede ser delegada explícitamente a la AR.

El Certificador o la AR deben notificar a los suscriptores antes de la expiración de sus certificados sobre la necesidad de renovarlos de acuerdo con la PC.

El Certificador debe emitir una notificación firmada a la AR, indicando que la renovación del certificado ha sido exitosa.

El Certificador debe hacer el nuevo certificado disponible a los suscriptores, de acuerdo con la PC.

4.3. De la re-emisión de llaves del certificado

El Certificador debe mantener controles para brindar una seguridad razonable de que las solicitudes de certificado de re-emisión de llaves son precisas, autorizadas y completas.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

El Certificador debe exigir que la entidad solicitante firme digitalmente con la llave privada previa la "Solicitud de re-emisión de certificado" que contiene la nueva llave pública.

El Certificador o la AR debe verificar que la "Solicitud de re-emisión de certificado" cumpla con los requisitos definidos en la PC correspondiente.

Si se utiliza una AR, el Certificador debe:

1) Solicitar que las AR envíen la "Solicitud de re-emisión de certificado" hacia el Certificador en un mensaje firmado por la AR;

2) Solicitar que la AR asegure la parte del proceso de la re-emisión del certificado, por el cual (la AR) asume la responsabilidad;

3) Solicitar que las AR almacenen sus acciones en una bitácora de auditoría; y,

4) Verificar la firma de la AR en la "Solicitud de re-emisión del Certificado".

El Certificador o la AR debe verificar errores u omisiones en la "Solicitud de re-emisión del Certificado"

Previo a la generación y emisión de nuevos certificados, el Certificador o la AR debe verificar lo siguiente:

1) La firma en la presentación de los datos de re-emisión del certificado por parte del suscriptor;

2) La existencia y validez de la información que respalda la solicitud de re-emisión; y

3) Que la solicitud cumpla los requisitos definidos en la PC.

Cuando un nuevo certificado es solicitado por el suscriptor después de la revocación, se le debe solicitar al mismo la aplicación por un nuevo certificado, de acuerdo con la PC.

Cuando un nuevo certificado es solicitado por el suscriptor después de la expiración del certificado, el mismo puede ser generado automáticamente, o se le puede solicitar al suscriptor que aplique por un nuevo certificado, de acuerdo con la PC.

4.4. De la emisión del certificado

El Certificador debe mantener controles, para brindar una seguridad razonable de que los certificados son generados y emitidos de acuerdo con la PC.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

El Certificador debe generar los certificados utilizando los datos de la solicitud de certificado y crear el certificado como se define en el perfil de certificado apropiado, según lo establecido en el ISO-9594/X.509 e ISO 15782-1, o en la PC y DPC apropiada.

Los períodos de validez de los certificados deben ser definidos en la PC y formateados de acuerdo con el ISO 9594/X.509 e ISO 15782-1, o como lo defina la EGP.

Los campos de extensión deben ser formateados conforme al ISO 9594/X.509 e lSO 15782-1 o como lo defina la EGP.

El tamaño de los campos debe ser formateado conforme al ISO 9594/X.509 e ISO 15782-1 o como lo defina la EGP.

El Certificador debe firmar la llave pública y otra información importante del suscriptor, con la llave privada del Certificador.

Los certificados se deben emitir basados en la aprobación del registro del suscriptor, la aprobación de la solicitud de renovación del certificado o la aprobación de solicitudes de re-emisión de llaves, conforme a las cláusulas 4.1 - 4.3.

El Certificador debe emitir una notificación firmada a la AR, cuando se emita un certificado a un suscriptor, para el cual la AR envió una solicitud de certificado.

El Certificador debe emitir una notificación "fuera de banda" (*"out-of-band"*) al suscriptor cuando un certificado es emitido. Cuando esta notificación incluya los datos de activación inicial, procesos de control deben garantizar la entrega segura al suscriptor.

Si los certificados expiran, son revocados o suspendidos, se deben conservar copias de los certificados durante un período adecuado, especificado en la PC.

4.5. De la distribución del certificado

El Certificador mantendrá controles para brindar una seguridad razonable de que, tras su emisión, certificados completos y exactos estén disponibles para cualquier entidad, según lo dispuesto en la PC.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

1) El Certificador debe mantener disponibles los certificados emitidos, a las partes relevantes utilizando mecanismos establecidos (Ej. Un repositorio en forma de directorio), de acuerdo con la PC;

2) Solo el personal autorizado del Certificador debe administrar el mecanismo de distribución;

3) El funcionamiento del mecanismo de distribución debe ser supervisado y administrado;

4) La integridad del mecanismo de distribución debe ser preservada y administrada; y,

5) Cuando se requiera por la legislación de privacidad, los certificados deben estar disponibles para su recuperación, solamente en aquellos casos en que se obtenga el consentimiento del suscriptor.

4.6. De la revocación de certificados

El Certificador debe mantener los controles para brindar una seguridad razonable de que los certificados serán revocados de manera oportuna (como lo defina el riesgo), basados en solicitudes de revocación de certificado validadas y autorizadas.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

El Certificador debe de proveer de un medio de comunicación rápido para facilitar la revocación segura y autenticada de:

1) Uno o más certificados de uno o más suscriptores;

2) El conjunto de todos los certificados emitidos por el Certificador, basados en un par de llaves pública/privada específico, utilizado por el Certificador para generarlo;

3) Todos los certificados emitidos por el Certificador, independientemente del par de llaves publica/privada utilizado.

El Certificador debe verificar, o requerir a la AR que verifique, la identidad y autoridad de la entidad que solicita la revocación de un certificado conforme a la PC

Si una AR acepta una solicitud de revocación, el Certificador debe pedirle a la AR que le remita las solicitudes de revocación de certificado firmadas, en forma autenticada de acuerdo con la PC.

Si una AR acepta y reenvía una solicitud de revocación al Certificador, este último debe brindar una confirmación firmada de la solicitud de revocación y una confirmación de las acciones a la AR.

El Certificador debe actualizar la lista de revocación de certificados (LRC) y cualquier otro mecanismo con el estado de los certificados, en los periodos

establecidos en la PC y conforme al formato definido en el ISO 9594/X 509 y el ISO 15782-1 o el definido por la EGP.

El Certificador debe registrar todas las solicitudes de revocación y su resultado en una bitácora de auditoría, como se especifica en el Anexo F del ISO 15782-1 o como lo defina la EGP.

El Certificador o la AR puede brindar una confirmación autenticada (firmada o similar) de la revocación a la entidad que realizó la solicitud de revocación.

Donde se permita la renovación de certificados, cuando un certificado es revocado, todas las instancias válidas del certificado también deben ser revocadas y no deberán ser reestablecidas.

El suscriptor de un certificado revocado o suspendido debe ser informado del cambio de estado de su certificado.

4.7. De la suspensión y reactivación del certificado (si se ofrece)

Si se ofrece la suspensión de certificados, el Certificador debe mantener los controles para brindar una seguridad razonable de que los certificados serán suspendidos o reactivados de manera oportuna (como lo defina el riesgo), basados en solicitudes de suspensión o reactivación de certificado validadas y autorizadas.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

De acuerdo con la DPC del Certificador, este debe de proveer un medio de comunicación rápido para facilitar la suspensión o reactivación segura y autenticada de:

1) Uno o más certificados de uno o más suscriptores;

2) El conjunto de todos los certificados emitidos por el Certificador, basados en un par de llaves pública/privada específico, utilizado por el Certificador para generarlo;

3) Todos los certificados emitidos por el Certificador, independientemente del par de llaves publica/privada utilizado.

El Certificador debe verificar, o requerir a la AR que verifique, la identidad y autoridad de la entidad que solicita la suspensión o reactivación de un certificado conforme a la PC

Si una AR acepta una solicitud de suspensión o reactivación de certificado, la AR debe remitir las solicitudes firmadas al Certificador, en forma autenticada de acuerdo con la PC.

El Certificador o la AR debe notificar al suscriptor, sobre la suspensión o reactivación de su certificado, según lo establezca la PC.

Las solicitudes de suspensión o reactivación de certificado se deben procesar y validar de acuerdo con los requerimientos de la PC.

El Certificador debe actualizar la LRC y otros mecanismos, que tengan que ver con el estado del certificado, cuando se realice la suspensión de un certificado. Los cambios en el estado del certificado deben realizarse en los tiempos establecidos en la PC

Los certificados deben ser suspendidos, sólo durante el tiempo permitido por la PC.

Una vez que la suspensión del certificado ("*hold*") ha sido aplicada, esta debe ser manejada en una de las siguientes tres formas:

1) Un registro del certificado suspendido permanece en la LRC sin más acciones;

2) El registro en la LRC para el certificado suspendido es sustituido por una entrada de revocación para el mismo certificado;

3) El certificado suspendido explícitamente es liberado y la entrada removida de la LRC.

Una entrada de la suspensión del certificado debe permanecer en la LRC hasta la expiración del certificado en cuestión o la expiración de la suspensión, la que ocurra primero. La PC se debe especificar el número máximo de veces en que un certificado puede ser suspendido y el período máximo para este estado. Si el número máximo de veces es alcanzado, la EGP puede ser notificada para mayor investigación.

El Certificador debe actualizar la LRC y otros mecanismos con el estado de certificados, cuando se reactive un certificado de acuerdo con la PC del Certificador.

El Certificador debe verificar, o requerir que la AR verifique, la identidad y autoridad de la entidad que solicita la reactivación de un certificado.

La suspensión o reactivación de los certificados debe ser registrada en las bitácoras de auditoría como se especifica en el Anexo F del ISO 15782-1 o como lo determine la EGP.

4.8. De los servicios de validación de certificados

El Certificador debe mantener controles para brindar una seguridad razonable de que esté disponible para las partes relevantes (suscriptores, partes confiantes,

etc.), información oportuna, completa y precisa del estado del certificado (incluyendo la LRC y otros mecanismos que mantengan el estado de certificados), de acuerdo con la PC.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

El Certificador debe poner la información del estado del certificado a disposición de las partes o entidades interesadas, utilizando un mecanismo establecido de acuerdo con la PC. Esto puede ser obtenido mediante:

1) Método de Entrega - una LRC firmada por el Certificador y publicada con una periodicidad establecida en la PC.

2) Método de Respuesta de Solicitud – de una petición por la parte confiante enviada al servicio de respuesta del Certificador sobre el estado de certificados ("certificate status provider´s responder"). De vuelta, el servicio de respuesta contesta con el estado del certificado debidamente firmado. (OCSP es un protocolo de ejemplo que usa este método.)

Los siguientes procedimientos de control son aplicables donde se utilizan LRC:

El Certificador debe firmar digitalmente cada LRC que emita, de modo que las entidades puedan validar la integridad de la misma y la fecha y hora de emisión.

El Certificador debe publicar la LRC a intervalos regulares, según lo especificado en la PC, incluso si no han ocurrido cambios desde la última emisión.

Se deben mantener registros en la LRC, de todos los certificados revocados hasta el final del período de validez de los mismos. Además, una vista retrospectiva del estado de un certificado, en un punto dado del tiempo, puede ser requerida. Por lo tanto, los registros de la LRC deben mantenerse más allá del período de validez de certificado para demostrar su validez en el momento de su uso.

Si la suspensión de certificados es ofrecida, un registro de la suspensión del certificado debe permanecer en la LRC, indicando la fecha de la acción original y la fecha de expiración de la suspensión, hasta la expiración del certificado o hasta que la suspensión sea levantada.

Las LRC se deben archivar de acuerdo con los requerimientos de la PC, incluyendo el método de recuperación.

Las LRC viejas deben ser conservados por un período apropiado establecido en la PC del Certificador

Los procedimientos de control siguientes son aplicables donde se utilizan los mecanismos que manejan del estado del certificado en línea (Ej., OCSP):

Si se utiliza un método en línea para publicar el estado del certificado (Ej., OCSP), el Certificador debe requerir que las consultas sobre el estado de certificados (Ej. Solicitudes OCSP) contengan todos los datos requeridos de acuerdo con la PC.

Cuando se recibe una petición, sobre el estado de un certificado (Ej. Solicitudes OCSP), proveniente de una parte confiante, el Certificador debe retornar una respuesta definitiva a la parte confiante si:

1) El mensaje de solicitud está bien formado;

2) El servicio de respuesta del proveedor de estado de certificados ("certificate status provider´s responder") está configurado para proporcionar el servicio solicitado;

3) La solicitud contiene la información (es decir, la identidad del certificado-el número de serie, OID, etc.) requeridos por el servicio de respuesta del proveedor de estado de Certificados conforme a la PC; y

4) El servicio de respuesta del proveedor de estado de certificados, es capaz de localizar el certificado e interpretar su estado.

Cuando estas condiciones se cumplan, el servicio de respuesta del Certificador sobre el estado de certificados debe generar un mensaje de respuesta firmado, indicando el estado del certificado de acuerdo con la PC. Si cualquiera de las condiciones anteriores no se cumplen, entonces un estado de "desconocido" puede ser devuelto.

Todos los mensajes de respuesta deben ser firmados digitalmente e incluir todos los datos requeridos de acuerdo con la PC.

5. Controles de administración del ciclo de vida del certificado del Certificador

5.1.1. De la administración del ciclo de vida del certificado en un Certificador subordinado

El Certificador padre, debe mantener controles para brindar una seguridad razonable de que:

- Las solicitudes de certificado para un Certificador subordinado son exactas, autenticadas y aprobadas;

- Las solicitudes de un reemplazo de certificado para un Certificador subordinado (renovación y re-emisión) son exactas, autorizadas y completas;

- Los certificados nuevos (renovados o re-emitidos) de un Certificador Subordinado, se generan y se emiten de acuerdo con la PC

- Luego de la emisión, los certificados completos y exactos de los certificadores subordinados están disponibles para las entidades relevantes (los suscriptores y terceras partes interesadas) de acuerdo con la PC;

- Los certificados de un Certificador subordinado, son revocados basados en solicitudes autorizadas y validadas, de acuerdo con la PC; y,

- La información de estado del certificado, oportuna, completa y exacta (incluyendo la LRC y otros mecanismos que mantengan el estado de certificados) se pone a disposición de cualquier entidad de acuerdo con la PC.

Para alcanzar el objetivo anterior, al menos se debe cumplir con lo siguiente:

5.1.2. Registro de un Certificador subordinado

La PC padre debe especificar los requerimientos para la presentación de solicitudes de certificación de un Certificador subordinado.

El Certificador padre debe autenticar la solicitud de certificado del Certificador subordinado, de acuerdo con la PC padre.

El Certificador padre debe auditar el cumplimiento de los requerimientos de su PC, por parte del Certificador subordinado que está aplicando por el certificado, antes de aprobar la solicitud. Alternativamente el Certificador subordinado puede presentar su DPC para ser auditado.

5.1.3. Renovación de un Certificador subordinado

Cuando la renovación del certificado de un Certificador subordinado es permitida, la PC del Certificador padre debe especificar los requerimientos para la presentación de la solicitud de renovación y los requerimientos para verificar su autenticidad

5.1.4. Regeneración de llaves del Certificador subordinado

La PC de un Certificador padre debe especificar los requerimientos para la presentación de las solicitudes de regeneración de llaves de un Certificador subordinado.

El Certificador padre debe autenticar la solicitud de regeneración de llaves del Certificador subordinado, conforme a la PC.

5.1.5. Emisión de certificados de un Certificador subordinado

El Certificador padre debe generar certificados:

1) Usando el perfil de certificado apropiado de acuerdo con la PC e ISO 9594/X.509 y las reglas de formato del ISO 15782-1, o como lo defina la EGP;

2) Con los períodos de validez ajustados de acuerdo con el ISO 9594/X.509, ISO 15782-1 y la PC o como lo defina la EGP; y,

3) Cuando sean utilizadas extensiones, los campos son formateados conforme al ISO 9594/X.509, ISO 15782-1 y la PC, o como lo defina la EGP.

El Certificador padre debe; con su llave privada de firma, firmar el certificado del Certificador subordinado.

5.1.6. Distribución del certificado del Certificador subordinado

El Certificador padre debe, de acuerdo con su PC, poner a disposición de las partes relevantes, los certificados del Certificador subordinado; utilizando un mecanismo establecido (Ej., Un repositorio como un directorio).

5.1.7. Revocación del certificado del Certificador subordinado

El Certificador padre debe, de acuerdo con su PC, verificar la identidad y la autoridad de la entidad que solicita la revocación del certificado de un Certificador subordinado**.**

El Certificador padre debe; de acuerdo con su PC, actualizar la LRC y los otros mecanismos que mantengan el estado del certificado del Certificador subordinado; tras la revocación del mismo.

5.1.8. Información del estado del certificado del Certificador subordinado

El Certificador padre debe; de acuerdo con su PC, poner a disposición de las partes confiantes, la información del estado del certificado del Certificador subordinado, utilizando un mecanismo establecido.

6. Normas complementarias

6.1.1. Sobre la DPC y la PC

La o las DPC y PC de los certificadores, deberán ser redactados de conformidad con el RFC 3647, establecido por el IETF. Este RFC es un documento que plantea una estructura para la redacción de la DPC y la PC, para regular la operación de una infraestructura de llave pública.

6.1.2. Sobre la seguridad de la información

El Certificador deberá utilizar como complemento a las normas estipuladas en este reglamento, especialmente en lo relativo a la seguridad de la información la norma IRAM-ISO/IEC 17799-2002 o bien la norma ISO/IEC 17799:2005.

La norma ISO 17799, establece los guías y principios generales para iniciar, implementar, mantener y mejorar la seguridad del manejo de la información en una organización.