**Guía de Evaluación de Requisitos para la acreditación de una Autoridad de Certificación como Prestador de Servicios Criptográficos de Certificación en la República de Cuba**

Como principal documento regulador de la actividad se asumirá el **"Reglamento sobre el Funcionamiento de la Infraestructura de Llave Pública en interés de la protección de la información oficial en la República de Cuba"**, en lo adelante el Reglamento**.**

Para garantizar la correcta evaluación y acreditación de la entidad y la prestación de los servicios asociados, la Dirección de Criptografía evaluará como cumplidos, parcialmente cumplidos o incumplidos los requisitos siguientes:

**REQUISITOS DE ACREDITACIÓN**

**1. ADMISIBILIDAD**
**2. REQUISITOS GENERALES**
**3. ASPECTOS LEGALES Y DE PRIVACIDAD**
**4. ESTRUCTURA CERTIFICADOS**
**5. ESTRUCTURA CRL y SERVICIO OCSP**
**6. REGISTRO DE ACCESO PÚBLICO**
**7. EVALUACIÓN DE RIESGOS Y AMENAZAS**
**8. PLAN DE PREVENCIÓN DE RIESGOS**
**9. POLÍTICA DE SEGURIDAD**
**10. PLAN DE ADMINISTRACIÓN DE LLAVES**
**11. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**
**12. EVALUACIÓN DE LA PLATAFORMA TECNOLÓGICA.**
**13. SEGURIDAD FÍSICA**
**14. POLÍTICA PARA EL TRABAJO CON LA INFRAESTRUCTURA DE LLAVE PÚBLICA**
**15. DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN**
**16. MANUAL DE OPERACIONES DE AUTORIDAD CERTIFICADORA**
**17. MANUAL DE OPERACIONES DE LA AUTORIDAD DE REGISTRO**
**18. AUTORIZACIÓN Y CAPACITACIÓN DEL PERSONAL**

## 1. REQUISITOS DE ADMISIBILIDAD

### 1.1. ESPECIFICACIÓN DEL REQUISITO

| | |
|---|---|
| Nombre | Requisitos de admisibilidad del Prestador de Servicios Criptográficos de Certificación (PSCC) en el proceso de evaluación y acreditación. |
| Objetivo | Comprobar que el Prestador de Servicios Criptográficos de Certificación (PSCC) cumpla con la entrega a la Entidad Acreditadora (DC), de la solicitud inicial para la creación de un PSCC y de la documentación necesaria para iniciar el procedimiento. |
| Descripción | Los requisitos de admisibilidad son aquellos requisitos previos necesarios para iniciar el procedimiento de evaluación del PSCC, los que incluyen la presentación de la solicitud inicial para la creación de un PSCC, entrega de la documentación solicitada y el cumplimiento del plazo establecido para la entrega de documentación faltante en caso de ser necesario. |
| Referencias en el "*Reglamento*". | Reglamento Art. 5 y Art. 43 |
| Documentación solicitada | Solicitud inicial para la creación de un PSCC conteniendo los datos siguientes:<br>a.- Nombre o razón social de la entidad solicitante<br>b.- Dirección de la entidad.<br>c.- Teléfonos, FAX y Dirección de correo electrónico<br>d.- Nombre del representante legal de la entidad solicitante<br>e.- Alcance de la prestación del mencionado servicio en el territorio nacional y/o internacional<br>f.- Fundamentación sobre la necesidad de creación del PSCC<br>g.- Estudio de factibilidad para su puesta en explotación y sostenibilidad, elaborado en |

| | |
|---|---|
| | base a la evaluación de la existencia de condiciones tangibles para cumplir con las obligaciones y facultades establecidas para la operación del prestador de servicio propuesto.<br>h.- Otros datos contenidos en la plantilla del documento.<br>Adicionalmente toda la documentación especificada en las guías de evaluación para cada uno de los requisitos del proceso de evaluación. |
| Evidencias solicitadas | Solicitud inicial para la creación de un PSCC en la entidad solicitante. |

## 1.2. ASPECTOS ESPECÍFICOS A EVALUAR

| **Aspecto** | **Evaluación** |
|---|---|
| Entrega de Documentación solicitada. | 1.2.1 Se comprueba que el PSCC haya entregado la solicitud inicial para la creación de un PSCC y que la misma contenga los datos necesarios de acuerdo a la especificación del requisito. |

## 2. REQUISITOS GENERALES

## 2.1. ESPECIFICACIÓN DEL REQUISITO

| | |
|---|---|
| Nombre | Requisitos generales del "*Reglamento*". |
| Objetivo | Comprobar que la entidad que solicita la creación de un PSCC cumple con los aspectos generales que dispone o se derivan del Reglamento, si es capaz de entregar un servicio criptográfico de certificación y si presenta evidencias que permitan asegurar su permanencia y continuidad en la actividad. |
| Descripción | Se verificará que el PSCC cumple con los aspectos generales del procedimiento de acreditación, definidos en el "*Reglamento*". |
| Referencias en el "*Reglamento*". | Artículos 9, 11, 17, 24, 38, 39, 41y 52. |
| Documentación | • Declaración de Practicas de Certificación de |

| | |
|---|---|
| solicitada | la AC,<br>• Los procedimientos de operación, seguridad y administración de cada rol específico para la segregación de funciones de las autoridades de certificación y registro y los relacionados con el enfrentamiento a las contingencias. |

## 2.2. ASPECTOS ESPECÍFICOS A EVALUAR

| **Aspecto** | **Evaluación** |
|---|---|
| Organización y servicios | 2.2.1 Los servicios a prestar solicitados se corresponden con lo autorizado en el Reglamento. Artículos 11y 38 |
| | 2.2.2 Disponen de medios técnicos seguros para el sellado de tiempo de las operaciones del ciclo de vida de los certificados digitales de llave pública. Artículo 9 |
| | 2.2.3 Las autoridades de certificación y registro cumplen con los plazos establecidos en las operaciones de solicitud y otorgamiento de certificados digitales. Artículo 17 |
| | 2.2.4 Tienen implementado el control, seguimiento y registro sistemático de eventos y los participantes en los mismos, que se producen durante la operación de las actividades críticas del proceso de certificación.<br>• Uso de la llave privada de la AC.<br>• Proceso de Generación de llaves y certificados.<br>• Impresión de las contraseñas y la entrega segura al usuario de los certificados y llaves en caso que exista.<br>• Destrucción de las llaves<br>• Destrucción segura del fichero contenedor de las contraseñas en caso que exista.<br>Artículos 24, 41y 52 |

| | |
|---|---|
| | 2.2.5 Tienen habilitados los medios para la revisión de todos los materiales desechables donde se almacena información para la eliminación segura de residuos informativos comprometedores de la seguridad de los suscriptores, la Infraestructura y los servicios de certificación.<br>• Borrado seguro,<br>• Trituradora de papel<br>Artículo 41 |
| | 2.2.6 El certificado digital de la AC del PSCC debe estar firmado por la llave privada de la AC del Servicio Central Cifrado del MININT o la AC madre. Artículo 39 |

## 3. REQUISITO – ASPECTOS LEGALES Y DE PRIVACIDAD

### 3.1. ESPECIFICACIÓN DEL REQUISITO

| | |
|---|---|
| Nombre | Requisitos legales y de privacidad del solicitante a crear un PSCC. |
| Objetivo | Comprobar que el Prestador de Servicios Criptográficos de Certificación que solicita la acreditación, cumple con los requisitos legales en conformidad al "*Reglamento*". |
| Descripción | La entidad que solicita crear el PSCC debe presentar la documentación necesaria para demostrar al menos lo siguiente:<br>Que es una persona jurídica constituida según la legislación vigente en la República de Cuba con domicilio en la misma, que en su objeto social se encuentra la prestación de servicios asociados a la seguridad en la protección de información y que posea las licencias correspondientes para la operación en el ámbito de las telecomunicaciones.<br>Que está autorizado y registrado para ejercer la actividad comercial en el país. |
| Referencias en el "*Reglamento*". | Artículo 7, 16, 17, 19, 20, 38, 45 g, 54. |

| | |
|---|---|
| Documentación solicitada | 1. Certificado de Inscripción en el REEUP.<br>2. Autorización o poder del Representante legal de la entidad PSCC y sus datos personales.<br>3. Certificado de inscripción en el Registro Mercantil de Cuba. Se puede comprobar en los registros públicos digitales. En caso que se comercialicen los certificados.<br>4. Licencia de la OTC del MINCOM para la operación (en caso que corresponda).<br>5. Contrato firmado con la AC del Servicio Central Cifrado del MININT.<br>6. Modelo del contrato con los suscriptores de los servicios de la empresa. |

## 3.2. ASPECTOS ESPECÍFICOS A EVALUAR

| **Aspecto** | **Evaluación** |
|---|---|
| Personalidad Jurídica | 3.2.1 Validez y vigencia de la personalidad jurídica del solicitante, mediante la revisión y comprobación del Certificado de Inscripción en el REEUP. Artículo 7 |
| | 3.2.2 Autorización del representante. Artículo 17 |
| Giro de la empresa | 3.2.3 El giro de la empresa sea compatible con la actividad de Prestador de Servicios Cifrados de Certificación. Artículo 38 |
| Privacidad de la Información | 3.2.4 Se verificará que en los contratos con los suscriptores existan cláusulas que definan sus deberes y derechos previstos en el reglamento. Artículo 16, 45g |
| Contratación | 3.2.5 Se verificará que exista el contrato del PSCC con la AC raíz. Artículo 54 |
| Licencia operación | 3.2.6 Se verificará que posea la Licencia de la OTC del MINCOM para la operación. Artículo 17 y 19 |
| Comercialización | 3.2.7 Se verificará que la entidad esté inscrita en el Registro Mercantil de Cuba (para los prestadores comerciales) Artículo 38 |

## 4. REQUISITO – ESTRUCTURA CERTIFICADOS

### 4.1. ESPECIFICACIÓN DEL REQUISITO

| | |
|---|---|
| Nombre | Estructura e información del certificado de firma digital |
| Objetivo | Comprobar los aspectos que dispone el "Reglamento" con relación a la conformidad con el estándar, contenidos mínimos, y atributos del certificado de firma digital. |
| Descripción | 1. La estructura de datos que conforma el certificado digital emitido por el PSCC, debe estar en conformidad al estándar X.509 de la Unión Internacional de Telecomunicaciones (UIT-T) y la Organización Internacional de Estándares ISO/IEC 9594-8.<br>2. El certificado digital emitido por el PSCC debe contener como mínimo los siguientes datos obligatorios:<br>a) Los datos que identifican al sujeto titular del certificado, siendo estos:<br>• el nombre y los apellidos del titular,<br>• número de identidad permanente o de pasaporte, o identificación de equipo según corresponda,<br>• órgano, organismo o entidad a la que pertenezca y<br>• país de procedencia.<br>b) Los datos del certificado:<br>• Versión del certificado y su identificador único o número de serie,<br>• denominación de la autoridad de certificación que lo emitió y firmó,<br>• tiempo de validez del certificado, especificando el plazo de inicio y fin de su vida útil, en fecha y hora exacta nacional y del GMT.<br>c) Los datos de las llaves criptográficas:<br>• Se fijarán los usos permitidos para las llaves criptográficas adquiridas para los servicios |

| | |
|---|---|
| | de protección de la información oficial, así como se publicará la llave pública del suscriptor en notación ASN.1 y el algoritmo criptográfico con el cual se generó.<br>d) Relacionados con la autenticidad de la Autoridad de Certificación:<br>• Se especifica la secuencia de campos que llena la Autoridad de Certificación y que identifican la firma electrónica digital de los campos previos. Dicha secuencia contiene tres atributos: el algoritmo de firma utilizado, el resumen (hash) de la firma, y la propia firma digital.<br>3. Los certificados se clasificarán en las siguientes categorías:<br>a) Categoría 1: Certificados Digitales de Llave Pública para firma digital de mensajería y ficheros electrónicos (CD-Firma).<br>b) Categoría 2: Certificados Digitales de Llave Pública para la protección cifrada de canales y servicios web y de correo electrónico (CD-SSL).<br>c) Certificado para aplicaciones de cifrado.<br>4. El formato criptográfico de las llaves a entregar será en PKCS 12, DER, PEM y PEC. |
| Referencias en el "Reglamento". | Artículo 10-15, 22, 24, 25 y 41. |
| Estándares de evaluación | ISO/IEC 9594-8 |
| Evidencias solicitadas | Certificado digital tipo, emitido por el PSCC en evaluación y certificado digital de la AC que los emite. |

## 4.2. ASPECTOS ESPECÍFICOS A EVALUAR

| **Aspecto** | **Evaluación** |
|---|---|
| Conformidad con el estándar ISO/IEC | 4.2.1 Se verificará que la estructura básica del certificado esté en conformidad a la norma y que la gramática utilizada en la estructura |

| | |
|---|---|
| 9594-8 | básica, puedan ser leídos por cualquier aplicación que cumpla dicho el estándar. Artículos 10 y 12 |
| Contenido básico del certificado de firma digital emitido por PSCC | 4.2.2 Se verificará que el certificado contiene la información obligatoria de la estructura del certificado relacionada en el reglamento. Articulo 12 |
| Lectura y reconocimiento del contenido mínimo cuando existen atributos adicionales en el certificado de firma digital emitido por PSCC | 4.2.3 Se verificará que el PSCC estructure sus certificados de firma digital de forma que los atributos adicionales que introduzca con el fin de incorporar límites al uso del certificado no impidan la lectura de las menciones señaladas en el artículo 12 del Reglamento ni su reconocimiento por terceros. Artículos 12, 13 y 14 |
| Uso de clave pública acreditada | 4.2.4 Se verificará que el certificado de la AC del PSCC no sea utilizado para otras funciones no autorizadas. Artículos 11, 22 y 25 |
| Algoritmos de firma | 4.2.5 Se verificará que el PSCC utilice algoritmos de firma aprobados por la Dirección de Criptografía del MININT que provean el adecuado nivel de seguridad tanto para su propia firma como para la firma del titular. Artículo 41 |
| Largos de llaves | 4.2.6 Se verificará que el PSCC utilice largos de llave pública y privada aprobados por la Dirección de Criptografía del MININT para los distintos usuarios. Los largos mínimos de llaves serán 8192 para AC Raíz, 4096 para AC Intermedia y 2048 para usuarios finales. Artículo 41. |
| Funciones Hash | 4.2.7 Se verifica que el PSCC utilice funciones Hash aprobados por Dirección de Criptografía del MININT para el proceso de firma, que |

| | |
|---|---|
| | provean el adecuado nivel de seguridad tanto para su propia firma como para la firma titular. Articulo 24 |
| Validez del certificado | 4.2.8 Se comprobará que, en los campos del certificado digital destinados a nombre, razón social y/o denominación de su solicitante, se admiten solo los datos de identidad verdaderos del titular. Articulo 15 |

## 5. REQUISITO –ESTRUCTURA CRL y SERVICIO OCSP.

### 5.1. ESPECIFICACIÓN DEL REQUISITO

| | |
|---|---|
| Nombre | Estructura e información de la lista de certificados revocados (CRL) y del Servicio en línea de estado de los Certificados (OCSP). Funcionamiento del servicio de información sobre certificados revocados y suspendidos. |
| Objetivo | Verificar que las listas de certificados revocados de firma digital tengan el formato y contenido especificado en el estándar, y permita al usuario identificar plenamente al PSCC emisor de la CRL.<br>Verificar el estado de los certificados de firma digital tengan el formato y contenido especificado en el estándar, y permita al usuario identificar plenamente el estado del certificado emitido por la PSCC emisor. |
| Descripción | La lista de certificados revocados de firma digital (CRL) debería contener la información y estructura que especifica el estándar ISO/IEC 9594-8.<br>Este estándar especifica que la lista debería contener al menos la identificación del emisor, fecha de su emisión e identificación de los certificados revocados a dicha fecha.<br>Ya que la lista podría ser almacenada y transmitida en medios inseguros, debería estar debidamente firmada por el PSCC emisor.<br>El servicio en línea del estado de los certificados |

| | |
|---|---|
| | (OCSP) debería contener la información y estructura que especifica el estándar RFC 2560 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol" actualizada según RFC 6277 "Online Certificate Status Protocol Algorithm Agility" |
| Referencias en el "Reglamento". | Artículo 4 y 30, 31 y 34. |
| Estándares de evaluación | ISO/IEC 9594-8<br>RFC 2560 y RFC 6277 |
| Documentación solicitada | Política para el trabajo de la AC, DPC o documento donde se dispongan las especificaciones de la estructura del CRL y el servicio de OCSP del PSCC. |
| Evidencias solicitadas | Lista de certificados revocados de firma digital (CRL) emitida por el PSCC en evaluación y el certificado digital de la AC que la emite.<br>Respuesta a Consulta de Estado de Certificado al Servicio OCSP de la PSCC. |

## 5.2. ASPECTOS ESPECÍFICOS A EVALUAR

| **Aspecto** | **Evaluación** |
|---|---|
| Contenido Mínimo | Se verificará que la CRL contenga al menos la siguiente información:<br>5.2.1 Algoritmo de firma. Este campo debe contener la identificación del algoritmo de firma utilizado. |
| | 5.2.2 Nombre del emisor. Este campo debe contener el nombre de la entidad que emitió y firmó la lista de certificados revocados. Artículo 30 |
| | 5.2.3 Fecha actual. Este campo debe contener la fecha y hora en que fue emitida la lista de certificados revocados (CRL). Artículo 31 |
| | 5.3.4 Próxima actualización. Se debería incluir en este campo la fecha en que, a más tardar, se emitirá la próxima lista de certificados revocados. Artículo 31 |

| | |
|---|---|
| | 5.2.5 Certificados revocados. En este campo se deben incluir los números de serie de los certificados revocados por el emisor, indicando además la fecha y hora de revocación correspondiente. Artículo 31 |
| | 5.2.6 Se verificará que el Servicio OSCP del PSCC este implementado de acuerdo al estándar RFC 2560 en sus mecanismos de:<br>• Petición de Validación<br>• Respuesta a la Validación |
| Comprobación de firma | 5.2.7 Se verificará que la lista de certificados revocados esté debidamente firmada por el PSCC emisor. |
| Mecanismo de suspensión de certificados | 5.2.8 El mecanismo de publicación incluye los certificados suspendidos. Artículo 34 |

## 6. REQUISITO – REGISTRO DE ACCESO PÚBLICO

### 6.1. ESPECIFICACIÓN DEL REQUISITO

| | |
|---|---|
| Nombre | Servicios, contenido y accesibilidad electrónica del sistema público de información del PSCC. |
| Objetivo | Asegurar el acceso a información relevante descriptiva del sistema por parte de los titulares y terceros. |
| Descripción | Se verificará que el PSCC interesado:<br>• Garantice la existencia de un servicio seguro de consulta remota del registro de certificados emitidos, en el que quede constancia de los certificados emitidos indicando si el mismo se encuentra vigente, revocado o suspendido.<br>• Provea acceso al registro público de certificados a los titulares y partes interesadas por medios electrónicos de manera continua y regular.<br>• Cuente con procedimientos para informar a los titulares las características generales de los procesos de creación y verificación de |

| | |
|---|---|
| | firma digital, así como de las reglas sobre prácticas de certificación y las demás que el PSCC se comprometa a utilizar en la prestación del servicio.<br>• Tenga procedimientos para dejar sin efecto temporal o definitivamente (suspender o revocar) los certificados, fundados en, a lo menos, una de las causas o circunstancias que indica el "Reglamento".<br>• Cuente con procedimientos para publicar y actualizar en su(s) sitio(s) Web, la Política para el trabajo con la infraestructura de llave pública y la Declaración de Prácticas de Certificación (DPC) |
| Referencias en el "Reglamento" | Artículos 17e, 26, 30, 31, 32, 33, 34, 41c, e, i, y j. |
| Estándares de Evaluación | No |
| Documentación solicitada | Documento descriptivo que contenga al menos la siguiente información:<br>• Especificación del sitio de acceso electrónico,<br>• Descripción de la tecnología,<br>• Disponibilidad, accesibilidad, conexión, esquemas y diagramas de funcionamiento,<br>• Medidas de seguridad. |
| Evidencias solicitadas | Sitio de acceso electrónico público con las funcionalidades descritas. |

## 6.2. ASPECTOS ESPECÍFICOS A EVALUAR

| **Aspecto** | **Evaluación** |
|---|---|
| Existencia y contenido mínimo del sitio de información pública. | 6.2.1 Existencia del Sitio WEB de la entidad y la disponibilidad de publicación en el mismo de los datos necesarios y suficientes de los suscriptores para que puedan realizar el ejercicio de los procesos de firma digital de documentos y su verificación por terceros, así como el precio de comercialización de los |

| | |
|---|---|
| | certificados digitales y de los servicios de certificación en los casos que corresponda. Artículo 41c |
| | Debe contener al menos los siguientes documentos:<br>6.2.2 Registro de certificados emitidos, indicando código de identificación único del certificado y su estado (vigente, suspendido o revocado) Artículo 17e. |
| | 6.2.3 Disponen de las condiciones para la publicación de su certificado digital en el repositorio especificado, incluida la huella digital de dicho CID para su comprobación por terceros, su Declaración de Prácticas de Certificación actualizadas y aprobadas, asegurando los mecanismos de acceso publicitario para el conocimiento de todos los participantes en el servicio, incluidos los suscriptores. Artículo 41c |
| | 6.2.4 Se debe asegurar una disponibilidad del sitio. Para esto se verificará la existencia de mecanismos redundantes o alternativos de conexión y sitios de emergencia que se levanten manual o automáticamente en caso de desastres. Artículo 41j |
| | 6.2.5 Copia de la Lista de certificados revocados (CRL) actualizada cada 24 horas. Artículo 26 |
| | 6.2.6 Acceso seguro a los titulares para realizar la solicitud de revocación o suspensión de certificados vigentes. Artículo 30 |
| | 6.2.7 Declaración de sus Prácticas de Certificación. Artículo 41c |
| Requerimiento sobre el Servicio de CRL y OCSP | Se verificará que:<br>6.2.8 Cada vez que se produzca la revocación de un certificado, la autoridad de certificación correspondiente, genera y publica en su repositorio y en un plazo no mayor a las |

| | |
|---|---|
| | veinticuatro (24) horas después de aprobarse dicha revocación, una nueva lista de revocación de certificados (CRL). Artículo 31 |
| | 6.2.9 El servicio de consulta tenga la doble opción para consultar en línea de forma activa, mediante el uso del protocolo OCSP y la descarga de la lista de revocación por métodos clásicos. Artículo 41e |
| | 6.2.10 Verificar si en caso de revocación de un certificado se informa en un término no mayor a las veinticuatro (24) horas a la autoridad de registro que lo aprobó y al órgano, organismo o entidad que ampara al suscriptor afectado. Artículo 26 |
| | 6.2.11 Verificar si en la DPC están descritas las causas para la extinción de la vigencia de un certificado y existan los procedimientos de cómo actuar en cada caso. Artículos 32 y 33 |
| | 6.2.12 Verificar si la Autoridad de registro posee los procedimientos de cómo actuar ante la presentación de una solicitud de revocación de certificados. Artículo 30 |
| Servicio de certificados suspendidos | 6.2.13 Se verificará que la lista de certificados revocados puede incluir la información necesaria para indicar el estado de suspensión de un certificado o exista algún otro mecanismo para informar sobre este aspecto a los suscriptores. Artículo 41e |

## 7. REQUISITO – REVISIÓN DE LA EVALUACIÓN DE RIESGOS

### 7.1. ESPECIFICACIÓN DEL REQUISITO

| | |
|---|---|
| Nombre | Revisión de la Evaluación de Riesgos |
| Objetivo | Determinar la consistencia del análisis de riesgos de la entidad PSCC |
| Descripción | Dado que el producto principal de un PSCC es la "confianza", el requerimiento fundamental para un PSCC es demostrar una clara comprensión de las amenazas de seguridad |

| | |
|---|---|
| | enfrentadas por el servicio que se presta y poder mostrar planes efectivos para reducir el riesgo residual a un nivel aceptable.<br>La Gestión del Riesgo incluye los siguientes procesos:<br>• Establecimiento del contexto: Se definen los objetivos, alcance y la organización para todo el proceso.<br>• Identificación de riesgos: Consiste en determinar qué puede provocar pérdidas en la organización.<br>• Diagnóstico de riesgos: Utilizar métodos cuantitativos o cualitativos para obtener una cuantificación de los riesgos identificados, teniendo en cuenta las debilidades, amenazas, fortalezas y oportunidades.<br>• Evaluación y clasificación de los riesgos: Se evalúan la frecuencia de ocurrencia, el ámbito de acción (interno o externo), severidad y cuantía de las pérdidas.<br>• Tratamiento de riesgos: Se define la estrategia para tratar cada uno de los riesgos valorados; reducción, aceptación, evitación o transferencia.<br>• Aceptación de riesgos: Se determinan los riesgos que se decide aceptar y su justificación correspondiente.<br>• Elaboración del Plan de Prevención de Riesgos: Se elaboran medidas medibles para prevenir, o reducir los riesgos.<br>• Monitorización y revisión de riesgos: El análisis de riesgos se actualiza sistemáticamente con todos los cambios internos o externos que afectan a la valoración de los riesgos.<br>La gestión de riesgos se evalúa por lo establecido en cada organismo a partir de lo dispuesto en la Resolución 60/11 de la |

| | |
|---|---|
| | Contraloría General de la Republica. |
| Referencias en el "Reglamento" | Reglamento Art. 41i, j, m, n, o, p, q, r y s |
| Estándares de evaluación | "Resolución 60/11" y documentos regulatorios de la actividad en la entidad. |
| Documentación solicitada | Copia del documento correspondiente al Diagnóstico de Riesgos.<br>Ultima auditoría realizada según Resolución 60/11. |

## 7.2. ASPECTOS ESPECÍFICOS A EVALUAR

| **Aspecto** | **Evaluación** |
|---|---|
| Diagnóstico y Prevención de riesgos | 7.2.1 Verificar la existencia del diagnóstico y que los riesgos considerados sean reales y se clasifiquen de acuerdo a lo establecido. Artículo 41m) |
| | 7.2.2 Verificar que riesgos relevantes no hayan sido omitidos a partir de la valoración del cumplimiento de los aspectos relacionados en el artículo 41. |
| | 7.2.3 Está protegida la integridad y disponibilidad de la información mediante el uso de tecnología y medidas de seguridad tanto físicas como lógicas que reduzcan los riesgos y consecuencias de ataques maliciosos en contra de los sitios tanto internos como externos. Artículo 41i) |
| Estructura del proceso de Gestión de riesgos | 7.2.4 Verificar que el proceso de gestión de Riesgos ha sido auditado en el año precedente y si los resultados son positivos. Artículo 41r), s) |
| | 7.2.5 Gestionan la seguridad de la parte de la Infraestructura de Llave Pública bajo su jurisdicción de forma permanente para identificar posibles debilidades y establecer las correspondientes acciones correctoras. Esto implica el análisis de la ocurrencia de los |

| | |
|---|---|
| | posibles riesgos varias veces al año. Artículo 41n) |

## 8. REQUISITO – PLAN DE PREVENCIÓN DE RIESGOS
## 8.1. ESPECIFICACIÓN DEL REQUISITO

| | |
|---|---|
| Nombre | Planes de Prevención de Riesgos y Recuperación de Desastres |
| Objetivo | Comprobar a través de los documentos que la organización tiene planes establecidos para disminuir a un nivel aceptable el efecto de interrupciones del servicio del PSCC, mediante una combinación de controles preventivos y planes de contingencia |
| Descripción | El Plan de Prevención de riesgos y el Plan contra Desastres deben describir cómo los servicios serán restaurados en el evento de desastres, una caída de los sistemas o fallas de seguridad. Su objetivo es disminuir a un nivel aceptable el efecto de interrupciones del servicio del PSCC. Tales planes deben ser mantenidos y probados periódicamente y debieran ser parte integral de los procesos de la organización.<br>En general, para lograr la implantación de proceso del diagnóstico y elaboración del Plan de Prevención de Riesgos se debe alinear con la Resolución 60/11 que establece dicho proceso.<br>En particular, se debe dar prioridad de restauración para asegurar la continuidad de los servicios a terceros que sean dependientes de la operación del PSCC.<br>Este documento también deberá describir los procedimientos de emergencia a ser seguidos en a lo menos los siguientes Escenarios:<br>• Desastres que afecten el funcionamiento de los productos de software en el cual el PSCC basa sus servicios,<br>• Incidente o posible incidente de seguridad |

| | |
|---|---|
| | que afecte la operación del sistema en el cual el PSCC basa sus servicios,<br>• Comprometimiento de la llave privada de firma del PSCC,<br>• Falla de los mecanismos de auditoría,<br>• Falla en el hardware donde se ejecuta la tecnología informática sobre la cual el PSCC basa sus servicios (incluyendo servidores, dispositivos criptográficos, dispositivos de seguridad y dispositivos de comunicaciones)<br>Parte del plan de manejo de contingencias es el Análisis de Impacto en los Servicios o la apreciación de los daños financieros, siendo esta una evaluación del efecto de las interrupciones no planificadas en el trabajo.<br>El plan deberá además incluir mecanismos para la preservación de evidencia de mal uso de los sistemas, cuyo propósito es proporcionar evidencia admisible en un proceso judicial en alguna fecha posterior<br>Tener actualizados y validados los resultados de auditorías, inspecciones y otros procedimientos de control interno, que demuestren la existencia de un ambiente de control en el entorno de funcionamiento del prestador de servicios cifrados de certificación, en correspondencia con lo establecido en la Resolución 60/11 de la Contraloría General de la República, teniendo en orden los mecanismos de solvencia económica para asegurar la prestación del servicio en general. |
| Referencias en el "Reglamento" | Reglamento Art. 41, 49 y 52. |
| Estándares de evaluación | ISO 27002, (17799 en Cuba) Sección 14<br>Resolución 60/11 de la Controlaría General de la República<br>ETSI TI 102 042, sección 7.4.8 |
| Documentación | Documentos correspondientes a los Planes de |

| | |
|---|---|
| solicitada | Prevención de Riesgos y Planes contra Desastres Diagnóstico de Riesgos |
| Evidencias solicitadas | Auditoría en Terreno<br>• Auditorías realizadas en función de lo establecido en la Resolución 60/11<br>• Planes de seguridad informática y contra desastres ambientales. |

## 8.2 ASPECTOS ESPECÍFICOS A EVALUAR

| **Aspecto** | **Evaluación** |
|---|---|
| Conformidad con el estándar ISO 27002 sección 14.1.1 al 14.1.4 y la Resolución 60/11 | 8.2.1 Verificar que los requerimientos indicados, están incorporados.<br>• Incluir la seguridad de la información en el proceso de gestión de continuidad del negocio.<br>• Continuidad del negocio y evaluación del riesgo.<br>• Desarrollar e implementar los planes de continuidad incluyendo la seguridad de la información. |
| Conformidad con el estándar ISO 27002 sección 14.1.5 y la Resolución 60/11 | 8.2.2 Verificar que se ha incluido un procedimiento de revisión y evaluación periódico de los planes de prevención de riesgos y contra desastres. |
| Conformidad con el estándar ETSI TI 102 042 sección 7.4.8 | 8.2.3 Verificar que el plan incorpora procedimientos especialmente detallados para el caso de compromiso de la llave privada de firma tal como lo indica el estándar ETSI. |
| Relación entre el diagnóstico de Riesgos y los planes para su prevención. | 8.2.4 Verificar que los principales riesgos contemplados en el Plan de Prevención y Plan contra desastres son coherentes con los niveles de riesgo determinados en el Diagnóstico de riesgos. |
| Análisis de apreciación de daños | 8.2.5 Verificar la coherencia del Análisis de Impacto en los Servicios o apreciación de daños, que debe ser parte del plan de manejo |

| | |
|---|---|
| | de contingencias. |
| Viabilidad de las facilidades computacionales alternativas | 8.2.6 Verificar que las facilidades computacionales alternativas consideradas en el plan, cumplen con los requerimientos mínimos para la operación del PSCC. |
| Elementos de auditoría | 8.2.7 Verificar que el sistema en el cual el PSCC basa sus servicios provee mecanismos de preservación de los elementos de auditoría. Artículos 49 y 52 |
| Requerimientos de los planes | 8.2.8 Tienen implementadas medidas y planes para evitar y extinguir tempranamente incendios, inundaciones, excesos de humedad y otros desastres tecnológicos; la vitalidad energética y telemática del servicio, así como para la salva y restauración segura de la información de interés. |
| | Verificar si existen los procedimientos de emergencia a ser seguidos en a lo menos los siguientes Escenarios:<br>8.2.9 Desastre que afecte el funcionamiento de los productos de software en el cual el PSCC basa sus servicios, |
| | 8.2.10 Incidente o posible incidente de seguridad que afecte la operación del sistema en el cual el PSCC basa sus servicios, |
| | 8.2.11 Falla de los mecanismos de auditoría |
| | 8.2.12 Falla en el hardware donde se ejecuta el producto en el cual el PSCC basa sus servicios (incluyendo servidores, dispositivos criptográficos, dispositivos de seguridad y dispositivos de comunicaciones). |

## 9. REQUISITO – POLÍTICA DE SEGURIDAD

### 9.1. ESPECIFICACIÓN DEL REQUISITO

| | |
|---|---|
| Nombre | Documentación y Mantención de la Política de Seguridad de la Información. |

| | |
|---|---|
| Objetivo | Comprobar a través de este documento que la organización tiene claros los objetivos de seguridad relevantes para el servicio y que las instancias de gestión del PSCC apoyan formalmente esta política. |
| Descripción | La política de seguridad es una declaración de objetivos de seguridad. Solo contiene objetivos de seguridad que son factibles de lograr a través de acciones, procedimientos y mecanismos implementados por el PSCC.<br>La política de seguridad deberá cumplir a lo menos con los siguientes requerimientos:<br>• Los objetivos de seguridad deben ser consecuencia de la Evaluación de Riesgos, de forma tal que los objetivos de la política de seguridad y sus defensas asociadas correspondan al nivel de riesgo requerido para que un PSCC sea un ente de confianza.<br>• Debe estar basada en las recomendaciones del estándar ISO 27002 (17799 en Cuba) Sección 5.<br>• Los elementos de la política de seguridad que estén incorporados en la Declaración de Prácticas de Certificación (DPC) deben estar incluidos en este documento.<br>Se recomienda que este documento identifique los objetivos de seguridad relevantes y las amenazas potenciales relacionadas a los servicios suministrados, así como las medidas tomadas para evitar o limitar los efectos de estas amenazas.<br>Adicionalmente, se recomienda que la documentación describa las reglas, directivas y procedimientos que indican como son provistos los servicios específicos y las medidas de seguridad asociadas. |
| Referencias en el | Reglamento Art. 47 y 56 |

| | |
|---|---|
| "Reglamento" | |
| Estándares de evaluación | ISO/IEC 27002, Sección 5 |
| Documentación solicitada | Copia del documento correspondiente a la Política de Seguridad de Información de la Entidad. |
| Evidencias solicitadas | Auditoría en terreno que permita verificar aspectos relevantes. |

## 9.2. ASPECTOS ESPECÍFICOS A EVALUAR

| **Aspecto** | **Evaluación** |
|---|---|
| Conformidad con el estándar ISO 27002 sección 5.1.1 | 9.2.1 Verificar que los requerimientos de la sección 5.1.1 están incorporados. |
| Conformidad con el estándar ISO 27002 sección 5.1.2 | 9.2.2 Verificar que se ha incluido un procedimiento de revisión y evaluación periódico de la política de seguridad. |
| Correspondencia entre la política de seguridad y la DPC de la PSCC | 9.2.3 Verificar la correspondencia de la política de seguridad con la DPC y las medidas implementadas en la entidad PSCC. |
| Relación entre la Evaluación de Riesgos y la política de seguridad | 9.2.4 Verificar que los principales aspectos de la política de seguridad son coherentes con los riesgos determinados en la el diagnóstico y Plan de Prevención contra riesgos. |
| Claridad de los objetivos de seguridad | 9.2.5 Verificar que se establecen objetivos de seguridad claros y relacionados con la protección de los procesos de trabajo, activos y servicios del PSCC. |

## 10. REQUISITO PLAN DE ADMINISTRACIÓN DE LLAVES

## 10.1. ESPECIFICACIÓN DEL REQUISITO

| | |
|---|---|
| Nombre | Implementación y Mantención del Plan de Administración de Llaves Criptográficas |

| | |
|---|---|
| Objetivo | Comprobar que la organización implementa procedimientos de administración del ciclo de vida de sus llaves criptográficas coherente con su política de seguridad, que permita mostrar un nivel de confianza consistente con los objetivos del servicio. |
| Descripción | Las llaves criptográficas son la base de una infraestructura de llaves públicas (PKI), siendo el elemento principal a resguardar y administrar por el PSCC, y por lo tanto requiere de un plan específico para su administración (ETSI TS 102 042 sección 7.2)<br>Documentación del procedimiento para la<br>• Generación de las llaves de la autoridad de certificación del PSCC<br>• Almacenamiento, respaldo y recuperación de la llave privada de la AC.<br>• Distribución de la llave pública de la AC.<br>• Uso de la llave privada por parte de la AC<br>• Término del tiempo de vida de las llaves de la AC<br>• Administración del tiempo de vida del hardware criptográfico utilizado por la AC.<br>• Servicios de administración de las llaves de los titulares suministrados por la AC (generación de llave, entrega segura de las mismas y renovación después de vencimiento)<br>• Preparación de los dispositivos seguros de los usuarios.<br>• Borrado seguro y destrucción de borradores y registros.<br>• A su vez el plan debe ser consistente con la Política de Certificación del PSCC. |
| Referencias en el "Reglamento" | Reglamento Artículos No 21, 24, 25, 41h, o, p, 45h, 46 y 56 |
| Estándares de evaluación | ETSI TS 102 042<br>FIPS 140-2 L3 |

| | |
|---|---|
| Documentación solicitada | Documento descriptivo de la implementación de los procedimientos de la Administración de Llaves Criptográficas del PSCC. |
| Evidencias solicitadas | Auditoría en terreno |

## 10.2. ASPECTOS ESPECÍFICOS A EVALUAR

| **Aspecto** | **Evaluación** |
|---|---|
| Relación entre el Plan de Administración de Llaves y los recursos asignados | 10.2.1 Verificar que el PSCC dispone de los recursos y capacidades adecuados para implementar los procedimientos de administración de llaves. |
| Relación entre Plan de Administración de Llaves y Evaluación de Riesgos | 10.2.2 Verificar que los procedimientos y mecanismos de administración de llaves implementados permiten lograr el riesgo residual determinado en la Evaluación de Riesgos |
| Plan de Administración de Llaves | 10.2.3 Verificar que los procedimientos implementados de acuerdo al Plan de Administración de Llaves posibilitan que la seguridad de las llaves se mantiene en el tiempo ante cambios en: amenazas, personal, servicios, componentes tecnológicos, etc. |
| Relación del Plan de Administración de Llaves con las prácticas y política de certificación | 10.2.4 Verificar que los objetivos de seguridad enunciados en las Política de Seguridad y la Política de Certificados se logran a través de la implementación del Plan de Administración de Llaves. |
| Requerimientos ETSI TS 102 042, sección 7.2.1 | 10.2.5 Verificar que los requerimientos de la seguridad de la Generación de Llaves de la AC, del estándar ETSI TS 102 042 están considerados. |

| | |
|---|---|
| Requerimientos ETSI TS 102 042, sección 7.2.2 | 10.2.6 Verificar que los requerimientos de Almacenamiento, Respaldo y Recuperación, del estándar ETSI TS 102 042 están considerados. |
| Requerimientos ETSI TS 102 042, sección 7.2.3 | 10.2.7 Verificar que los requerimientos de Distribución de la llave pública de la AC, del estándar ETSI TS 102 042 están considerados. |
| Requerimientos ETSI TS 102 042, sección 7.2.5 | 10.2.8 Verificar que los requerimientos de Uso de Llave de la AC, del estándar ETSI TS 102 042 están considerados. |
| Requerimientos ETSI TS 102 042, sección 7.2.6 | 10.2.9 Verificar que los requerimientos de Fin del Ciclo de Vida de la Llave de la AC, del estándar ETSI TS 102 042 están considerados. |
| Requerimientos ETSI TS 102 042, sección 7.2.7 | 10.2.10 Verificar que los requerimientos de Administración del hardware criptográfico del estándar ETSI TS 102 042 están considerados. |
| Nivel de seguridad del dispositivo seguro de los usuarios | 10.2.11 Verificar que el dispositivo seguro de los usuarios cumple como mínimo con los requerimientos del estándar FIPS 140-2 nivel 3 en sus elementos de seguridad e implementación de los algoritmos criptográficos estándares. |
| Seguridad del Funcionamiento | 10.2.12 Se encuentran en funcionamiento permanente todas las medidas de seguridad, físicas y lógicas, así como de trazología auditables de los eventos para el aseguramiento del dispositivo de confidencialidad de su llave criptográfica privada( de la AC), y otros datos y medios requeridos en el proceso de emisión y entrega del certificado digital y llaves asociadas al suscriptor (dispositivo informático o electrónico seguro, con medidas de protección cifrada de dicha llave y control de acceso a ella por medio de una clave o código PIN). Artículo 41h |

| | |
|---|---|
| | 10.2.13 La generación de la llave privada por los usuarios se realiza a partir de los procedimientos y tecnologías designados por la DC. Artículo 24 |
| | 10.2.14 Los suscriptores conocen sus deberes en cuanto a la seguridad de la generación, conservación y uso de la llave privada. Artículo 56 |
| | 10.2.15 La aplicación para la generación de criptomateriales debe trabajar de forma independiente o como parte de una red restringida y no puede estar conectada físicamente a redes de alcance global. |
| | 10.2.16 La generación de la llave privada para firma digital a solicitud del suscriptor se realizará por tres funcionarios de la AC, y se entregará al mismo en un dispositivo informático o electrónico protegido con medidas de cifrado de dicha llave y control de acceso a ella por medio de una contraseña o código PIN. Artículo 24 |
| | 10.2.17 La autoridad de certificación no guardará copia de la llave criptográfica privada del suscriptor, con el objetivo de asegurar la posesión exclusiva de su titular Artículo 24 |
| | 10.2.18 Disponen del Módulo Criptográfico de Alta Seguridad (MCAS) para la custodia y conservación de la llave privada de la autoridad o prestador de servicios criptográficos de certificación según corresponda. Artículo 41o |

**NOTA:** A todos los efectos, lo establecido en los documentos rectores y técnicos aprobados por la Dirección de Criptografía tiene prioridad ante lo establecido en los estándares internacionales.

## 11. REQUISITO GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

### 11.1. ESPECIFICACIÓN DEL REQUISITO

| | |
|---|---|
| Nombre | Implementación de la gestión de incidentes de seguridad de la información |
| Objetivo | Evaluar los requisitos relacionados con la gestión de incidentes de seguridad de la Información.<br>Para ello debe fundamentalmente valorarse la generación de reportes de los eventos críticos y las debilidades de la seguridad de la información, así como establecer la Gestión de los incidentes y mejoras en la seguridad de la información. |
| Descripción | El PSCC debe asegurar que existan reportes y trazas de los eventos críticos y debilidades de la seguridad de la información asociados con los sistemas de información.<br>Se debieran establecer procedimientos formales de reporte y de control de los eventos.<br>Todos los usuarios, funcionarios y terceros debieran estar al tanto de los procedimientos para el reporte de los diferentes tipos de eventos y debilidades que podrían tener un impacto en la seguridad de los activos organizacionales.<br>Debe estar establecido que reporten cualquier evento y debilidad de la seguridad de la información lo más rápido posible al PSCC.<br>Se debieran establecer las responsabilidades y procedimientos para manejar de manera efectivo los eventos y debilidades en la seguridad de la información una vez que han sido reportados.<br>Se debiera aplicar un proceso de mejoramiento continuo para la respuesta a, monitoreo, evaluación y la gestión general de los incidentes en la seguridad de la información. |

| | |
|---|---|
| Referencias en el "Reglamento" | Artículos No 41, 45, 51, 52 y 56. |
| Estándares de evaluación | ISO/IEC 27002 Sección13 |
| Documentación solicitada | Documento descriptivo de los Procedimientos de Gestión de Incidentes de Seguridad de la Información.<br>Trazas y reportes de las actividades críticas del proceso de certificación.<br>Reportes de Incidentes de Seguridad de la Información |
| Evidencias solicitadas | Auditoria en el terreno |

## 11.2. ASPECTOS ESPECÍFICOS A EVALUAR

| **Aspecto** | **Evaluación** |
|---|---|
| Relación entre los Procedimientos de Gestión de Incidentes y Política de Seguridad | 11.2.1 Verificar que los procedimientos y mecanismos de seguridad implementados permiten lograr los objetivos de la política de seguridad. |
| Relación entre los Procedimientos de gestión de Incidentes y la Evaluación de Riesgos | 11.2.2 Verificar que los procedimientos y mecanismos de seguridad implementados permiten corregir los riesgos determinados en el Diagnóstico de Riesgos asociados a los incidentes de Seguridad de la Información. |
| Organizativos | 11.2.3 Tienen organizado el sistema de trabajo para el análisis y esclarecimiento de hechos contrarios al buen empleo de los certificados digitales bajo su jurisdicción, así como para la tramitación de las informaciones requeridas por los órganos administrativos, de control, fiscales y judiciales, según corresponda. Artículo 41 |
| | 11.2.4 Se realiza el control, seguimiento y registro sistemático de los eventos que se producen durante la operación de las actividades críticas |

| | |
|---|---|
| | del proceso de certificación los que se catalogan como mínimo en:<br>• Informativo: Significa que una acción se realizó de forma exitosa.<br>• Marca: Inicio y finalización de una sesión.<br>• Advertencia: Presencia de un hecho anormal pero no de una falla.<br>• Error: Una operación genera una falla predecible.<br>• Error fatal: Una operación genera una falla impredecible.<br>Artículo 52 |
| | 11.2.5 Tienen en funcionamiento permanente todas las medidas de seguridad física y lógicas, así como las trazas auditables de los eventos para el aseguramiento del dispositivo de confidencialidad de su llave criptográfica privada, y otros datos y medios requeridos por los suscriptores. Artículo 41 |
| | 11.2.6 Tienen implementados, sistemas técnicos y/u organizativos de control, bloqueo, aviso y seguimiento de acceso y proximidad a los medios de trabajo especializados, y la aplicación racional de métodos de defensa criptológica frente a intercepciones de sus comunicaciones e intromisiones informáticas o eléctricas en los equipos de prestación del servicio. Artículo 41 |
| | 11.2.7 Se realiza una vez al año, una auditoría a todos los procesos de gestión de certificados digitales, en al menos una muestra del dos por ciento (2 %) de los certificados digitales gestionados. Artículo 41 |
| | 11.2.8 Toda la información y documentación relativa a la gestión de los certificados digitales, se conservará durante un período mínimo de quince (15) años en archivos protegidos con |

| | |
|---|---|
| | técnicas de cifrado y autenticación, que aseguren el acceso solo a funcionarios autorizados para llevar a cabo verificaciones de integridad u otras, empleando aplicaciones específicas y aprobadas de visualización y gestión de eventos. Artículo 41 |

## 12. REQUISITO EVALUACIÓN DE LA PLATAFORMA TECNOLÓGICA.

### 12.1. ESPECIFICACIÓN DEL REQUISITO

| **Nombre** | **Evaluación de la Plataforma Tecnológica.** |
|---|---|
| Objetivo | Evaluar los elementos de seguridad de la plataforma tecnológica utilizada para la generación, publicación y administración de certificados, CRL y OCSP. |
| Descripción | Evaluar la seguridad de los elementos que constituyen la plataforma tecnológica del PSCC. Se debe considerar componentes hardware y software que componen la infraestructura PKI del PSCC, como, asimismo, todos los elementos de apoyo a su operación e interrelación, como protocolos y servicios.<br>Los elementos a considerar son:<br>• Módulo criptográfico.<br>• Módulo AC (Autoridad Certificadora)<br>• Módulo AR (Autoridad de Registro)<br>• Módulo de Almacenamiento y Publicación de Certificados.<br>• Protocolos de comunicación entre AC y AR.<br>• Elementos de administración de logs y auditoría. |
| Referencias en el "Reglamento" | Reglamento Artículos No 10, 17, 21, 24, 26-34 y 41 |
| Estándares de evaluación | FIPS 140-2 L3<br>ISO/IEC 15408 o equivalente |
| Documentación solicitada | Documento descriptivo de la implementación de la infraestructura tecnológica y de los módulos criptográficos implementados en la misma. |

| | |
|---|---|
| | Este documento debería incluir al menos, planos de interconexión de sistemas, cableado de red de datos, cableado de poder principal y auxiliar, dispositivos de seguridad y control de acceso, y todo aquello relevante que permita demostrar la confiabilidad de la infraestructura tecnológica. |
| Evidencias solicitadas | Documentación de la infraestructura que acredite el correspondiente nivel de seguridad.<br>Instaladores de la plataforma |

## 12.2. ASPECTOS ESPECÍFICOS A EVALUAR

| **Aspecto** | **Evaluación** |
|---|---|
| Requisitos generales | 12.2.1 La plataforma tecnológica es propia o adaptada a partir de plataformas de código abierto o propietario que cumpla lo establecido en el Reglamento. |
| Módulo criptográfico. | 12.2.2 Los algoritmos criptográficos de generación de números primos y de cifrado empleados, son los autorizados por la Dirección de Criptografía del MININT |
| | 12.2.3 Las aplicaciones y MCAS en que se implementan los algoritmos criptográficos de generación de números primos y de cifrado (confidencialidad) empleados son los autorizados por la Dirección de Criptografía del MININT Artículo 41 |
| | 12.2.4 Los largos de llaves generados son:<br>Para cifrado simétrico mayor o igual a 255 bits |
| | 12.2.5 Funcionalidad y operación:<br>• Generar las llaves en formato PEM y DER. |
| | 12.2.6 En la generación de certificados digitales para la protección de los canales de comunicaciones, sitios web y otras aplicaciones de confidencialidad, se realizará a partir de los criptomateriales entregados por la AC raíz del servicio central Cifrado en formatos PEM, DER o |

| | |
|---|---|
| | PEC. Artículo 21 |
| | 12.2.7 Seguridad.<br>Realizan la activación de la llave privada de la AC bajo el principio de control multipersona, que garantice que ningún funcionario en particular, tenga el dominio exclusivo de las actuaciones críticas y existencia de sistema control de acceso para acceder a la llave privada. Artículo 41 |
| | 12.2.8 Existencia de controles de acceso para acceder a funcionalidades de generación, firma y cifrado. |
| | 12.2.9 Auditoría.<br>Capacidad de generar logs auditables para administración de contingencias y accesos maliciosos. |
| | 12.2.10 Capacidad para recibir solicitudes de emisión de certificados de una AR de un órgano organismo o entidad que tenga firmado contrato con la AC |
| | 12.2.11 Funcionalidad y operación:<br>Capacidad para generar certificados con llaves de 4096 y 2048 bit. |
| | 12.2.12 Capacidad para la emisión de certificados a partir de las llaves criptográficas generadas por el usuario para el caso de firma digital. |
| | 12.2.13 Capacidad para generar llaves para firma digital de forma compartida por tres funcionarios de la entidad. Artículo 24 |
| | 12.2.14 Capacidad de suspensión y revocación de certificados. Artículos 26 al 34 |
| | 12.2.15 Existencia de sistema de control de acceso para acceder a los sistemas de administración y auditoria |
| | 12.2.16 Capacidad de revocar certificado raíz y generar uno nuevo. |

| | |
|---|---|
| | 12.2.17 Disponibilidad de la AC.<br>Disponer de los medios de redundancia de los componentes técnicos más críticos. |
| | 12.2.18 Disponen del equipamiento para mantener los Servicios de copia de respaldo. |
| Módulo de AR (Autoridad de Registro) | 12.2.19 - Funcionalidad y operación:<br>Capacidad de recibir requerimientos de certificados |
| | 12.2.20 Seguridad.<br>Existencia de sistema control de acceso para acceder al registro de certificados. |
| | 12.2.21 Existencia de sistema de control de acceso para acceder a los sistemas de administración y auditoria. |
| | 12.2.22- Ciclo de vida.<br>Capacidad de suspender y revocar certificados. |
| | 12.2.23 Capacidad de revocar certificado raíz y generar uno nuevo. |
| | 12.2.24 Auditoría.<br>Capacidad de generar trazas auditables para administración de contingencia y accesos maliciosos. |
| | 12.2.25 Capacidad para el registro de certificados a partir de las llaves criptográficas generadas por el usuario para el caso de firma digital. |
| | 12.2.26 Capacidad para el envío de solicitud para emisión de certificados digitales con la constancia de la verificación realizada y firmado digitalmente por el jefe de la autoridad y el funcionario que la proceso |
| Módulo de Almacenamiento y Publicación de Certificados | 12.2.27 Almacenamiento de certificados en base de datos X500, y publicación a través de protocolos LDAP y/o OCSP. |

## 13. REQUISITO SEGURIDAD FÍSICA

### 13.1. ESPECIFICACIÓN DEL REQUISITO

| | |
|---|---|
| Nombre | Seguridad física y contra desastres de la infraestructura del PSCC |
| Objetivo | Evaluar los requisitos relacionados con la protección de áreas restringidas, equipos e información y contra desastres |
| Descripción | El PSCC debe asegurar que el acceso físico a los servicios que manejan información sensible esté controlado y los riesgos físicos para los activos estén reducidos a su valor mínimo.<br>Los accesos físicos a las áreas de servicios concernientes a la generación de certificados, entrega de dispositivos seguros a suscriptores, servicios de gestión de revocación y al área de ubicación de los servidores del PSCC, deben ser limitados a individuos debidamente autorizados y deben asegurarse que no habrá accesos no autorizados.<br>Los controles deben ser implementados de manera de evitar las pérdidas, daños o comprometimiento de los activos propios de la actividad del negocio y el comprometimiento o robo de información.<br>La protección física deberá ser alcanzada a través de la creación de perímetros de seguridad (zonas controladas) definidos alrededor de las áreas de servicios de generación de certificados, aseguramiento de dispositivos seguros y gestión de la revocación de los certificados emitidos. Cualquier parte de los servicios compartida con otra organización debe estar fuera del perímetro de seguridad.<br>Los controles de seguridad físicos y contra desastres deben ser implementados para proteger los servicios de los sistemas propios, la infraestructura utilizada para soportar su operación y contra la suspensión no autorizada |

| | |
|---|---|
| | de servicios externos.<br>La política de seguridad física y contra desastres del PSCC en lo concerniente a los sistemas de generación de certificados, aseguramiento de dispositivos seguros a los suscriptores y gestión de revocación de los certificados emitidos debe contemplar al menos de los siguientes aspectos:<br>• Controles físico de acceso (identificación y evaluación de los perímetros de seguridad de los locales, sistema de control de acceso a los mismos manual o técnico que permita obtener evidencias para análisis de seguridad en casos de incidentes, sistemas de vigilancia por personal especializado, de video vigilancia y alarmas).<br>• Protección y recuperación ante desastres naturales, incendios y redes húmedas (existencia de planes contra desastres, incendios y otros, existencia de los medios de protección contra incendios, plan de evacuación de los medios, preparación del personal para enfrentar las contingencias identificadas).<br>• Protección contra robos, forzamiento y entrada (condiciones de seguridad de los locales, puertas y ventanas, sellaje de puertas y control de los sellos, identificación de los autorizados a entrar a los locales incluyendo el personal del servicio de limpieza,<br>• Medidas ante falla de servicios de soporte (electricidad, telecomunicaciones, etc (respaldo de energía eléctrica, inmediato y permanente).<br>• Servicio técnico para los servicios básicos (planes de seguridad informática y contingencias, sistemas de respaldo y mantenimiento de datos y de medios |

| | |
|---|---|
| | informáticos críticos. |
| Referencias en el "Reglamento" , Resolución No 1 del 2000 del Ministro del Interior, sobre seguridad y protección de la información oficial, Resolución No 60 /11 de la CGR y la Resolución No 2 del 2001 del Ministro del interior (Reglamento de la Seguridad y Protección Física) | Reglamento Artículo No 41 |
| Estándares de evaluación | ETSI 102 042 V2.1.2 (2010-4), 7.4.4<br>ISO/IEC 27002, , (17799 en Cuba) Sección 9 |
| Documentación solicitada | Análisis de Riesgos del PSCC.<br>Políticas de Seguridad y de Certificación del PSCC.<br>Declaración de Prácticas de Certificación.<br>Plan de Seguridad y Protección Física<br>Documento descriptivo de la implementación de seguridad física en el PSCC |
| Evidencias solicitadas | Auditoría a las instalaciones del PSCC |

## 13.2. ASPECTOS ESPECÍFICOS A EVALUAR

| **Aspecto** | **Evaluación** |
|---|---|
| Perímetro de seguridad física(ISO 27002, sección 9.1.1) | 13.2.1Se verificará: Evaluación de Seguridad Física según ISO 27002-Sección 9, Ítem 1.1: Sección 9.1.1 Perímetro de seguridad física |

| | |
|---|---|
| Controles de acceso físico (ISO 27002, sección 9.1.2) | 13.2.2 Se verificará: Evaluación de Seguridad Física según ISO 27002-Sección 9, Ítem 1.2: Sección 9.1.2 Controles de acceso físico |
| Seguridad de oficinas, recintos e instalaciones (ISO 27002, sección 9.1.3) | 13.2.3 Se verificará: Evaluación de Seguridad Física según ISO 27002-Sección 9, Ítem 1.3: Sección 9.1.3 Seguridad de oficinas, recintos e instalaciones |
| Protección contra amenazas externas y ambientales (ISO 27002, sección 9.1.4) | 13.2.4 Se verificará: Evaluación de Seguridad Física según ISO 27002-Sección 9, Ítem 1.4: Sección 9.1.4 Protección contra amenazas externas y ambientales |
| Trabajo en áreas seguras(ISO 27002, sección 9.1.5) | 13.2.5 Se verificará: Evaluación de Seguridad Física según ISO 27002-Sección 9, Ítem 1.5: Sección 9.1.5 Trabajo en áreas seguras |
| Áreas de carga, despacho y acceso público (ISO 27002, sección 9.1.6) | 13.2.6 Se verificará: Evaluación de Seguridad Física según ISO 27002-Sección 9, Ítem 1.6: Sección 9.1.6 Áreas de carga, despacho y acceso público |
| Ubicación y protección de los equipos (ISO 27002, sección 9.2.1) | 13.2.7 Se verificará: Evaluación de Seguridad Física según ISO 27002-Sección 9, Ítem 2.1: Sección 9.2 y 9.2.1 Ubicación y protección de los equipos |
| Servicios de suministro (ISO 27002, sección 9.2.2) | 13.2.8 Se verificará: Evaluación de Seguridad Física según ISO 27002-Sección 9, Ítem 2.2. Sección 9.2.2 Elementos de soporte |
| Seguridad del cableado (ISO 27002, sección 9.2.3) | 13.2.9 Se verificará: Evaluación de Seguridad Física según ISO 27002-Sección 9, Ítem 2.3: Sección 9.2.3 Seguridad del cableado |
| Mantenimiento de los equipos (ISO | 13.2.10 Se verificará: Evaluación de Seguridad Física según ISO 27002-Sección 9, Ítem 2.4: |

| | |
|---|---|
| 27002, sección 9.2.4) | Sección 9.2.4 Mantenimiento de los equipos |
| Seguridad de los equipos fuera de las instalaciones(ISO 27002, sección 9.2.5) | 13.2.11 Se verificará: Evaluación de Seguridad Física según ISO 27002-Sección 9, Ítem 2.5: Sección 9.2.5 Seguridad de los equipos fuera de las instalaciones |
| Seguridad en la reutilización o eliminación de los equipos (ISO 27002, sección 9.2.6) | 13.2.12 Se verificará: Evaluación de Seguridad Física según ISO 27002-Sección 9, Ítem 2.6: Sección 9.2.6 Seguridad en la reutilización o eliminación de los equipos |
| Retiro de activos (ISO 27002, sección 9.2.7) | 13.2.13 Se verificará: Evaluación de Seguridad Física según ISO 27002-Sección 9, Ítem 2.7: Sección 9.2.7 Retiro de activos |
| Requerimientos del "Reglamento | 13.2.14 Tienen implementados, sistemas técnicos y/u organizativos de control, bloqueo, aviso y seguimiento de acceso y proximidad a los medios de trabajo especializados; y la aplicación racional de métodos de defensa criptológica frente a intercepciones de sus comunicaciones e intromisiones informáticas o eléctricas en los equipos de prestación del servicio (ver Aislamiento de redes públicas, controles de acceso, sistema de trazas, empleo de borrado seguro, zona controlada, medidas protección emisiones EM, control de los soportes digitales, plan de seguridad informática, protección contra virus y otros). Artículo 41i |
| | 13.2.15 Tener en funcionamiento permanente todas las medidas de seguridad, física y lógicas, así como las trazas auditables de los eventos para el aseguramiento del dispositivo de confidencialidad de su llave criptográfica privada, y otros datos y medios requeridos por los suscriptores. De igual forma tener |

| | |
|---|---|
| | implementados, sistemas técnicos y/u organizativos de control, bloqueo, aviso y seguimiento de acceso y proximidad a los medios de trabajo especializados, y la aplicación racional de métodos de defensa criptológica frente a intercepciones de sus comunicaciones e intromisiones informáticas o eléctricas en los equipos de prestación del servicio. Artículo 41h |

## 14. REQUISITO POLÍTICA DE CERTIFICADOS

### 14.1. ESPECIFICACIÓN DEL REQUISITO

| | |
|---|---|
| Nombre | Política de Certificados |
| Objetivo | Comprobar que La Política de Certificados contiene los aspectos dispuestos en el "Reglamento". |
| Descripción | Este requisito es relevante no sólo para el titular del certificado, sino que, para todas las entidades involucradas, incluyendo quienes reciben un documento firmado electrónicamente.<br>Se verificarán los siguientes aspectos:<br>• La Política de Certificados, debe brindar la confianza necesaria para que los documentos firmados en forma electrónica por el titular de un certificado, que se ciña a la forma de operar recomendada, permitan brindar seguridad y validez a la información que se procesa, almacena y/o transmite a través de las tecnologías de la información y otros medios electrónicos, lo cual facilita la informatización de los trámites y procesos socio-económicos frente a las amenazas de ataques tecnológicos que pueden realizar entes nocivos en el ciberespacio y las comunicaciones.<br>• La Política de Certificados deberá permitir la interoperabilidad con otro PSCC.<br>• Las Prácticas de Certificación deberán |

| | |
|---|---|
| | establecer como el PSCC brinda la confianza establecida en la Política de Certificados. |
| Referencias en el "Reglamento" | Reglamento, Artículos No 39, 48 y 56 |
| Estándares de evaluación | ETSI TS 102 042 |
| Documentación solicitada | Documento conteniendo la Política de Certificados del PSCC |
| Evidencia | Auditoría a la PSCC |

## 14.2. ASPECTOS ESPECÍFICOS A EVALUAR

| **Aspecto** | **Evaluación** |
|---|---|
| Titulares | 14.2.1 La Política de certificación deberá indicar quienes pueden hacer uso de un certificado. |
| Procedimiento de registro | 14.2.2 la política de certificación deberá indicar la verificación del registro del titular, la autenticación, verificación de su identidad en forma fehaciente y forma de política para verificar el nombre del titular. |
| Usos del certificado | 14.2.3 La Política deberá indicar los propósitos para el cual se emiten los certificados y sus limitaciones. |
| Obligaciones CA, AR, titular y receptor | 14.2.4 Descripción de las obligaciones que contraen las entidades involucradas en la emisión y empleo de un certificado. |
| Privacidad y Protección de los datos | 14.2.5 Verificación de las políticas de privacidad y protección de datos.<br>Que estas políticas sean las apropiadas para la firma electrónica, pero que sean publicadas y de conocimiento del subscriptor. |
| Suspensión y revocación del certificado | 14.2.6 Verificar bajo qué circunstancias un certificado es suspendido o revocado, y quién puede solicitarlo. |

## 15. REQUISITO DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN.

## 15.1. ESPECIFICACIÓN DEL REQUISITO

| **Nombre** | **Declaración de Prácticas de certificación** |
|---|---|

| | |
|---|---|
| Objetivo | Verificar que el PSCC disponga de un documento, que señale los modelos operacionales y los procedimientos de operación para la prestación de los servicios de certificación digital, según lo establece el "Reglamento". |
| Descripción | Los elementos principales que debe contener la práctica de certificación, son las delimitaciones de responsabilidad y las obligaciones tanto del PSCC, como del representante o suscriptor<br>Además debe quedar explícito, tanto el ciclo de vida de los certificados, desde su solicitud hasta el término de su vida útil, como los procesos de trabajo del PSCC y la documentación necesaria para su trabajo y las relaciones contractuales. |
| Referencias en el "Reglamento" | Reglamento Artículos No 17, 39, 41, 45, 46, 48, 56, 55, 57, y 61 |
| Estándares de evaluación | RFC 3647<br>ETSI TS 102 042 |
| Documentación solicitada | Documentación de las prácticas de certificación. |
| Evidencias solicitadas | Auditoría al PSCC |

## 15.2. ASPECTOS ESPECÍFICOS A EVALUAR

| **Aspecto** | **Evaluación** |
|---|---|
| Existencia del documento DPC | 15.2.1 Verificar que exista la DPC y que esté debidamente aprobada por quien corresponda de acuerdo al reglamento. Artículos 39e, 41d y 61d |
| Verificar estructura de la DPC | 15.2.2 Verificar que la DPC contiene a lo menos los tópicos indicados en los estándares de evaluación. |
| Acceso a la DPC | 15.2.3 Verificar que la DPC esté debidamente publicada en el sitio WEB del PSCC. Artículo 41d |

| | |
|---|---|
| Las obligaciones y responsabilidades del PSCC: Confidencialidad de la información de los solicitantes /protección de datos. | 15.2.4 Verificar que exista una declaración de las obligaciones y deberes del PSCC. Artículo 41 y 45<br>Existencia de procedimientos de protección de la información de los solicitantes. Artículos 17, 18, 21 y 24. |
| Las obligaciones y responsabilidades del suscriptor. | 15.2.5 Verificar que existan definiciones de los deberes y obligaciones de los suscriptores de certificados digitales. Artículos 56 y 57 |
| Ciclo de vida de los certificados: Emisión / Revocación/Suspensión /Expiración /Renovación. | 15.2.6 Verificar que existan procedimientos que definan el ciclo de vida de los certificados (emitir / revocar / suspender / renovar y las definiciones sobre la expiración de los certificados). Artículos 17-21,26-37.<br>15.2.7 Verificar que los tiempos máximos de vigencia de los mismos y las llaves criptográficas asociadas se corresponden con lo previsto en el Reglamento. Artículo 36 |
| Modelo operacional de la AC y la AR | 15.2.7 Comprobar a través de la documentación presentada que el modelo operacional cumple con los requerimientos en relación con la confiabilidad e interoperabilidad en la forma de operar y prestar los servicios de la Autoridad Certificadora (AC) y Autoridad de Registro (AR) en el PSCC.<br>El modelo operacional deberá responder a lo menos a las siguientes preguntas:<br>• Cuales son los servicios prestados por las AC y AR del PSCC.<br>• Como se interrelacionan los diferentes servicios<br>• En que lugares se operará.<br>• Que tipos de certificados se entregarán<br>• Como se protegerán los activos |

| | |
|---|---|
| | Se verificará que el modelo comprenda los siguientes aspectos:<br>a. Interfaces con de la AC con la AR y viceversa<br>b. Implementación de elementos de seguridad<br>c. Procesos de administración<br>d. Sistema de directorios para los certificados<br>e. Procesos de auditoría y respaldo |
| | Se verificará que existan los roles de la AC y la AR, de acuerdo a lo establecido en los artículos No 46 y 55 del "reglamento". |

## 16. REQUISITO MANUAL DE OPERACIONES DE AUTORIDAD CERTIFICADORA

### 16.1. ESPECIFICACIÓN DEL REQUISITO

| **Nombre** | **Manual de Operaciones de la Autoridad Certificadora del PSCC.** |
|---|---|
| Objetivo | Comprobar a través de la documentación presentada que se incluyen los aspectos operacionales mínimos que dispone el "Reglamento" con relación a los requisitos de confiabilidad e interoperabilidad en la forma de operar y prestar los servicios de la Autoridad Certificadora (AC) de un PSCC. |
| Descripción | El propósito del manual es describir la gestión diaria y las prácticas operacionales de la AC y debería ser la guía que garantice que las directrices primarias de la Política de Certificación están implementadas operacionalmente. Para mejorar la comunicación de esta información al personal de operaciones y a los evaluadores, pueden usarse los procedimientos de trabajo de cada rol o puesto de trabajo, gráficos, diagramas de flujo funcionales, líneas de tiempo, etc.<br>El manual de operaciones de la AC deberá tener a lo menos las siguientes características:<br>• Deberá ser consistente con la Política de Certificación. |

| | |
|---|---|
| | • Deberá incluir la interacción entra la AC y la AR.<br>• Deberá describir los controles de seguridad física, de red, del personal y de procedimientos.<br>• Deberá incluir los procedimientos adoptados para el manejo de llaves públicas y privadas |
| Referencias en el "Reglamento" | Reglamento, Artículos No 17, 21, 24, 27, 31, 32-36, 41, 45, 46, 49-54, 56 y 57 |
| Estándares de evaluación | ETSI TS 102 042<br>RFC 3647 |
| Documentación solicitada | Manual de operaciones PSCC (AC) |
| Evidencias solicitadas | Auditoría en terreno |

## 16.2. ASPECTOS ESPECÍFICOS A EVALUAR

| **Aspecto** | **Evaluación** |
|---|---|
| Nómina y descripción de cargos | 16.2.1 Que se describan las responsabilidades del personal y los procedimientos para ejecutar las funciones de cada rol en específico. Artículos 17, 21, 24, 27, 30, 31, 34, 41, 45, 46, 49-52, 56 y 57 |
| Descripción de las operaciones | 16.2.2 Descripción detallada de los siguientes procedimientos:<br>• Generación de pares de llaves<br>• Publicación de la CRL<br>• Publicación de la información del certificado<br>• Distribución de llaves y certificados<br>• Renovación de certificados<br>• Renovación de certificados luego de una revocación<br>• Medidas de control de acceso<br>• Procedimientos de respaldo y recuperación |
| Actualización de la DPC y la Política de certificación | 16.2.4 Procedimiento de actualización de la Declaración de Prácticas de Certificación y Política de Certificación. Artículo 41d |

| | |
|---|---|
| Servicios de la AC | 16.2.5 Descripción de los servicios de la AC |
| Interacción AC - AR | 16.2.6 El documento cubre la interacción entre la AC y AR |

## 17. REQUISITO MANUAL DE OPERACIONES DE LA AUTORIDAD DE REGISTRO

### 17.1. ESPECIFICACIÓN DEL REQUISITO

| | |
|---|---|
| Nombre | Manual de Operaciones de la Autoridad de Registro (AR) |
| Objetivo | Comprobar a través de la documentación presentada los aspectos operacionales mínimos que dispone el "Reglamento" con relación a los requisitos de confiabilidad e interoperabilidad de la opera el PSCC para realizar las funciones de Autoridad de Registro. |
| Descripción | El manual de operaciones deberá describir como operará el servicio de registro del PSCC y su administración diaria, pueden usarse los procedimientos de trabajo de cada rol o puesto de trabajo, gráficos, diagramas de flujo funcionales, líneas de tiempo, etc.<br>Entre otros aspectos debería tener las siguientes características:<br>• Deberá ser consistente con las políticas de certificación.<br>• Deberá incluir la forma en que se verifica la identidad de las personas.<br>• Deberá incluir procedimientos de entrega y uso de la llave privada por los titulares de los certificados. Se entiende que el PSCC tiene la obligación de generar y entregar en forma segura la llave privada del titular de un certificado emitido por él, asegurándose además de la fiabilidad del dispositivo seguro y los mecanismos que el titular utiliza para firmar.<br>• Deberá incluir la interacción entre las unidades internas que cumplen la función de AC y AR |

| | |
|---|---|
| Referencias en el "Reglamento" | "Reglamento" Artículos No 17, 18,19, 20, 26, 27, 30, 37, 53-55, 56 y 57 |
| Estándares de evaluación | RFC 3647 |
| Documentación solicitada | Manual de Operaciones de la AR |
| Evidencias solicitadas | Auditoría en terreno |

## 17.2. ASPECTOS ESPECÍFICOS A EVALUAR

| **Aspecto** | **Evaluación** |
|---|---|
| Nómina y descripción de cargos | 17.2.1 Que se describan las responsabilidades del personal y los procedimientos para ejecutar las funciones de cada rol en específico. Artículos No 17, 18,19, 20, 26, 27, 30, 37, 53-55, 56 y 57 |
| Procedimiento de registro | 17.2.2 Se verifica el registro del titular. La autenticación, verificación de su identidad. Artículo 17 |
| Entrega segura de los datos de creación de firma | 17.2.3 El PSCC debe tener implementados procedimientos y prácticas que permitan entregar en forma personal y segura los datos de creación de firma al titular del certificado. Artículos 17 y 24 |
| Dispositivo seguro y mecanismos de firma del titular | 17.2.4 PSCC debe tener implementados procedimientos y prácticas que aseguren que una vez entregados los datos de creación de firma sólo el titular tenga control de ellos. Artículos 17 y 24 |
| | 17.2.5 El mecanismo de control de acceso a la llave privada sólo debe ser conocido por el titular al momento de la entrega del dispositivo y en lo posible modificable por el mismo titular, antes de ser utilizado por primera vez. Artículos 17 y 24 |
| | 17.2.6 El PSCC debe entregar al titular herramientas, aplicaciones e instrucciones para que el titular pueda firmar en forma segura. |

| | |
|---|---|
| | Artículos 56 y 57 |
| Capacitación y servicio al titular. | 17.2.7 El PSCC debe tener implementados procedimientos de capacitación que permitan al titular manejar en forma segura e informada el dispositivo de firma, y además mantener un servicio de atención para responder y solucionar dudas de los usuarios. Artículos 56 y 57 |
| Descripción de las operaciones | 17.2.8 Descripción detallada de los siguientes eventos:<br>1. Procedimiento seguro de suspensión y revocación de certificados<br>2. Medidas de control de acceso<br>3. Procedimientos de respaldo y recuperación |
| Interacción entre AR y AC del PSCC | 17.2.9 El documento cubre los procedimientos que involucren la interacción entre la AC y AR |

## 18. REQUISITO AUTORIZACIÓN Y CAPACITACIÓN DEL PERSONAL

### 18.1. ESPECIFICACIÓN DEL REQUISITO

| | |
|---|---|
| Nombre | Autorización y Evaluación del personal que participa en el desarrollo, mantenimiento y operación de las instalaciones del PSCC. |
| Objetivo | Verificar el cumplimiento de los requerimientos y la competencia profesional de los funcionarios que prestan servicios en las instalaciones del PSCC. |
| Descripción | Los funcionarios que laboran en las entidades prestadoras de servicios criptográficos de certificación, serán previamente aprobados de acuerdo a los procedimientos estatales vigentes por los jefes del órgano, organismo o entidad de su jurisdicción, teniendo que haber recibido la preparación especializada y aprobar la evaluación que le realiza la Autoridad Raíz, la cual los acredita con el instrumento de titulación y el CID correspondientes.<br>Los funcionarios que laboran en los PSCC para |

| | |
|---|---|
| | el cumplimiento de sus funciones deben estar integrados en los roles especificados en los Artículos No 46 y 55 del "Reglamento". |
| Referencias en el "Reglamento" | Artículo 39 i, 40, 41a,b, 42, 45b, 46, 47 y 55. |
| Documentación solicitada | Documento del jefe del órgano, organismo o entidad de su jurisdicción aprobando al personal que cumplirá diferentes roles en el PSCC.<br>Documento aprobado en el cual se relacionen los participantes en el equipo de desarrollo de la infraestructura, sus Nos de CI, y que participación especifica tuvo en el proyecto de desarrollo o en el mantenimiento del mismo. |
| Evidencias solicitadas | Certificado expedido por la Autoridad Raíz del SCC acreditándolo para uno o varios roles en las autoridades de certificación o de registro.<br>Documento de nivel personal de acceso y acta de responsabilidad sobre el conocimiento de IOC.<br>Documento de firma del código de Ética de la entidad.<br>Especificación en la DPC de los roles implementados en las AC o AR del PSCC: |

## 18.2. ASPECTOS ESPECÍFICOS A EVALUAR

| **Aspecto** | **Evaluación** |
|---|---|
| Requerimiento de los funcionarios | 18.2.1 Se verificará que cada funcionario que cumpla un rol en el PSCC esté aprobado por el documento del jefe del órgano, organismo o entidad de su jurisdicción. Artículo 42 |
| | 18.2.2 Se verificará que cada funcionario que cumpla un rol en el PSCC posea el certificado de acreditación emitido por la Autoridad de certificación de la AC correspondiente. Artículo 45b |
| | 18.2.3 Se verificará que cada funcionario este |

| | |
|---|---|
| | acreditado como Auditor Criptográfico Internacional (solo para la Autoridad Raíz). Artículo 40 |
| | 18.2.4 Se verificará que los funcionarios que cumplen roles en el PSCC tengan firmado el documento de nivel personal de acceso y acta de responsabilidad sobre el conocimiento de IOC. |
| | 18.2.5 Se verificará la entrega del documento los funcionarios que participaron en el equipo de desarrollo de la infraestructura, sus Nos de CI, y que participación especifica tuvieron en el proyecto de desarrollo o trabajan actualmente en el mantenimiento del mismo. |
| | 18.2.6 Se verificará que se tenga un control de la actuación del personal que posee conocimientos críticos de la infraestructura del PSCC y que se tomen las medidas correspondientes al análisis de riesgos efectuado sobre ese personal. |
| | 18.2.7 Se verificará que los funcionarios que cumplen roles en el PSCC tengan firmado el código de ética de la entidad. Artículo 41b |
| Requerimientos del sistema de preparación | 18.2.8 Se verificará que la entidad tenga organizado el sistema de preparación especializada de los funcionarios que cumplen roles en el PSCC. Artículo 47 |
| | 18.2.9 Se evaluará que en el sistema de preparación de los funcionarios de las autoridades de certificación para poder ser acreditados en la operación de los sistemas estén incluidos los aspectos siguientes:<br>• El Reglamento para el Empleo de los Certificados Digitales en la República de Cuba.<br>• La Declaración de Prácticas de Certificación.<br>• Las Políticas de Seguridad y Certificación<br>• Las normativas vigentes en materia de |

| | |
|---|---|
| | Seguridad de la Información Oficial, Criptografía.<br>• El Código de Ética.<br>• Lo que se establezca por el MININT para la confidencialidad sobre la información que maneja en virtud de su rol.<br>• La operación de los medios computacionales y/o electrónicos, así como de las aplicaciones informáticas para cada puesto de trabajo específico.<br>• Los procedimientos de seguridad criptográficos en general y en particular para cada rol específico en la autoridad.<br>• Los procedimientos de operación y administración de cada rol específico para la segregación de funciones de certificación y los relacionados con el enfrentamiento a las contingencias. Artículo 47 |