

**INFRAESTRUCTURA DE FIRMA DIGITAL DE LA PROVINCIA DE SAN LUIS**

**LEY N° V-0591-2007**

**REQUISITOS PARA EL LICENCIAMIENTO DE CERTIFICADORES PROVINCIALES**

**AGENCIA DE CIENCIA, TECNOLOGIA Y SOCIEDAD SAN LUIS**

**Contenido**

|  |    |
|--|----|
| INTRODUCCIÓN .....   | 4  |
| SECCIÓN 1: DOCUMENTACIÓN QUE DEBE PRESENTAR EL SOLICITANTE PARA OBTENER UNA LICENCIA PROVINCIAL PARA SU POLITICA DE CERTIFICACION..... | 4  |
| 1.- Responsables de la presentación de la solicitud .....  | 4  |
| 2.- Documentos específicos.....  | 5  |
| 3.- Documentación adicional requerida en caso de personas jurídicas privadas.....  | 5  |
| SECCIÓN 2: PAUTAS DE CONTROL A LAS QUE SERA SOMETIDO EL SOLICITANTE PARA OBTENER UNA LICENCIA PROVINCIAL, SEGÚN SEA EL CASO .....      | 5  |
| I) REQUISITOS LEGALES GENERALES.....   | 6  |
| 1.- Obligación de información .....  | 6  |
| 2.- Garantías .....  | 6  |
| 3.- Acuerdos entre partes.....   | 6  |
| 4.- Política de Privacidad .....   | 6  |
| II) POLÍTICA DE CERTIFICACIÓN Y MANUAL DE PROCEDIMIENTOS DE CERTIFICACION .....  | 6  |
| 1.- Contenido de la Política de Certificación.....   | 6  |
| 2.- Compatibilidad de la Política de Certificación y el Manual de Procedimientos .....   | 7  |
| 3.- Administración de la Política de Certificación .....   | 7  |
| III) PLAN DE SEGURIDAD.....  | 7  |
| 1.- Normas que debe cumplir el Plan de Seguridad .....   | 7  |
| 2.- Documentos que componen el Plan de Seguridad .....   | 8  |
| 3.- Conocimiento de la Política de Certificación y demás documentos relacionados.....  | 8  |
| IV) PLAN DE CESE DE ACTIVIDADES .....  | 8  |
| 1.- Publicación y notificación del cese de actividades.....  | 8  |
| 2.- Prestación de servicios en el período previo al cese.....  | 8  |
| 3.- Administración de los certificados por cese de actividades del Certificador Licenciado Provincial....                              | 9  |
| 4.- Destrucción de la clave privada del Certificador Licenciado Provincial .....   | 9  |
| V) PLAN DE CONTINUIDAD DE LAS OPERACIONES .....  | 9  |
| 1.- Normas que debe cumplir el Plan de Continuidad de las Operaciones .....  | 9  |
| 2.- Documentos que componen el Plan de Continuidad de las Operaciones .....  | 9  |
| 3.- Conocimiento del Plan de Continuidad de las Operaciones.....   | 10 |
| VI) PLATAFORMA TECNOLÓGICA.....  | 10 |
| VII) CICLO DE VIDA DE LAS CLAVES CRIPTOGRÁFICAS DEL CERTIFICADOR LICENCIADO PROVINCIAL .....   | 10 |
| 1.- Consideraciones generales respecto de las claves criptográficas .....  | 10 |
| 2.- Tamaño de las claves criptográficas .....  | 10 |
| 3.- Estándares para los dispositivos criptográficos vinculados al ciclo de vida de los certificados .....                              | 11 |
| 4.- Generación del par de claves criptográficas del Certificador Licenciado Provincial .....   | 11 |
| 5.- Almacenamiento, respaldo y recuperación de las claves criptográficas del Certificador Licenciado Provincial .....                  | 11 |
| 6.- Distribución de las claves públicas del Certificador Licenciado Provincial .....   | 11 |
| 7.- Custodia de las claves criptográficas del Certificador Licenciado Provincial.....  | 11 |

|   |    |
|---|----|
| 8.- Utilización de las claves privadas del Certificador Licenciado Provincial .....   | 11 |
| 9.- Destrucción de las claves criptográficas del Certificador Licenciado Provincial .....                                   | 11 |
| 10.- Almacenamiento de las claves del Certificador Licenciado Provincial .....  | 11 |
| 11.- Administración de ciclo de vida de los dispositivos criptográficos del Certificador Licenciado Provincial .....        | 11 |
| VIII) CICLO DE VIDA DE LOS CERTIFICADOS DE SUSCRIPTORES .....   | 12 |
| 1.- Registro y procesamiento de la solicitud del suscriptor .....   | 12 |
| 2.- Renovación del certificado con el mismo par de claves .....   | 12 |
| 3.- Renovación de certificado con un nuevo par de claves .....  | 12 |
| 4.- Emisión del certificado .....   | 12 |
| 5.- Distribución del certificado .....  | 12 |
| 6.- Aceptación del certificado .....  | 12 |
| 7.- Revocación del certificado .....  | 12 |
| 8.- Suspensión del certificado .....  | 12 |
| 9.- Procesamiento de la información sobre el estado de un certificado .....   | 13 |
| IX) ESTRUCTURA Y CONTENIDO DE LOS CERTIFICADOS Y LISTA DE CERTIFICADOS REVOCADOS .....                                      | 13 |
| X) MECANISMOS DE ACCESO A LA DOCUMENTACIÓN PUBLICADA, CERTIFICADOS Y CRLS .....   | 13 |
| 1.- Certificados .....  | 13 |
| 2.- Información de estado de certificados .....   | 13 |
| 3.- Publicación de documentos .....   | 13 |
| 4.- Contactos .....   | 13 |
| 5.- Actualización .....   | 13 |
| 6.- Seguridad .....   | 13 |
| SECCIÓN 3: REGISTRO DE EVENTOS .....  | 13 |
| SECCIÓN 4: CONTROLES FÍSICOS .....  | 16 |
| Ubicación de las instalaciones .....  | 17 |
| Seguridad física de una Autoridad Certificante .....  | 17 |
| a. Seguridad física de las operaciones de baja complejidad de una autoridad certificante .....                              | 17 |
| b. Seguridad física de las operaciones de alta complejidad de una autoridad certificante .....                              | 18 |
| c. Seguridad física para el resguardo de los elementos de activación de la clave privada de la autoridad certificante ..... | 18 |
| d. Seguridad física de una autoridad .....  | 19 |
| Consideraciones para Certificadores que operen más de UNA autoridad certificante .....                                      | 19 |
| Consideraciones para Certificadores que compartan UNA misma infraestructura tecnológica .....                               | 19 |

## INTRODUCCIÓN

Conforme lo dispuesto en el Decreto Nº 0428-MP-2008 modificado por Decreto Nº 6011-MCyT-2018, reglamentario de la Ley Nº V-0591-2007, y la Resolución Nº 17-ASLCTyS-2017, se establecen a continuación los requisitos que debe cumplir un solicitante para obtener una licencia en el marco de la Infraestructura de Firma Digital de la Provincia de San Luis. El presente documento tiene la siguiente estructura:

- Sección 1: Documentación que debe entregar el solicitante para obtener una licencia provincial para su Política de Certificación.
- Sección 2: Pautas de control a las que será sometido el solicitante para obtener la licencia provincial.
- Sección 3: Registro de eventos.
- Sección 4: Controles Físicos.

Todas las referencias al Certificador Licenciado Provincial, en este documento, se entenderán también válidas para el solicitante en proceso de obtener una licencia, en la medida en que sean aplicables.

Ante cualquier duda en la interpretación del presente documento, podrá dirigirse al Ente Licenciante Provincial: INSTITUTO FIRMA DIGITAL DE SAN LUIS, dependiente de la AGENCIA DE CIENCIA, TECNOLOGÍA Y SOCIEDAD SAN LUIS, en Edificio de Descentralización Administrativa "Terrazas del Portezuelo" - Torre III Piso 3º - Autopista de las Serranías Puntanas Km. 783, Ciudad de San Luis, Provincia de San Luis, o remitir su consulta a la siguiente dirección de correo electrónico: [entelicenciante@sanluis.gov.ar](mailto:entelicenciante@sanluis.gov.ar)

## SECCIÓN 1: DOCUMENTACIÓN QUE DEBE PRESENTAR EL SOLICITANTE PARA OBTENER UNA LICENCIA PROVINCIAL PARA SU POLÍTICA DE CERTIFICACION.

Para tramitar su licencia provincial, el solicitante debe presentar ante el INSTITUTO FIRMA DIGITAL DE SAN LUIS, dependiente de la AGENCIA DE CIENCIA, TECNOLOGÍA Y SOCIEDAD SAN LUIS, su Política de Certificación y los documentos complementarios señalados en la presente norma en formato digital, firmados digitalmente. A excepción de aquellos supuestos que, por las características de la documentación, sólo puedan tramitarse en soporte papel.

Si se trata de una Persona Jurídica Privada, además deberá presentar la documentación correspondiente a esta condición, lo cual se describe en detalle más adelante.

### 1.- Responsables de la presentación de la solicitud

El trámite de licenciamiento se inicia con la presentación de la solicitud de licencia provincial firmada conforme lo dispuesto a continuación:

- En caso de personas jurídicas privadas, debe encontrarse firmada por su representante legal o apoderado.
- Si se trata de algún organismo de la Administración Pública Provincial, de los previstos en el artículo 4º de la Ley Nº VIII-0256-2004, se requerirá que la presentación se encuentre firmada por la máxima autoridad de la jurisdicción de que se trate, acompañada del acto administrativo correspondiente.
- En caso de tratarse de un organismo nacional, provincial y/o municipal, diferentes a los previstos en el párrafo precedente, el acto administrativo deberá estar firmado por la máxima autoridad del organismo o jurisdicción acompañada de una copia autenticada del acto administrativo correspondiente.

- Si se tratara de un Registro Público de Contrato, deberá presentar documentación que acredite su condición, acompañando nota de solicitud firmada por el máximo responsable del Registro, acompañada de una copia autenticada del acto administrativo correspondiente.

## 2.- Documentos específicos

Los Certificadores que soliciten una licencia provincial deben presentar conjuntamente con la Nota de solicitud de licenciamiento la siguiente documentación:

- a) Política de Certificación, con los datos del solicitante.
- b) Acuerdo tipo con suscriptores.
- c) Términos y condiciones tipo con Terceros Usuarios ("*relying parties*").
- d) Política de Privacidad.
- e) Contratos con los proveedores de la infraestructura tecnológica, de corresponder.
- f) Manual de Procedimientos.
- g) Plan de Cese de Actividades.
- h) Plan de Seguridad (incluye política y procedimientos de seguridad).
- i) Plan de Continuidad de las Operaciones.
- j) Descripción de la plataforma tecnológica.
- k) Descripción de los servicios que pretende brindar.

## 3.- Documentación adicional requerida en caso de personas jurídicas privadas

Adicionalmente, en el caso de personas jurídicas privadas, deberán presentar:

- a) Garantía de Caución (en sus términos y condiciones; su vigencia será constatada en el momento de otorgamiento de la licencia al Certificador Provincial).
- b) Documentación de la constitución de la entidad (Estatuto o Contrato Social) en copia certificada por escribano, y de corresponder, legalizada.
- c) Última acta de Asamblea, con designación de autoridades, y última acta de Directorio y/o distribución de cargos en copias certificadas por escribano, y de corresponder, legalizadas.
- d) Constancia de inscripción en el Registro de Comercio, o en el registro público de la jurisdicción pertinente, en copia certificada, y de corresponder, legalizada.
- e) Constancia de inscripción ante la Administración Federal de Ingresos Públicos.
- f) Últimos estados contables auditados, certificados por Contador Público, y de corresponder, legalizados.
- g) Comprobante de pago de iniciación del trámite.
- h) Copia autenticada, y de corresponder, legalizada, del poder que acredita el carácter de representante legal o apoderado de la persona autorizada a iniciar el trámite.

## SECCIÓN 2: PAUTAS DE CONTROL A LAS QUE SERA SOMETIDO EL SOLICITANTE PARA OBTENER UNA LICENCIA PROVINCIAL, SEGÚN SEA EL CASO

Toda la documentación presentada será sometida a controles legales y técnicos y se efectuarán revisiones en las instalaciones del Certificador Provincial, según sea el caso, como pasos previos al otorgamiento de la licencia, o el eventual rechazo de la solicitud.

Por lo tanto, el Certificador Provincial deberá permitir el acceso del personal designado por el Ente Licenciante Provincial, a sus instalaciones, a la información y a su infraestructura tecnológica a fin de dar cumplimiento a las funciones de auditoría, de acuerdo con lo establecido en la Ley Nº V-0591-2007, en su Decreto reglamentario Nº 0428-MP-2008

modificado por Decreto N° 6011-MCyT-2018, las Resoluciones N° 17-ASLCTyS-2017 y N° 34-ASLCTyS-2017.

Los controles y auditorías a realizar, en el caso de los solicitantes de licencia provincial cubrirán los siguientes aspectos:

- I. Requisitos legales generales.
- II. Política de Certificación y Manual de Procedimientos de Certificación.
- III. Plan de Seguridad.
- IV. Plan de Cese de Actividades.
- V. Plan de Continuidad de las Operaciones.
- VI. Plataforma Tecnológica.
- VII. Ciclo de vida de las claves criptográficas del certificador licenciado provincial.
- VIII. Ciclo de vida de los certificados de suscriptores.
- IX. Estructura y contenido de los certificados y CRLs.
- X. Mecanismos de acceso a la documentación publicada, certificados y CRLs.

Los controles mencionados tienen por objetivo verificar el cumplimiento de los requisitos exigidos para obtener la condición de Certificador Licenciado Provincial.

## **I) REQUISITOS LEGALES GENERALES**

Los siguientes puntos corresponden al Solicitante de una licencia provincial.

### **1.- Obligación de información**

El Certificador Provincial debe informar a los potenciales suscriptores, terceros usuarios y otros posibles interesados, las condiciones de utilización del certificado digital, su tramitación y revocación, así como las condiciones de la Política de Certificación. Dicho mecanismo de información debe constar en la documentación presentada.

### **2.- Garantías**

Las entidades privadas que soliciten licencia de Certificador Provincial deberán constituir un seguro de caución a fin de garantizar el cumplimiento de sus obligaciones.

### **3.- Acuerdos entre partes**

El Certificador Provincial debe tener claramente definidos los textos de los modelos de compromisos con Suscriptores y Terceros Usuarios (“relying parties”) según los Anexos IV y V de la presente Resolución, que establecen los contenidos mínimos para los siguientes documentos:

- a) Acuerdos con suscriptores.
- b) Términos y condiciones con Terceros Usuarios.

### **4.- Política de Privacidad**

El Certificador Provincial debe presentar su Política de Privacidad a los efectos de evaluarla en relación con la correspondiente Política de Certificación. Para ello debe tener en cuenta lo expresado en el Anexo VI de la presente Resolución.

## **II) POLÍTICA DE CERTIFICACIÓN Y MANUAL DE PROCEDIMIENTOS DE CERTIFICACION**

### **1.- Contenido de la Política de Certificación**

La Política de Certificación deberá incluir los contenidos establecidos en el Anexo II de la presente Resolución.

## **2.- Compatibilidad de la Política de Certificación y el Manual de Procedimientos**

El Manual de Procedimientos deberá adecuarse a la Política de Certificación y no deberá contener cláusulas contradictorias o incompatibles con ella.

## **3.- Administración de la Política de Certificación**

El Certificador Provincial deberá mantener procedimientos de administración de la Política de Certificación de modo de asegurar que todo cambio dispuesto por la Autoridad de Aplicación Provincial del régimen de firma digital, se encuentre debidamente autorizado, aprobado y difundido.

### **III) PLAN DE SEGURIDAD**

#### **1.- Normas que debe cumplir el Plan de Seguridad**

El Plan de Seguridad deberá cumplir con los lineamientos de la Norma IRAM ISO/IEC 27002, no siendo exigible la certificación, y sus correspondientes actualizaciones o reemplazos vigentes al momento de la presentación de la solicitud de la licencia provincial, en lo referente a todos aquellos aspectos relacionados directa o indirectamente con las actividades de certificación.

En caso de que alguno de los lineamientos no resultara aplicable a la estructura de la organización, se deberán justificar por escrito y someter a aprobación las razones para no cumplirlo.

Adicionalmente a lo que indica la Norma IRAM ISO/IEC 27002, el Certificador Provincial deberá mantener controles que permitan cumplir con los siguientes puntos:

- **Seguridad física y ambiental**

Se deberán mantener controles que permitan asegurar que las áreas en las cuales se desarrolle cada etapa del ciclo de vida de las claves criptográficas sean tratadas como de alta seguridad. El acceso físico a dichas áreas debe limitarse sólo a personal autorizado.

La Sección 4 del presente Anexo indica los controles físicos vinculados al proceso de certificación que se deberán implementar en cada instalación.

La infraestructura tecnológica necesaria para la generación de certificados y CRL's del Certificador Provincial debe encontrarse alojada en servidores físicos o virtuales, independientes del resto de los servidores utilizados y afectados en forma exclusiva a las tareas de certificación, condiciones que serán controladas durante el proceso de licenciamiento provincial.

- **Intercambios de información y software**

Las comunicaciones entre las autoridades de registro y la autoridad certificante referidas a la aprobación o revocación de certificados deberán ser llevadas a cabo mediante un mecanismo que garantice el no repudio.

- **Revisiones post-licenciamiento**

El Ente Licenciante Provincial en sus inspecciones post-licenciamiento podrá solicitar la información relevada por las auditorías encaradas por el Certificador Provincial que controlen el cumplimiento de su Política de Certificación y demás documentación aplicable.

- **Registro de eventos**

Se deberá dejar evidencia de todas las actividades realizadas sobre los registros de eventos actuales y archivados. Además, se deberán implementar procedimientos que determinen:

- a) Frecuencia de procesamiento y archivo.

- b) Período de retención.
- c) Mecanismos de protección contra accesos no autorizados.
- d) Mecanismos de resguardo y consulta.
- e) Mecanismos para asegurar la integridad de los registros de eventos actuales y archivados.
- f) Ubicación de los resguardos.
- g) La utilización exclusiva de un par de claves en caso de que los registros de eventos sean firmados.

La Sección 3 del presente Anexo indica los eventos del proceso de certificación que deberán ser registrados por el Certificador Licenciado Provincial.

## **2.- Documentos que componen el Plan de Seguridad**

- Una Política de Seguridad de la información, documentada y aprobada por la máxima autoridad del Certificador Licenciado Provincial, en la que se indicará cuáles son las acciones que se realizarán para cumplir con sus objetivos.
- Un Manual que documente detalladamente los procedimientos para ejecutar las acciones necesarias para cumplir con los objetivos de la política de seguridad.

## **3.- Conocimiento de la Política de Certificación y demás documentos relacionados**

El personal que participa en el proceso de certificación y en los servicios relacionados deberá conocer la Política de Certificación y los procedimientos con ella relacionados y será responsable de su cumplimiento. El Certificador Licenciado Provincial deberá establecer mecanismos de capacitación y de documentación del compromiso de cumplimiento por parte del personal afectado.

# **IV) PLAN DE CESE DE ACTIVIDADES**

## **1.- Publicación y notificación del cese de actividades**

Se deberá disponer de procedimientos para la publicación del cese de actividades del Certificador Licenciado Provincial durante un día en el Boletín Oficial y Judicial de la Provincia de San Luis y en el Boletín Oficial de la Nación sesenta días antes del cese o suspensión, en su sitio web publicado en Internet, en un todo de acuerdo a lo dispuesto en el artículo 34º del Decreto Nº 0428-MP-2008 y sus modificatorias. Ello, además de su notificación al Ente Licenciantes Provincial, a los suscriptores de certificados y a otras entidades vinculadas.

Asimismo, cuando se hayan emitido certificados a entes, entidades o personas ajenas al Sector Público Provincial, el Certificador Licenciado publicará en un diario de difusión provincial durante un (1) día, el cese de sus actividades.

Si el alcance de la Política de Certificación permitiera la emisión de certificados a personas de otras jurisdicciones, el Certificador Licenciado publicará el cese de sus actividades en un diario de difusión nacional durante un (1) día.

Además el Certificador Licenciado podrá disponer de medios adicionales de comunicación del cese de sus actividades para notificar a los suscriptores de certificados que son ajenos al Sector Público Provincial. Si los certificados son transferidos a otro Certificador Licenciado, toda la documentación pertinente también deberá ser transferida a aquel.

## **2.- Prestación de servicios en el período previo al cese**

Se deberá disponer de procedimientos para el mantenimiento de servicios en el período anterior al de cese (revocación de certificados, actualización de repositorios y emisión de CRLs) y la transferencia de la custodia de archivos y de la documentación de soporte de los certificados emitidos.

### **3.- Administración de los certificados por cese de actividades del Certificador Licenciado Provincial**

Se deberá disponer de procedimientos para la revocación de los certificados emitidos al momento del cese de sus actividades.

### **4.- Destrucción de la clave privada del Certificador Licenciado Provincial**

Se deberán implementar procedimientos seguros para la inmediata destrucción de las claves privadas y de sus copias de seguridad de todas sus Autoridades Certificantes, cuando el Certificador Licenciado Provincial cesa sus actividades, una vez que hayan sido revocados todos los certificados emitidos.

## **V) PLAN DE CONTINUIDAD DE LAS OPERACIONES**

### **1.- Normas que debe cumplir el Plan de Continuidad de las Operaciones**

El Plan de Continuidad de las Operaciones deberá cumplir con los lineamientos de la Norma IRAM ISO/IEC 27002, no siendo exigible la certificación, sobre la administración de la continuidad de los negocios y sus correspondientes actualizaciones o reemplazos vigentes al momento de la presentación de la solicitud de licencia provincial.

En caso de que alguno de los lineamientos no resultara aplicable a la estructura de la organización, se deben justificar por escrito y someter a aprobación las razones para no cumplirlo.

Adicionalmente a lo que indica la Norma IRAM ISO/IEC 27002, el Certificador Licenciado Provincial debe mantener controles que permitan cumplir con los siguientes puntos:

- **Administración de la continuidad de las operaciones**

Se deberán mantener controles que aseguren:

- a) La continuidad de las operaciones en caso de compromiso de la clave privada del Certificador Licenciado Provincial, y
- b) La reducción al mínimo posible de las eventuales interrupciones en el servicio, sobre la base de la matriz de evaluación de riesgo, que se deberá acompañar.

Se considerarán procesos críticos indispensables para la actividad de certificación:

- a) La recepción de solicitudes de revocación.
- b) La revocación de certificados digitales.
- c) La emisión de la lista de certificados revocados.
- d) La publicación de la lista de certificados revocados.
- e) La respuesta o publicación acerca del estado de un certificado, en caso de que así correspondiese.

- **Prueba del plan**

Deberá existir un procedimiento de prueba del plan de continuidad de las operaciones. El mismo deberá llevarse a cabo con una periodicidad de UN (1) año y preverse la realización de una prueba durante el período de auditoría inicial previa al licenciamiento provincial.

### **2.- Documentos que componen el Plan de Continuidad de las Operaciones**

El Plan de Continuidad de las Operaciones, documentado y aprobado por la máxima autoridad de la entidad, contendrá las acciones que se realizarán para el cumplimiento de sus objetivos y los procedimientos para su ejecución.

Se deberán documentar todas las pruebas y ejecuciones reales efectuadas.

### **3.- Conocimiento del Plan de Continuidad de las Operaciones**

El personal del Certificador Licenciado Provincial que participa en el proceso de gestión del ciclo de vida de los certificados, deberá conocer el Plan de Continuidad de las Operaciones y los procedimientos con él relacionados y será responsable de su cumplimiento, de acuerdo a los roles asignados. Se deberán establecer mecanismos de capacitación y de documentación del compromiso de cumplimiento por parte del personal afectado.

### **VI) PLATAFORMA TECNOLÓGICA**

Se deberá ajustar a los estándares tecnológicos vigentes que cubran las necesidades requeridas por el proceso de gestión del ciclo de vida de los certificados.

Se deberán implementar procedimientos que garanticen la confiabilidad de la plataforma tecnológica.

### **VII) CICLO DE VIDA DE LAS CLAVES CRIPTOGRÁFICAS DEL CERTIFICADOR LICENCIADO PROVINCIAL**

#### **1.- Consideraciones generales respecto de las claves criptográficas**

Deberán cumplirse los siguientes requerimientos mínimos:

- El par de claves deberá ser generado únicamente por el Certificador Licenciado Provincial.
- El medio de generación y almacenamiento de la clave privada utilizada en la generación de la firma deberá asegurar que:
  - La clave privada sea única.
  - No pueda ser deducida y se encuentre protegida contra réplicas fraudulentas realizadas con las tecnologías disponibles a la fecha.
  - Pueda ser eficazmente protegida por el Certificador Provincial contra su utilización ilegal.
  - El transporte entre el dispositivo de generación y el de almacenamiento se realice en forma segura.

#### **2.- Tamaño de las claves criptográficas**

Deberán respetarse las siguientes longitudes mínimas de claves:

- Las claves criptográficas que el Certificador Licenciado Provincial utilice para la firma de certificados, Lista de Certificados Revocados, y cualquier otro tipo de servicio no podrán ser inferiores a CUATRO MIL NOVENTA Y SEIS (4096) bits si utilizan los algoritmos RSA o DSA y TRESCIENTOS OCHENTA Y CUATRO (384) bits si utiliza el algoritmo ECDSA.
- Las claves criptográficas que los certificados utilicen en servicios relacionados con la firma digital, no podrán ser inferiores a DOS MIL CUARENTA Y OCHO (2048) bits si utilizan los algoritmos RSA o DSA y DOSCIENTOS VEINTICUATRO (224) bits, si utilizan el algoritmo ECDSA. En el caso particular de autoridades de sello de tiempo, las claves criptográficas no podrán ser inferiores a CUATRO MIL NOVENTA Y SEIS (4096) bits si utilizan los algoritmos RSA o DSA y TRESCIENTOS OCHENTA Y CUATRO (384) bits si utiliza el algoritmo ECDSA.
- Las claves criptográficas que utilicen las autoridades de registro para realizar actividades tales como aprobar solicitudes, renovaciones, revocaciones y demás servicios de certificación, deberán mantenerse permanentemente bajo su control, no podrán ser inferiores a DOS MIL CUARENTA Y OCHO (2048) bits si utilizan los

algoritmos RSA o DSA; y DOSCIENTOS VEINTICUATRO (224) bits si utiliza el algoritmo ECDSA.

### **3.- Estándares para los dispositivos criptográficos vinculados al ciclo de vida de los certificados**

Deberán respetarse las siguientes exigencias mínimas:

- a) Las claves criptográficas del Certificador Licenciado Provincial deberán ser generadas y almacenadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 3.
- b) Las claves criptográficas que utilicen los responsables de las autoridades de registro para realizar actividades tales como aprobar solicitudes, renovaciones, revocaciones y demás servicios de certificación deberán ser generadas y almacenadas en dispositivos que cumplan con certificación FIPS 140 (Versión 2) nivel 2 o superior.

### **4.- Generación del par de claves criptográficas del Certificador Licenciado Provincial**

El Certificador Licenciado Provincial deberá mantener exclusivo control sobre el proceso de generación de sus claves criptográficas.

### **5.- Almacenamiento, respaldo y recuperación de las claves criptográficas del Certificador Licenciado Provincial**

El Certificador Licenciado Provincial deberá mantener el control exclusivo sobre las claves criptográficas durante su almacenamiento y sobre sus copias de respaldo.

El Certificador Licenciado Provincial deberá disponer de procedimientos para realizar la recuperación de sus claves a partir de sus copias de respaldo.

### **6.- Distribución de las claves públicas del Certificador Licenciado Provincial**

El Certificador Licenciado Provincial deberá disponer de procedimientos seguros para distribuir sus claves públicas.

### **7.- Custodia de las claves criptográficas del Certificador Licenciado Provincial**

En caso de que el Certificador Licenciado Provincial guarde elementos críticos vinculados a sus claves criptográficas en dependencias de un tercero, deberá garantizar los niveles de resguardo y la imposibilidad de que el tercero en cuestión pueda acceder a ellas y producir su activación o alteración.

### **8.- Utilización de las claves privadas del Certificador Licenciado Provincial**

El Certificador Licenciado Provincial deberá disponer de procedimientos y controles que aseguren que las claves serán utilizadas exclusivamente para las funciones previstas y en las ubicaciones previamente establecidas.

El control de la utilización de las claves criptográficas del Certificador Licenciado Provincial deberá estar dividido de forma tal que para activar su uso sea necesaria la presencia de M personas de un total de N posibles, con M mayor o igual a DOS (2).

### **9.- Destrucción de las claves criptográficas del Certificador Licenciado Provincial**

El Certificador Licenciado Provincial deberá mantener procedimientos y controles que aseguren que sus claves se destruyen por completo al finalizar su ciclo de vida.

### **10.- Almacenamiento de las claves del Certificador Licenciado Provincial**

El Certificador Licenciado Provincial deberá mantener procedimientos y controles que aseguren la confidencialidad de las claves archivadas.

### **11.- Administración de ciclo de vida de los dispositivos criptográficos del Certificador Licenciado Provincial**

El Certificador Licenciado Provincial deberá mantener procedimientos y controles que aseguren que:

- a) Solo personal expresamente autorizado pueda acceder al dispositivo criptográfico del Certificador Licenciado Provincial,
- b) El dispositivo criptográfico funciona adecuadamente.

## **VIII) CICLO DE VIDA DE LOS CERTIFICADOS DE SUSCRIPTORES**

### **1.- Registro y procesamiento de la solicitud del suscriptor**

El Certificador Licenciado Provincial deberá implementar procedimientos de solicitud aplicables a los certificados a emitir, que aseguren que los suscriptores sean debidamente identificados.

El Certificador Licenciado Provincial deberá implementar procedimientos para asegurar que los suscriptores generen sus claves criptográficas de manera segura y bajo exclusivo control de éstos últimos.

### **2.- Renovación del certificado con el mismo par de claves**

El Certificador Licenciado Provincial podrá implementar un procedimiento para la renovación del certificado de un suscriptor, que deberá contemplar la validación de la solicitud correspondiente.

### **3.- Renovación de certificado con un nuevo par de claves**

El Certificador Licenciado Provincial podrá implementar un procedimiento por el cual un suscriptor pueda solicitar la reemisión de un certificado con un nuevo par de claves, que deberá contemplar la validación de la solicitud correspondiente.

### **4.- Emisión del certificado**

El Certificador Licenciado Provincial deberá mantener controles que aseguren que los certificados nuevos, renovados y reemitidos sean generados de acuerdo con sus políticas, prácticas y procedimientos.

### **5.- Distribución del certificado**

El Certificador Licenciado Provincial deberá implementar controles que aseguren que los certificados generados sean puestos a disposición de los suscriptores y usuarios de manera segura.

### **6.- Aceptación del certificado**

El Certificador Licenciado Provincial deberá implementar procedimientos para la aceptación, por parte de los suscriptores, de los certificados emitidos.

### **7.- Revocación del certificado**

El Certificador Licenciado Provincial deberá implementar procedimientos y controles que aseguren que:

- a) Los certificados sean revocados conforme a solicitudes autorizadas y válidas de revocación.
- b) El usuario cuente con medios para solicitar la revocación de sus certificados.
- c) Las vías de comunicación disponibles para recibir la solicitud de revocación operen correctamente.
- d) Se respeten los plazos de revocación establecidos en la Política de Certificación.

### **8.- Suspensión del certificado**

El Certificador Licenciado Provincial debe informar que el estado de suspensión no es admitido conforme lo previsto en la Ley Nacional N° 25.506, de aplicación conforme el artículo 1º de la Ley Provincial N° V-0591-2007.

**9.- Procesamiento de la información sobre el estado de un certificado**

El Certificador Licenciado Provincial deberá mantener procedimientos que aseguren la puesta a disposición de los suscriptores y usuarios, de información oportuna, completa y adecuada, referida al estado de los certificados (incluida la emisión y publicación de la Listas de Certificados Revocados y otros mecanismos referidos a dicho estado).

**IX) ESTRUCTURA Y CONTENIDO DE LOS CERTIFICADOS Y LISTA DE CERTIFICADOS REVOCADOS**

El formato, codificación, contenido e interpretación de los certificados digitales y listas de certificados revocados (CRL) deberán ajustarse a los contenidos definidos en el Anexo III-Perfiles de los Certificados y de las Listas de Certificados Revocados.

**X) MECANISMOS DE ACCESO A LA DOCUMENTACIÓN PUBLICADA, CERTIFICADOS Y CRLS**

La información a publicar por el Certificador Licenciado Provincial en su sitio web contendrá:

**1.- Certificados**

El Certificador Licenciado Provincial está obligado a publicar los certificados digitales de las autoridades certificadoras correspondientes a la Política de Certificación que hayan sido licenciadas y el estado de cada uno de ellos, así como el resto de los certificados que compongan su cadena de certificación.

**2.- Información de estado de certificados**

El Certificador Licenciado Provincial está obligado a publicar el estado de los certificados por él emitidos, debiendo garantizar el acceso permanente, eficiente y gratuito de los titulares al repositorio de certificados revocados, según lo dispuesto por el inciso 11) del artículo 34 del Decreto N° 0428-MP-2008. Adicionalmente, podrá hacerlo por algún otro mecanismo que brinde dicha información.

**3.- Publicación de documentos**

El Certificador Licenciado Provincial está obligado a la publicación de las versiones vigentes y anteriores de la Política de Certificación y el Manual de Procedimientos de Certificación (en sus partes públicas) y el Acuerdo Tipo con Suscriptores y los Términos y Condiciones con Terceros Usuarios.

**4.- Contactos**

El Certificador Licenciado Provincial está obligado a la publicación de la información sobre la forma de comunicarse tanto con él como con el Ente Licenciente Provincial. Debe proveer como mínimo: denominación del servicio de atención de consultas, dirección de correo electrónico y número de teléfono.

**5.- Actualización**

El Certificador Licenciado Provincial es responsable de actualizar estas publicaciones cada vez que sean modificadas.

**6.- Seguridad**

El Certificador Licenciado Provincial debe implementar mecanismos de seguridad para controlar el acceso a la información publicada y para prevenir accesos o modificaciones no autorizados.

**SECCIÓN 3: REGISTRO DE EVENTOS**

El Certificador Licenciado Provincial, en los puntos aplicables, deberá mantener la confidencialidad e integridad de los registros de eventos actuales y archivados. Deberá indicar

los procedimientos utilizados para su tratamiento registrando, de corresponder, la información y eventos que se indican a continuación para cada uno de ellos.

En el siguiente cuadro de descripción de eventos se entiende por “entidad” a toda persona humana, jurídica, dispositivo o aplicación que intervenga en el proceso de licenciamiento provincial (tales como, autoridad certificante, autoridad de registro, suscriptor, tercero usuario, servidor de aplicación, etcétera).

|                                     | <b>INFORMACIÓN REGISTRADA</b>  |
|-------------------------------------|--|
| <b>Contenido mínimo a Registrar</b> | a) Fecha y hora del registro.<br>b) Número de serie o secuencia del registro.<br>c) Tipo de registro.<br>d) Fuente del registro (Ej.: terminal, puerto, etcétera).<br>e) Identificación de la entidad que efectuó el registro. |

|   | <b>EVENTOS A REGISTRAR</b>  |
|---|---|
| <b>Administración del ciclo de vida de las claves criptográficas del Certificador</b> | a) Generación y almacenamiento de las claves criptográficas.<br>b) Resguardo de las claves criptográficas.<br>c) Recuperación de las claves criptográficas.<br>d) Utilización de las claves criptográficas.<br>e) Archivo de las claves criptográficas.<br>f) Retiro de servicio de datos relacionados con las claves criptográficas.<br>g) Destrucción de las claves criptográficas.<br>h) Identificación de la entidad que autoriza una operación de administración de las claves criptográficas.<br>i) Identificación de la entidad que administra los datos relativos a las claves criptográficas (tal como los componentes de claves, o claves almacenadas en dispositivos criptográficos u otros medios).<br>j) Compromiso de la clave privada. |
|   | <b>EVENTOS A REGISTRAR</b>  |

|   |   |
|---|---|
| <b>Administración del ciclo de vida de los certificados</b> | <ul style="list-style-type: none"> <li>a) Recepción de solicitudes de certificados (inicial, de renovación con el mismo o un nuevo par de claves).</li> <li>b) Transferencia de claves públicas para la emisión del certificado.</li> <li>c) Cambios en los datos de la solicitud del certificado.</li> <li>d) Generación de certificados.</li> <li>e) Distribución de la clave pública del Certificador.</li> <li>f) Solicitudes de revocación de certificados.</li> <li>g) Generación y emisión de listas de certificados revocados.</li> <li>h) Acciones tomadas en relación con la expiración de un certificado.</li> </ul> |
|---|---|

| EVENTOS A REGISTRAR   |   |
|---|---|
| <b>Administración del ciclo de vida de los dispositivos Criptográficos del Certificador</b> | <ul style="list-style-type: none"> <li>a) Recepción del dispositivo.</li> <li>b) Ingreso o retiro del dispositivo del lugar de almacenamiento.</li> <li>c) Instalación del dispositivo</li> <li>d) Uso del dispositivo.</li> <li>e) Desinstalación del dispositivo.</li> <li>f) Envío de dispositivos para servicio técnico o reparación.</li> <li>g) Retiro, baja o borrado de información del dispositivo.</li> </ul> |

| EVENTOS A REGISTRAR   |   |
|---|---|
| <b>Información relacionada con la solicitud de certificados</b> | <ul style="list-style-type: none"> <li>a) Tipos de documentos de identificación presentados por el solicitante.</li> <li>b) Otra información de identificación, en caso de ser aplicable.</li> <li>c) Ubicación del archivo de las copias de las solicitudes de certificados y de los documentos de identificación.</li> <li>d) Identificación de la entidad que recibe y acepta la solicitud.</li> <li>e) Método utilizado para validar los documentos de identificación.</li> <li>f) Identificación de la autoridad de registro, de ser aplicable.</li> </ul> |
| EVENTOS A REGISTRAR   |   |

|                             |   |
|-----------------------------|---|
| <b>Eventos de seguridad</b> | <ul style="list-style-type: none"> <li>a) Lectura o modificación de archivos o registros críticos de seguridad, incluyendo el registro diario de eventos.</li> <li>b) Borrado de datos críticos.</li> <li>c) Cambios en los perfiles de seguridad.</li> <li>d) Registro de intentos exitosos y fallidos de accesos al sistema, los datos y los recursos.</li> <li>e) Caídas del sistema, fallas en el hardware y software, u otras anomalías.</li> <li>f) Acciones desarrolladas por los operadores y administradores del sistema y responsables de seguridad.</li> <li>g) Cambios en la relación entre el Certificador o sus autoridades certificadoras con: <ul style="list-style-type: none"> <li>▪ Sus autoridades de registro.</li> <li>▪ El personal relacionado con el proceso de certificación.</li> </ul> </li> <li>h) Modificaciones en los procesos o procedimientos de cifrado y/o autenticación.</li> <li>i) Accesos al sistema de la autoridad certificante o a cualquiera de sus componentes.</li> </ul> |
|-----------------------------|---|

| <b>OBSERVACIONES GENERALES</b>                       |   |
|--|---|
| <b>Información crítica Sincronización de eventos</b> | <ul style="list-style-type: none"> <li>a) Los registros de eventos no deben reflejar los valores en texto plano de claves privadas o contraseñas.</li> <li>b) Los relojes de las computadoras deben estar sincronizados con un desvío menor a UN (1) segundo para permitir un correcto registro de eventos, deben utilizar Hora Universal Coordinada (UTC) y estar configurados según el huso horario oficial de la CIUDAD AUTÓNOMA DE BUENOS AIRES, que actualmente es UTC-3.</li> <li>c) Toda información de horarios deberá estar expresada en formato: yyyy/mm/dd hh:mm:ss huso-horario.</li> </ul> |

#### **SECCIÓN 4: CONTROLES FÍSICOS**

En esta sección se definen los niveles de seguridad física mínimos exigidos para las áreas funcionales de las Autoridades Certificantes de un Certificador Licenciado Provincial. Lo dispuesto contempla tanto a las autoridades certificadoras como a sus autoridades de registro, cuando sea aplicable.

Los requerimientos de seguridad descriptos a continuación representan la exigencia mínima a cumplir y consideran niveles de acceso físico numerados de UNO (1) a SEIS (6), con características de seguridad crecientes. Toda barrera y control de seguridad que no cumpla con todos y cada uno de los requisitos establecidos en esta sección, no podrá ser considerado como el paso a un área de mayor nivel de seguridad. Se aclara que los niveles CINCO (5) y SEIS (6) se destinan únicamente a la guarda de elementos críticos vinculados a las claves privadas.

Sin perjuicio de los controles que se detallan a continuación, siempre debe estar en condiciones de funcionamiento comprobado la opción de salida de emergencia, con los controles que aseguren su apropiada utilización y eviten cualquier exposición.

### **Ubicación de las instalaciones**

Los Certificadores Provinciales que soliciten una licencia deben detallar los aspectos de construcción de las instalaciones de sus áreas funcionales, referidos a los controles de seguridad física.

Las autoridades de registro pueden funcionar en una ubicación física diferente a las autoridades certificantes o bien prestar un servicio en una instalación móvil, siempre que no se vulneren los controles de seguridad que garanticen un proceso confiable de aprobación de solicitudes de emisión, renovación o revocación de certificados.

### **Seguridad física de una Autoridad Certificante**

Las autoridades certificantes deberán implementar un sistema de seguridad física que cuente con CUATRO (4) niveles de acceso físico, por lo menos, para llegar desde las áreas de libre circulación al ambiente donde reside su equipamiento informático afectado a la firma de certificados y CRLs. Además, deberá disponer de DOS (2) niveles adicionales para la protección de los elementos críticos vinculados a la activación de la clave privada de cada autoridad certificante y otros elementos críticos. Estos DOS (2) niveles pueden consistir en cajas de seguridad, gabinetes reforzados o compartimentos, siendo el nivel SEIS (6) de uso exclusivo de cada Certificador Provincial. En el caso que varias Autoridades Certificantes, pertenecientes a distintos Certificadores, utilicen la misma infraestructura tecnológica, se debe contar con N+1 cajas de seguridad, gabinetes o compartimentos, siendo N la cantidad de Certificadores Licenciados, a los que se agrega un contenedor adicional para el resguardo de otros elementos de operación del dispositivo criptográfico HSM, que deban ser compartidos.

Las claves privadas de las autoridades certificantes podrán residir en particiones físicas o lógicas siempre que se garantice la exclusividad en el acceso establecida en el Capítulo III de la Ley Nº 25.506, conforme lo dispuesto en el artículo 1º de la Ley Nº V-0591-2007.

La ubicación del área funcional de las autoridades certificantes no deberá tener identificación visible.

Los requerimientos de seguridad física de la autoridad certificante abarcan:

- a) Operaciones de baja complejidad.
- b) Operaciones de alta complejidad.
- c) Resguardo de elementos críticos de activación de la clave privada.
- d) Autoridades de Registro Delegadas.

#### **a. Seguridad física de las operaciones de baja complejidad de una autoridad certificante**

Se definen como de baja complejidad a todas las operaciones de la autoridad certificante, con excepción de las vinculadas con el proceso de firma propiamente dicho y de las que requieran el acceso físico a los equipos informáticos asignados a la firma de certificados y CRLs. Estas operaciones de baja complejidad deberán realizarse a partir del nivel 2 de seguridad física.

El nivel 1 se considera a partir de la primera barrera de control de las dependencias donde se encuentre alojada la autoridad certificante. Para acceder a este nivel, todo individuo deberá ser identificado y su ingreso debidamente registrado.

El nivel 2 debe ser interno al nivel 1. Se deberá exigir el registro de ingreso, por medio electrónico, y el uso de una identificación visible a las personas que permanezcan en él. A partir de este nivel, los equipos de grabación, fotográficos, de video u otros dispositivos

electrónicos, así como computadoras portátiles, tendrán su entrada registrada y sólo podrán ser utilizados mediante autorización formal y bajo supervisión.

El nivel 2, debe ser de uso exclusivo de los Certificadores que utilicen una misma plataforma tecnológica compartida y únicamente utilizado para tareas específicas de las autoridades certificadoras. Por lo tanto, no podrá compartirse con otras áreas funcionales de la organización del Certificador o proveedor de la plataforma tecnológica. Para el ingreso de personas que no estén relacionadas con las operaciones de las autoridades certificadoras, se requiere autorización expresa de los responsables de los Certificadores involucrados y en su permanencia, deberán estar acompañadas por UNA (1) persona designada formalmente para ello. En este nivel deberán ser registradas tanto las entradas como las salidas de cada persona. A partir de este nivel se podrá ubicar el equipamiento destinado a la gestión de la infraestructura de firma digital de los Certificadores, tales como la administración del firewall, de los servidores web, bases de datos, etcétera.

Será permitido el acceso lógico al equipamiento descrito en el párrafo anterior desde la intranet o remoto, vía VPN (L2TP, PPTP, IPSEC o los protocolos que los replacen en el futuro) siempre y cuando se garantice la autenticación de doble vía mediante certificados digitales, dispositivos criptográficos o del tipo OTP (One Time Password), OATH (Initiative for Open Authentication), OCRA (Challenge/Response Algorithms Specification), TOTP (Time-based One-time Password Algorithm) o similar.

Los teléfonos celulares y equipos de comunicación necesarios para las operaciones de las autoridades certificadoras, si fuera el caso, sólo se pueden ingresar a este nivel previa autorización expresa y registración.

El nivel 3 debe ser interno al nivel 2, de uso exclusivo de los Certificadores. La identificación deberá realizarse por DOS (2) métodos distintos, tanto para la entrada como para la salida, tales como tarjeta de identificación electrónica, contraseña de ingreso o identificación biométrica.

#### **b. Seguridad física de las operaciones de alta complejidad de una autoridad certificante**

Se definen como de alta complejidad aquellas operaciones de una autoridad certificante vinculadas con el proceso de firma y las que requieren acceso físico a los equipos informáticos asignados a la firma de certificados y CRLs. Las mismas se deberán realizar en un nivel 4 de seguridad física.

El nivel 4 debe ser interno al nivel 3 y repetir los mismos controles de acceso físico que los descritos para ese nivel. Para realizar cualquier actividad en este nivel se requiere la presencia de al menos DOS (2) operadores autorizados por todos los Certificadores involucrados. Las personas ajenas al área deberán ingresar acompañadas de por lo menos DOS (2) personas autorizadas formalmente para ello.

Las operaciones críticas de emisión o revocación de certificados deberán ser realizadas en ambientes cerrados, físicamente protegidos, no compartidos con otras áreas de la organización, y exclusivos para funciones vinculadas a los procesos de certificación digital. Se podrán compartir infraestructuras físicas entre autoridades certificadoras del mismo o de distintos Certificadores siempre que se implementen adecuados controles que impidan los accesos no autorizados o que pudieran afectar la seguridad de los procesos de certificación.

#### **c. Seguridad física para el resguardo de los elementos de activación de la clave privada de la autoridad certificante**

La seguridad física para la protección de los elementos críticos de activación de la clave privada de firma de la autoridad certificante corresponde a los niveles 5 y 6.

El nivel 5 debe ser interno al nivel 4 descrito anteriormente y estar constituido por una caja de seguridad, gabinete reforzado con cerradura o compartimento de acceso exclusivo, con una disposición interna de manera tal que permita la protección individual de distintos componentes críticos. Este nivel funciona como un perímetro de seguridad física que permite administrar el acceso a los elementos protegidos contenidos en dicha caja, gabinete o compartimento.

El nivel 6 debe ser interno al nivel 5 y contar con una disposición interna según se describe precedentemente. La función de la disposición interna de la caja o gabinete es almacenar los elementos de activación de la clave privada de la autoridad certificante.

Cada Autoridad Certificante debe contar con su propio nivel 6 de protección.

#### **d. Seguridad física de una autoridad de registro delegada**

Las autoridades de registro deben implementar un sistema de seguridad física que garantice su correcto funcionamiento y la protección adecuada de la información y documentación presentada por el solicitante o titular. En este sentido, deberán extremarse las medidas que impidan el acceso no autorizado al puesto de trabajo de la autoridad de registro y a la documentación que se le confía para su resguardo, así como a los datos de los solicitantes. Deberán contar asimismo con adecuados procedimientos y mecanismos de recuperación frente a eventos imprevistos.

Las autoridades de registro podrán realizar su actividad en puestos móviles cuando se presenten las condiciones que ameriten tal servicio, siempre que lo haya aprobado el INSTITUTO FIRMA DIGITAL DE SAN LUIS, dependiente de la AGENCIA DE CIENCIA, TECNOLOGÍA Y SOCIEDAD SAN LUIS, y no se vulneren los controles de seguridad que garanticen un proceso confiable de aprobación de solicitudes de emisión, renovación o revocación de certificados.

#### **Consideraciones para Certificadores que operen más de UNA autoridad certificante**

En el caso que el Certificador Provincial opere más de UNA (1) autoridad certificante, todos los controles físicos definidos en esta sección pueden ser compartidos por las distintas autoridades certificadoras, con excepción del nivel 6, donde cada autoridad certificante deberá tener sus propios compartimentos con llave.

#### **Consideraciones para Certificadores que compartan UNA misma infraestructura tecnológica**

En el caso que DOS (2) o más Certificadores operen sus autoridades certificadoras en UNA (1) misma infraestructura tecnológica, podrán compartir todos los controles físicos definidos en esta sección excepto el nivel 6 de protección de los elementos de activación. En este caso cada autoridad certificante deberá tener acceso de manera segura a su nivel 6.