Jefe de Gabinete de Ministros

FOLIO 826

ANEXO II

Infraestructura de Firma Digital – REPÚBLICA ARGENTINA

Ley N° 25.506

Requisitos para el licenciamiento de certificadores

Subsecretaría de Tecnologías de Gestión
Secretaría de Gabinete y Coordinación Administrativa
Jefatura de Gabinete de Ministros

Jefe de Gabinete de Ministros

FOLIO 827

ÍNDICE

Jefe de Gabinete de Ministros

FOLIO 828

INTRODUCCIÓN

De acuerdo con el inciso h) del artículo 30 de la Ley N° 25.506, 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 REPÚBLICA ARGENTINA. El presente documento tiene la siguiente estructura:

- Sección 1: Documentación que debe entregar el solicitante para obtener una licencia.
- Sección 2: Pautas de control a las que será sometido el solicitante para obtener la licencia, según sea el caso.
- Sección 3: Registro de eventos.
- Sección 4: Controles Físicos.

Todas las referencias al certificador, 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 por escrito al ente licenciante, sito en Av. Roque Sáenz Peña 511 - C1035AAA - CIUDAD AUTÓNOMA DE BUENOS AIRES - REPÚBLICA ARGENTINA, o remitir su consulta a la siguiente dirección de correo electrónico: licenciamiento@jefatura.gob.ar.

SECCIÓN 1: DOCUMENTACIÓN QUE DEBE ENTREGAR EL SOLICITANTE PARA OBTENER UNA LICENCIA

Para tramitar su licencia, el solicitante debe presentar ante el ente licenciante los documentos específicos relacionados con su Política Única de Certificación y, si se trata de una Persona Jurídica Privada, la documentación correspondiente a esta condición, lo cual se describe en detalle más adelante. Cada uno de los documentos deberán estar debidamente firmados y presentados como documentos electrónicos firmados digitalmente, de acuerdo a las pautas que fije el ente licenciante.

1.- Responsables de la presentación de la solicitud

En caso de personas jurídicas privadas, el trámite de licenciamiento, según sea el caso, se inicia con la presentación de la nota de solicitud, firmada por su representante legal o apoderado, en las condiciones establecidas en el artículo 45 de la presente decisión administrativa, junto con el Formulario de Adhesión del Anexo I.

Si se tratara de un organismo integrante de la Administración Pública Nacional (tal como se define en el artículo 8° Ley N° 24.156 y sus modificatorias) se requerirá la presentación de una copia autenticada del acto administrativo correspondiente firmado por la máxima autoridad de la jurisdicción de que se trate, autorizando el inicio del trámite de licenciamiento, e incluyendo la información prevista en el artículo 45 de la presente decisión administrativa, junto con el Formulario de Adhesión del Anexo I.

En caso de tratarse de un organismo provincial, municipal y de otros poderes del Estado, el acto administrativo deberá estar firmado por la máxima autoridad del organismo o jurisdicción, debiendo incluirse la información prevista en el artículo 45 de la presente decisión administrativa, junto con el Formulario de Adhesión del Anexo I.

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, en las condiciones establecidas en el artículo 45 de la presente decisión administrativa, junto con el Formulario de Adhesión del Anexo I.

2.- Documentos específicos

Los certificadores que soliciten una licencia deben presentar:

a) Formulario de Adhesión del Anexo I, debidamente conformado.

b) Política Única de Certificación, con los datos del solicitante.

c) Acuerdo tipo con suscriptores.

d) Términos y condiciones tipo con Terceros Usuarios ("*relying parties*").

e) Política de Privacidad.

f) Contratos con los proveedores de la infraestructura tecnológica, de corresponder.

g) Manual de Procedimientos.

h) Plan de Cese de Actividades.

i) Plan de Seguridad (incluye política y procedimientos de seguridad).

j) Plan de Continuidad de las Operaciones.

k) Descripción de la plataforma tecnológica.

l) Descripción de los servicios que brinda.

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

Se deben presentar:

a) Garantía de Caución (en sus términos y condiciones; su vigencia será constatada en el momento de otorgamiento de la licencia al certificador).

b) Documentación de la constitución de la entidad (Estatuto o Contrato Social) en copia certificada por escribano.

c) Última acta de Asamblea, con designación de autoridades, y última acta de Directorio y/o distribución de cargos en copias certificadas por escribano.

d) Constancia de inscripción en la INSPECCIÓN GENERAL DE JUSTICIA, organismo dependiente del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, o en el registro público de la jurisdicción que corresponda, en copia certificada.

e) Constancia de inscripción ante la ADMINISTRACIÓN FEDERAL DE INGRESOS PÚBLICOS, entidad autárquica actuante en el ámbito del MINISTERIO DE ECONOMÍA Y FINANZAS PÚBLICAS.

f) Últimos estados contables auditados, certificados por Contador Público.

g) Comprobante de pago de iniciación del trámite.

h) Copia autenticada 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 ESTARÁ SOMETIDO EL SOLICITANTE PARA OBTENER UNA LICENCIA, SEGÚN SEA EL CASO

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

Por lo tanto, el certificador deberá permitir el acceso del personal designado por el ente licenciante y por las entidades de auditoría precalificadas, 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 25.506 y en el Decreto Nº 2628 del 19 de diciembre de 2002 y sus modificatorios.

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

I. Requisitos legales generales.

II. Política Única 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.

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.

I) REQUISITOS LEGALES GENERALES

Los siguientes puntos corresponden al solicitante de una licencia.

1.- Obligación de información

El certificador 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 Única de Certificación. Dicho mecanismo de información debe constar en la documentación presentada.

2.- Garantías

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

3.- Acuerdos entre partes

El certificador debe tener claramente definidos los textos de los modelos de compromisos con suscriptores y Terceros Usuarios ("relying parties") según los Anexos V y VI de la presente decisión administrativa, 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 debe presentar su Política de Privacidad a los efectos de evaluarla en relación con la Política Única de Certificación. Para ello debe tener en cuenta lo expresado en el Anexo VIII de la presente decisión administrativa.

II) POLÍTICA DE CERTIFICACIÓN Y MANUAL DE PROCEDIMIENTOS

1.- Contenido de la Política Única de Certificación

La Política Única de Certificación deberá incluir los contenidos establecidos en el Anexo III de la presente decisión administrativa, excepto en los casos específicamente indicados en el Formulario de Adhesión del Anexo I.

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

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

3.- Administración de la Política Única de Certificación

El certificador deberá mantener procedimientos de administración de la Política Única de Certificación de modo de asegurar que todo cambio dispuesto por el ente licenciante o de los datos contenidos en el Formulario de Adhesión del Anexo I de la presente medida, 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 licencia, 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 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 CRLs del certificador debe encontrarse alojada en servidores preferentemente 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.

FOLIO 837

- **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 y/o las entidades de auditoría en sus auditorías anuales o en las inspecciones extraordinarias que realice dicho ente, de acuerdo a lo establecido en los artículos 58 a 60 de la presente decisión administrativa, podrán solicitar la información relevada en las auditorías previas vinculadas al cumplimiento de la Política Única 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.

FOLIO 838

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.

2.- Documentos que componen el Plan de Seguridad

- Una política de seguridad de la información, documentada y aprobada por la máxima autoridad del certificador, 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 Única de Certificación y demás documentos relacionados

El personal que participa en el proceso de certificación y en los servicios relacionados deberá conocer la Política Única de Certificación y los procedimientos con ella relacionados y será responsable de su cumplimiento. El certificador 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 en el BOLETÍN OFICIAL DE LA REPÚBLICA ARGENTINA, en su

sitio web publicado en Internet y en al menos otro medio de difusión nacional y su notificación al ente licenciante, a los suscriptores de certificados y a otras entidades vinculadas, con la antelación correspondiente según lo establecido en el artículo 32 de la presente decisión administrativa.

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

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

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 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.

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 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, 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.

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 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

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.
- 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 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 utilice para la firma de certificados, CRLs, 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 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 "overall" FIPS 140 (Versión 2) nivel 2 o superior.

4.-Generación del par de claves criptográficas del certificador

El certificador deberá mantener exclusivo control sobre el proceso de generación de sus claves criptográficas.

5.- Almacenamiento, respaldo y recuperación de las claves criptográficas del certificador

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

El certificador 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

El certificador deberá disponer de procedimientos seguros para distribuir sus claves públicas.

7.- Custodia de las claves criptográficas del certificador

En caso de que el certificador 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

El certificador 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 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

El certificador 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

El certificador 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

El certificador deberá mantener procedimientos y controles que aseguren que:

a) Solo personal expresamente autorizado pueda acceder al dispositivo criptográfico del certificador,

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 deberá implementar procedimientos de solicitud aplicables a los certificados a emitir, que aseguren que los suscriptores sean debidamente identificados y que las solicitudes respondan a un modelo adecuado y se encuentren autorizadas y completas.

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

FOLIO 847

5.- Distribución del certificado

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

7.- Revocación del certificado

El certificador 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 Única de Certificación.

8.- Suspensión del certificado

El certificador debe informar que el estado de suspensión no es admitido en el marco de la Ley N° 25.506.

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

El certificador 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 Listas de Certificados Revocados y otros mecanismos referidos a dicho estado).

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 IV- Perfiles de los Certificados y de las Listas de Certificados Revocados.

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

La información a publicar por el certificador en su sitio web contendrá:

1.- Certificados

El certificador está obligado a publicar los certificados digitales de las autoridades certificantes correspondientes a la Política Única de Certificación y a otras políticas que hayan sido aprobadas, y el estado de cada uno de ellos.

2.- Información de estado de certificados

El certificador 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 g) del artículo 34 del Decreto N° 2628/02 y sus modificatorios. Adicionalmente, podrá hacerlo por algún otro mecanismo que brinde dicha información.

3.- Publicación de documentos

El certificador está obligado a la publicación de las versiones vigentes y anteriores de la Política Única 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 está obligado a la publicación de la información sobre la forma de comunicarse tanto con él como con el ente licenciante. Debe proveer como mínimo: denominación del servicio de atención de consultas, dirección de correo electrónico y número de teléfono.

5.- Actualización

El certificador es responsable de actualizar estas publicaciones cada vez que sean modificadas.

6.- Seguridad

El certificador 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, 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 física, jurídica, dispositivo o aplicación que intervenga en el proceso de licenciamiento (tales como, autoridad certificante, autoridad de registro, suscriptor, Tercero Usuario, servidor de aplicación, etcétera).

	Información Registrada
Contenido mínimo a registrar	a) Fecha y hora del registro. b) Número de serie o secuencia del registro. c) Tipo de registro. d) Fuente del registro (Ej.: terminal, puerto, etcétera). e) Identificación de la entidad que efectuó el registro.

	Eventos a Registrar
Administración del ciclo de vida de las claves criptográficas del certificador	a) Generación y almacenamiento de las claves criptográficas. b) Resguardo de las claves criptográficas. c) Recuperación de las claves criptográficas. d) Utilización de las claves criptográficas. e) Archivo de las claves criptográficas. f) Retiro de servicio de datos relacionados con las claves criptográficas. g) Destrucción de las claves criptográficas. h) Identificación de la entidad que autoriza una operación de administración de las claves criptográficas. 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). j) Compromiso de la clave privada.

Administración del ciclo de vida de los certificados	a) Recepción de solicitudes de certificados (inicial, de renovación con el mismo o un nuevo par de claves). b) Transferencia de claves públicas para la emisión del certificado. c) Cambios en los datos de la solicitud del certificado. d) Generación de certificados. e) Distribución de la clave pública del certificador. f) Solicitudes de revocación de certificados. g) Generación y emisión de listas de certificados revocados. h) Acciones tomadas en relación con la expiración de un certificado.
Administración del ciclo de vida de los dispositivos criptográficos	a) Recepción del dispositivo. b) Ingreso o retiro del dispositivo del lugar de almacenamiento. c) Instalación del dispositivo d) Uso del dispositivo. e) Desinstalación del dispositivo. f) Envío de dispositivos para servicio técnico o reparación. g) Retiro, baja o borrado de información del dispositivo.

Información relacionada con la solicitud de certificados	a) Tipos de documentos de identificación presentados por el solicitante. b) Otra información de identificación, en caso de ser aplicable. c) Ubicación del archivo de las copias de las solicitudes de certificados y de los documentos de identificación. d) Identificación de la entidad que recibe y acepta la solicitud. e) Método utilizado para validar los documentos de identificación. f) Identificación de la autoridad de registro, de ser aplicable.

Eventos de seguridad	a) Lectura o modificación de archivos o registros críticos de seguridad, incluyendo el registro diario de eventos. b) Borrado de datos críticos. c) Cambios en los perfiles de seguridad. d) Registro de intentos exitosos y fallidos de accesos al sistema, los datos y los recursos. e) Caídas del sistema, fallas en el hardware y software, u otras anomalías. f) Acciones desarrolladas por los operadores y administradores del sistema y responsables de seguridad. g) Cambios en la relación entre el certificador o sus autoridades certificantes con: • Sus autoridades de registro. • El personal relacionado con el proceso de certificación. h) Modificaciones en los procesos o procedimientos de cifrado y/o autenticación. i) Accesos al sistema de la autoridad certificante o a cualquiera de sus componentes.

	Observaciones generales
Información crítica Sincronización de eventos	a) Los registros de eventos no deben reflejar los valores en texto plano de claves privadas o contraseñas. 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. c) Toda información de horarios deberá estar expresada en formato: yyyy/mm/dd hh:mm:ss huso-horario.

FOLIO 856

SECCIÓN 4: CONTROLES FÍSICOS

En esta sección se definen los niveles de seguridad física mínimos exigidos para las áreas funcionales del certificador que solicite una licencia. Lo dispuesto contempla tanto a las autoridades certificantes 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 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 cada certificador 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, de uso exclusivo de cada certificador. Debe tenerse en cuenta que en el caso que varias autoridades certificantes pertenecientes a distintos certificadores licenciados utilicen la misma infraestructura tecnológica, se deberá 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" (Hardware Security Module), 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 la Ley Nº 25.506 (artículo 21, inciso c).

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

FOLIO 858

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.

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 en un nivel 3 de seguridad física, como mínimo.

Se aclara que todo lo referido a las autoridades de registro se trata en el apartado correspondiente.

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 3 debe ser interno al nivel 2, de uso exclusivo de los certificadores que utilicen una misma plataforma tecnológica compartida y únicamente utilizado para tareas específicas de las autoridades certificantes. 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 certificantes, 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. 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.

En este nivel se ubicará 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 descripto en el párrafo anterior desde la intranet o remoto, vía VPN (L2TP, PPTP, IPSEC o los protocolos que los remplacen 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 certificantes, si fuera el caso, sólo se pueden ingresar a este nivel previa autorización expresa y registración.

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 descriptos 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 certificantes 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 reguardo 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 descripto 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 certificador deberá contar con su propio ambiente de nivel 5 y cada autoridad certificante, con su nivel 6 de protección.

Seguridad física de una autoridad de registro

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 ente licenciante 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 licenciados que operen más de UNA (1) autoridad certificante

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

Consideraciones para certificadores licenciados que compartan UNA (1) misma infraestructura tecnológica

En el caso que DOS (2) o más certificadores licenciados operen sus autoridades certificantes en UNA (1) misma infraestructura tecnológica, podrán compartir todos los controles físicos definidos en esta sección excepto el nivel 5 de protección de los elementos de activación. En este caso cada certificador deberá tener su propia caja de seguridad, gabinete reforzado o compartimento de acceso exclusivo y cada autoridad certificante deberá contar con su propio nivel 6, interno al anterior.