

ANEXO II

**INFRAESTRUCTURA DE FIRMA DIGITAL REPÚBLICA ARGENTINA
LEY N° 25.506.**

**REQUISITOS PARA EL LICENCIAMIENTO DE CERTIFICADORES PARA
OPERAR CON FIRMA DIGITAL**

**SECRETARÍA DE INNOVACIÓN, CIENCIA Y TECNOLOGÍA
JEFATURA DE GABINETE DE MINISTROS**

INTRODUCCIÓN

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.
- 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.

Toda consulta acerca de la interpretación del presente documento debe ser presentada por los interesados a través del trámite "Presentación ante el Ente Licenciante" de la plataforma de Trámites a Distancia (TAD), o, en caso de corresponder, a través del sistema de Gestión Documental Electrónica (GDE).

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

Para tramitar su licencia, el solicitante debe presentar ante la SUBSECRETARÍA DE INNOVACIÓN dependiente de la SECRETARÍA DE INNOVACIÓN, CIENCIA Y TECNOLOGÍA de la JEFATURA DE GABINETE DE MINISTROS o quien en el futuro la reemplace, los documentos específicos indicados en esta sección. Cada uno de los documentos deberán ser presentados como documentos electrónicos firmados con firma digital.

1. Responsables de la presentación de la solicitud

En relación a los responsables de la presentación de la solicitud resulta de aplicación lo establecido en el artículo 37 del Anexo I de la presente resolución.

2. Documentos específicos

Los solicitantes de una licencia deberán presentar los siguientes documentos:

- a) Política Única de Certificación.
- b) Acuerdo con Suscriptores.
- c) Términos y condiciones con Terceros Usuarios.
- 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.
- i) Plan de Contingencia.
- j) Descripción de la plataforma tecnológica.
- k) Descripción de los servicios que brinda.

3. Documentación adicional requerida en caso de personas jurídicas del Sector Privado

En el caso de personas jurídicas del Sector Privado, además de lo detallado en el punto anterior, deberá presentar lo siguiente:

- a) Seguro de Caución (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 público.
- c) Última acta de Asamblea, con designación de autoridades, y última acta de Directorio y/o distribución de cargos en copias certificadas por escribano público.
- d) Constancia de inscripción en la INSPECCIÓN GENERAL DE JUSTICIA o en el registro público de la jurisdicción que corresponda, en copia certificada.
- e) Constancia de inscripción ante la Agencia de Regulación y Control Aduanero (ARCA).
- f) Último estado contable auditado, certificado por Contador Público.
- g) Comprobante de pago de iniciación del trámite.

Asimismo se aclara, que tanto para el caso de persona jurídica del sector público o privado se solicitará la constancia de apoderamiento, que acredite el carácter de representante legal o apoderado de la persona autorizada a iniciar el trámite, con poder suficiente a dichos efectos.

La solicitud debe ser presentada únicamente a través de la plataforma de Trámites a Distancia (TAD), o del sistema de Gestión Documental Electrónica – (GDE) en caso de corresponder.

SECCIÓN 2: PAUTAS DE CONTROL A LAS QUE ESTARÁ SOMETIDO EL SOLICITANTE PARA OBTENER UNA LICENCIA

Toda la documentación presentada será sometida a controles legales y técnicos y se efectuarán inspecciones y auditorías en las instalaciones del solicitante de la licencia, como pasos previos al otorgamiento o al eventual rechazo de la solicitud.

Por lo tanto, el solicitante deberá permitir el acceso del personal designado por el Ente Licenciante y por la SINDICATURA GENERAL DE LA NACIÓN 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 N° 25.506, su modificatoria N° 27.446 y en el Decreto N° 182/2019 y sus modificatorias.

Las inspecciones y auditorías cubrirán los siguientes aspectos:

- a) Requisitos legales generales.
- b) Política Única de Certificación y Manual de Procedimientos.
- c) Plan de Seguridad.
- d) Plan de Cese de Actividades.
- e) Plan de Contingencia.
- f) Plataforma Tecnológica.
- g) Ciclo de vida de las claves criptográficas del Certificador.
- h) Ciclo de vida de los certificados de suscriptores.
- i) Estructura y contenido de los certificados y CRLs.
- j) Mecanismos de acceso a la documentación publicada, certificados y CRLs.

I) REQUISITOS LEGALES GENERALES

Los siguientes puntos corresponden al solicitante de una licencia.

1. Obligación de información

El solicitante debe informar a los potenciales suscriptores, Terceros Usuarios y otros posibles interesados, en los términos del artículo 21 inciso a) de la Ley N° 25.506, las condiciones de utilización del certificado digital, su tramitación, renovación y revocación, así como las condiciones de la Política Única de Certificación. Dicha información debe constar en la documentación presentada.

2. Garantías

Los Entes Públicos no estatales y las entidades privadas que soliciten licencia de Certificador deberán constituir un seguro de caución a fin de garantizar el cumplimiento de sus obligaciones, en los términos del artículo 35 del Anexo al Decreto N° 182/2019.

3. Acuerdos entre partes

El solicitante debe tener claramente definidos los Acuerdos con Suscriptores y Terceros Usuarios según los Anexos V y VI de la presente resolución.

4. Política de Privacidad

El solicitante de la licencia debe presentar su Política de Privacidad de acuerdo al Anexo VIII de la presente resolución.

II) POLÍTICA ÚNICA 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 resolución.

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 se encuentre debidamente autorizado, aprobado y difundido.

III) PLAN DE SEGURIDAD

1. Lineamientos del Plan de Seguridad

Para la confección del Plan de Seguridad deberán considerarse 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 particular, 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 de la Autoridad Certificante 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 situada en territorio de la REPÚBLICA ARGENTINA y 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.

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 según lo establecido en los artículos 21 y 22 del Anexo 1 de la presente resolución.

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 administración 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 sus copias de seguridad cuando el Certificador Licenciado cese sus actividades.

V) PLAN DE CONTINGENCIA

1. Lineamientos del Plan de Contingencia

Para la confección del Plan de Contingencia deberán considerarse 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.

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.
- b) La reducción al mínimo posible de las eventuales interrupciones en el servicio.

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 de Contingencia**

Deberá existir un procedimiento de prueba del Plan de Contingencia. El mismo deberá llevarse a cabo con una periodicidad de UN (1) año, previéndose la realización de una prueba durante el período de auditoría inicial previa al licenciamiento.

2. Contenido del Plan de Contingencia

El Plan de Contingencia, 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 Contingencia

El personal del Certificador que participa en el proceso de gestión del ciclo de vida de los certificados, deberá conocer el Plan de Contingencia y los procedimientos con él relacionados y será responsable de su cumplimiento, de acuerdo a los roles asignados.

VI) 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:
 - a) La clave privada sea única.
 - b) No pueda ser deducida y se encuentre protegida contra réplicas fraudulentas realizadas con las tecnologías disponibles a la fecha.
 - c) Pueda ser eficazmente protegida por el Certificador contra su utilización indebida.

- d) 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:

- a) 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.
- b) Las claves criptográficas que el Certificador 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.
- c) 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 o superior FIPS 140 (Versión 3) nivel 3 o superior.
- b) Las claves criptográficas que utilicen los Oficiales de Registro 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 o FIPS 140 (Versión 3) nivel 2 o superior.

- c) Los dispositivos criptográficos de los suscriptores certificados, incluyendo a los Oficiales de Registro, deberán encontrarse clasificados como **ACTIVOS (ACTIVE)** por el NIST.
- d) Las claves criptográficas que utilicen las Autoridades de Sello de Competencia deberán ser generadas y almacenadas en un dispositivo criptográfico que cumpla con certificación FIPS 140 (Versión 2) nivel 3 o superior o FIPS 140 (Versión 3) nivel 3 o superior.
- e) Las Claves Criptográficas que hayan sido generadas mediante el Servicio de Firma Digital con Custodia Centralizada deberán ser generadas y almacenadas en un dispositivo criptográfico que cumpla con certificación FIPS 140 (Versión 2) nivel 3 o superior o FIPS 140 (Versión 3) nivel 3 o superior.

Excepcionalmente, en el caso de los suscriptores que no sean Oficiales de Registro, se admitirán dispositivos que se encuentren clasificados como **HISTÓRICOS (HISTORICAL)** por el *National Institute of Standards and Technology* (por su sigla en inglés, NIST). Los suscriptores no deberán utilizar estos dispositivos transcurridos TRES (3) años desde su incorporación a dicha clasificación. Se recomienda que los suscriptores no realicen nuevas adquisiciones de dispositivos que se encuentren en tal condición.

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 del 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.

VII) CICLO DE VIDA DE LOS CERTIFICADOS DE SUSCRIPTORES

1. Registro y procesamiento de la solicitud del suscriptor

El Certificador podrá 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 podrá implementar un procedimiento por el cual un suscriptor pueda solicitar la renovación 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 y renovados sean generados de acuerdo con sus políticas, prácticas y procedimientos.

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 podrá 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.
- e) La revocación de certificados digitales se puede llevar a cabo de dos maneras:
 1. A través del PIN de revocación: Este PIN es proporcionado al usuario en el momento de la emisión del certificado. Utilizando este código, el usuario podrá solicitar la revocación de su certificado de forma directa.
 2. Validación de identidad alternativa: En caso de que la Autoridad Certificante no ofrezca el método de revocación mediante PIN, se requerirá la validación de la identidad del solicitante a través de mecanismos biométricos aprobados. Este proceso asegurará que la revocación se realice de manera segura y confiable, garantizando la integridad del sistema de certificación.

8. Suspensión del certificado

El Certificador deberá informar que el estado de suspensión no se encuentra contemplado en el marco de la Ley N° 25.506.

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

El Certificador deberá asegurar la puesta a disposición de los suscriptores y usuarios, de la 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 deberán ajustarse a los contenidos definidos en el Anexo IV “Perfiles de los Certificados y de las Listas de Certificados Revocados”.

VIII) 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 a la Lista de Certificados Revocados, según lo dispuesto por el Decreto N° 182/2019 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, el Manual de Procedimientos, el Acuerdo con Suscriptores, los Términos y Condiciones con Terceros Usuarios y la Política de Privacidad.

4. Contactos

El Certificador está obligado a publicar las formas disponibles de comunicación. 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 las mencionadas 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 humana, jurídica, dispositivo o aplicación que intervenga en el proceso de licenciamiento (tales como Autoridad Certificante, Autoridad de Registro, suscriptor, Tercero Usuario, servidor de aplicación, etc.).

	INFORMACIÓN REGISTRADA
Contenido mínimo a registrar	<ul style="list-style-type: none"> 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, etc.). e) Identificación de la entidad que efectuó el registro.

	EVENTOS A REGISTRAR
Administración del ciclo de vida de las claves criptográficas del Certificador	<ul style="list-style-type: none"> a) Generación y almacenamiento de las claves criptográficas. b) Resguardo de las claves criptográficas. c) Recuperación de las claves criptográficas. d) Retiro de datos relacionados con las claves criptográficas. e) Destrucción de las claves criptográficas. f) Identificación de la entidad que autoriza una operación de administración de las claves criptográficas. g) Identificación de la entidad que administra los datos relativos a las claves criptográficas (tal como los componentes de claves, claves almacenadas en dispositivos criptográficos u otros medios). h) Compromiso de la clave privada.

<p>Administración del ciclo de vida de los certificados</p>	<ul style="list-style-type: none"> a) Recepción de solicitudes de certificados (inicial, de renovación con el mismo o un nuevo par de claves). b) Cambios en los datos de la solicitud del certificado. c) Generación de certificados. d) Solicitudes de revocación de certificados.
<p>Administración del ciclo de vida de los dispositivos criptográficos</p>	<ul style="list-style-type: none"> a) Ingreso o retiro del dispositivo del lugar de almacenamiento. b) Envío de dispositivos para servicio técnico o reparación. c) Retiro, baja o borrado de información del dispositivo.
<p>Información relacionada con la solicitud de certificados</p>	<ul style="list-style-type: none"> a) Tipos de documentos de identificación presentados por el solicitante u otra información de identificación, en caso de ser aplicable. b) Ubicación del archivo de las copias de las solicitudes de certificados y de los documentos de identificación. c) Identificación de la entidad que recibe y acepta la solicitud. d) Método utilizado para validar los documentos de identificación. e) Identificación de la Autoridad de Registro, de ser aplicable.

<p>Eventos de seguridad</p>	<ul style="list-style-type: none">a) Lectura, modificación o borrado de archivos o registros críticos de seguridad, incluyendo el registro diario de eventos.b) Cambios en los perfiles de seguridad.c) Registro de intentos exitosos y fallidos de accesos al sistema, los datos y los recursos.d) Caídas del sistema, fallas en el <i>hardware</i> y <i>software</i>, u otras anomalías.e) Acciones desarrolladas por los operadores y administradores del sistema y responsables de seguridad.f) Modificaciones en los procesos o procedimientos de cifrado y/o autenticación.g) Accesos al sistema de la Autoridad Certificante o a cualquiera de sus componentes.
------------------------------------	--

	OBSERVACIONES GENERALES
Información crítica sobre sincronización de eventos	<p>a) Los registros de eventos no deben reflejar los valores en texto plano de claves privadas o contraseñas.</p> <p>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.</p> <p>c) Toda información de horarios deberá contener año, mes, día, hora, minuto, segundo y huso horario.</p>

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 descritos 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.

1. 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.

2. 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. Las Autoridades Certificantes pertenecientes a una misma razón social que utilicen la misma infraestructura tecnológica, deberán 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 el artículo 21, inciso c) de la Ley N° 25.506.

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.

2.1. 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.

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 bajo una misma razón social 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. 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 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 Certificantes, si fuera el caso, sólo se pueden ingresar a este nivel previa autorización expresa y registración.

2.2. 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 el Certificador Licenciado. 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, siempre que se implementen adecuados controles que impidan los accesos no autorizados o que pudieran afectar la seguridad de los procesos de certificación.

2.3. 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 Certificador deberá contar con su propio ambiente de nivel 5 y cada Autoridad Certificante, con su nivel 6 de protección.

3. 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 del Oficial de Registro y a la documentación que se le confía para su resguardo, así como a los datos de los solicitantes.

Las Autoridades de Registro podrán realizar su actividad en puestos móviles cuando se presenten las condiciones que ameriten tal servicio, siempre que lo haya notificado al 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.

Las Autoridades de Registro que operen con modalidad móvil deberán facilitar a sus Oficiales de Registro un equipamiento propio que garantice la seguridad de la información (sistema operativo, antivirus actualizados y soporte, así como otras configuraciones de seguridad aplicables).

4. 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.

5. 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.



República Argentina - Poder Ejecutivo Nacional
AÑO DE LA RECONSTRUCCIÓN DE LA NACIÓN ARGENTINA

Hoja Adicional de Firmas
Informe gráfico

Número:

Referencia: ANEXO II - REQUISITOS PARA EL LICENCIAMIENTO DE CERTIFICADORES PARA OPERAR
CON FIRMA DIGITAL

El documento fue importado por el sistema GEDO con un total de 23 pagina/s.