GOBIERNO DE MENDOZA
SECRETARÍA ADMINISTRATIVA LEGAL Y TÉCNICA
UNIDAD DE REFORMA DEL ESTADO

firma Digital

"Análisis de factibilidad para la implementación de Firma Digital"

Segundo Informe de Etapa

Consejo Federal de Inversiones

CONSULTOR: LIC. PABLO GUILLERMO LIOY

ÍNDICE

SEGUNDO INFORME PARCIAL

PROPUESTA ORGANIZATIVA: INFRAESTRUCTURA DE CLAVE PÚBLICA PARA LA PROVINCIA DE MENDOZA

I. Introducción

En el marco del proyecto Firma Digital Mendoza y de acuerdo con el Plan de Actividades propuesto, se presentan a continuación, como Segundo Informe de Etapa, el desarrollo de la actividad y de las tareas que la integran, identificada como número 3 dentro del mismo:

Desarrollar organizativa y funcionalmente una infraestructura de certificación coherente para la implementación de firma digital:

- Definición de una estructura de autoridades certificantes
- Diseño de Manual de Funciones: determinación de Funciones, Responsabilidades y Obligaciones
- Definición de Políticas de Certificación
- Diseño de Manual de Procedimientos
- Diseño de Plan de Cese de Actividad
- Diseño de Plan de Contingencia
- Diseño de Política de Seguridad

Antes de empezar resulta preciso aclarar que los desarrollos que aquí se presentan son base de las posteriores propuestas legales contempladas por el proyecto, lo cual implica probables cambios futuros de los contenidos ahora presentados según la naturaleza de las interconexiones que se susciten y el avance normativo legal nacional en materia de firma digital.

II. Definición estructural

De acuerdo con los conceptos plasmados en el estudio de factibilidad que precede este informe y desde una concepción estratégica, es preciso otorgarle al espectro de criptografía de clave pública una **estructura sistémica** que posibilite su implementación a través de aplicaciones relacionadas y con una idea coherente de conjunto. Sólo una completa y adaptada implementación de una **Infraestructura de Clave Pública** (con un determinado sistema de hardware, de software, de políticas, de procedimientos y de personas) hace factible proporcionar el conjunto de seguridades informáticas que la Administración Pública Provincial necesita.

Misión

Su misión es la de **difundir y facilitar** el uso de tecnología de firma digital así como también **securizar** las transacciones electrónicas de la Administración Pública Provincial en su entorno proveyendo claves y gestionando eficientemente certificados confiables, para lograr las preciadas garantías de autenticación, integridad, confidencialidad y no repudiación.

Objetivos

Nuestra definición de una **Infraestructura de Clave Pública** (PKI) de propósito general para la provincia de Mendoza sustenta los siguientes objetivos:

- Prestar **asesoramiento y apoyo** a proyectos relacionados con la tecnología de firma digital en el ámbito de la Provincia de Mendoza.

- Posibilitar, desde una perspectiva administrativa y técnica, la utilización de **servicios de firma digital** en una amplia variedad de aplicaciones en la Administración Pública Provincial,

atendiendo a nociones de eficiencia, optimización y despapelización del Estado

Estructura formal

Ha sido nuestro objetivo plasmar aquí la organización estructural que le daremos a nuestra implementación inicial de la PKI Mendoza. Es conveniente señalar que en su diseño se materializan las premisas planteadas en el estudio de factibilidad sobre condiciones de interoperabilidad y de escalabilidad.

Por consiguiente en la *figura 1* se muestra tanto la estructuración inicial de la PKI, como también la tendencia ordenada y gradual de crecimiento planificado para nuestra infraestructura (Sombreado).

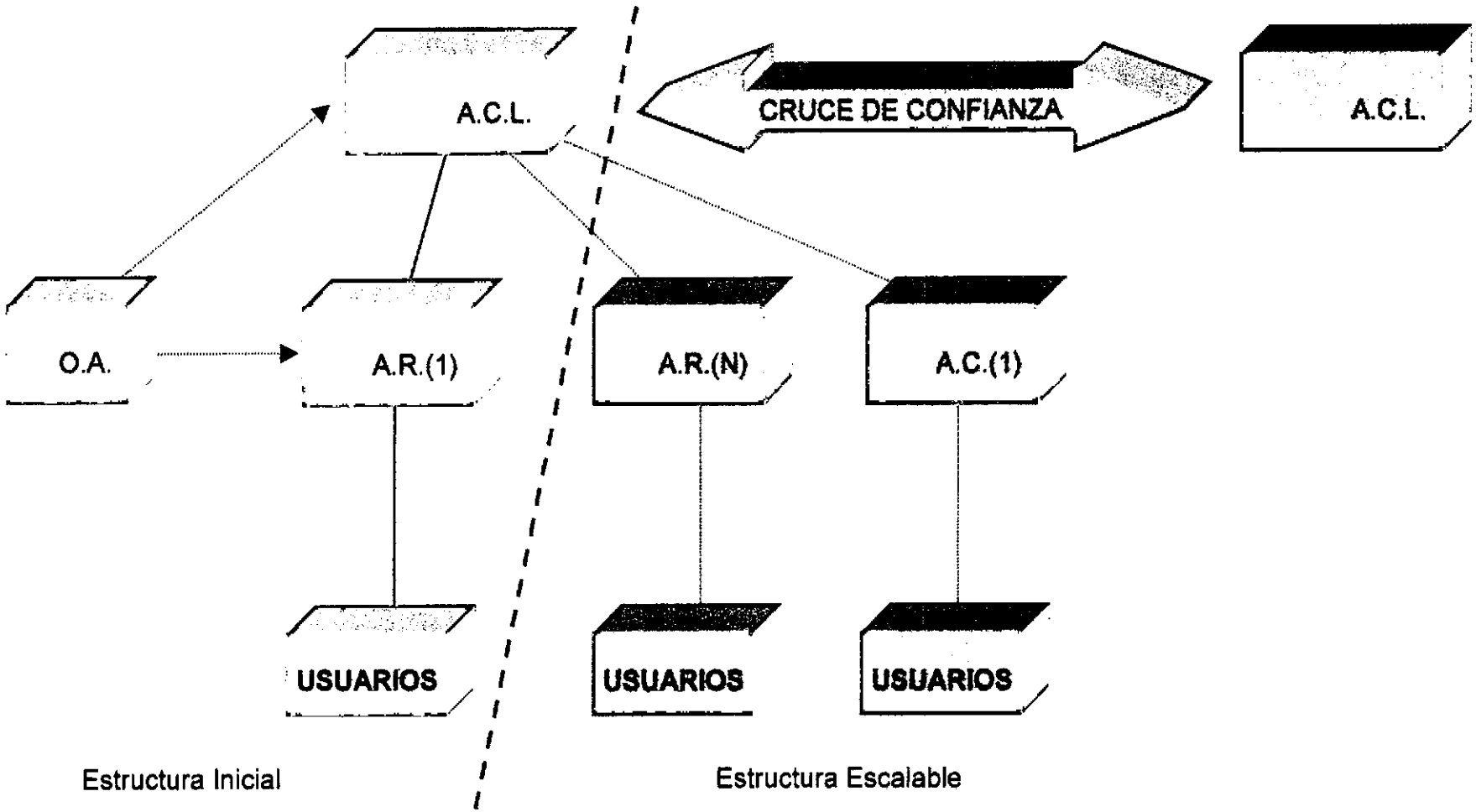

Figura 1 – Estructura inicial y escalabilidad

Componentes

Como vimos en la *figura 1* la implementación inicial de la PKI Mendoza contempla la existencia de los siguientes entes en orden de jerarquía:

- **Una Autoridad Certificante Licenciada (CA):** Es el órgano responsable de la emisión de los certificados, luego de una correcta verificación por los métodos que considere en la política de certificación. Es el principal proveedor de la tecnología de criptografía asimétrica. Debe contar con medidas de seguridad que infundan la total confianza requerida para considerara a su gestión seria y exitosa y ostentar altos niveles de calidad en la prestación y disponibilidad de sus servicios.

  La cualidad de "Licenciada" viene dada por la oportuna solicitud y obtención de la autorización por parte del Ente Administrador de firma digital una vez cumplidas las exigencias que, a la fecha del presente informe aún no han sido definidas. Sin embargo queremos dejar claro aquí, que sin perjuicio del funcionamiento piloto de la infraestructura, la intención es adherir al régimen de licenciamiento propuesto por ley.
  Designación: se propone a la Gobernación por medio de su Secretaría Administrativa Legal y Técnica (UNIDAD DE REFORMA Y MODERNIZACIÓN DEL ESTADO)

- **Una Autoridad de Registro (RA):** Cuya misión es realizar meticulosamente la verificación de las personas (validación de identidad) que requieren la emisión de un certificado y realizar la solicitud formal pertinente(Registro de presentaciones). Gracias a esta descentralización se agiliza el proceso de certificación y se aumenta la eficacia en la gestión de solicitudes.

  Designación: se propone que en un primer momento las funciones correspondientes a una (RA) sean llevadas en paralelo por el **organismo encargado de certificar (C.A.L)** hasta tanto la infraestructura se desarrolle y se identifiquen Autoridades de Registro de acuerdo

con los principios plasmados en su política y manuales de procedimiento.

- **Organismo Auditante:** se propone al **Honorable Tribunal de Cuentas de la Provincia** a través de una comisión especial formada a tales efectos, hasta tanto se designe éste u otro organismo a través del sistema de Auditoría propuesto por el Decreto Reglamentario o por algún otro sistema según corresponda.

- **Políticas de Certificación** y **Manuales de Procedimiento** que rigen el funcionamiento general de la PKI definiendo cuestiones tan esenciales como el tipo de certificado a emitir por la Autoridad de Certificación, el alcance de la información almacenada en el certificado, los procedimientos de registro, el tipo y alcance del compromiso de la Autoridad de Certificación con los usuarios y viceversa, las restricciones en el uso del certificado, etc.

- **Suscriptores de certificados:** Pueden serlo todos aquellos funcionarios y agentes dependientes de los organismos que soliciten y obtengan un certificado de clave pública emitido por la Autoridad Certificante Licenciada como así también los servidores o equipos cuya identificación deba estar respaldada por un certificado de firma digital.

Modelo de Escalabilidad

Como se puede ver en la *figura 1* nuestra definición de la estructura posibilita en términos de escalabilidad y en función de requerimientos futuros:

- La incorporación de nuevas **Autoridades de Registro (AR)** que podrán tener funciones distribuidas por Ministerio o por Unidad de Gestión o alternativamente por tipo de certificados que se gestionen.

- La subordinación de eventuales **Autoridades Certificantes** que se ajusten a la Autoridad Certificante Licenciada y que posean una estructura orgánica consistente en términos de políticas, estándares y manuales de procedimientos. De ésta manera se puede favorecer los mecanismos de división de la carga del trabajo para garantizar la confiabilidad y flexibilidad de la PKI.

- La eventual interconexión de la jerarquía provincial con otras infraestructuras el país a través de cruces de confianza.

Alcance de la Infraestructura

La infraestructura propuesta pretende atender aquellas necesidades técnicas relacionadas con la firma digital y aquellas necesidades de apoyo y asesoramiento sobre tales temas a todos aquellos usuarios, funcionarios, agentes, organismos o entidades en el ámbito de la organización institucional Centralizada y Descentralizada del Gobierno de la Provincia de Mendoza, entes autárquicos, organismos provinciales y municipales, de otros Poderes del Estado Provincial y de los representantes del sector privado, a través de convenios específicos firmados en cada caso en particular.

Aplicaciones y Servicios

De acuerdo con la premisa de **difundir y facilitar** el uso de tecnología de firma digital así como también **securizar** las transacciones electrónicas se prevé que nuestra PKI Provincial desarrolle las siguientes prestaciones:

- **Correo electrónico seguro/secure messaging, firma digital y no repudio.** La naturaleza distribuida del correo electrónico y la necesidad de almacenar y reenviar información a muchos destinatarios en-

cuentran en la criptografía de clave pública las capacidades de firma digital de mensajes y cifrado masivo sin establecimiento previo de claves secretas compartidas.

- **Autenticación de identidad:**

  De Servidores (sitio seguro), para que los usuarios puedan comprobar el servidor con el que se comunican.

  De clientes (control de acceso) para que los servidores puedan comprobar la identidad del cliente y en función de ésta tomar decisiones de control de acceso

- **Canal Seguro (SSL):** Confidencialidad en la transferencia de datos a través de enlaces públicos de Internet mediante protocolos de la capa de transporte.

- **Secure Desktop:** Cifrado de archivos (acuerdo de clave privada mediante clave pública) y cifrado masivo de datos (sin establecimiento previo de claves secretas compartidas).

- **Secure e-forms:** firma digital y seguridad para formularios basados en web.

- **Encripción de bases de datos**

Estándares Tecnológicos y Normas de Seguridad

A través de la Resolución N° 54 / 99 y del Decreto-Acuerdo N° 1806 del 1999, el Gobierno de la Provincia de Mendoza, a través del Comité de Información Pública (COM.I.P.) órgano dependiente de la Unidad de Reforma del Estado, adopta para el ámbito del Poder Ejecutivo Provincial el uso del ***COBIT*** (Objetivos de Control para la Información y Tecnología Relacionadas y sus posteriores actualizaciones), se adoptan además las ***Normas de Seguri-***

dad de Sistemas de Información, sus posteriores modificaciones y agregados y fundamentalmente el uso de los **Estándares Tecnológicos de la Administración Pública Nacional** (E.T.A.P y sus posteriores modificaciones) que fueron oportunamente desarrollados por la Subsecretaría de Tecnologías para el Sector Público, dependiente de la Secretaría Administrativa Legal y Técnica de la Gobernación de la Jefatura de Gabinete de Ministros, así como también se ha seguido la línea de los **Estándares Internacionales de Seguridad en Sistemas de Información** y los **Estándares sobre tecnología de Firma Digital** de vigencia provisoria dictados por la Secretaria de la Función Publica dependiente de la Jefatura de Gabinete de Ministros hasta tanto se aprueben las actualizaciones previstas por el Decreto Reglamentario 2628/2002 en su Art. 22.

III. Manual de Funciones

Determinación de Funciones, responsabilidades y obligaciones

Funciones de la Autoridad Certificante Licenciada (CA)

1. Recibir una solicitud de emisión de certificado digital, firmada digitalmente con los correspondientes datos de verificación de firma digital del solicitante.
2. Emitir certificados digitales de acuerdo a lo establecido en sus políticas de certificación, y de acuerdo con:
   a) Lo previsto en la normativa provincial propuesta
   b) Los estándares tecnológicos adoptados por la Provincia.
3. Identificar inequívocamente los certificados digitales emitidos.
4. Mantener copia de todos los certificados digitales emitidos, consignando su fecha de emisión y de vencimiento si correspondiere, y de sus correspondientes solicitudes de emisión.
5. Revocar los certificados digitales por él emitidos en los siguientes casos:
   a) A solicitud del titular del certificado digital.
   b) Si determinara que un certificado digital fue emitido sobre la base de una información falsa, que en el momento de la emisión hubiera sido objeto de verificación.
   c) Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros. En tales casos deberá sustituir en forma gratuita aquellos certificados digitales que han dejado de ser seguros por otro que cumpla efectivamente con tales requisitos.

   Esta función queda sujeta a los procedimientos aplicables a estos casos de reemplazo de certificados que se encuentran pendientes de fijación por parte de la autoridad nacional de aplicación.
   d) Por condiciones especiales definidas en su política de certificación.
   e) Por resolución judicial o de la autoridad nacional de aplicación.

En los casos en los que un certificado digital haya dejado de ser seguro por razones atribuibles a su titular, la autoridad certificante licenciada no estará obligado a sustituir el certificado digital.

6. Comprobar por sí o por medio de una Autoridad de Registro que actúe en nombre y por cuenta suya, la identidad y cualquier otro dato de los solicitantes considerado relevante para los procedimientos de verificación de identidad previos a la emisión del certificado digital, según la Política de Certificación bajo la cual se solicita.
7. Cumplir cabalmente con las políticas de certificación acordadas con el titular y con su Manual de Procedimientos.
8. Informar al solicitante de un certificado digital, en un lenguaje claro y accesible, en idioma nacional, respecto de las características del certificado solicitado, las limitaciones a la responsabilidad, si las hubiere, los precios de los servicios de certificación, uso, administración y otros asociados, incluyendo cargos adicionales y formas de pago, los niveles de servicio al proveer, las obligaciones que el suscriptor asume como usuario del servicio de certificación, su domicilio en la Provincia de Mendoza y los medios a los que el suscriptor puede acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema o presentar sus reclamos.
9. Informar públicamente el estado de los certificados digitales por él emitidos. Los certificados digitales revocados deben ser incluidos en una lista de certificados revocados indicando fecha y hora de la revocación. La validez y autoría de dicha lista de certificados revocados deben ser garantizadas.
10. Disponer de un servicio de atención a titulares y terceros, que permita evacuar las consultas y la pronta solicitud de revocación de certificados.
11. Garantizar el acceso permanente, eficiente y gratuito de los titulares y terceros al repositorio de certificados revocados.
12. Garantizar la prestación establecida según los niveles definidos en el acuerdo de servicios pactados con sus usuarios, relativo a los servicios para los cuales solicitó el licenciamiento.
13. Mantener a disposición permanente del público las Políticas de Certificación y el Manual de Procedimientos correspondiente.

14. Mantener actualizados los repositorios de certificados revocados por el período establecido en sus políticas de certificación.

Obligaciones de la Autoridad Certificante Licenciada (CA)

1. Informar a quien solicita un certificado con carácter previo a su emisión y utilizando un medio de comunicación las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de un sistema de licenciamiento y los procedimientos, forma que garantiza su posible responsabilidad patrimonial y los efectos de la revocación de su propio certificado digital y de la licencia que le otorga el ente licenciante. Esa información deberá estar libremente accesible en lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros.
2. Notificar al solicitante las medidas que está obligado a adoptar para crear firmas digitales seguras y para su verificación confiable, y las obligaciones que asume por el solo hecho de ser titular de un certificado digital.
3. Poner a disposición del solicitante de un certificado digital toda la información relativa a su tramitación.
4. Incorporar en su política de certificación los efectos de la revocación de su propio certificado digital y/o de la licencia que le otorgara la autoridad de aplicación.
5. Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, la lista de certificados digitales revocados, las políticas de certificación, la información relevante de los informes de la última auditoría de que hubiera sido objeto, su manual de procedimientos y toda información que determine la autoridad de aplicación nacional.
6. Informar en las políticas de certificación si los certificados digitales por él emitidos requieren la verificación de la identidad del titular.

7. Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a los datos de creación de firma digital de los titulares de certificados digitales por él emitidos.
8. Abstenerse de generar, exigir, tomar conocimiento o acceder bajo ninguna circunstancia a la clave privada del suscriptor.
9. Mantener el control exclusivo de sus propios datos de creación de firma digital e impedir su divulgación.
10. Proteger el manejo de la clave privada de la entidad mediante un procedimiento de seguridad que impida el acceso a la misma a personal no autorizado.
11. Proteger el acceso y el uso de la clave privada mediante procedimientos que exijan la participación de más de una persona.
12. Operar utilizando un sistema técnicamente confiable de acuerdo con lo que determine la autoridad de aplicación nacional.
13. Garantizar la confiabilidad de los sistemas de acuerdo con los estándares tecnológicos adoptados por la Provincia.
14. Garantizar la existencia de sistemas de seguridad física y lógica que cumplimenten las normativas vigentes.
15. Utilizar con exclusividad los sistemas que cumplan las funciones de certificación con ese propósito, sin que se les asigne ninguna otra función.
16. Proteger a todos los sistemas utilizados directa o indirectamente en la función de certificación con procedimientos de autenticación y seguridad de alto nivel de protección, que deban ser actualizados de acuerdo a los avances tecnológicos para garantizar la correcta prestación de los servicios de certificación.
17. Recabar únicamente aquellos datos personales del titular del certificado digital que sean necesarios para su emisión, quedando el solicitante en libertad de proveer información adicional.
18. Mantener la confidencialidad de toda información que no figure en el certificado digital.
19. Mantener la documentación respaldatoria de los certificados digitales emitidos, por diez (10) años a partir de su fecha de vencimiento o revocación.

20. Publicar en el Boletín Oficial aquellos datos que la autoridad de aplicación nacional determine.
21. Publicar en el Boletín Oficial de la Provincia de Mendoza durante UN (1) día, el certificado de clave pública correspondiente a la política para la cual obtuvo licenciamiento.
22. Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas.
23. Registrar las transacciones realizadas, a fin de identificar el autor y el momento de cada una de las operaciones.
24. Verificar, de acuerdo con lo dispuesto en su manual de procedimientos, toda otra información que deba ser objeto de verificación, la que debe figurar en las políticas de certificación y en los certificados digitales.
25. Solicitar inmediatamente al ente licenciante la revocación de su certificado, o informarle la revocación del mismo, cuando existieren indicios de que los datos de creación de firma digital que utiliza hubiesen sido comprometidos o cuando el uso de los procedimientos de aplicación de los datos de verificación de firma digital en él contenidos hayan dejado de ser seguros.
26. Informar inmediatamente al ente licenciante sobre cualquier cambio en los datos relativos a su licencia.
27. Informar a la autoridad nacional de aplicación de modo inmediato la ocurrencia de cualquier evento que comprometa la correcta prestación del servicio.
28. Permitir el ingreso de los funcionarios autorizados de la autoridad de aplicación, del ente licenciante o de los auditores a su local operativo, poner a su disposición toda la información necesaria y proveer la asistencia del caso
29. Emplear personal idóneo que tenga los conocimientos específicos, la experiencia necesaria para proveer los servicios ofrecidos y en particular, competencia en materia de gestión, conocimientos técnicos en el ámbito de la firma digital y experiencia adecuada en los procedimientos de seguridad pertinentes.
30. Disponer de recursos humanos y tecnológicos suficientes para operar de acuerdo a las exigencias establecidas en la normativa provincial propuesta.

31. Disponer de los recursos financieros adecuados al tipo de actividad de certificación que desarrolla, acorde con los niveles de responsabilidad derivados de la misma.
32. Someter a aprobación del ente licenciante el manual de procedimientos, el plan de seguridad y el de cese de actividades, así como el detalle de los componentes técnicos a utilizar.
33. Constituir domicilio legal en la Provincia de Mendoza.
34. Cumplir con toda otra obligación emergente de su calidad de titular de la licencia adjudicada por el ente licenciante.
35. Generar en un ambiente seguro las firmas digitales propias y todos los servicios para los cuales solicite licencia.
36. Cumplir con lo previsto en sus políticas y procedimientos de certificación.
37. Garantizar la continuidad de las operaciones mediante un Plan de Contingencia actualizado y aprobado.
38. Respetar el derecho del titular del certificado digital a no recibir publicidad de ningún tipo por su intermedio, salvo consentimiento expreso de éste.
39. Cumplir las normas y recaudos establecidos para la protección de datos personales.

Responsabilidad/Atribuciones de la Autoridad Certificante Licenciada (CA)

1. La relación entre el certificador licenciado que emite un certificado digital y el titular de ese certificado se rige por el contrato que celebren entre ellos, en las condiciones que marca la normativa provincial propuesta.
2. Responsabilidad ante terceros: El certificador es responsable por los daños y perjuicios que provoque, por los incumplimientos a las previsiones de la normativa provincial propuesta, por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos, en legal tiempo y forma cuando así correspondiere y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles. Corresponderá al prestador del servicio demostrar que actuó con la debida diligencia.

3. Limitaciones de responsabilidad: el certificador licenciado no es responsable en los siguientes casos:
    a) Por los casos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados y que no estén expresamente previstos en la normativa provincial propuesta.
    b) Por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización.
    c) Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y en los manuales de procedimientos respectivos, deba ser objeto de verificación, siempre que el certificador pueda demostrar que ha tomado todas las medidas razonables.

4. Cumplir con los requisitos establecidos por la ley y tramitar la solicitud respectiva ante el ente licenciante, el que otorgará la licencia previo dictamen legal y técnico que acredite la aptitud para cumplir con sus funciones y obligaciones.
5. Contar con personal idóneo y confiable, con antecedentes profesionales acordes a la función desempeñada.
6. Responder a los pedidos de informes por parte de un tercero respecto de la validez y alcance de un certificado digital emitido por él.
7. Podrá delegar en Autoridades de Registro las funciones de validación de identidad y otros datos de los suscriptores de certificados y de registro de las presentaciones y trámites que les sean formuladas cumpliendo las normas y procedimientos establecidos por la normativa provincial propuesta.
8. A su vez, podrá autorizar mediante su aprobación, la delegación de funciones en autoridades de registro dependientes jerárquicamente de sus autoridades de registro de acuerdo con las necesidades concretas del caso.
9. En los casos que delegue parte de sus funciones en Autoridades de Registro, sigue siendo responsable por éstas sin perjuicio del derecho de la Auto-

ridad Certificante a reclamar las indemnizaciones por los daños y perjuicios que aquel sufriera como consecuencia de los actos y/u omisiones de su Autoridad de Registro.

Funciones de la Autoridad de Registro

1. La recepción de las solicitudes de emisión de certificados.
2. La validación de la identidad y autenticación de los datos de los titulares de certificados.
3. La validación de otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue la Autoridad Certificante Licenciada.
4. La remisión de las solicitudes aprobadas a la Autoridad Certificante Licenciada con la que se encuentre operativamente vinculada.
5. La recepción y validación de las solicitudes de revocación de certificados; y su direccionamiento a la Autoridad Certificante Licenciada con el que se vinculen.
6. La identificación y autenticación de los solicitantes de revocación de certificados.
7. El archivo y la conservación de toda la documentación respaldatoria del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por la Autoridad Certificante Licenciada.
8. El cumplimiento de las normas y recaudos establecidos para la protección de datos personales.
9. El cumplimiento de las disposiciones que establezca la Política de Certificación y el Manual de Procedimientos de la Autoridad Certificante Licenciada con la que se encuentre vinculada, en la parte que resulte aplicable.

Derechos de los suscriptores de certificados

1. A ser informados durante la solicitud de un certificado digital, en un lenguaje claro y accesible, en idioma nacional, respecto de las características del certificado solicitado, las limitaciones a la responsabilidad, si las hubiere, los precios de los servicios de certificación, uso, administración y otros asociados, incluyendo cargos adicionales y formas de pago, los niveles de servicio

al proveer, las obligaciones que el suscriptor asume como usuario del servicio de certificación, su domicilio en la Provincia de Mendoza y los medios a los que el suscriptor puede acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema o presentar sus reclamos.

2. A tener disponible la totalidad de la información relativa a la tramitación de un certificado digital.
3. A ser notificado de las medidas que está obligado a adoptar para crear firmas digitales seguras y para su verificación confiable, y las obligaciones que asume por el solo hecho de ser titular de un certificado digital.
4. A disponer de un servicio de atención, que permita evacuar sus consultas y la pronta solicitud de revocación de sus certificados.
5. A disponer de acceso permanente, eficiente y gratuito al repositorio de certificados revocados.
6. A proveer información adicional a la necesaria para la emisión de su certificado y siendo conciente de ello.
7. A no recibir publicidad de ningún tipo por su intermedio, salvo consentimiento expreso de éste.

Obligaciones de los suscriptores de certificados

1. Mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, e impedir su divulgación.
2. Utilizar un dispositivo de creación de firma digital técnicamente confiable.
3. Solicitar la revocación de su certificado a la Autoridad Certificante Licenciada ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma.
4. Informar sin demora a la Autoridad Certificante Licenciada el cambio de alguno de los datos contenidos en el certificado digital que hubiera sido objeto de verificación.

IV. Política de Certificación

Criterios generales para el otorgamiento de certificados a favor de suscriptores

Autoridad Certificante

Gobernación de Mendoza

Secretaría Administrativa Legal y Técnica

Unidad de Reforma y Modernización del Estado

Los contenidos de esta política quedan sujetos a ajuste en función de la futura fijación de los contenidos mínimos que oportunamente haga la Autoridad de Aplicación Nacional.

Hasta tanto, la presente política de Certificación se encuentra de acuerdo con los estándares nacionales e internacionales vigentes y cumplen con la información mínima establecida por la ley:

- Identificación del certificador licenciado.
- Política de administración de los certificados y detalles de los servicios arancelados.
- Obligaciones de la entidad y de los suscriptores de los certificados.
- Tratamiento de la información suministrada por los suscriptores, y resguardo de la confidencialidad en su caso.
- Garantías que ofrece para el cumplimiento de las obligaciones que se deriven de sus actividades.

1- Ambito de aplicación

El presente documento define los términos que rigen la relación entre la Unidad de Reforma y Modernización del Estado de la Secretaría Administrativa Legal y Técnica de la Gobernación, en su carácter de Autoridad Certificante de la Administración Pública Provincial y sus funcionarios y agentes que soliciten la emisión de certificados de clave pública de acuerdo con las políticas particulares de emisión. Asimismo, regula la relación que pueda crearse entre dicha

Autoridad Certificante y otros organismos o dependencias de la Administración Pública Provincial Centralizada y Descentralizada, de entes autárquicos, organismos provinciales y municipales, de otros Poderes del Estado Provincial y de los representantes del sector privado, a través de convenios específicos firmados en cada caso en particular.

Además, provee el marco necesario para la aplicación de políticas particulares adaptadas al uso de certificados para aplicaciones específicas que se considerarán complementarias a la presente.

El presente documento forma parte de la documentación técnica emitida por la Autoridad Certificante de la Unidad de Reforma y Modernización del Estado junto con los siguientes documentos:

- Manual de Procedimientos
- Política de Seguridad
- Plan de Contingencias
- Plan de Cese de Actividades

2- Sujetos

Esta política es aplicable por:

a) **La Autoridad Certificante de la Unidad de Reforma del Estado** (en adelante AC-URME) que otorga certificados a favor de los funcionarios y agentes pertenecientes a los organismos o dependencias de la Administración Pública Provincial Centralizada y Descentralizada, entes autárquicos, organismos provinciales y municipales, de otros Poderes del Estado Provincial y de representantes del sector privado.

b) **Las Autoridades de Registración** que se constituyan en el ámbito de aplicación de esta política.

c) El **Honorable Tribunal de Cuentas de la Provincia** a través de una comisión especial designada para cumplir funciones de Organismo Auditante, hasta tanto se designe éste u otro organismo a

través del sistema de Auditoría propuesto por la Reglamentación Nacional de la Ley 25.506.

d) **Los suscriptores de certificados** en el ámbito de aplicación de esta política de alcance general, sin perjuicio de la aplicabilidad de la que gozarán aquellas políticas particulares por uso de certificados en aplicaciones específicas.

3- Objeto

Esta política regula el empleo de la firma digital en la instrumentación de:

a) Los actos internos del Sector Público Provincial, Municipal, y de otros Poderes del Estado Provincial que no produzcan efectos individuales en forma directa.

b) Los actos que vinculen al Sector Público Provincial, municipal, a otros Poderes del Estado Provincial con representantes del sector privado.

4- Contactos/Sugerencias

Esta política es administrada por la Autoridad Certificante de la Unidad de Reforma del Estado (AC-URME) cuyas funciones ejerce la Unidad de Reforma y Modernización del Estado de la Secretaría Administrativa Legal y Técnica de la Gobernación.

Por consultas o sugerencias, por favor dirigirse a:

E-mail:

ComitedeReforma@mendoza.gov.ar

Personalmente o por correo:

Provincia de Mendoza
Casa de Gobierno
Peltier 351 4° Piso Cuerpo Central
CP 5500

5- Responsabilidades

5 -1 - Responsabilidad de la Autoridad Certificante

En su carácter de Autoridad Certificante, la Unidad de Reforma y Modernización del Estado es responsable de todos los aspectos relativos a la emisión y administración de los certificados emitidos a favor de todos los suscriptores que adhieran a esta política, funcionarios o agentes de organismos o dependencias de la Administración Pública Nacional, entes autárquicos, organismos provinciales o municipales, de otros Poderes del Estado Provincial, y de representantes del sector privado, que gestionen su certificado ante la AC-URME, con el alcance que se establezca para cada caso en particular.

En particular, su responsabilidad se extiende a:

a) El proceso de identificación y autenticación del suscriptor, en el ejercicio de sus funciones de Autoridad de Registración.
b) La emisión de certificados.
c) La administración de certificados, incluyendo el proceso de revocación.

5 -2 - Responsabilidades asumidas por la Autoridad Certificante al emitir un certificado

Al emitir un certificado, la Autoridad Certificante garantiza:

a) Que el certificado ha sido emitido siguiendo las pautas establecidas en esta política y en el Manual de Procedimientos para la validación de los datos en él incluidos.
b) Que el certificado satisface todos los requisitos exigidos por los Estándares Tecnológicos adoptados por la Provincia.
c) Que los algoritmos y longitudes de claves utilizados cumplen con la última versión aprobada por Resolución de la Autoridad de Aplicación en relación a los Estándares sobre Tecnología de Firma Digital adoptados por la Provincia.

d) Que el certificado y su eventual revocación, serán publicados según lo dispuesto en esta política.

5 -3 - Obligaciones de las Autoridades de Registración

Las Autoridades de Registración que se constituyan en el ámbito de aplicación de esta política, cualquiera sea la modalidad que adopten, están obligadas a cumplir las funciones de validación de la identidad y autenticación de los datos de los suscriptores que soliciten sus certificados por su intermedio y a archivar y conservar toda la documentación respaldatoria de dicho proceso.

5 -4 - Responsabilidad del Suscriptor

El suscriptor de un certificado de clave pública de acuerdo a los lineamientos de esta política asume la absoluta responsabilidad por su utilización, incluyendo la custodia exclusiva y permanente de su clave privada. En particular, el suscriptor es responsable de solicitar la revocación de su certificado en caso de finalizar su vínculo laboral con la Administración Pública o con el organismo en que se desempeñe y en los demás casos previstos en esta normativa. La AC-URME no asume ninguna responsabilidad por el uso que el suscriptor eventualmente pudiera darle al certificado fuera del alcance establecido en el apartado 1 de esta política.

6- Interpretación

La interpretación, obligatoriedad, diseño y validez de esta política se encuentran sometidos a los avances en materia de normativa legal sobre firma digital de la provincia.

7- Publicación/Repositorios

La AC-URME mantiene un repositorio en línea de acceso público que contiene:

a) Certificados emitidos que hagan referencia a esta política.

b) Listas de certificados revocados.

c) El certificado de clave pública de la AC-URME

d) Copia de esta política y de toda otra documentación técnica referida a la AC-URME que se emita.

e) Toda otra información referida a certificados que hagan referencia a esta política.

El repositorio se encontrará disponible en las páginas web de firma digital del gobierno de Mendoza.

7 -1 - Frecuencia de la actualización

Toda información que corresponda incluir en el repositorio debe serlo inmediatamente después de haber sido conocida y verificada por la AC-URME.

Las emisiones de certificados y revocaciones de certificados deben ser incluidas tan pronto como se hayan cumplido los procedimientos de validación de identidad de los solicitantes establecidos en esta política y en el Manual de Procedimientos para cada caso en particular.

7 -2 - Acceso

El repositorio se encuentra disponible para uso público durante VEINTICUATRO (24) horas diarias SIETE (7) días a la semana, sujeto a un razonable calendario de mantenimiento.

La AC-URME no puede poner restricciones al acceso a esta política, a su certificado de clave pública y a las versiones anteriores y actualizadas de la documentación técnica que emita.

7-3- Confidencialidad

Toda información referida a suscriptores que sea recibida por la AC-URME en los requerimientos es confidencial y no puede hacerse pública sin el consentimiento previo de aquellos, salvo que sea requerida judicialmente.

Lo indicado no es aplicable cuando se trate de información que se transcriba en el certificado o sea obtenida de fuentes públicas.

8 - Identificación y Autenticación

Dentro del marco de aplicación de esta política, son admitidos los siguientes procedimientos de identificación de los suscriptores de certificados en función de los distintos esquemas de Autoridades de Registración previstos:

Tipo de Registración	Descripción	Opciones	Responsables intervinientes
1. ***Registración Centralizada***	✔ La AR reside en el mismo lugar físico donde funciona la AC	✔ Verificación de datos por la Autoridad de Registración	✔ Responsable de la AR local
		✔ Verificación de datos vía área de recursos humanos	✔ Responsable de la AR local ✔ Responsable del área de recursos humanos
		✔ Verificación a través del máximo responsable del organismo	✔ Responsable de la AR local ✔ Máxima autoridad del organismo al que pertenece el suscriptor
		✔ Servicio de registración itinerante	✔ Responsable de la AR local

2. ***registración Descentraliza-da***	✔ Existe una AR que reside fuera del lugar físico donde funciona la AC	✔ Verificación de datos en la AR remota ✔ Verificación de datos por un auxiliar de la AR remota	✔ Responsable de la AR remota ✔ Responsable de la AR remota ✔ Auxiliar de la AR remota

Los procesos a seguir en cada una de las opciones mencionadas son los siguientes:

8 -1 - Registración Centralizada

8-1-1- Verificación de datos por la Autoridad de Registración local

El suscriptor debe iniciar el pedido de emisión del certificado ingresando al sitio web de la AC-URME completando el formulario de solicitud y siguiendo el procedimiento allí indicado. Posteriormente debe presentarse personalmente ante el Responsable de la Autoridad de Registración local a fin de validar su identidad, provisto de la siguiente documentación:

a) Documento de identidad (DNI u otro de validez nacional), en original y fotocopia.

b) Código de identificación del requerimiento

c) Nota firmada por el máximo responsable del área de recursos humanos intervenida por Mesa de Entradas, Salidas y Archivo del organismo a que pertenece, que incluirá:

- Nombre y Apellido

- Documento de Identidad
- Jurisdicción/Organismo/Dependencia/Cargo

8-1-2- Verificación de datos vía área de recursos humanos

El suscriptor debe iniciar el pedido de emisión del certificado siguiendo el procedimiento indicado en el apartado anterior. El responsable del área de Recursos Humanos del organismo donde reside la AC-URME, o bien un funcionario de dicho sector designado al efecto, colaborarán con el Responsable de la Autoridad de Registración local en el proceso de identificación, validando los datos complementarios del suscriptor (jurisdicción, organismo, dependencia y cargo).

Posteriormente el suscriptor debe presentarse ante el Responsable de la Autoridad de Registración local provisto de:

a) Documento de Identidad (DNI u otro de validez nacional), en original y fotocopia.

b) Código de identificación del requerimiento

8-1-3- Verificación de identidad a través del responsable del organismo

El suscriptor debe iniciar el pedido de emisión del certificado siguiendo el procedimiento indicado en el apartado 8.1.1.. Posteriormente debe presentarse ante la máxima autoridad del organismo al que pertenece a fin de validar su identidad, provisto de la siguiente documentación:

a) Documento de Identidad (DNI u otro de validez nacional), en original y fotocopia.

b) Código de identificación del requerimiento

c) Nota firmada por el máximo responsable del área de recursos humanos del organismo consignando:

- Nombre y Apellido
- Documento de Identidad
- Jurisdicción/Organismo/Dependencia/Cargo

8-1-4- Servicio de registración itinerante

El funcionario solicitante debe iniciar el pedido de emisión del certificado siguiendo el procedimiento indicado en el apartado 8.1.1.

El Responsable de la Autoridad de Registración local debe concurrir a la dependencia u organismo a fin de efectuar la validación de la identidad del funcionario, para lo cual requerirá:

a) Documento de Identidad (DNI u otro de validez nacional), en original y fotocopia.
b) Nombramiento (Decreto o Resolución)

8 -2 - Registración Descentralizada

La AC-URME admite la constitución de Autoridades de Registración externas al ámbito físico donde desarrolla sus actividades. En particular, se admitirán aquellos organismos o dependencias que se encuentren en condiciones de efectuar un adecuado control de identidad de los suscriptores de certificados que les presentaran una solicitud de emisión, dado el tipo de información que manejan y su cercanía al usuario final (tales como áreas de recursos humanos). En todos los casos, es atribución de la AC-URME autorizar el funcionamiento de las Autoridades de Registración.

Toda Autoridad de Registración autorizada por la AC-URME asume las siguientes obligaciones:

a) Designar un responsable del proceso de validación de identidad de los suscriptores (Responsable de la Autoridad de Registración) y su correspondiente sustituto.
b) Cumplir con las obligaciones establecidas en la Política de Certificación y en el Manual de Procedimientos de la AC-URME respecto al proceso de validación de identidad de los suscriptores.
c) Cumplir con las disposiciones establecidas en la Política de Certificación y en el Manual de Procedimientos de la AC-URME respecto a la conservación de archivos y documentación respaldatoria referida al proceso de validación de identidad de los suscriptores.

d) Permitir la realización de las revisiones periódicas que realice la AC-URME a fin de garantizar la seguridad del sistema.

c) Toda otra obligación específica que se establezca en el Manual de Procedimientos de la AC-URME

d) Toda Autoridad de Registración debe adherir a los términos de la Política de Certificación, del Manual de Procedimientos y del resto de la documentación técnica de la AC-URME. Dicha adhesión se instrumentará mediante la firma de un Acuerdo de Responsabilidad.

8.2.1.- Autoridades de Registración Remotas con nombramiento de auxiliares en el proceso de validación de identidad.

Se admitirá que las Autoridades de Registración que se constituyan designen funcionarios que actuarán como colaboradores en el proceso de validación de la identidad de sus suscriptores. En tal caso, los auxiliares mencionados asumen las mismas obligaciones que la Autoridad de Registración en cuya órbita se constituyan respecto al cumplimiento de los procedimientos de validación de identidad de los suscriptores.

8 -3 - Solicitudes de renovación

Dentro de los TREINTA (30) días anteriores a la expiración del período operacional de un certificado emitido según los lineamientos de esta política, un suscriptor puede solicitar a la AC-URME la emisión de un nuevo certificado.

8 -4 - Período de validez

Los certificados emitidos por la AC-URME tienen un período máximo de validez de UN (1) año desde la fecha de emisión.

9 - Requisitos operativos

9 -1 - Requerimiento

La emisión del certificado a favor de un suscriptor implica su autorización para utilizarlo con los alcances definidos por esta política y por las políticas

particulares que se fijen para cada caso y caduca por expiración o revocación del certificado.

Todo suscriptor que se postule para obtener un certificado debe completar un requerimiento, el que estará sujeto a revisión y aprobación por la Autoridad de Registración según las previsiones indicadas en el apartado 8.

El proceso de solicitud puede ser iniciado solamente por el interesado, quien debe acreditar fehacientemente su identidad.

9 -2 - Emisión del certificado

Cumplidos los recaudos del proceso de identificación y autenticación de acuerdo con esta política y una vez completada y aprobada la solicitud, la AC-URME debe emitir el correspondiente certificado.

Debe firmarlo digitalmente y ponerlo a disposición del interesado, notificándolo de tal situación.

9 -3 - Contenido del certificado – Atributos

Un certificado emitido de acuerdo a los requerimientos de esta política incluye los datos identificatorios mínimos recomendados por la última versión de los Estándares sobre Tecnología de Firma Digital para la Administración Pública Nacional. En particular, deben incluirse los siguientes datos a efectos de distinguir unívocamente al suscriptor:

a) Número de versión X.509 del certificado

b) Nombre y apellido del suscriptor del certificado.

c) Localidad, provincia y país de residencia habitual.

d) Dirección de correo electrónico.

e) Clave pública del suscriptor.

f) Algoritmos de firma de la clave pública.

g) Número de serie del certificado.

h) Período de validez del certificado.

i) Nombre de la Autoridad Certificante emisora del certificado.

j) Dirección de consulta de la lista de certificados revocados (CRL).

k) URL donde se encuentra disponible esta Política de Certificación.

l) Todo otro dato relevante para la utilización del certificado según disponga el Manual de procedimientos de la AC-URME.

9 -4 - Condiciones de validez del certificado de clave pública

El certificado de clave pública correspondiente a un suscriptor en los términos de la presente Política es válido únicamente si:

a) Ha sido emitido por la AC-URME

b) No ha sido revocado.

c) No ha expirado su período de vigencia.

d) El certificado de la AC-URME no ha sido revocado ni ha expirado su período de vigencia.

El certificado de clave pública de la AC-URME es válido únicamente si:

a) No ha sido revocado.

b) No ha expirado su período de vigencia.

9 -5 - Revocación de certificados

9-5-1- Clases de revocación

9-5-1-1- Revocación voluntaria

El Responsable de la Autoridad de Registración admitirá solicitudes de revocación recibidas vía interfaz web o a través de un correo electrónico firmado digitalmente por el suscriptor.

El suscriptor podrá también efectuar la solicitud presentándose personalmente ante el Responsable mencionado, debiendo acreditar fehacientemente su identidad.

Asimismo, se admitirán solicitudes de revocación firmadas digitalmente por el responsable del área de Recursos Humanos o por la máxima autoridad competente del organismo o dependencia a que pertenece el suscriptor a la dirección de correo electrónico mencionada anteriormente o presentadas personalmente por cualquiera de los nombrados.

El Responsable de la Autoridad de Registración está facultado para aceptar solicitudes de revocación que reciba por otros medios (telefónicamente, vía fax) siempre que, a su juicio, la urgencia de la situación justifique la acepta-

ción. En tales casos, debe efectuar una confirmación telefónica de la solicitud o bien, de no ser posible, utilizar otro medio de verificación alternativo a fin de validar la identidad del solicitante.

9-5-1-2- Revocación obligatoria

Un suscriptor debe solicitar la inmediata revocación de su certificado:

a) Cuando se produzcan cambios en la información que el certificado contiene o ésta se desactualice.
b) Cuando la clave privada asociada al certificado de clave pública, o el medio en que se encuentre almacenada, se encuentren comprometidos o corran peligro de estarlo.
c) Cuando cese su vínculo laboral con el organismo, dependencia o institución.

La AC-URME debe revocar el certificado de su suscriptor:

a) A solicitud del suscriptor cuando se verifiquen los procedimientos de recepción y validación establecidos en el Manual de Procedimientos.
b) A solicitud del responsable del área de recursos humanos o de la máxima autoridad del organismo o dependencia cuando se verifiquen los procedimientos de recepción y validación establecidos en el Manual de Procedimientos.
c) Ante incumplimiento por parte del suscriptor de las obligaciones establecidas por la normativa provincial propuesta, por el Manual de Funciones, por esta política, por el Manual de Procedimientos o por cualquier otro acuerdo, regulación o ley aplicable al certificado.
d) Si toma conocimiento de que existe sospecha de que la clave privada del suscriptor se encuentra comprometida.
e) Si la AC-URME determina que el certificado no fue emitido de acuerdo a los lineamientos de la normativa provincial propuesta, de esta política, del Manual de Procedimientos o de los Estándares sobre Tecnología de Firma Digital para la Administración Pública Nacional.
f) Si se verifica cualquier otro supuesto que se contemple en el Manual de Procedimientos.

9-5-2- Autorizados a requerir la revocación

Unicamente el suscriptor, el responsable del área de Recursos Humanos o la máxima autoridad del organismo o dependencia pueden solicitar la revocación de un certificado emitido según lo dispuesto en esta política.

9-5-3- Procedimiento para solicitar la revocación

La solicitud de revocación del certificado de un suscriptor debe ser comunicada en forma inmediata a la AC-URME por alguno de los autorizados indicados en el apartado anterior o bien por el Responsable de la Autoridad de Registración remota. Debe presentarse vía interfaz web, por correo electrónico firmado digitalmente o bien personalmente según lo establecido en el apartado 9.5.1.1.

9-5-4- Actualización de repositorios

Una vez recibida una solicitud de revocación y efectuada la validación de la identidad del solicitante, el repositorio indicando el estado de los certificados se actualizará de inmediato.

Todas las solicitudes y la información acerca de los procedimientos cumplimentados deben ser archivadas, según lo dispuesto en el apartado 9.7.

9-5-5- Emisión de listas de certificados revocados

La AC-URME debe emitir listas de certificados revocados, efectuando como mínimo una actualización semanal.

Asimismo, toda vez que la AC-URME reciba una solicitud de revocación aprobada por el Responsable de la Autoridad de Registración, deberá emitir una lista de certificados revocados dentro de un plazo máximo de VEINTICUATRO (24) horas. En todos los casos, las listas de certificados revocados deben ser firmadas digitalmente por la AC-URME.

9 -6 - Auditoría - Procedimientos de seguridad

Todos los hechos significativos que afecten la seguridad del sistema de la AC-URME deben ser almacenados en archivos de transacciones de auditoría.

Serán conservados en el ámbito de la AC-URME al menos durante un año.

Posteriormente, serán archivados en un lugar físico protegido hasta completar un período mínimo de DIEZ (10) años.

9 -7 - Archivos

9-7-1- Información a ser archivada

La AC-URME debe conservar información acerca de:

a) Solicitudes de certificados y toda información que avale el proceso de identificación.
b) Solicitudes de revocación de certificados
c) Certificados emitidos y listas de certificados revocados.
d) Archivos de auditoría.
e) Toda comunicación relevante entre la AC-URME y los suscriptores.

9-7-2- Plazo de conservación

La información acerca de los certificados debe conservarse por un plazo mínimo de DIEZ (10) años.

9-7-3- Protección de archivos

Los medios de almacenamiento de la información deben ser protegidos física y lógicamente, utilizando criptografía cuando fuera apropiado.

9-7-4- Archivos de resguardo

Es obligación de la AC-URME la implementación de procedimientos para la emisión de copias de resguardo actualizadas, las cuales deben encontrarse disponibles a la brevedad en caso de pérdida o destrucción de los archivos.

9 -8 - Situaciones de Emergencia

9-8-1- Plan de Contingencias

La AC-URME debe implementar un plan de contingencias. Este debe garantizar el mantenimiento mínimo de la operatoria (recepción de solicitudes de revocación y consulta de listas de certificados revocados actualizadas) y su puesta en operaciones dentro de las VEINTICUATRO (24) horas de producirse una emergencia.

El plan debe ser conocido por todo el personal que cumpla funciones en la AC-URME y debe incluir una prueba completa de los procedimientos a utilizar en casos de emergencia, por lo menos una vez al año.

9-8-2- Plan de protección de claves

La AC-URME debe implementar procedimientos a seguir cuando su clave privada se vea comprometida. Deben incluirse las medidas a tomar para revocar los certificados emitidos y notificar en forma inmediata a sus suscriptores.

9-8-3- Cese de operaciones de la Autoridad Certificante

En caso de que la AC-URME cese en sus funciones, todos los suscriptores de certificados por ella emitidos deben ser notificados de inmediato.

Resulta de aplicación lo dispuesto en 9-5-1-2 último párrafo.

10 - Controles de Seguridad

10 -1 - Controles de seguridad física

10-1-1- Control de acceso

La AC-URME debe implementar controles apropiados que restrinjan el acceso a los equipos, programas y datos utilizados para proveer el servicio de certificación, solamente a personas debidamente autorizadas.

10 -2 - Controles funcionales

10-2-1- Determinación de roles

Todo el personal que tenga acceso o control sobre operaciones criptográficas que puedan afectar la emisión, utilización o revocación de los certificados, incluyendo modificaciones en el repositorio, debe ser confiable. Se inclu-

yen, entre otros, a administradores del sistema, operadores, técnicos y supervisores de las operaciones de la AC-URME.

10-2-2- Separación de funciones

Con el fin de mantener una adecuada separación de funciones, cada uno de los roles definidos en la AC-URME deben ser desempeñados por diferentes responsables.

Las designaciones deben ser notificadas por escrito a cada uno de los interesados, quienes deben dejar constancia de su aceptación.

10 -3 - Controles de seguridad personal

10-3-1- Calificación del personal

La AC-URME debe seguir una política de administración de personal que provea razonable seguridad acerca de la confiabilidad y competencia del personal para el adecuado cumplimiento de sus funciones.

10-3-2- Antecedentes

Todo el personal involucrado en la operatoria de la AC-URME debe ser sometido a adecuados procesos de investigación que permitan demostrar su confiabilidad y competencia para las funciones a cumplir.

Esta investigación es obligatoria como paso previo al inicio de la relación laboral.

10-3-3- Entrenamiento

Todo el personal de la AC-URME debe tener acceso a toda la documentación técnica pública que sea emitida y aprobada en respaldo de los procesos de emisión, actualización y revocación de los certificados, así como sobre aspectos funcionales del sistema informático.

10 -4 - Controles de seguridad lógica

10-4-1- Generación e instalación de claves

10-4-1-1- Generación

El par de claves del suscriptor de un certificado emitido en los términos de esta política debe ser generado de manera tal que su clave privada se encuentre bajo su exclusivo y permanente conocimiento y control. El suscriptor es considerado titular del par de claves; como tal, debe generarlo en un sistema

confiable, no debe revelar su clave privada a terceros bajo ninguna circunstancia y debe almacenarla en un medio que garantice su confidencialidad.

10-4-1-2- Envío de la clave pública

La clave pública del suscriptor del certificado debe ser transferida a la AC-URME de manera tal que asegure que:

a) No pueda ser cambiada durante la transferencia.
b) El remitente posea la clave privada que corresponde a la clave pública transferida.
c) El remitente de la clave pública sea el suscriptor del certificado.

El requerimiento de un certificado debe emitirse en formato PKCS#10. según se establece en los Estándares sobre Tecnología de Firma Digital para la Administración Pública Nacional o bien en el que se establezca en futuras ediciones de los mismos.

10-4-1-3- Características criptográficas

En los Estándares sobre Tecnología de Firma Digital para la Administración Pública Nacional adoptados por la provincia se define:

a) Los tipos de algoritmos de firma aceptables.
b) Las longitudes mínimas de clave aceptables de las Autoridades Certificantes y de los suscriptores.

El algoritmo de firma utilizado por la AC-URME es SHA-1 con RSA. según se establece en los Estándares sobre Tecnología de Firma Digital para la Administración Pública Nacional adoptados por la provincia o bien en el que se establezca en futuras ediciones de los mismos.

En caso de conocerse un mecanismo que vulnere cualquiera de los algoritmos mencionados en las longitudes indicadas, es obligación de la AC-URME revocar todos los certificados comprometidos y notificar a suscriptores.

10-4-2- Protección de la clave privada

La AC-URME debe proteger su clave privada de acuerdo con lo previsto en esta política.

10-4-2-1- Estándares criptográficos

La generación y almacenamiento de claves y su utilización deben efectuarse utilizando un equipamiento técnicamente confiable que cumpla con los estándares aprobados por la Subsecretaría de la Gestión Pública de la Jefatura de Gabinete de Ministros para la Administración Pública Nacional adoptados por la provincia.

10-4-2-2- Destrucción de la clave privada

Si por cualquier motivo deja de utilizarse la clave privada de la AC-URME para crear firmas digitales, la misma debe ser destruida.

10-4-3- Otros aspectos del manejo de claves

10-4-3-1- Reemplazo de claves

El par de claves de la AC-URME debe ser reemplazado cuando las mismas hayan sido vulneradas o exista presunción en tal sentido.

10-4-3-2- Restricciones al uso de claves privadas

La clave privada de la AC-URME empleada para emitir certificados según los lineamientos de esta política debe utilizarse para firmar certificados a favor de suscriptores. Adicionalmente, la mencionada clave sólo puede usarse para firmar listas de certificados revocados.

10-4-4- Controles de seguridad del computador

Todos los servidores de la AC-URME incluyen los controles de seguridad enunciados en los Estándares sobre Tecnología de Firma Digital para la Administración Pública Nacional adoptados por la provincia de Mendoza .

10-4-5- Controles de seguridad de conectividad de red

Los servicios que provee la AC-URME que deban estar conectados a una red de comunicación pública, deben ser protegidos por la tecnología apropiada que garantice su seguridad. Además, debe asegurarse que se exija autorización de acceso a todos los servicios que así lo requieran.

11- Certificados y listas de certificados revocados

Características

Todos los certificados que hacen referencia a esta política se emiten en formato X509 versión 3 o superior según se establece en los Estándares sobre

Tecnología de Firma Digital para la Administración Pública Nacional adoptados por la provincia o bien en el que se establezca en futuras ediciones de los mismos. Los certificados incluyen una referencia que identifica la política aplicable.

Las listas de certificados revocados se emiten en formato X509 versión 2. según se establece en los Estándares sobre Tecnología de Firma Digital para la Administración Pública Nacional adoptados por la provincia o bien en el que se establezca en futuras ediciones de los mismos.

12 - Administración de esta política

12 -1 - Cambios a la política

12-1-1- Listado de propuestas

La AC-URME informará a los suscriptores de certificados acerca de todos aquellos cambios significativos que se efectúen a esta Política. Las modificaciones indicadas serán publicadas en el sitio web de la AC-URME .

12 -2 - Publicación y notificación

Una copia de esta política de certificación y de sus versiones anteriores se encuentra disponible en la interfaz web de la AC-URME.

V. Manual de Procedimientos

Autoridad Certificante

Gobernación de Mendoza

Secretaría Administrativa Legal y Técnica

Unidad de Reforma y Modernización del Estado

1- Introducción

El presente manual describe el conjunto de procedimientos utilizados por la Autoridad Certificante de la Administración Pública de la Provincia de Mendoza cuyas funciones son ejercidas por la Unidad de Reforma y Modernización del Estado de la Secretaría Administrativa Legal y Técnica de la Gobernación (en adelante AC-URME) en el cumplimiento de sus responsabilidades de emisión y administración de certificados de clave pública emitidos a favor de sus suscriptores.

Este Manual de Procedimientos forma parte de la documentación técnica emitida por la AC-URME junto con los siguientes documentos:

- Política de Certificación
- Política de Seguridad
- Plan de Contingencias
- Plan de Cese de Actividades.

2- Definición de roles

Para el cumplimiento de sus funciones, la AC-URME define los siguientes roles en su estructura:

a) Operador Técnico de la AC-URME

b) Responsable de la Autoridad de Registración de la AC-URME

c) Oficial Certificador de la AC-URME

d) Sustitutos de los anteriormente mencionados

e) Responsable de Seguridad Informática

El responsable de la AC-URME es el Coordinador de la Unidad de Reforma y Modernización del Estado de la Secretaría Administrativa Legal y Técnica de la Gobernación, o bien el funcionario que fuera designado a tal efecto.

2.1. - Funciones del Operador Técnico de la AC -ONTI

a) Administrar los recursos informáticos que integran la estructura de la AC-URME.

b) Habilitar la intervención digital del Responsable de la Autoridad de Registración y del Oficial Certificador en los procesos de emisión y revocación de certificados

c) Archivar las copias de resguardo generadas por el sistema y la copia del software de la AC-URME

c) Implementar y cumplir los procedimientos de seguridad.

2.2. - Funciones del Responsable de la Autoridad de Registración local

a) Recibir las solicitudes de nuevos certificados para suscriptores.

b) Verificar los datos de identidad y de competencia del solicitante.

c) Aprobar la emisión del certificado solicitado.

d) Aprobar la revocación de certificados

e) Archivar la información respaldatoria.

En caso de utilizarse un esquema de Autoridades de Registración remotas, según se indica en el apartado 3.2.2, las funciones mencionadas serán cumplidas por el Responsable de la Autoridad de Registración remota.

2.3. - Funciones del Oficial Certificador

a) Ser el depositario de la clave privada de la AC-URME.

b) Firmar digitalmente los certificados de los suscriptores.

d) Firmar digitalmente las listas de certificados revocados (CRLs).

2.4. - Funciones del Responsable de Seguridad Informática

Las funciones del Responsable de Seguridad Informática se definen en la Política de Seguridad de la AC-URME

2.5. - Designación

Cada uno de los responsables de los roles mencionados será designado por Disposición de la máxima autoridad de la Unida de Reforma y Modernización del Estado, comunicándose dicho nombramiento a cada una de las partes involucradas. Estas deberán notificarse debidamente, manifestando por escrito su aceptación del cumplimiento de las obligaciones inherentes a su función.

2.6. - Entrega de los dispositivos criptográficos

Al momento de la entrega de los dispositivos criptográficos a los distintos responsables (Oficial Certificador y Responsable de la Autoridad de Registración) se procederá a labrar un acta como respaldo.

El Oficial Certificador y el Responsable de la Autoridad de Registración deben conservar los dispositivos criptográficos bajo su absoluto y exclusivo control, para lo cual cumplirán los procedimientos indicados en el Manual de Procedimientos de Seguridad. El Oficial Certificador sólo utilizará el dispositivo criptográfico de firma en presencia de otro funcionario designado según lo establecido en el apartado anterior.

2.7. - Funcionarios sustitutos

Los funcionarios designados como sustitutos para cubrir los roles descriptos en el apartado 2 reemplazarán a los responsables mencionados en caso de ausencia temporaria de éstos. El reemplazo continuará hasta tanto el responsable ausente se reintegre a sus actividades o se nombre un nuevo titular. El procedimiento a seguir se encuentra definido en el Plan de Contingencias.

2.8. - Cese de funciones

En caso de renuncia de alguno de los responsables, remoción en su cargo o cambio en el rol asignado, el sustituto designado lo reemplazará en

forma permanente. En estos casos el responsable que no continúe con sus actividades debe entregar el dispositivo criptográfico que tenga en su poder al responsable de la AC-URME. Se procederá asimismo a la destrucción de las claves de activación correspondientes al dispositivo y a su copia de resguardo, a la entrega del dispositivo al nuevo responsable, a la generación de la nueva clave de activación y a la entrega de la copia de resguardo y clave de activación al responsable de su custodia.

Todo lo actuado deberá figurar en un acta que será firmada por los responsables intervinientes y por el responsable de la AC-URME.

Toda nueva designación para cubrir los roles mencionados en el apartado 2 así como cualquier modificación en los servicios brindados o documentación técnica a utilizar debe ser aprobada por el responsable de la AC-URME y notificada según lo indicado en el presente apartado.

3- Solicitud de emisión del certificado

3.1. - Iniciación del proceso

Todo suscriptor de un certificado en los términos del presente documento debe iniciar el trámite de solicitud ingresando al sitio web de la AC-URME. Debe completar el formulario de solicitud de certificado, incluyendo sus datos identificatorios, generar su propio par de claves y remitir todo el conjunto de datos en formato PKCS#10 a la AC-URME.

El solicitante obtendrá el valor de la función de hash SHA-1 para la clave pública del requerimiento de certificado en formato PKCS#10. Este código identificatorio le será pedido para validar su identidad y la integridad de la solicitud ante la AC-URME.

El procedimiento indicado debe ser cumplido por todos los suscriptores de certificados, independientemente del esquema de identificación utilizado por la AC-URME según se describe en los apartados siguientes.

3.2. - Validación de la identidad del solicitante

Los procedimientos a utilizar para la identificación de los solicitantes de certificados diferirán en función de los distintos esquemas de registración admitidos por la AC-URME.

3.2.1.- Registración centralizada

3.2.1.1.- Verificación de datos por la Autoridad de Registración local

En este caso, el Responsable de la Autoridad de Registración local tiene a su cargo la verificación de los datos del suscriptor. Este debe iniciar el pedido de emisión del certificado, ingresando al sitio web de la AC-URME, completando el formulario de solicitud de certificado, generando su par de claves y remitiendo datos y clave pública a la AC-URME.

Posteriormente debe presentarse personalmente ante el Responsable de la Autoridad de Registración local, con nota firmada por el máximo responsable de la Oficina de Recursos Humanos del organismo al que pertenece, certificada por su Mesa de Entradas, Salidas y Archivo. En la nota deberá especificarse:

a) Nombre y Apellido

b) Documento de Identidad (DNI u otro de validez nacional)

c) Jurisdicción/Organismo/Dependencia/Cargo

Deberá presentar además su documento de identidad (original y fotocopia) y el código de identificación del requerimiento.

El Responsable de la Autoridad de Registración local verificará:

a) Que el documento corresponde a la persona que se presentó.

b) Que dicha persona es aquella cuyos datos figuran en la nota presentada. A tal fin debe cotejar los datos del documento con los que figuran en la mencionada nota. Verificará que la misma haya sido certificada por la Mesa de Entradas, Salidas y Archivo del organismo.

c) Que el código de identificación del requerimiento coincide con el cálculo de la función de hash SHA-1 aplicada a la solicitud que será utilizada para la emisión del certificado (ver apartado 4). El Responsable de la Autoridad de Registración local está facultado para solicitar cualquier ti-

po de documentación adicional que considere necesaria a efectos de cumplimentar el proceso de identificación.

Efectuada la validación de identidad, el Responsable de la Autoridad de Registración local devolverá el documento de identidad al solicitante, inicialará la fotocopia del mismo y la nota presentada, en prueba de conformidad. Posteriormente, procederá a archivar toda la documentación de respaldo según lo previsto en el apartado 12.

Cumplida la etapa de validación de la identidad del solicitante, el Responsable de la Autoridad de Registración local puede:

a) Aprobar la emisión del certificado.

b) Suspender el requerimiento, si no se han reunido elementos de juicio suficientes para validar la identidad del solicitante según los procedimientos indicados. En este caso se informará al solicitante acerca de los elementos necesarios para finalizar satisfactoriamente el proceso de validación de su identidad. El solicitante tendrá un plazo de DIEZ (10) días para proveer la información complementaria que se le solicite, vencido el cual deberá reiniciar el proceso de solicitud de emisión del certificado, efectuando un nuevo requerimiento de emisión.

En caso que el proceso de validación de la identidad del solicitante no hubiera finalizado satisfactoriamente, debe dejarse constancia de lo acontecido en un acta que será firmada por el Responsable de la Autoridad de Registración local y el solicitante cuya identidad no se hubiera podido verificar. En ella se indicará el plazo para la nueva presentación. Se efectuarán dos copias del acta, entregándose un ejemplar al solicitante quien acusará recibo. El otro ejemplar y el acuse de recibo de la copia serán archivados por el Responsable de la Autoridad de Registración local.

Si el proceso de validación de identidad ha sido exitoso, interviene el Oficial Certificador quien procede a verificar el cumplimiento de las distintas instancias del proceso, haciéndolo constar en la documentación recibida. A continuación, se iniciará el proceso de emisión del certificado.

3.2.1.2.- Verificación de datos vía área de recursos humanos

Definimos los siguientes roles en el proceso de validación de la identidad:

a) El Responsable de la Autoridad Registración local, quien validará la identidad del suscriptor.

b) El Responsable del área de Recursos Humanos del organismo, quien será encargado de validar los datos complementarios del suscriptor (jurisdicción, organismo, dependencia y cargo del suscriptor del certificado).

De ser necesario, el responsable mencionado podrá ser reemplazado por otro funcionario perteneciente al área de Recursos Humanos. Este debe ser designado mediante nota firmada por el máximo responsable de la misma, intervenida por la Mesa de Entradas, Salidas y Archivo del organismo donde ésta resida. En la nota debe nombrarse al funcionario o agente como responsable de la verificación de los datos complementarios del suscriptor, incluyendo su dirección de correo electrónico.

El procedimiento a seguir para la emisión del certificado del funcionario de la Oficina de Recursos Humanos seguirá los pasos indicados en el apartado anterior.

El suscriptor debe iniciar la solicitud de emisión del certificado, ingresando al sitio web de la AC-URME y completando el formulario de requerimiento, generando su par de claves y remitiendo datos y clave pública a la AC-URME.

El Responsable de la Autoridad de Registración local recibirá la solicitud y enviará un formulario digital firmado digitalmente solicitando la verificación de los datos complementarios al responsable del área de Recursos Humanos. Si los datos son correctos, éste lo especificará en el campo Anexo y devolverá el formulario recibido firmándolo digitalmente.

En caso que los datos complementarios hayan sido verificados correctamente, el Responsable de la Autoridad de Registración local convocará al suscriptor quien deberá presentarse portando documento de identidad y fotocopia y el código de identificación del requerimiento. El Responsable de la Autoridad de Registración local verificará:

a) Que el documento corresponde a la persona que se presentó.

b) Que dicha persona es aquella cuyos datos figuran en el formulario digital validado por el responsable del área de Recursos Humanos. A tal fin debe cotejar los datos del documento con los que figuran en dicho formulario.

c) Que el código de identificación del requerimiento coincide con el cálculo de la función de hash SHA-1 aplicada a la solicitud que será utilizada para la emisión del certificado (ver apartado 4) Efectuada la validación de identidad, el Responsable de la Autoridad de Registración local devolverá el documento de identidad al solicitante, inicialará la fotocopia del mismo y el formulario recibido, en prueba de conformidad. Posteriormente, procederá a archivar toda la documentación de respaldo según lo previsto en el apartado 12.

Cumplida la etapa de validación de la identidad del solicitante, se continuará con el proceso de emisión del certificado según lo establecido en el apartado anterior.

En caso de que existieran discrepancias en los datos recibidos, el responsable del área de Recursos Humanos lo especificará en el campo Anexo y devolverá el formulario firmado digitalmente. En tal caso, el Responsable de la Autoridad de Registración local se contactará con el solicitante, a fin de que éste convalide la corrección y efectúe un nuevo requerimiento de certificado. Se dejará constancia escrita de lo actuado, firmada por el Responsable de la Autoridad de Registración local.

3.2.1.3.- Procedimientos de excepción

En casos de excepción, se utilizarán los procedimientos indicados a continuación a fin de validar la identidad del suscriptor:

3.2.1.3.1.- Verificación de identidad a través del responsable del organismo

Excepcionalmente se admitirá la emisión del certificado sin la concurrencia personal del suscriptor ante el Responsable de la Autoridad de Registración local. En tal caso, el suscriptor debe completar el formulario de solicitud de cer-

tificado a través de la interfaz web, generando su par de claves y remitiendo datos y clave pública a la AC-URME.

El suscriptor debe presentarse personalmente ante la máxima autoridad del organismo al que pertenece a fin de efectuar la validación de su identidad. Para ello debe acompañar su documento de identidad (original y fotocopia) y una nota firmada por el máximo responsable del área de Recursos Humanos del organismo, o bien de un funcionario perteneciente a dicha oficina nombrado según lo dispuesto en 3.2.1.2, consignando los siguientes datos:

a) Nombre y Apellido

b) Documento de Identidad

c) Jurisdicción/Organismo/Dependencia/Cargo

d) Código de identificación del requerimiento del certificado

Efectuada la validación, la máxima autoridad del organismo remitirá al Responsable de la Autoridad de Registración local una nota firmada e intervenida por Mesa de Entradas, Salidas y Archivo en la que indicará su conformidad con la información recibida del suscriptor, informando el código de identificación del requerimiento. El Responsable de la Autoridad de Registración local verificará la nota recibida y la correspondencia de los datos informados con los que figuraban en el requerimiento. De ser correcta la verificación, archivará la documentación de respaldo y continuará con el proceso de emisión del certificado según lo previsto en el apartado 3.2.1.1.

3.2.1.3.2.- Servicio de registración itinerante

En caso que la aprobación de la emisión del certificado sea requerida en el lugar de trabajo del funcionario solicitante, el Responsable de la Autoridad de Registración local debe concurrir a la misma a efectos de efectuar la validación de la identidad del suscriptor.

El funcionario solicitante debe completar a través de la interfaz web el formulario de solicitud de certificado, generando su par de claves y remitiendo datos y clave pública a la AC-URME.

El funcionario solicitante debe presentar su nombramiento (Decreto o Resolución), su documento de identidad (original y fotocopia) y copia del código de identificación del requerimiento del certificado.

Firmará la fotocopia de su documento y la copia del código mencionado, acreditando haber efectuado el requerimiento. El Responsable de la Autoridad de Registración verificará que el documento corresponde al funcionario, inicialando su fotocopia en prueba de validez.

Efectuadas las mencionadas verificaciones, el Responsable de la Autoridad de Registración local accederá a través de una conexión segura a la AC-URME, a fin de efectuar la aprobación de todos los atributos del requerimiento, continuándose con el proceso de emisión del certificado.

3.2.2.- Registración Descentralizada

Podrá admitirse la existencia de Autoridades de Registración fuera del organismo donde reside la AC-URME. En tal caso, la Autoridad de Registración que se constituya tendrá a su cargo el proceso de validación personal de la identidad de los suscriptores de certificados que se postulen por su intermedio.

A fin de cumplir con los procedimientos de validación de identidad de los suscriptores, deberá designar un funcionario Responsable de la Autoridad de Registración remota y su correspondiente sustituto. Ambos deben ser designados por Resolución de la máxima autoridad del organismo donde se constituya la Autoridad de Registración, informándose a la AC-URME de tal nombramiento.

Asimismo, las Autoridades de Registración constituidas en forma remota podrán recibir la colaboración de Auxiliares, quienes colaborarán en el proceso de validación de la identidad de los suscriptores de certificados. Los mencionados auxiliares serán designados por Resolución de la máxima autoridad del organismo donde se constituyan.

Los procedimientos de designación de los responsables mencionados y de validación de la identidad de los suscriptores que utilicen el presente esquema de registración son los siguientes:

3.2.2.1.- Procedimiento de designación del responsable de la Autoridad de Registración remota (RARR)

1. Funcionario responsable de la Autoridad de Registración remota

a) Ingresa al sitio web de la AC-URME

b) Efectúa el requerimiento y genera su par de claves.

c) Envía el requerimiento a la AC-URME. Obtiene una nota de confirmación de su recepción, que incluye:

Datos personales

Código de identificación del requerimiento

a) Obtiene una nota de aceptación de condiciones y responsabilidades inherentes al cumplimiento de la función de RARR.

b) Imprime y firma ambas notas (confirmación y aceptación).

2. Máxima autoridad del organismo

a) Recibe la nota de confirmación de recepción del requerimiento del funcionario designado como RARR.

b) Emite la designación (Resolución u otro nombramiento según lo establecido en 3.2.2) del funcionario como RARR, incluyendo:

- Nombre y Apellido del funcionario designado
- Organismo al que pertenece
- Cargo

a) La máxima autoridad del organismo o el funcionario competente que hubiera firmado la designación deberán asimismo intervenir la nota de confirmación, acreditando de tal forma que el requerimiento fuera efectuado por el RARR designado. Opcionalmente, podrán incluir el código de identificación del requerimiento y la mencionada acreditación en el nombramiento.

El nombramiento firmado por funcionarios competentes, la nota de aceptación y de confirmación son remitidas a la AC-URME

3. AC-URME:

Responsable de la Autoridad de Registración Local (RARL)

a) Recibe el nombramiento y las notas de aceptación y de confirmación

b) Verifica su integridad, la coincidencia de los datos indicados en ambas notas y las firmas indicadas en 2.

c) Verifica que el código identificatorio del requerimiento informado en la nota de confirmación coincida con el cálculo de la función de hash SHA-1 aplicada a la solicitud que será utilizada para la emisión del certificado.

d) Si la verificación es exitosa aprueba los atributos del requerimiento, aprobando la emisión del certificado para el RARR.

e) Por último, archiva la documentación de respaldo del proceso de validación de identidad (nombramiento, nota de confirmación y nota de aceptación).

Oficial Certificador

Firma el nuevo certificado incorporándolo a la lista de Autoridades de Registración habilitadas, informando al RARR de la emisión del certificado a través de un mensaje de correo electrónico firmado digitalmente.

3-2-2-2- Procedimiento de solicitud de certificados ante el RARR

4. Solicitante

a) Ingresa al sitio web de la AC-URME.

b) Efectúa el requerimiento y genera su par de claves.

c) Envía el requerimiento a la AC-URME. Obtiene una nota de confirmación de su recepción, que incluye:

- Nombre y Apellido del solicitante
- Organismo al que pertenece
- Cargo
- Código de identificación del requerimiento

d) Imprime y firma la nota recibida.

e) Valida su identidad personalmente ante el RARR presentando la nota de confirmación firmada y su documento de identidad.

5. Responsable de la Autoridad de Registración Remota

a) Verifica integridad de la nota de confirmación.

b) Valida la identidad del solicitante mediante la verificación de su documento de identidad.

c) Firma la nota como constancia de verificación de la identidad del solicitante y de la realización del requerimiento.

d) Verifica la validez de los datos que figuran en la nota y su correspondencia con los que figuran en la interfaz web, incluyendo el código de identificación del requerimiento.

e) Si los controles son exitosos, aprueba la emisión del certificado.

f) Informa la aprobación a la AC-URME a través un correo electrónico firmado digitalmente.

g) Archiva la documentación de respaldo del proceso de validación (nota de confirmación y fotocopia de documento de identidad).

6. AC-URME

Oficial Certificador

a) Recibe la aprobación.

b) Firma el nuevo certificado informando al suscriptor acerca de su emisión a través de un mensaje de correo electrónico firmado digitalmente.

En caso de constituir Autoridades de Registración en jurisdicción de los Poderes Judiciales provinciales, se admitirá la intervención del Secretario del Juzgado a fin de firmar la nota de confirmación como constancia de realización de los controles indicados en 3.2.2.2.2.a y 3.2.2.2.2.b A continuación, remitirá la nota mencionada al RARR, continuando el proceso de emisión con los procedimientos previstos. Si el solicitante fuera el titular del Juzgado, la nota de confirmación podrá ser firmada por dicho funcionario, remitiéndola posteriormente al RARR.

Este procedimiento alternativo será de aplicación en el proceso de solicitud de certificados ante el auxiliar del RARR (apartados 3-2-2-4-2-a y 3-2-2-4-2-b).

3-2-2-3- Designación de auxiliares del RARR

1. Auxiliar del RARR

a) Ingresa al sitio web de la AC-URME.

b) Efectúa el requerimiento y genera su par de claves.

c) Envía el requerimiento a la AC-URME. Obtiene una nota de confirmación de su recepción, que incluye:

- Datos personales
- Código de identificación del requerimiento
- Obtiene una nota de aceptación de condiciones y responsabilidades inherentes al cumplimiento de la función de auxiliar del RARR en el proceso de validación.
- Imprime y firma ambas notas (confirmación y aceptación).

2. Máxima autoridad del organismo donde se constituye el auxiliar del RARR.

a) Recibe la nota de confirmación del funcionario designado como auxiliar del RARR.

b) Emite designación (Resolución u otro nombramiento según lo establecido en 3.2.2) del funcionario como RARR, incluyendo:

- Nombre y Apellido del funcionario designado.
- Organismo.
- Cargo.

a) La máxima autoridad del organismo o el funcionario competente que hubiera firmado la designación deberán asimismo intervenir la nota de confirmación, verificando la validez de los datos incluidos en ella y su correspondencia con los que figuran en la interfaz web, acreditando de tal forma que el requerimiento fuera efectuado por el RARR designado. Opcionalmente, podrán incluir el código de identificación del requerimiento y la mencionada acreditación en el nombramiento.

El nombramiento firmado por funcionarios competentes y la nota de aceptación y de confirmación son remitidas al RARR de la jurisdicción.

3. Responsable de la Autoridad de Registración Remota

a) Recibe el nombramiento y la nota de aceptación y de confirmación

b) Verifica su integridad, la coincidencia de los datos indicados en ambas notas y las firmas indicadas en 2.

c) Verifica que el código identificatorio del requerimiento informado en la nota de confirmación coincida con el cálculo de la función de hash SHA-1 aplicada a la solicitud que será utilizada para la emisión del certificado.

d) Si la verificación es exitosa aprueba los atributos del requerimiento, aprobando la emisión del certificado para el RARR.

e) Archiva la documentación respaldatoria del proceso de validación (nombramiento y notas de confirmación y aceptación).

4. AC-URME

Oficial Certificador

a) Recibe la autorización

b) Firma el nuevo certificado informando al Auxiliar del RARR acerca de su emisión a través de un mensaje de correo electrónico firmado digitalmente.

3-2-2-4- Procedimiento de solicitud de certificados ante el Auxiliar del RARR

5. Solicitante

a) Ingresa al sitio web de la AC-URME

b) Efectúa el requerimiento y genera su par de claves.

c) Envía el requerimiento a la AC-URME. Obtiene una nota de confirmación de su recepción, que incluye:

- Nombre y Apellido del solicitante
- Organismo al que pertenece
- Cargo
- Código de identificación del requerimiento

d) Imprime y firma la nota obtenida.

e) Valida su identidad personalmente ante el auxiliar del RARR presentando la nota de confirmación firmada y su documento de identidad.

6. Auxiliar del RARR

a) Verifica integridad de la nota de confirmación

b) Valida la identidad del solicitante mediante la verificación de su documento de identidad

c) Firma la nota de confirmación como constancia de verificación de la identidad del solicitante y de la realización del requerimiento

d) Informa al RARR de su jurisdicción acerca de la verificación efectuada. A tal fin el auxiliar podrá comunicarlo:

- por correo electrónico firmado digitalmente, incluyendo todos los datos contenidos en la nota de confirmación. En este caso el auxiliar conservará la documentación de respaldo del requerimiento (nota de confirmación y fotocopia del documento de identidad)
- por correo remitiendo la nota de confirmación firmada y fotocopia del documento de identidad del solicitante. En este caso, el auxiliar conservará copia de la documentación remitida.

7. Responsable de la Autoridad de Registración Remota

a) Verifica integridad de la información recibida

b) Verifica que los datos coincidan con los atributos del certificado que figuran en la interfaz web y su coincidencia con el código de identificación del requerimiento

c) Si los controles son exitosos, aprueba la emisión de certificado

d) Informa la aprobación a la AC-URME a través un correo electrónico firmado digitalmente

e) Archiva la documentación de respaldo que hubiera recibido (nota de confirmación y fotocopia de documento de identidad) en caso de haberse cumplido el procedimiento indicado en 2.d.II.

8. AC-URME

Oficial Certificador

a) Recibe la aprobación

b) Firma el nuevo certificado informando al suscriptor acerca de su emisión a través de un mensaje de correo electrónico firmado digitalmente.

4- Emisión del certificado

Una vez finalizado exitosamente el proceso de validación de la identidad del suscriptor según los procedimientos indicados en el apartado 3, se iniciará el proceso de emisión del certificado.

Este comprende los siguientes procedimientos:

a) El Responsable de la Autoridad de Registración local accede al sistema, selecciona el requerimiento de certificado, verifica sus atributos con los que figuran en la nota presentada y controla que su código de identificación coincida con el informado. De ser exitosos los controles, ingresa su dispositivo de firma a fin de firmar la aprobación de la emisión. En caso de intervenir una Autoridad de Registración remota en la validación de la identidad del solicitante, el procedimiento mencionado será efectuado en forma remota por el Responsable de dicha Autoridad de Registración (RARR).

De utilizarse el servicio de registración itinerante previsto en el apartado 3-2-1-3-2, el procedimiento mencionado se efectuará en forma remota por el Responsable de la Autoridad de Registración local.

b) El Oficial Certificador ingresa al sistema, verificando la lista de certificados cuya emisión ha sido aprobada y aún no han sido firmados. A continuación habilita la clave privada de la AC-URME ingresando su dispositivo de firma y procede a firmar los certificados.

c) El solicitante recibirá un mensaje de correo electrónico que le informar á acerca de la emisión de su certificado.

d) Por último, se cierran todos los servicios. Se entiende que el solicitante acepta la totalidad de las obligaciones establecidas por la Política de Certificación de la AC-URME y por este Manual de Procedimientos a partir de la fecha y hora de inicio de validez del certificado emitido. En consecuencia, asume la absoluta y exclusiva responsabilidad por su utilización, y por los daños emergentes que la no observancia de la regulación pudiera implicar.

5- Contenido del certificado

El certificado de clave pública debe contener como mínimo los siguientes datos:

a) Número de versión X.509 del certificado

b) Nombre y apellido del suscriptor del certificado.

c) Localidad, provincia y país de residencia habitual.

d) Dirección de correo electrónico.

e) Clave pública del suscriptor.

f) Algoritmos de firma de la clave pública.

g) Número de serie del certificado.

h) Período de validez del certificado.

i) Nombre de la Autoridad Certificante emisora del certificado.

j) Dirección de consulta de la lista de certificados revocados (CRL).

k) URL donde se encuentra disponible esta Política de Certificación.

6- Revocación del Certificado

6 -1 - Clases de revocación

6-1-1- Revocación voluntaria:

El suscriptor de un certificado puede solicitar su revocación por cualquier motivo y en cualquier momento, para lo cual debe comunicarlo a la AC-URME siguiendo el procedimiento que establece este manual.

6-1-2- Revocación obligatoria:

Un suscriptor debe obligatoriamente pedir la revocación de su certificado cuando:

a) Se produzcan cambios en la información que el certificado contiene o ésta se desactualice.

b) La clave privada asociada al certificado de clave pública, o el medio en que se encuentre almacenada se encuentren comprometidos o corran peligro de estarlo.

c) Se produzca el cese de su relación laboral con el organismo, dependencia o institución, sin perjuicio de la obligación que le corresponde al responsable del área de Recursos Humanos del organismo donde desempeña sus funciones.

La AC-URME debe obligatoriamente revocar el certificado de un suscriptor en las siguientes situaciones:

a) A solicitud del suscriptor cuando se verifiquen los procedimientos de recepción y validación establecidos en los apartados 6.3.1 y 6.3.2 de este manual.

b) A solicitud del responsable del área de recursos humanos o de la máxima autoridad del organismo o dependencia cuando se verifiquen los procedimientos de recepción y validación establecidos en los apartados 6.3.1 y 6.3.2 de este manual.

c) Ante incumplimiento por parte del suscriptor de las obligaciones establecidas por la normativa provincial propuesta, por la Política de Certificación de la AC-URME, por este Manual de Procedimientos o cualquier otro acuerdo, regulación o ley aplicable al certificado.

d) Si toma conocimiento que existe sospecha que la clave privada del suscriptor se encuentra comprometida.

e) Si la AC-URME determina que el certificado no fue emitido de acuerdo a los lineamientos de la normativa provincial propuesta, de la Política de Certificación, de este Manual de Procedimientos o de los Estándares sobre Tecnología de Firma Digital para la Administración Pública Nacional.

En caso que el suscriptor cese en su vinculación laboral, el responsable del área de Recursos Humanos del organismo, dependencia o institución donde se desempeñara, o en su caso, el funcionario que administre el registro de personal, está obligado a informar de inmediato a la AC-URME acerca de tal situación, a fin de efectuar la correspondiente revocación.

6 -2 - Autorizados a pedir revocación

Sólo pueden pedir la revocación de un certificado:

a) El suscriptor, si se da alguno de los supuestos de revocación indicados en el apartado 6-1-2.

b) La máxima autoridad del organismo o dependencia donde se desempeñe el suscriptor o bien el responsable del área de Recursos Humanos o el funcionario que administre el registro de personal.

6 -3 - Revocación a solicitud del suscriptor o de funcionario autorizado

6-3-1- Recepción e identificación

Producida una causa de revocación del certificado, el suscriptor del certificado, o bien alguno de los responsables indicados en el apartado 6-2-b deben comunicarlo a la AC-URME..

Son aceptados los pedidos de revocación que se efectúen por los siguientes medios:

a) A través del sitio web de la AC-URME.

b) Por correo electrónico firmado digitalmente por el suscriptor, el responsable del área de Recursos Humanos o la máxima autoridad del organismo o dependencia donde aquel desempeñe sus funciones. El texto

del mensaje debe incluir los datos personales del suscriptor y la causa que origina el pedido de revocación y se dirigirá al Responsable de la Autoridad de Registración de la AC-URME, quien revocará el certificado.

c) Personalmente, presentándose alguno de los funcionarios mencionados ante el Responsable de la Autoridad de Registración de la AC-URME. Si quien concurre es el suscriptor, se dará curso al pedido de revocación en forma inmediata, previa verificación de su documento de identidad. Si quien concurre es un funcionario autorizado, debe acreditar su identidad mediante presentación de su documento de identidad y copia de su nombramiento o nota de autorización firmada por la máxima autoridad del organismo o dependencia certificada por Mesa de Entradas, Salidas y Archivo. Se acompañará una nota de solicitud de revocación firmada por la máxima autoridad del organismo o dependencia o por el responsable del área de Recursos Humanos.

d) Dada la urgencia del caso, el Responsable de la Autoridad de Registración de la AC-URME puede autorizar la revocación obviando la presentación del pedido de revocación y efectuando una confirmación telefónica de la solicitud.

6-3-2- Recepción por otros medios

El Responsable de la Autoridad de Registración se encuentra facultado para aceptar las solicitudes de revocación de certificados que reciba por otros medios (teléfono o fax). En estos casos debe verificar telefónicamente la identidad de quien efectuara el pedido de revocación, solicitando su número de documento de identidad y verificándolo con los datos del solicitante del certificado que figuran en sus archivos. De no ser posible dicha verificación, podrá aceptar la solicitud de revocación si a su juicio la urgencia de la situación lo justifica, debiendo efectuar las verificaciones que estime necesarias para validar la identidad del solicitante.

En caso de constituirse Autoridades de Registración remotas, los procedimientos de recepción de solicitudes de revocación indicados serán cumplidos por el Responsable de la Autoridad de Registración remota (RARR).

6-3-3- Procedimientos complementarios

En todos los casos en que se efectúe una revocación se labrará un acta en la que conste lo actuado en el proceso mencionado, firmada por el Responsable de la Autoridad de Registración y el Oficial Certificador. Un ejemplar del acta quedará a disposición del solicitante de la revocación; el otro ejemplar del acta quedará en poder del Responsable de la Autoridad de Registración para su archivo.

6-3-4- Actualización de repositorios de certificados revocados

Recibida y aceptada una solicitud de revocación el certificado será revocado automáticamente. El repositorio con el estado de los certificados se actualizará de inmediato.

6-3-5- Emisión de listas de certificados revocados (CRLs)

La AC-URME emite semanalmente una lista de certificados revocados actualizada.

Asimismo, toda vez que se produzca una revocación, la AC-URME emite una lista de certificados revocados actualizada en un plazo máximo de VEINTICUATRO (24) horas de aceptada la solicitud.

Dicha lista indica claramente la fecha y la hora de la última actualización.

El Oficial Certificador de la AC-URME es el responsable de firmar digitalmente la lista de certificados revocados, pudiendo utilizar el mismo par de claves utilizado para firmar certificados.

El acceso a las listas de certificados revocados es público, no pudiendo establecerse ninguna clase de restricción. Se encuentra disponible en el sitio web de la AC-URME.

6 -4 - Revocación decidida por la AC-URME

Si la AC-URME toma conocimiento, por cualquier medio que fuera, acerca de irregularidades cometidas por el suscriptor de un certificado, las cuales, a su juicio, impliquen un posible incumplimiento de sus obligaciones que puedan originar causales de revocación, debe iniciar de inmediato la investigación pertinente.

En caso de confirmar dicho incumplimiento, la AC-URME procede a revocar de inmediato el certificado comprometido.

De toda denuncia o notificación que se reciba e investigación que se inicie, así como sus resultados, debe dejarse documentación respaldatoria asentada en archivos que estarán a disposición del Organismo Auditante. Lo mismo debe hacerse con los incumplimientos que se detecten y que motiven revocación de certificados.

7- Expiración del certificado

Todos los certificados emitidos por la AC-URME a favor de suscriptores tienen un período de vigencia de UN (1) año, contados a partir de la fecha de emisión. Esta información consta expresamente en el certificado.

Transcurrido el plazo mencionado, el certificado expirará automáticamente, perdiendo toda validez.

En tal caso, el suscriptor debe gestionar uno nuevo, para lo cual iniciará el correspondiente proceso de solicitud de emisión.

7 -1 - Renovación de certificados

Un suscriptor puede solicitar la renovación de su certificado dentro de los TREINTA (30) días anteriores a la fecha de su vencimiento. La utilización de este procedimiento de renovación evitará que aquel deba presentar nuevamente la documentación necesaria para emitir un certificado nuevo. El período de validez del certificado renovado se extenderá por UN (1) año a partir de la fecha de la renovación. El suscriptor efectuará su solicitud de renovación vía interfaz web, identificándose con su certificado vigente. El Responsable de la Autoridad de Registración recibe las solicitudes de renovación, verificando que el certificado a renovar se encuentra vigente. Efectuado el control mencionado, aprobará la renovación, interviniendo el Oficial Certificador quien emitirá el nuevo certificado que tendrá la misma clave pública que el certificado vencido.

En caso de constituirse Autoridades de Registración remotas, los procedimientos de recepción de solicitudes de renovación indicados serán cumplidos por el Responsable de la Autoridad de Registración remota (RARR).

8- Responsabilidades

8 -1 - Responsabilidad de la AC-URME

En el cumplimiento de sus funciones relativas a la emisión y administración de certificados, la AC-URME garantiza:

a) Que el certificado ha sido emitido siguiendo las pautas establecidas en el Manual de Procedimientos para la validación de los datos en él incluidos.

b) Que el certificado satisface todos los requisitos exigidos por los Estándares sobre Tecnología de Firma Digital adoptados por la Provincia.

c) Que los algoritmos y longitudes de claves utilizados cumplen con la última versión aprobada de los Estándares sobre Tecnología de Firma Digital adoptados por la Provincia.

d) Que el certificado será publicado de acuerdo a lo dispuesto en la Política de Certificación.

8 -2 - Responsabilidad de la Autoridad de Registración remota

a) Dar cumplimiento a los procedimientos establecidos en la Política de Certificación de la AC-URME, de este Manual de Procedimientos y de las normas reglamentarias sobre firma digital.

b) Mantener el control de su clave privada e impedir su divulgación.

c) Solicitar la inmediata revocación de su certificado en caso de compromiso de la clave privada.

d) Resguardar el secreto de su clave privada aún en caso de que el certificado se encuentre expirado.

e) Solicitar la inmediata revocación de su certificado en caso de producirse algún cambio en su situación laboral que implique la discontinuidad de su función como Responsable de la Autoridad de Registración remota (RARR).

f) Mantener actualizados los certificados emitidos

g) Permitir las auditorías y controles necesarios para garantizar la seguridad de la operatoria del sistema.

h) Mantener el archivo y resguardo de la información

i) Mantener la debida confidencialidad respecto a toda información recibida durante el desempeño de su función, cumpliendo las previsiones establecidas en el apartado 9.

8 -3 - Responsabilidad de los Suscriptores

Es responsabilidad de los suscriptores de certificados mantener informada a la AC-URME acerca de cualquier cambio en la información que se incluya en los mismos. En particular el suscriptor es responsable de informar a la AC-URME acerca del cese de su relación laboral con el organismo o dependencia del que dependiera al momento de efectuar la solicitud del certificado. Las responsabilidades mencionadas se hacen extensivas al responsable del área de Recursos Humanos del organismo o dependencia del que dependiera el suscriptor o al funcionario que administre el registro de personal.

9- Confidencialidad

La información referida a los suscriptores recibida o generada por la AC-URME puede clasificarse en:

a) No confidencial: la información que obligatoriamente debe figurar en el certificado según lo indicado en la Política de Certificación.

b) Confidencial: toda otra información recibida o generada por la AC-URME en el proceso de identificación, emisión y administración del certificado, no incluida en el mismo, así como cualquier otra información vinculada a la operatoria de la AC-URME.

La información considerada confidencial no puede ser revelada por la AC-URME a terceros bajo ninguna circunstancia, excepto que se dé alguno de los siguientes supuestos:

a) Que exista consentimiento previo del suscriptor para su divulgación.

b) Esta autorización debe otorgarse a través de un mensaje de correo electrónico firmado digitalmente por el suscriptor o bien personalmente por éste, debiendo validar su identidad siguiendo los procedimientos previstos en el apartado 3-2-1-1 en cuanto sean pertinentes.

c) Que la información sea requerida legalmente, por orden judicial emanada de juez competente.

Toda solicitud de información confidencial que se reciba es archivada por el Responsable de la Autoridad de Registración en las condiciones establecidas en el apartado 12.

La información acerca de las causas de la revocación de un certificado es considerada confidencial y sujeta a las mencionadas restricciones informativas.

El deber de confidencialidad debe notificarse por escrito a todo el personal, como requisito de su designación.

10- Interpretación y obligatoriedad

La interpretación de toda la documentación técnica emitida por la AC-URME se encuentra sometida a lo dispuesto en la reglamentación provincial propuesta.

Las disposiciones contenidas en los documentos indicados emitidos en acuerdo a la normativa mencionada son de aplicación obligatoria para los sujetos involucrados. Se considera que éstos se han notificado de tal circunstancia a partir de la fecha y hora de inicio de validez del certificado emitido.

Toda discrepancia respecto de la interpretación y/o aplicación de las políticas y procedimientos, así como los conflictos que pudieran suscitarse entre la AC-URME y el suscriptor del certificado, serán resueltos por la Autoridad de Aplicación

11- Auditorías

El propósito de las auditorías es verificar que las Autoridades Certificantes implementen un sistema que asegure la calidad de los servicios de certificación, cumpliendo con los lineamientos establecidos en su documentación técnica.

11 -1 - Archivos de Auditoría

La AC-URME mantiene un sistema de archivos de transacciones de auditoría que permita mantener en un entorno de seguridad toda la información considerada relevante que pueda ser requerida oportunamente por el Organismo Auditante.

El sistema prevé la generación de:

a) Logs del sistema

Se mantiene un registro de logs que incluye información sobre los siguientes eventos:

- Encendido y apagado del equipo
- Ingreso y salida del sistema de cada usuario
- Programas ejecutados
- Acceso a los objetos del sistema (base de passwords, base de datos de certificados)
- Cambios en los archivos o políticas de definición de logs

Para cada uno de estos eventos, se conserva la siguiente información mínima:

- Usuario
- Fecha y hora
- Tipo de evento
- Datos particulares del evento

b) Registros de transacciones de auditoría que permitan el seguimiento de las distintas etapas del ciclo de vida de los certificados.

c) Copia de la documentación respaldatoria del proceso de validación de identidad de los suscriptores.

Todos los archivos (digitales o en soporte papel) que respalden las transacciones deben encontrarse actualizados en forma permanente y a disposición del Organismo Auditante.

Los archivos de auditoría son generados por el Operador Técnico de la AC-URME. Se conservan bajo llave bajo la responsabilidad del Responsable de Seguridad Informática. Este tendrá en su poder un juego de llaves, junto al Operador Técnico y su sustituto. Una copia de la misma se encuentra en poder del responsable de la AC-URME. Debe quedar constancia de los datos de quienes poseen una copia de las llaves. Los archivos de transacciones de auditoría sólo pueden ser visualizados por representantes de dicho organismo.

Los archivos deben conservarse en un espacio físico acondicionado dentro del ámbito de la AC-URME por un plazo mínimo de DIEZ (10) años. Aquellos con antigüedad mayor a un año pueden trasladarse a un archivo se-

cundario en un lugar físico protegido manteniendo las mismas medidas de seguridad.

De utilizarse un esquema de registración descentralizada, los Responsables de la Autoridades de Registración remotas (RARR) están obligados a mantener a disposición del Organismo Auditante archivo de copias de toda la documentación que reciban o generen como respaldo del proceso de validación de la identidad de los suscriptores. El mencionado archivo se conservará bajo la responsabilidad del RARR y su sustituto, en lugar físico seguro y por el plazo establecido en el presente apartado. Esta obligación se extiende a los auxiliares de los RARR que se hubieran designado.

La AC-URME efectuará auditorías periódicas sobre las Autoridades de Registración remotas con el fin de verificar el cumplimiento por parte de éstas de los procedimientos de validación y la revisión de su documentación respaldatoria.

Asimismo, el Responsable de una Autoridad de Registración remota está obligado a efectuar una auditoría semestral sobre sus auxiliares y en aquellos casos en los que se hubiera aplicado el procedimiento opcional indicado en el apartado 3-2-2-2-3. A tal fin efectuará una revisión de la documentación respaldatoria de dicho proceso, así como de los procedimientos de validación utilizados.

11 -2 - Copias de resguardo de Archivos de transacciones de Auditoría

Las copias de resguardo de los archivos de transacciones de auditoría se mantienen a disposición del Organismo Auditante.

12- Archivos

La AC-URME mantiene un sistema de archivos que permite la conservación, en condiciones adecuadas de seguridad, de toda la información referida a los procesos de emisión y administración de los certificados.

La información mínima a conservar es la siguiente:

a) Solicitudes de emisión de certificados, incluyendo documentación de respaldo del proceso de identificación

b) Solicitudes de revocación de certificados.

c) Notificaciones de compromiso de claves.

d) Emisión de certificados.

e) Revocación de certificados.

f) Emisión de listas de certificados revocados.

g) Cambios de claves.

h) Nombramiento de personal en roles confiables.

i) Actas de actividades efectuadas por dicho personal

j) Nombramiento de Responsables de Autoridades de Registración remotas y de sus auxiliares

k) Toda comunicación entre la AC-URME y el Organismo Licenciante.

Los archivos se conservarán bajo llave. Es función del Responsable de la Autoridad de Registración local su mantenimiento y resguardo. En caso de ausencia, su función será cubierta por su sustituto.

Cada uno de los responsables mencionados tendrá en su poder un juego de llaves. Una copia de la misma se encuentra en poder del responsable de la AC-URME. Debe quedar constancia escrita de los datos de quienes poseen una copia de las llaves.

Los archivos deben conservarse en un espacio físico acondicionado dentro del ámbito de la ACURME por un plazo mínimo de DIEZ (10) años. Aquellos con antigüedad mayor a un año pueden trasladarse a un archivo secundario en un lugar físico protegido, manteniendo las mismas medidas de seguridad.

De utilizarse un esquema de registración descentralizada, los Responsables de la Autoridades de Registración remotas (RARR) están obligados a mantener archivo de toda la documentación que reciban o generen como respaldo del proceso de validación de la identidad de sus auxiliares. El mencionado archivo se conservará bajo la responsabilidad del RARR y su sustituto, en lugar físico seguro y por el plazo establecido en el presente apartado. Esta obligación se extiende a los auxiliares de los RARR que se hubieran designado respecto a la documentación respaldatoria del proceso de validación de identidad de los suscriptores que hubieran solicitado sus certificados por su intermedio.

En caso que se optara por centralizar el archivo de dicha información bajo la responsabilidad del RARR, su auxiliar le remitirá la documentación recibida, conservando copia de la misma en su poder.

12 -1 - Copias de resguardo

Se mantendrán copias de resguardo de todos los archivos referidos a los procesos de emisión y administración de certificados que se encuentren en el servidor de la AC-URME.

13- Planes de emergencia

La AC-URME posee un plan de contingencias que permite garantizar el mantenimiento mínimo de la operatoria y la recuperación de los recursos comprometidos dentro de las VEINTICUATRO (24) horas de producida una emergencia.

Los procedimientos detallados a cumplir se encuentran descriptos en el Plan de Contingencias.

14- Controles de Seguridad

14 -1 - Controles de Seguridad Física y Personal

La AC-URME implementa controles de seguridad físicos y personales a fin de dotar de un adecuado marco de seguridad a las funciones que desarrolla (generación de claves, autenticación, emisión y revocación de certificados, archivos, etc.).

Estos controles son críticos para otorgar confiabilidad a los certificados, ya que su ausencia comprometerá todas las instancias del sistema.

14 -2 - Controles de Seguridad Lógica:

La AC-URME define en el Manual de Procedimientos de Seguridad:

a) Las medidas de seguridad a fin de proteger sus claves criptográficas pública y privada y todos los demás datos críticos necesarios para operar con módulos criptográficos (números pin, passwords, claves manuales compartidas o no por el personal, etc.).

b) Otros controles de seguridad lógica que garantizan las funciones de generación de claves, identificación de usuarios, emisión y renovación de certificados, auditoría y archivos.

14 -3 - Controles de Seguridad del Computador:

Son aplicables los controles indicados en los Estándares sobre Tecnología de Firma Digital para la Administración Pública Nacional adoptados por la Provincia

15- Certificados y listas de certificados revocados – Características

Se emplean certificados en formato x509 versión 3 o superior y listas de certificados revocados en formato x509 versión 2.

La información a incluir en los certificados se encuentra detallada en los Estándares sobre Tecnología de Firma Digital para la Administración Pública Nacional adoptados por la Provincia y en el apartado 5 del presente manual.

16- Administración de la documentación técnica emitida por la AC-URME

En este capítulo se incluyen disposiciones acerca del mantenimiento de la documentación técnica emitida por la AC-URME, sus eventuales modificaciones y notificaciones.

16 -1 - Cambios a la documentación técnica:

La AC-URME informará a sus suscriptores acerca de todos aquellos cambios significativos que se efectúen a la documentación técnica pública mencionada en el presente manual. Las modificaciones indicadas serán publicadas en el sitio web de la AC-URME.

16 -2 - Publicación y Notificación:

El Manual de Procedimientos y demás documentación técnica pública emitida por la AC-URME se encuentran disponibles en su sitio web en el siguiente.

VI. PLAN DE CESE DE ACTIVIDADES

Autoridad Certificante

Gobernación de Mendoza

Secretaría Administrativa Legal y Técnica

Unidad de Reforma y Modernización del Estado

1- Componentes involucrados

El cese de actividades de la Autoridad Certificante de la Unidad de Reforma y Modernización del Estado de la Secretaría Administrativa Legal y Técnica de la Gobernación, en su carácter de Autoridad Certificante de la Administración Pública Provincial (en adelante ACURME) tiene efectos que involucrarán a todos los suscriptores de sus certificados. Cualquiera sea el motivo que lo ocasione, la AC-URME tomará una serie de recaudos a fin minimizar el impacto de la finalización de sus servicios.

En caso de producirse un cese de actividades, los procedimientos correspondientes serán supervisados conjuntamente por el Organismo Licenciante y el Organismo Auditante.

2- Procedimientos a seguir

2 -1 - Procedimiento general

Si la AC-URME dejara de operar, no emitirá nuevos certificados a favor de sus suscriptores. Unicamente garantizará la posibilidad de emitir las Listas de Certificados Revocados con la periodicidad habitual o ante el pedido de revocación de un certificado por parte de alguno de sus suscriptores.

Los procedimientos generales a seguir son los siguientes:

a) Publicar el cese de actividades en el Boletín Oficial durante TRES (3) días consecutivos, indicando fecha y hora de cese de actividades, que no podrá ser anterior a los NOVENTA (90) días corridos contados desde la fecha de la última publicación.

b) Notificar acerca de la situación al Organismo Licenciante con una antelación no menor a los NOVENTA (90) días corridos de la fecha de cese, indicando expresamente la fecha prevista. La notificación se efectua-

rá mediante un mensaje de correo electrónico firmado digitalmente o personalmente por el responsable de la AC-URME o un representante autorizado. Además, en ella se informará si la AC-URME efectuará transferencia de los certificados emitidos a favor de otra Autoridad Certificante.

c) Notificar a los suscriptores acerca del cese de sus actividades mediante un mensaje de correo electrónico firmado digitalmente con una antelación no menor a los NOVENTA (90) días corridos de la fecha prevista de cese.

d) Publicar durante TRES (3) días consecutivos en uno o más diarios de difusión provincial el cese de sus actividades, si hubiera emitido certificados a personas ajenas a la Administración Pública Provincial.

e) Rechazar toda solicitud de emisión de un nuevo certificado por parte de un suscriptor dentro de los NOVENTA (90) días corridos anteriores a la fecha prevista para el cese.

f) Rechazar toda solicitud de renovación de un certificado por parte de un suscriptor dentro de los NOVENTA (90) días corridos anteriores a la fecha prevista para el cese.

g) Emplear la clave privada de la AC-URME solamente para firmar las Listas de Certificados Revocados.

h) Brindar el servicio de revocación de certificados, actualización de repositorios y emisión de listas de certificados revocados hasta la fecha prevista de cese de actividades. Solamente podrá efectuar revocaciones a solicitud de sus suscriptores, quienes serán los únicos responsables de pedir la revocación de sus certificados.

i) Revocar la totalidad de los certificados que hubiera emitido y que se encuentren vigentes a la fecha de cese de sus actividades.

j) Destruir los dispositivos de soporte de su clave privada mediante un procedimiento que garantice su destrucción total según el último estado del arte disponible a la fecha, una vez revocados o expirados los certificados de sus suscriptores. El procedimiento de destrucción se hará en presencia del responsable de la AC-URME, del Responsable de Seguri-

dad, del Oficial Certificador y del Responsable de la Autoridad de Registración, dejando constancia de lo actuado en el acta correspondiente.

2 -2 - Cese de actividades con transferencia de certificados

Al producirse el cese de sus actividades, se admitirá que la AC-URME efectúe una transferencia de los certificados emitidos a sus suscriptores a favor de otra Autoridad Certificante. Para ello se requerirá un acuerdo previo entre ambas Autoridades Certificantes, con aprobación del Organismo Licenciante, que deberá ser firmado por las máximas autoridades respectivas.

Dicho acuerdo debe indicar que la Autoridad Certificante continuadora toma a su cargo la administración de la totalidad de los certificados emitidos por la AC-URME que cesa sus actividades, que no hubieran sido revocados a la fecha de la transferencia. Sendas copias del mencionado acuerdo se remitirán al Organismo Licenciante para su aprobación y al Organismo Auditante, para su archivo.

Asimismo, la AC-URME transferirá a la Autoridad Certificante continuadora toda la documentación que obre en su poder y que hubiera generado en el proceso de emisión y administración de certificados, así como la totalidad de los archivos y copias de resguardo, en cualquier formato y toda otra documentación referida a su operatoria.

El proceso de transferencia será supervisado conjuntamente por el Organismo Licenciante y el Organismo Auditante.

La AC-URME informará acerca de la transferencia en las publicaciones y notificaciones que efectúe referidas al cese de sus actividades mencionadas en el apartado 2.1. Además, con excepción de lo dispuesto en el punto i), cumplirá con la totalidad de los procedimientos indicados en el mismo.

En caso que la AC-URME optara por no transferir sus certificados, procederá a revocar la totalidad de los certificados que hubiere emitido y que se encuentren vigentes a la fecha de cese de sus actividades. En tal caso, toda la documentación de la Autoridad Certificante discontinuada quedará en custodia del Organismo Licenciante y a disposición del Organismo Auditante.

VII. PLAN DE CONTINGENCIAS

Autoridad Certificante

Gobernación de Mendoza

Secretaría Administrativa Legal y Técnica

Unidad de Reforma y Modernización del Estado

1- Componentes involucrados

El plan de contingencias del la Autoridad Certificante de la Unidad de Reforma y Modernización del Estado de la Secretaría Administrativa Legal y Técnica de la Gobernación, en su carácter de Autoridad Certificante de la Administración Pública Provincial (en adelante ACURME) involucra a todos los recursos físicos, de hardware, software y humanos integrantes de la estructura con el fin de garantizar su adecuado y continuo funcionamiento.

Su propósito es asegurar el mantenimiento de su operatoria mínima y la recuperación de los recursos que fueran comprometidos en un plazo máximo de 24 horas.

Al menos una vez al año debe efectuarse una prueba de recuperación ante contingencias, restaurando los datos respaldados en un ambiente provisorio a fin de constatar la corrección de las copias realizadas y el funcionamiento del mecanismo de respaldo.

En caso de producirse un evento que impida la continuidad de las operaciones de la AC-URME, se procederá a notificar inmediatamente a la máxima autoridad del organismo y al Oficial Certificador de la AC-URME. Este se comunicará con el Operador de la Autoridad de Registración y comenzará las operaciones de recuperación correspondientes. Con el fin de iniciar las operaciones de recuperación se debe prever la existencia de los siguientes elementos:

- Un ambiente separado físicamente de las oficinas de AC-URME, que posea las configuraciones mínimas de hardware necesarias para el mantenimiento de la operatoria.

- Copia del software resguardada en las condiciones especificadas en el Plan de Seguridad.
- Copias de resguardo actualizadas de la información procesada, conservadas en las condiciones indicadas en el Plan de Seguridad.

Se conservará en una oficina designada para tal efecto, un disco preinstalado con el sistema operativo y el software utilizado por la AC-URME. En caso de producirse un siniestro, Oficial Certificador de la AC-URME procederá a retirar de la mencionada oficina equipo que funciona como servidor. Se retirará el disco del equipo mencionado reemplazándoselo por el disco preinstalado con el sistema operativo y el software del Organismo Licenciante. A continuación se comenzará la operatoria de emergencia utilizándose las correspondientes copias de resguardo de archivos que serán provistas por el Oficial Certificador de la AC-URME o en su defecto por el Operador Técnico de la AC-URME.

La utilización del equipamiento de emergencias puede extenderse por un plazo máximo de treinta (30) días, salvo que la gravedad de la situación justifique la extensión de dicho plazo.

La AC-URME ofrece los servicios de Emisión de Certificados y el acceso a las Listas de Certificados Revocados por medio de un protocolo HTTP.

El servicio de Solicitud de Certificación y Publicación de Lista de Certificados Revocados se encuentra implementado sobre el *servidor público de la AC-URME*

El servicio de Emisión, Renovación y Revocación de Certificados y emisión de Listas de Certificados Revocados se encuentra en un servidor independiente cuyas únicas funciones son las indicadas anteriormente. Dicho servidor se encuentra protegido del acceso físico externo y sobre el mismo solo tienen acceso lógico el Operador Técnico de la AC-URME, el Responsable de la Autoridad de Registración de la AC-URME y el Oficial Certificador de la AC-URME.

Los componentes adicionales que se encuentran involucrados en la operatoria del Organismo Licenciante son los siguientes

- red de interconexión
- firewall

- dispositivos criptográficos

El *servidor de certificación* se encuentra desconectado físicamente de la *red de interconexión* excepto en los momentos en que se realizan transferencias de archivos de resguardo.

La *red de interconexión* se encuentra aislada de toda otra red de computadoras. La administración de esta red como el router que da acceso a Internet será controlado por el Responsable Informático de la Secretaría Administrativa- Legal y Técnica de la Gobernación y el control del Comité de Información Pública dependiente de la Unidad de Reforma del Estado.

El *firewall* se encuentra dedicado a proteger la red sobre la que se monta la aplicación de la Firma Digital en el Sector Público Provincial.

2- Procedimientos

Se describen a continuación una serie de procedimientos que deben cumplimentarse ante distintas situaciones de emergencia que pueden presentarse en el transcurso de la operatoria de la AC-URME.

Los procedimientos que a continuación se detallan se aplicarán sin perjuicio de la aplicación que se haga de las normas de seguridad que se aplican en todo el **ámbito provincial** y que se encuentran identificadas como: ***COBIT*** (Objetivos de Control para la Información y Tecnología Relacionadas y sus posteriores actualizaciones), el uso de los ***Estándares Tecnológicos de la Administración Pública Nacional*** (E.T.A.P. y sus posteriores modificaciones) desarrollados por la Subsecretaría de Tecnologías para el Sector Público, dependiente de la Secretaría Administrativa – Legal y Técnica de la Gobernación de la Jefatura de Gabinete de Ministros y las ***Normas de Seguridad de Sistemas de Información***, sus posteriores modificaciones y agregados.

Esta lista será revisada y actualizada periódicamente.

2-1- Acceso indebido

En caso de producirse un acceso lógico indebido a los servidores de emisión de certificados o al servidor público, se desconectarán los servidores involucrados de la red y se notificará a la Unidad de Reforma del Estado

como administrador de la Firma Digital. Las propuestas que presente esta Unidad de Reforma del Estado serán implementadas por el Operador Técnico de la AC-URME.

En caso de producirse un acceso físico indebido se notificará a la máxima autoridad de la AC-URME para que determine los pasos a seguir.

En función de los informes elevados por los grupos consultados, se evaluará si es conducente pasar al procedimiento indicado en el apartado 2.4.

2-2-.No acceso a los servicios de publicación de Listas de Certificados Revocados

En caso de no poder ofrecer el servicio de consulta de la Lista de Certificados Revocados, esta será publicada en el servidor de la Gobernación ***(http://www.mendoza.gov.ar)*** hasta que el servicio haya sido restablecido.

2-3- Destrucción del dispositivo criptográfico.

Si el dispositivo criptográfico principal de emisión de certificados es destruido o inutilizado se procederá a proveer al Oficial Certificador de la copia de resguardo que se ha almacenado en un lugar seguro, debiendo iniciarse inmediatamente la tramitación de su reposición.

Una vez obtenida una copia del mismo se procederá a su réplica, entrega a los responsables involucrados y redacción del acta correspondiente.

2-4- Destrucción o inutilización de equipamiento.

Si alguno de los servidores utilizados para la emisión o publicación de certificados es destruido o inutilizado, en un plazo no mayor a 24 horas será sustituido por un equipamiento que permita la misma funcionalidad según los procedimientos descriptos en el punto 1, debiendo procederse a su instalación y restauración de la última copia de resguardo disponible almacenada en un lugar seguro.

2-5- No disponibilidad del Oficial Certificador

En caso de ausencia temporaria del Oficial Certificador, este será reemplazado en sus funciones por su sustituto, nombrado según lo dispuesto

en el Manual de Procedimientos. A tales efectos, el sustituto utilizará la copia de resguardo del dispositivo criptográfico que se encuentra bajo custodia. Para ello se le hará entrega de la copia junto con la clave de activación. El responsable sustituto creará una nueva clave que utilizará para activar la copia en el período de tiempo en que ejerza su función. Este acto debe quedar asentado debidamente con la firma de los responsables intervinientes. Una vez que el Oficial Certificador se reintegre a sus funciones, deberá cambiar la clave de activación utilizando una nueva, diferente a la que utilizara anteriormente. Se procederá a replicar la nueva clave de activación y a entregar la copia del dispositivo al responsable de su custodia junto con la nueva clave, dejándose constancia escrita del procedimiento efectuado.

Si el Oficial Certificador y su sustituto se encontraran temporariamente ausentes, la máxima autoridad de la AC-URME, quien es el responsable de la custodia de la copia de resguardo y de su código de activación, es el encargado de activar el dispositivo criptográfico de resguardo

Idénticas previsiones se tomarán en caso de ausencia temporaria del Responsable Operador de la Autoridad de Registración o bien de este y su sustituto.

VIII. POLITICA DE SEGURIDAD

Autoridad Certificante

Gobernación de Mendoza

Secretaría Administrativa Legal y Técnica

Unidad de Reforma y Modernización del Estado

1.- Introducción

La información es un activo que, como el resto de los recursos importantes de la organización, tiene valor para la misma y por consiguiente debe ser debidamente protegido. La Seguridad de la Información resguarda a este activo de una amplia gama de amenazas, a fin de garantizar la continuidad del negocio, minimizar el riesgo de posibles daños y maximizar el retorno sobre las inversiones y oportunidades.

La información puede existir en muchas formas. Cualquiera sea la forma que adquiere, o los medios por los cuales se distribuye y almacena, siempre debe ser protegida en forma adecuada.

La Seguridad de la Información se define aquí como la preservación de las siguientes características:

- confidencialidad: se garantiza que la información es accesible sólo para aquellas personas autorizadas
- integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento
- disponibilidad: se garantiza que los usuarios autorizados tienen acceso a la información y a los recursos relacionados con la misma, toda vez que se requiera
- autenticidad: se garantiza la procedencia y autoría de la información

La Seguridad de la Información se logra implementando un conjunto adecuado de controles, que comprenden políticas, prácticas, procedimientos, estructuras organizacionales y funciones relativas al software. Estos controles deben ser establecidos para garantizar que se logren los objetivos específicos de seguridad de la organización.

El objeto principal de la Autoridad Certificante de la Unidad de Reforma y Modernización del Estado de la Secretaría Administrativa Legal y Técnica de la Gobernación, en su carácter de Autoridad Certificante de la Administración Pública Provincial (en adelante ACURME) es estructurar un esquema de confianza válido para los suscriptores de sus certificados y para los terceros que se relacionen con ella. El cumplimiento de todos los procedimientos operativos y de seguridad descriptos en la documentación técnica emitida resulta un requisito básico para el mantenimiento de la confiabilidad de dicho esquema. En particular, es crítico el adecuado seguimiento de los procedimientos previstos respecto a la emisión de los certificados y a la validación de la identidad de los solicitantes.

Por último, es necesario resaltar que la Seguridad de la Información es un proceso continuo cuya calidad está determinada por la del componente con menor grado de seguridad.

2.- Compromiso

El responsable de la AC-URME asume el compromiso de apoyar y dirigir los principios básicos que guían la gestión de la Seguridad de la Información, obligándose a exigir el cumplimiento de las disposiciones de la presente política a todo el personal asignado a funciones en el mismo.

3.- Principios aplicables

La presente Política de Seguridad está basada en los siguientes principios:

3.1. - Normas legales y contractuales

Esta política se dicta en todo de acuerdo con las normas y regulaciones de carácter general que resulten aplicables a la Unidad de Reforma y Modernización del Estado de la Secretaría Administrativa Legal y Técnica de la Gobernación.

Asimismo, resulta aplicable toda legislación vigente relativa al diseño, operación, uso y administración de los recursos informáticos.

La normativa a contemplar se refiere a:

a) Derechos de Propiedad Intelectual

b) Protección de los registros de la organización

c) Protección de datos y privacidad de la información personal

d) Prevención del uso inadecuado de los recursos de procesamiento de la información

e) Regulación de controles para el uso de criptografía

f) Recolección de evidencias

g) Cualquier otra norma relacionada con la materia.

3.2. - Capacitación

Los objetivos y procedimientos de esta política serán comunicados a todo el personal que desarrolle funciones en la AC-URME, incluyendo al personal ajeno al mismo asignado a tareas temporarias, quienes serán capacitados en la comprensión de sus objetivos y procedimientos de aplicación en cuanto correspondan a las funciones que debe cumplir.

3.3. - Cumplimiento

La presente política resulta de cumplimiento obligatorio para todo el personal designado para cumplir funciones en la AC-URME. La obligación se extiende a todo el personal ajeno al mismo que sea asignado al cumplimiento de tareas temporarias. El personal mencionado está obligado a adherir a la política y a cumplir sus disposiciones.

El incumplimiento de las disposiciones de la presente política se considera falta grave y dará lugar a las sanciones establecidas en el régimen jurídico de la función pública.

De tratarse de terceros no alcanzados por el régimen legal mencionado, serán pasibles de las sanciones previstas en la legislación administrativa, civil, comercial y penal vigente.

La documentación técnica de la AC-URME se encontrará en todo momento disponible para ser consultada por su personal. La documentación técnica de carácter público actualizada se encontrará disponible en todo momento en el sitio web de la AC-URME.

3.4. - Protección de la integridad del software y la información

Dado que el software y las instalaciones de procesamiento de información son vulnerables a la introducción de software malicioso (por ejemplo, virus

informáticos) la AC-URME tomará precauciones para su detección y prevención a fin de garantizar la integridad de la información, procedimientos y sistemas.

3.5. - Gestión de continuidad de las operaciones

A fin de garantizar la continuidad de las operaciones de la AC-URME, se establecen medidas para proteger el correcto funcionamiento de los servicios y prevenir incidentes. En casos de necesidad extrema, se prevén los mecanismos necesarios para instrumentar un plan de contingencias que permita la continuidad de las operaciones.

3.6. - Separación de funciones

Los roles definidos en la operatoria de la AC-URME (Operador Técnico de la Autoridad Certificante, Oficial Certificador, Responsable de la Autoridad de Registración, Responsable de Seguridad Informática y sustitutos de cada uno de ellos) son desempeñados por diferentes responsables. Ninguno de los nombrados concentrará más de una función, aun cuando fuera en forma transitoria. En caso de ausencia temporaria, el responsable será reemplazado por su correspondiente sustituto.

4.- Normas y Procedimientos

La presente Política de Seguridad se instrumenta a través de diversos procedimientos que permiten llevar a la práctica los principios enunciados en el apartado 3. Los procedimientos mencionados se refieren a los siguientes aspectos:

4.1. - Seguridad física y ambiental

El entorno de trabajo de la AC-URME garantiza en forma adecuada las condiciones de seguridad física y ambiental para su funcionamiento, existiendo procedimientos de seguridad que los respaldan.

4.2. - Seguridad de acceso de terceros

Ningún tercero tiene acceso a las operaciones críticas de la AC-URME. El personal ajeno al mismo que cumple funciones temporarias se encuentra debidamente autorizado y sus actividades son permanentemente supervisadas mientras se encuentre en el recinto de la Autoridad Certificante.

4.3. - Clasificación y control de activos

Se establecen responsables para cada uno de los activos de la AC-URME. Estos son clasificados por su nivel de criticidad y se determinan procedimientos para su protección.

4.4. - Administración de recursos humanos

El personal que desempeña funciones en la AC-URME debe demostrar su probidad y destreza para las funciones asignadas, conservándose evidencia al respecto.

4.5. - Respuesta a incidentes y anomalías

Los procedimientos de seguridad y de contingencias respaldan en forma adecuada la continuidad de las operaciones de la AC-URME.

4.6. - Protección de la integridad y legalidad del software

Toda instalación de software de la AC-URME se encuentra debidamente autorizada.

4.7. - Mantenimiento y resguardo de la información

La información de la AC-URME, cualquiera sea su soporte, se conserva según lo dispuesto por las normas y reglamentos aplicables.

4.8. - Controles de acceso lógico

El acceso a los sistemas y servicios de la AC-URME se encuentra restringido al personal debidamente autorizado.

4.9. - Administración de la continuidad de operaciones

Los procedimientos establecidos en el Plan de Contingencias garantizan la continuidad de las operaciones de la AC-URME con un tiempo mínimo de recuperación.

5.- Responsabilidades y Funciones

5.1. - Responsabilidad primaria

El responsable de la AC-URME tiene la responsabilidad primaria de la definición, aprobación, implementación, revisión, actualización y cumplimiento de la presente política.

5.2. - Funciones

A los fines de una efectiva implementación de la política y los procedimientos de seguridad, el responsable de la AC-URME asigna las siguientes funciones:

- Verificación y control del cumplimiento de las disposiciones de la política y los procedimientos de seguridad, a cargo del Responsable de Seguridad Informática de la AC-URME.

- Todo el personal que desempeñe funciones en la AC-URME, aun cuando estas fueran de carácter temporario, está obligado a instrumentar y cumplir las disposiciones de esta política, de los procedimientos de seguridad y de sus actualizaciones en su ámbito de competencia.

5.3. - Revisión y Actualización

Se establece un proceso mínimo de revisión anual a fin de garantizar respuestas a los cambios que afecten la base de evaluación de riesgos original. No obstante, en aquellos casos en que resulte necesario una actualización con una periodicidad menor. A tal fin, se tendrá en cuenta los siguientes aspectos para su evaluación:

a) la eficacia de la política, demostrada por la naturaleza, número e impacto de los incidentes de seguridad registrados

b) el costo e impacto de los controles en la eficiencia de los servicios

c) los efectos de los cambios en la tecnología

d) cambios que afecten en la infraestructura organizacional, técnica y de servicios de la AC-URME

e) cambios significativos en la exposición de los recursos frente a las amenazas nuevas o preexistentes

f) incidentes relativos a la seguridad ocurridos desde la revisión anterior

6.- Documentos de referencia

La presente Política de Seguridad se emite en acuerdo a lo dispuesto en los Estándares sobre Tecnología de Firma Digital para la Administración Públi-

ca Nacional adoptados por la Provincia y se complementa con los siguientes documentos referidos a la operatoria de la AC-URME:

a) Política de Certificación

b) Manual de Procedimientos

c) Plan de Cese de Actividades

e) Plan de Contingencias

IX. Referencias

- PKCS#10: Public Key Criptography Standards #10, desarrollado por RSA Laboratories. Disponible en:
  http://www.rsa.com/
- SHA-1: Secure Hash Standard-1, NIST FIPS PUB 180-1, desarrollado por National Institute of Standards and Technology, US Department of Commerce. Disponible en:
  http://www.itl.nist.gov/div897/pubs/fip180-1.htm
- RSA: Estándar criptográfico, desarrollado por RSA Laboratories. Disponible en:
  http://www.rsa.com/
- X509 versión 3: formato definido en estándar ISO/IEC/ITU X.509. Disponible en:
  http://www.ietf.org/
- Oficina Nacional de Tecnologías Informáticas Disposición 5/2002.
  Disponible en:
  http://ca.pki.gov.ar/
- Ley de Firma Digital - Boletín Oficial del 14/12/2001
  Disponible en:
  http://ca.pki.gov.ar/
- Decreto N° 427/98 Infraestructura de Firma Digital para el Sector Público Nacional
  Disponible en:
  http://ca.pki.gov.ar/
- B.O. 20/12/02 FIRMA DIGITAL Decreto 2628/2002 Reglamentación de la Ley N° 25.506.
  Disponible en:
  http://ca.pki.gov.ar/
- la Resolución N° 54 / 99 y del Decreto-Acuerdo N° 1806 del 1999, el Gobierno de la Provincia de Mendoza, a través del Comité de Información Pública (COM.I.P.)

- **X509 versión 2: formato definido en estándar ISO/IEC/ITU X.509. Disponible en:**
  http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki-part1-08.txt
  http://www.ietf.org/