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

Firma Digital

"Análisis de factibilidad para la implementación de Firma Digital"

Informe Final

CONSEJO FEDERAL DE INVERSIONES
CONSULTOR: LIC. PABLO GUILLERMO LIOY

Mendoza, 28 de Octubre del 2003

CONSEJO FEDERAL DE INVERSIÓN
SECRETARIA GENERAL
ING. JUAN JOSE CIÁCERA

Me dirijo a Ud. a efectos de presentar el Informe Final correspondiente a las tareas ejecutadas en el marco del Proyecto ***"Análisis de factibilidad para la implementación de Firma Digital"***

Detalle de Tareas

En el marco del proyecto e-firma/mza y de acuerdo con el Plan de Actividades propuesto, se presentan a continuación, como Informe Final, el desarrollo total de las siguientes actividades:

1. **Realizar un estudio general de factibilidad** para introducir la firma digital en el ámbito del Gobierno de la Provincia de Mendoza.
    - Análisis de Factibilidad Operativa
    - Análisis de Factibilidad Económica-Financiera
    - Análisis de Factibilidad Legal
2. **Determinación de estructuras técnicas aplicables** de soporte para la PKI (*Public Key Infrastructure)*
    - Análisis de Factibilidad Técnica
    - Definición de la Arquitectura de Soporte
    - Definición de necesidades a cubrir por la PKI
    - Presupuesto Estimado
    - Determinación de la arquitectura más adecuada a la vista del análisis de requerimientos
3. **Desarrollar organizativa y funcionalmente** una infraestructura de certificación coherente para la implementación de firma digital.
    - Definición de una estructura de autoridades certificantes
    - Definición de Políticas de Certificación

- Determinación de Funciones, Responsabilidades y Obligaciones
- Diseño de Manual de Funciones
- Diseño de Manual de Procedimientos
- Diseño de Plan de Cese de Actividad
- Diseño de Plan de Contingencia
- Diseño de Plan de Seguridad

4. **Desarrollar un Marco Legal** compatible con la normativa nacional e internacional existente sobre el tema.
    - Recopilación de antecedentes legales
    - Análisis de experiencias internacionales
    - Análisis y descripción del marco legal vigente
    - Propuesta de normativa legal sobre firma digital para la provincia de Mendoza

5. **Generar una Propuesta de implementación** en la Provincia de Mendoza en función de condiciones particulares.
    - Identificar del universo de procedimientos en el ámbito del Gobierno de la Provincia aquellos que por sus características sean susceptibles a la aplicación de firma digital.
    - Fundamentar y proponer la aplicación de la herramienta sobre un procedimiento factible.

"Se presentan así las tareas 1,2,3,4 y 5 programadas en la formulación total del proyecto, también se agregan las actividades adicionales que se pudieron desarrollar en función del éxito obtenido"

Lic. Pablo LIOY

ÍNDICE

I. Resumen de Contenidos

El presente informe se divide en 4 subinformes. Cada uno de ellos comienza con una descripción de las actividades desarrolladas en pos de la consecución de los objetivos del proyecto y en sus contenidos se presentan versiones abreviadas del contenido original presentado en su momento.

El primer informe representa una descripción de la etapa exploratoria del proyecto, aquí se presentan las conclusiones más importante del estudio completo de "Análisis de Factibilidad para la implementación de Firma digital" al momento del inicio temporal del proyecto.

En el segundo informe se consigna el desarrollo completo de la estructura organizacional y procedimental de una Infraestructura de Clave Pública de enfoque sistémico.

El tercer informe corresponde al desarrollo de una normativa legal integrada que nos permitiera sustentar los avances propuestos en materia de firma digital. De esta manera aparece el proyecto de norma legal que actualmente se encuentra en proceso de aprobación.

En el cuarto y último informe o **informe final,** se desarrolla una **propuesta de implementación** de la tecnología de firma digital con un importante valor agregado, el hecho de contar con la experiencia y el antecedente de **pruebas piloto ya desarrolladas** en el ámbito provincial por el equipo de este proyecto y **la implementación de la AC-URME**, la Autoridad Certificante de la Unidad de Reforma y Modernización del Estado; superando así ampliamente el plan de actividades previamente propuesto. Dichos pilotos y desarrollos se presentan en el cuerpo del informe, como así también la **Estrategia que nos permitirá priorizar las futuras aplicaciones** de firma digital en función de la continuidad de este proyecto.

Por último se hace la presentación del **sitio de Firma Digital** (www.firmadigital.mendoza.gov.ar) con el cual el proyecto logra la presencia web en el ámbito.

II. Primer Informe de Etapa: "Análisis de Factibilidad"

Introducción

En el marco del proyecto de Firma Digital y de acuerdo con el Plan de Actividades propuesto, se presentan a continuación, como Primer Informe de Etapa, el desarrollo de las siguientes actividades:

1. Realizar un estudio general de factibilidad para introducir la firma digital en el ámbito del Gobierno de la Provincia de Mendoza.
   - •Análisis de Factibilidad Operativa
   - •Análisis de Factibilidad Económico/Financiera
   - •Análisis de Factibilidad Legal

2. Determinación de estructuras técnicas aplicables de soporte para la PKI (Public Key Infrastructure)
   - •Análisis de Factibilidad Técnica
   - •Definición de la Arquitectura de Soporte
   - •Definición de necesidades a cubrir por la PKI
   - •Presupuesto Estimado
   - •Determinación de la arquitectura más adecuada a la vista del análisis de requerimientos

Idea Guía

Crear las condiciones necesarias para introducir las tecnologías criptográficas pertinentes para el soporte de la Firma Electrónica y sus servicios asociados. Con ello, a futuro, se espera poder facilitar el camino del desarrollo de proyectos reales de teleadministración y de proyectos que agilicen multitud de tramitaciones internas de la Administración Pública de la Provincia de Mendo-

za, llegando a disponer de sus propios servicios de Autoridad de Certificación y de Registro, con una estructura de certificación coherente.

Objetivo General

Estudio de factibilidad y Diseño de Infraestructura (PKI) tendiente a instrumentar la firma digital en el ámbito del Gobierno de la Provincia de Mendoza.

Objetivos Específicos:

•Determinar factibilidad para la implementación de tecnologías de firma digital que fomenten el ahorro y la celeridad en los procedimientos públicos provinciales.

•Diseñar una PKI de propósito general, para la emisión y gestión de certificados digitales que permitan la generación de firmas digitales y el cifrado en procesos internos, y que permitan a los ciudadanos y las empresas relacionarse con la Administración a través de Internet, en un entorno seguro.

•Proponer un marco regulatorio compatible pero adecuado a las circunstancias particulares de la provincia.

•Identificar ámbitos de aplicación de acuerdo con la demanda ciudadana local.

Anexo I: Análisis de Factibilidad Operativa

En este subestudio es preciso analizar si la Administración Pública provincial se encuentra en condiciones de convivir con una infraestructura de firma Digital y sus servicios asociados, es decir, de qué forma planeamos que

Digital y sus servicios asociados, es decir, de qué forma planeamos que su organización y su personal se adapten satisfactoriamente a los cambios necesarios para que el nuevo sistema funcione con éxito. Por otro lado resulta importante plantear las condiciones que deben cumplirse y las acciones que deben desarrollarse para lograr con alto grado de seguridad la funcionalidad u operatividad del modelo a plantear. En tal sentido a continuación se presenta una enumeración de factores que son considerados importantes para la consecución efectiva de los objetivos fijados.

Conclusiones

Sólo una completa y adaptada implementación de una Infraestructura de Clave Pública (con un determinado sistema de hardware, de software, de políticas y de personas) hace factible proporcionar el conjunto de seguridades informáticas que la Administración Pública Provincial necesita. En tal sentido, es muy importante realizar una fina valorización de ciertos factores que pueden entorpecer el desarrollo de nuestro proyecto pero que, correctamente tratados, pueden fortalecer su implementación, a saber:

El grado de interoperabilidad

El hecho de adherir a las especificaciones del estándar X.509.v3 no garantiza necesariamente que dos certificados generados por dos sistemas desarrollados por firmas distintas sean mutuamente compatibles. Pueden darse, y de hecho han ocurrido, ciertos inconvenientes en estas certificaciones cruzadas ya que existen problemas de confianza entre las Autoridades de Certificación de distintas organizaciones, que puede imposibilitar el éxito en la verificación de las cadenas de certificación cuya AC raíz sea desconocida o no confiable, invalidando todo el conjunto. Cabe destacar que este problema no es esen-

cialmente de orden técnico como tampoco del estado de desarrollo del espectro tecnológico actual.

Los costos

Cada empresa prestadora de servicios de clave pública tarifa en función de una diversidad amplia de criterios (por certificado, por uso de certificado, por servidores instalados, etc) al no existir aún un mercado totalmente desarrollado, los honorarios que se cobran también resultan dispares, de tal forma que la inversión en una PKI como respuesta a las necesidades de seguridad y accesibilidad puede resultar en algunos casos inesperadamente elevada. Muchas veces la respuesta estará en planificar una infraestructura escalable que comience con aplicaciones acotadas.

La escalabilidad

Si no se considera criteriosamente las posibilidades de expansión de una PKI, cuando la cantidad de certificados crece, pueden surgir situaciones conflictivas. Esto puede afectar, por ejemplo, a la gestión relacionada a las listas de revocación ya que deben ser consultadas en cada operación que involucre certificados y firmas digitales en las aplicaciones más serias del entorno de la PKI.

Complejidad tecnológica frente a usuarios finales no capacitados y participación activa

La tecnología PKI se torna un tanto lejana para el usuario final que no termina de entender toda la jerga relacionada. La costumbre de autenticarse sin más que introducir su nombre y contraseña, lo hace sentir rebasado por la complejidad tecnológica de las firmas digitales y la criptografía de clave pública. En este sentido la introducción de la tecnología sin niveles adecuados de capacitación se torna casi inviable.

La seguridad y almacenamiento de la clave privada

Ninguna solución de PKI es más fuerte de lo que lo es su eslabón más débil. En otras palabras, si no protege correctamente las claves privadas que forman el núcleo de la PKI, se estará comprometiendo la seguridad de la infraestructura de confianza y, en último término, de su organización.

No hay nada más crítico para la seguridad de una PKI que la integridad y el carácter secreto de la clave privada de la autoridad de certificación. En las PKI basadas en software, las claves son vulnerables, al ser creadas, almacenadas o gestionadas en servidores con arquitecturas y sistemas operativos abiertos. Cada vez que el sistema utiliza una clave, ésta queda expuesta a posibles ataques. Una vez que una clave ha sido robada, la integridad de todo el sistema puede quedar expuesta al riesgo de emisión de certificados falsos, expedidos por quien ha atacado el sistema, que pueden poner en peligro la validez de todas las identidades digitales expedidas con esa clave de CA.

Identificación de circuitos administrativos

Casi cualquier número de transacciones electrónicas puede requerir los niveles de seguridad que provee una PKI, sin embargo es importante hacer una adecuada elección del alcance y los ámbitos de aplicación de los servicios de criptografía asimétrica para lograr ahorros y no incurrir en sobrecostos de implementación

Estrategias y Propuestas

Por último, hemos intentado aquí resumir las acciones estratégicas principales que se desprenden de este subestudio de factibilidad operativa y que son consecuencia de los desarrollos plasmados en su contenido.

- Considerar la Planificación de la PKI de propósito general como un elemento realmente estratégico, que le de coherencia y unidad a las aplicaciones aisladas que se desarrollen en la Provincia.

- Generar Políticas, Normas y Procedimientos de alcance general para apoyar y realizar aplicaciones basadas en la tecnología de Firma digital en el ámbito administrativo y de prestación de servicios de la Administración Pública Provincial.

- Identificar aplicaciones a través de un diseño adecuado y coherente de una Infraestructura de Clave Pública

- Desarrollar actividades de sensibilización, capacitación y difusión de la tecnología asociada

- Cumplir ampliamente con los requisitos legales establecidos por la Ley 25506 y su Decreto Reglamentario

- Emplear tecnología estándar y certificada

- Transmitir seguridad, solidez y confiabilidad a través de la estructura funcional, procedimientos operativos, y políticas de registro y certificación.

- Estudiar ampliamente la aplicabilidad funcional de los certificados digitales.

- Mantener cierta flexibilidad y apertura operativa.

- Procurar una escalabilidad adecuada al entorno provincial planteando una Infraestructura de Clave Pública por etapas de crecimiento.

- Comenzar con aplicaciones piloto para luego escalar.

- Prestar asesoramiento y apoyo a proyectos relacionados con la tecnología de firma digital

- Como fin último desarrollar ampliamente los servicios prestados sobre la infraestructura planteada, ya que es lo que esencialmente determina su valor real

Anexo II: Análisis Factibilidad Económico- Financiera

Conclusiones

Hemos plasmado aquí un boceto de las características del sector en el que se desenvuelven las Infraestructuras de Clave Pública, así como también hemos determinado que tipos de costos deberemos de absorber en la implementación y de que tipo de beneficios disfrutaremos una vez alcanzados los objetivos.

Costos

Encarar un proyecto de implementación de aplicaciones basadas en la teoría de firma digital en la Administración Pública Provincial es una tarea laboriosa, por cuanto se deben considerar los costos que implica la adopción de este nuevo estilo de trabajo, no solo por los cambios tecnológicos sino por los cambios culturales que implica.

Entre los aspectos más destacados en cuanto costos resaltamos:

•Estratégicos, o aquellos costos que insume el tiempo invertido en el planeamiento de todo lo que tenga que ver con el diseño e implementación de una Infraestructura de Clave Pública.

•La inversión en el establecimiento y operación efectiva de autoridades certificadoras, depósitos de claves públicas y todos los servicios necesarios para el funcionamiento de estos procesos.

•Educación, este aspecto incluye tanto el entrenamiento del personal interno para redefinir y asumir nuevas responsabilidades en un ambiente de Firma Digital, como así también la educación de los usuarios externos que eventualmente queden implicados en una aplicación de ésta tecnología.

•Implementación, incluye el costo del personal del área de Sistemas de Información que asegura la compatibilidad de las aplicaciones internas con los sistemas.

•Intercambios, gasto en comunicaciones y el mantenimiento de todos los elementos que permitan el óptimo funcionamiento de la PKI.

•Desarrollo, adquisición de programas, desarrollo y programación de las interfaces de aplicación, mejoramiento del software de aplicación interno para aprovechar todas las ventajas de una PKI y las pruebas necesarias para la óptima implementación de la nueva Tecnología.

•Requerimientos de soft y Hardware definidos en el estudio de factibilidad técnica (Ver Anexo IV).

Beneficios

El despliegue de una PKI y la utilización de certificados digitales posee, desde varios puntos de vista un costo relativo más que eficiente debido al elevado nivel de seguridad que otorga. No resulta fuera de lo común que en los

países más avanzados se haya utilizado la tecnología de certificación digital y que goce de perspectivas firmes de expansión. Cabe señalar también, que en la actualidad es una tecnología que por sus características no posee sustitutos.

Entre los aspectos más destacados en cuanto a beneficios resaltamos:

•Disminución de costos materiales en papel, correo, cartuchos de impresora, horas hombre y principalmente en tiempo,

•Transparencia de información, ya sea en trámites internos o externos, lo que redunda en una mayor eficiencia y rapidez en los procesos internos o en la prestación de servicios al ciudadano.

•Potencialidad para dotar al sistema de una mayor transparencia y obtener la consecuente reducción del gasto público y restablecer la credibilidad en las instituciones democráticas.

•Ahorros de costos de transacción y almacenamiento

•Mayor agilidad y eficiencia en los procesos que involucran papeles y documentos oficiales.

•Creación de nuevos mercados, generará redes productivas más ágiles entre diversas empresas e introducirá mayor eficiencia en sectores público y privado, produciendo significativos avances en materias de productividad.

•Eliminación de trabas burocráticas.

•Trabajo cooperativo, educación a distancia, servicios de la administración pública como los trámites y el pago de impuestos.

•El mayor grado de seguridad que puede obtenerse de un documento firmado digitalmente.

•Amplio abanico de servicios de seguridad

•Facilidad de búsqueda y de acceso, liberación de espacio físico, limpieza, seguridad

Concretamente nos trae enormes beneficios en la relación:

Administración ⟶ **Administrado**

Tales como:

- La presencia segura de la administración en la red
- La consulta de información personal desde internet
- La realización de trámites varios en internet como pago de tributos u obtención de certificaciones.
- Acceso a aplicaciones informáticas de gestión
- Comunicación entre dependencias de la administración pública
- Integración de información al ciudadano desde distintas administraciones
- Aplicaciones de democracia electrónica tales como el plebiscito o el sufragio.

Por tanto dichas modalidades de trabajo, el incremento de la velocidad de circulación de la información a través de los documentos digitales y el notable incremento de la seguridad del entorno hará que se ofrezcan más y mejores servicios al ciudadano y simultáneamente se logren ahorros de tiempo y costos.

Beneficios concretos de la despapelización

En función de la enorme cantidad de tiempo y dinero que el Gobierno Provincial destina al papeleo, los potenciales beneficios de procesar tal cantidad de información por medios digitales son considerables.

Dicha afirmación es posible sustentarla en las siguientes reducciones:

Reducción de costos

Los llamados formularios digitales seguros pueden producir economías de hasta un 90% por sobre el procesamiento manual usado actualmente en el gobierno y en la prestación de servicios a los ciudadanos.

Costo unitario por formulario	De papel	Digital	Ahorro
Impresión y almacenamiento	U$S15	U$S1	U$S14
Llenado, procesado y codificado	U$S145*	U$S5**	U$S140
Costo por formulario completo	U$S160	U$S6	U$S154

EGovernment Solutions Secure eforms www.entrust.com

*Incluye el tiempo empleado en el llenado a mano, envío del formulario completo para su aprobación, envío al usuario final, el tecleo manual en la aplicación, el costo de formularios perdidos y los errores de tipeo.

**Incluye llenado del formulario, remisión del formulario, procesamiento de los datos del formulario en la base de datos o en aplicaciones de oficina.

Las fuentes de reducción de costos a partir del uso de herramientas digitales de despapelización son múltiples:

•Eliminación o reducción al mínimo de los costos de impresión.

•La eliminación de duplicaciones de entrada de información y errores de transcripción puede reducir los costos operativos.
•Las reglas automáticas para recolección de datos precisos reducen la necesidad de intervención manual y tiempo de procesamiento para corregir errores.
•La automatización de los procesos habilitada por los formularios digitales seguros, puede reducir los costos operativos que insume su procesamiento efectivo.
•Los servicios de distribución basados en aplicaciones Web son generalmente más económicos que los servicios de distribución manuales.

Reducción de errores

El procesamiento de errores puede reducirse drásticamente a través del uso de formularios digitales seguros. Cuando formulario digital se diseña, cada campo puede enmascararse para aceptar sólo un tipo de caracter o un formato de datos definido. Esto simplifica el trabajo de la persona que completa el formulario al incluir la información apropiada en el formato requerido. Si un usuario completa un campo con información errónea, un formulario electrónico seguro puede devolver el formulario inmediatamente al usuario para la corrección antes de que empiece a ser procesado, reduciendo tiempo y costo de gestión manual.

Reducción de los tiempos de procesamiento

Habilitando el uso de los formularios digitales seguros en línea, se puede disminuir significativamente el tiempo de proceso, ya que los datos no tienen que ser transferido manualmente del formulario de papel a una base de datos u otro sistema de procesamiento electrónico. Este retecleo de información, consume tiempo, dinero e incrementos en la tasa de error.

Cuando se controlan los errores durante la recolección de datos, el tiempo del proceso aumentado que es el resultado de los formularios incompletos o incorrectos se minimiza, produciendo la realización más rápida de la actividad.

Cuando los datos se procesan electrónicamente, la distribución de la información es casi instantánea. Usando los servicios estándar de mensajería sólo se agregan días que suman tiempo de proceso. Para los formularios de uso interno, el tiempo adicional se pierde con los movimientos de papeleo entre oficinas para lograr las firmas de la aprobación correspondiente. Cuando los formularios digitales seguros utilizan las tecnologías relacionadas con la firma digital, las firmas digitales pueden agregarse rápidamente y con la misma confianza depositada en las firmas manuscritas.

Finalmente, cuando pueden accederse a los formularios digitales a través de un portal gubernamental, la disponibilidad de acceso a toda hora permite a los ciudadanos completar y enviar los formularios a su conveniencia.

Los beneficios de usar los formularios digitales seguros para el gobierno se traducen en aplicaciones virtuales útiles de gobierno a ciudadano (G2C), de gobierno a empresas (G2B), de gobierno a gobierno (G2G) y en los procesos internos de gobierno.

El daño hecho a la confianza pública y a la seguridad por las brechas de seguridad electrónicas puede ser muy perjudicial para los gobiernos. Mientras que los beneficios de la despapelización son tremendos, los gobiernos deben focalizarse en la seguridad, a priori los requerimientos de privacidad y de firma digital deben tenerse en cuenta para llevar a cabo las soluciones gubernamentales electrónicas.

Anexo III: Análisis de Factibilidad Legal

Si bien se considera que las manifestaciones de voluntad, los contratos privados y las actuaciones administrativas ante y por el estado a través de me-

dios electrónicos y telemáticos, no difieren "sustancialmente" o en su contenido de los actos contractuales y administrativos realizados sobre la base del soporte en papel, resulta necesario dotar de seguridad jurídica a las declaraciones de voluntad emitidas digitalmente, atendiendo a las características especiales del proceso de formación de la voluntad y su manifestación digital.

Ante el impulso de la realidad y la significación de las contrataciones digitales, esta dificultad legal debió ser superada, llenando el vacío legislativo existente en una materia de reciente data, pero de una inusitada gravitación en la vida jurídica de las personas y las instituciones.

De tal manera se concibió la estructura técnica y jurídica de la firma digital, como sustituto válido y seguro en los documentos digitales, de la firma ológrafa prevista por el codificador, en el siglo 19 para los instrumentos privados escritos en soporte papel.

Antecedentes INTERNACIONALES

En el plano internacional tienen lugar actualmente múltiples actividades y debates en torno a los aspectos legales de la firma digital:

- La Comisión Europea ha redactado su borrador final de Directiva de Firma Digital ("Propuesta de Directiva del Parlamento Europeo y el Consejo sobre un Marco Común Para las Firmas Electrónicas") del 13 de mayo de 1998, publicado en el Diario Oficial de las Comunidades Europeas del 23 de octubre de 1998, que establece las pautas para la utilización de la firma digital por los Estados miembros.
- La Comisión de las Naciones Unidas para el Derecho Comercial Internacional (UNCITRAL) ha aprobado una Ley Modelo sobre Comercio Electrónico y ha comenzado a trabajar en la preparación de normas uniformes en materia de firma digital.
- Ley Modelo de la Comisión de las Naciones unidas para el derecho mercantil internacional (CNUDMI) sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno.

•La Organización de Cooperación y Desarrollo Económico (OCDE) prosigue sus trabajos en este ámbito, a modo de continuación de sus pautas de política criptográfica de 1997.

•Otras organizaciones internacionales, como la Organización Mundial del Comercio (OMC), han empezado también a interesarse en el tema.

•El Comité de Seguridad de la Información de la Sección de Ciencia y Tecnología de la American Bar Association ("ABA" – Asociación de Abogados de los EE.UU.) redactó su Normativa de Firma Digital en 1996, en la que participaron casi ochenta profesionales de las disciplinas del derecho, la informática y la criptografía de los sectores público y privado, en la que especifica un mecanismo de firma digital a base a criptografía asimétrica, los certificados de clave pública y los certificadores de clave pública.

•Directiva 99/93 de la Unión Europea que tiene por finalidad facilitar el uso de la firma electrónica y contribuir a su reconocimiento jurídico. Crea un marco jurídico para la firma electrónica y para determinados servicios de certificación con el fin de garantizar el correcto funcionamiento del mercado interior. No regula otros aspectos relacionados con la celebración y validez de los contratos u otras obligaciones legales cuando existan requisitos de forma establecidos en las legislaciones nacionales o comunitaria, ni afectan a las normas y límites, contenidos en las legislaciones nacionales o comunitaria, que rigen el uso de documentos.

Antecedentes NACIONALES

Una recopilación de este tipo de normativa en la República Argentina arrojó los siguientes resultados:

1. **Resolución MTSS N° 555/97 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL - Normas y Procedimientos para la Incorporación de Documentos y Firma Digital.** Define el documento digital,

la firma digital, el certificador de clave pública, el certificado, la clave privada, la clave pública y establece que los documentos digitales se considerarán válidos y eficaces, surtiendo todos los efectos legales y probatorios cuando estén firmados digitalmente.

2. **Resolución SAFJP N° 293/97 SUPERINTENDENCIA DE ADMINISTRADORAS DE FONDOS DE JUBILACION Y PENSIONES - Incorporación del Correo Electrónico con Firma Digital.** Establece que los CD-ROMs remitidos por las Administradoras de Fondos de Jubilaciones y Pensiones, debidamente identificados por el Sistema, serán válidos y eficaces, surtiendo todos los efectos legales y probatorios, a partir de la fecha y hora en que queden disponibles en las bandejas de entrada y que la firma electrónica o clave de seguridad habilitante para acceder al sistema poseerá el mismo valor legal que la firma manuscrita.

3. **Resolución SFP N° 45/97 SECRETARIA DE LA FUNCION PUBLICA - Incorporación de Tecnología de Firma Digital a los Procesos de Información del Sector Público.** La SECRETARIA DE LA FUNCION PUBLICA adhiere y hace suyos los conceptos vertidos por el Sub-Comité de Criptografía y Firma Digital del CUPI en el documento "Pautas Técnicas en la Materia de Normativa de Firma Digital" y autoriza el empleo de ésta tecnología para la promoción y difusión del documento y la firma digitales en el ámbito de la Administración Pública Nacional.

4. **Resolución SFP N° 212/98 SECRETARIA DE LA FUNCION PUBLICA** - Políticas de Certificación para el Licenciamiento de Autoridades Certificantes. La SECRETARIA DE LA FUNCION PUBLICA dicta los estándares de licenciamiento y operación de las autoridades certificantes de la Administración Pública Nacional.

5. **Decreto N° 427/98 del PODER EJECUTIVO - Firmas Digitales para la Administración Pública Nacional.** Autoriza el empleo de la firma

digital en la instrumentación de los actos internos del Sector Público Nacional, que no produzcan efectos jurídicos individuales en forma directa. El Decreto fue redactado por el Sub-Comité de Firma Digital del CUPI ("Comité de Usuarios de Procesamiento de Imágenes"), convocado por el BANCO CENTRAL DE LA REPUBLICA ARGENTINA y del que participaron representantes de distintos organismos estatales.

6. **Resolución SFP N° 194/98 SECRETARIA DE LA FUNCION PUBLICA** - Estándares Aplicables a la Infraestructura de Firma Digital para el Sector Público Nacional del Decreto N° 427/98. La SECRETARIA DE LA FUNCION PUBLICA dicta los estándares de homologación de algoritmos criptográficos para la Infraestructura de Clave Pública de la Administración Pública Nacional.

7. **Resolución General CNV N° 345/99:** Incorpora al libro VIII otras disposiciones de las Normas (T.O. 1997) el Capítulo 23 Autopista de la Información Financiera.

8. **Decreto 1347/99:** regula sobre el Servicio de Conciliación Laboral Obligatoria (SECLO) del Ministerio de Trabajo y Seguridad Social.

9. **El proyecto enviado por el PEN** el 18 de agosto de 1999, el trabajo realizado los Doctores Horacio Lynch y Mauricio Devoto publicado por el CENIT (Centro de Investigaciones en Information Technology)

10. **Decreto N° 1023/2001:** permite a través de su artículo 21 la realización de las contrataciones comprendidas en el régimen en formato digital firmado digitalmente.

11. **Decreto N° 889/2001:** aprueba la estructura organizativa de la Secretaría para la modernización del Estado en el ámbito de la subsecretaría de la Gestión Pública, creando la Oficina nacional de Tecnologías de la Información y otorgándole competencias en materia de firma digital.

12. **Decreto N° 677/2001:** otorga a los documentos digitales firmados digitalmente remitidos a la Comisión Nacional de Valores de acuerdo con las reglamentaciones dictadas por ese organismo, similar validez y eficacia que los firmados en soporte de papel.

13. **Decreto N° 673/2001:** Crea la Secretaría para la Modernización del Estado en el ámbito de la Jefatura de Gabinete de Ministros, asignándole competencia para actuar como Autoridad de Aplicación del régimen normativo que establece la infraestructura de Firma Digital para el Sector Público Nacional y para la aplicación de nuevas tecnologías informáticas.

14. **Ley N° 25237:** a través del artículo 61 establece que la Sindicatura General de la Nación ejercerá las funciones de Organismo Auditante en el régimen de empleo de la firma digital en la instrumentación de los actos internos de la Administración Pública Nacional.

15. **La Ley de Firma Digital:** el proyecto de Ley de Firma Digital en la Argentina, recibió sanción definitiva con fuerza de ley por el Congreso Nacional con fecha 14 de Noviembre de 2001. La Ley N° 25.506 ha sido publicada en el Boletín Oficial N° 29.796 del 14 de diciembre de 2001. El Poder Ejecutivo Nacional reglamentará la nueva norma en un plazo de 180 días a partir de dicha publicación.

Está organizada en XI Capítulos y un Anexo en que se encuentran previstos los principios y fundamentos que hemos comentado en esta exposición. La Ley argentina de Firma Digital, en el Capitulo I, denominado de **Consideraciones Generales**, establece las principales definiciones en cuanto al objeto, alcances, validez y presunciones legales referidas a la firma digital.

Este proyecto de ley impone al Sector Público Nacional - Poder Ejecutivo, Poder Judicial y Poder Legislativo nacional – la obligación de digitalizar los documentos y la utilización de la firma digital. De manera tal que en un plazo no mayor a cinco años por lo menos el cincuenta por ciento de los

expedientes estén digitalizados y el cien por cien de los Decretos, Resoluciones, Sentencias, Leyes etc. se firmen digitalmente.

16. **Proyecto de Simplificación e Informatización de Procedimientos Administrativos *(PROSIPA)*:** en el contexto del Plan Nacional de Modernización, la Decisión Administrativa N° 118/2001 de Jefatura de Gabinete de Ministros implementa el proyecto mencionado en forma obligatoria para toda la Administración Pública Nacional. Sus objetivos contemplan el diseño e implementación de un nuevo modelo de gestión administrativa con soporte de firma digital y la adecuación de la normativa vigente en materia de tramitación administrativa a las nuevas tecnologías de gestión. La Secretaría para la Modernización del Estado es la Autoridad de Aplicación de la nueva norma.

17. **Decreto Reglamentario 2628/2002:** el Decreto, publicado en el Boletín Oficial del 20 de diciembre de 2002 establece para el ámbito federal lo que se da en llamar una Infraestructura de Firma Digital para ofrecer la autenticación y garantía de integridad para los documentos digitales o electrónicos y constituir de esa forma la base tecnológica que permita otorgarles validez jurídica, regulando el funcionamiento de los certificadores licenciados de manera de garantizar la adecuada prestación de los servicios de certificación. A tal fin crea un Ente Administrador de Firma Digital, encargado de otorgar las licencias a los certificadores, supervisar su actividad y dictar las normas tendientes a asegurar el régimen de libre competencia en el mercado de los prestadores y protección de los usuarios de Firma Digital, supliendo de esa forma una falencia que tenía la Ley 25.506

Por su parte, en su articulado regula la conformación de una Comisión Asesora para la Infraestructura de Firma Digital, con un equipo multidisciplinario de especialistas en la materia, con el fin de asesorar y recomendar a la Autoridad de Aplicación estándares tecnológicos, y otros aspectos que hacen al

funcionamiento de la mencionada Infraestructura, designando al efecto a la Jefatura de Gabinete de Ministros.

18. **La Resolución 176/2002 de Jefatura de Gabinete de Ministros** habilita el Sistema de Tramitación Electrónica para la recepción, emisión y archivo de documentación digital firmada digitalmente. Este sistema, que funcionará en el Departamento de Mesa de Entradas y Despacho de la Subsecretaría de la Gestión Pública, permitirá el ingreso y despacho de documentos vía correo electrónico firmado digitalmente, emitiendo los correspondientes acuses de recepción fechados y firmados en formato electrónico. Publicada en el Boletín Oficial del 15 de Abril del 2002.

19. **La Resolución 17/2002 de la Subsecretaría de la Gestión Pública** regula el procedimiento para tramitar la certificación exigida al Registro del Personal acogido al Sistema de Retiro Voluntario, habilitando la modalidad de tramitación mediante el empleo de documentación digital firmada digitalmente, en lo que constituye la digitalización de un trámite interno de la Administración Pública con el empleo de la tecnología de firma digital. Publicada en el Boletín Oficial del 15 de Abril del 2002.

20. **Decreto N°78/2002:** faculta a la Subsecretaría de la Gestión Pública a actuar como autoridad de aplicación del Régimen Normativo que establece la Infraestructura de Firma Digital para el Sector Público Nacional, como así también en las funciones de organismo licenciante en la materia.

Además exhorta a la Oficina Nacional De Tecnologías De Información a promover la utilización de Firma Digital en los organismos del Sector Público Nacional actuando como autoridad certificante y a:

- Entender en la elaboración del marco regulatorio del régimen relativo a la validez legal del documento y firma digital, así co-

mo intervenir en aquellos aspectos vinculados con la incorporación de estos últimos a los circuitos de información del sector público y con su archivo en medios alternativos al papel.

- Ejercer las funciones de Organismo Licenciante de la Infraestructura de Firma Digital para el Sector Público Nacional.

21. **Decreto 283/2003:** que autoriza con carácter transitorio a la Oficina Nacional de Tecnologías Informáticas a proveer certificados digitales para su utilización en aquellos circuitos de la Administración Pública Nacional que requieran firma digital, de acuerdo a la política de certificación vigente.

Antecedentes PROVINCIALES (Mendoza)

- Con la aplicación de **la Resolución N° 54 / 99 y del Decreto – Acuerdo N° 1806 del 5 de octubre de 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 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.

Conclusiones y Propuestas

Ley de Adhesión.

Como primera medida, se estima conveniente emitir la norma legal fundante del resto del andamiaje jurídico sobre la materia, engarzando en la posibilidad que contempla la legislación nacional vigente, ley 25.506, art. 50, que expresamente dispone: "*Invitación. Invítase a las jurisdicciones provinciales a instrumentar los instrumentos legales pertinentes para adherir a la presente ley.*".

Así las cosas, la provincia debe contar con la ley de adhesión, la cual no reviste mayores dificultades técnicas, sin perjuicio de las variables políticas que correspondan ser evaluadas, atento al alto nivel de innovación que implica la implementación de la materia *sub examine*.

La mencionada ley 25.506, si bien es de alcance nacional (regula materia contemplada por el C.C.) y por lo tanto en sentido estricto no necesita de adhesión, siendo obligatoria; deja abierta la posibilidad de adhesión a los fines de su instrumentalización.

Ello por cuanto la materia de fondo constituye facultades delegadas al gobierno nacional (art. 75 inc. 12), pero la materia administrativa es de competencia local.

Decreto Reglamentario.

Así las cosas, el gobierno provincial debe proceder a emitir la norma correspondiente –decreto reglamentario de la ley de adhesión- a fin hacer operativa la norma básica.

Contenido básico del decreto reglamentario local.

Como dijimos, el dictado del decreto implica la instrumentalización concreta en el orden local de la legislación nacional referida.

Siendo competencia del Poder Ejecutivo (art. 128 inc. 2 CPr.), será éste quien deberá por lo tanto tomar las decisiones concretas que, plasmadas en el decreto, permitirán incorporar el producto elaborado.

Anexo IV: Análisis de Factibilidad Técnica

Ingeniería de Proyecto

5.1.4. El modelo propuesto para la PKI provincial

Como lo hemos planteado desde los objetivos del presente estudio, es nuestra intención proponer un diseño técnicamente confiable y ajustado a los estándares nacionales e internacionales de modo de garantizar confiabilidad, confidencialidad, integridad y disponibilidad permanente. Así mismo, hemos propuesto como premisas fundamentales para el modelo, asegurar la escalabilidad y la interoperabilidad con la mayor cantidad de aplicaciones posibles.

Estos objetivos, en el marco del análisis de estructuras previo, y tomando en cuenta las dimensiones que se definieron en el *punto 3. Tamaño Óptimo*, implican considerar el diseño de una infraestructura de pequeña escala, lo que no amerita en principio la existencia de más de una Autoridad Certificante (CA) y alternativamente una o más Autoridades de Registro (RA), pero que contemple un mecanismo de ***crecimiento gradual y ordenado*** ajustado a políticas y procedimientos unívocos o al menos con un alto grado de consistencia.

Es fundamental considerar, en relación a este último punto, que nuestro proyecto contempla la inclusión en la PKI de grupos de usuarios y entidades que pertenecen a ***una misma organización institucional***, el Gobierno de la Provincia de Mendoza. Por esto debe existir coherencia en los modelos de implementación, las políticas de certificación y los manuales de procedimientos.

Bajo estas consideraciones proponemos el siguiente diseño preliminar de PKI provincial:

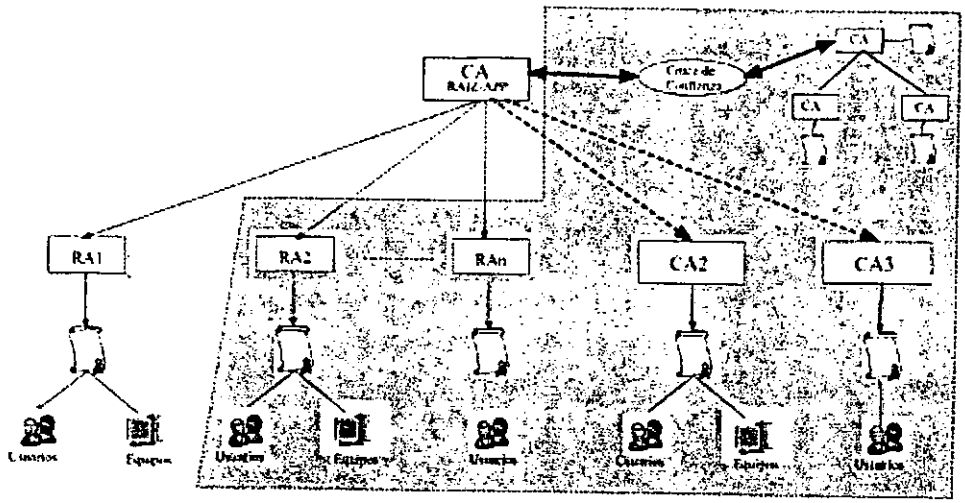


Figura 4

Esquema de diseño preliminar propuesto para la PKI provincial

Importante: La parte sombreada prevé como debe escalar el modelo. La implementación inicial propuesta, sólo contempla una CA y una RA.

El modelo precedente propone una **implantación inicial** de:

- ***Una Autoridad Certificante (CA):*** que permita el manejo del ciclo de vida de certificados , a través de la solicitud, aprobación, renovación, auditoría y revocación de certificados
- ***Una Autoridad de Registro (RA):*** que permita desarrollar funciones, tales como aprobación de certificados, remisión de solicitud aprobada a la CA, auditoría, manejo de las solicitudes de revocación y otras; de manera distribuida entre un número ilimitado de administradores, asegurando la separación de roles.

- Sistemas totalmente redundantes acordes a un Plan de Contingencia, de modo de prever la posible caída del punto único de confianza.
- Sistema de recupero ante desastres.
- Disponibilidad total las 24 horas del día, 7 días por semana, 365 días al año.
- Plena seguridad sobre la red y los datos. Enlaces altamente confiables.

Y prevé un **modelo de escalabilidad jerárquico** con las siguientes características:

- Posibilidad de agregar nuevas Autoridades de Registro, eventualmente con funciones distribuidas por Organismo de Gestión o Ministerio; ó alternativamente por tipo de certificados que gestionan.
- Posibilidad de subordinar a una CA Raíz, otras Autoridades Certificantes que se ajusten a políticas, estándares y procedimientos consistentes. Esto tiene por objetivo, proveer al modelo de mecanismos de división de la carga de trabajo, mejora de performance, actualización tecnológica, distribución de roles, aseguramiento de la disponibilidad del sistema, etc.
- Eventual posibilidad de interconectar a la jerarquía provincial con otras PKI jerárquicas o en red a través de un Bridge o puente de confianza. *(Ver Federal Bridge Certification Autority of USA* – http://www.cio.gov/fpkisc*)*

5.2. Especificaciones funcionales que debe satisfacer la Infraestructura de Clave Pública

Teniendo en cuenta las expectativas expresadas en el diseño preliminar de la PKI provincial que se presentó en el punto anterior, se expone a continuación una vista de los requerimientos funcionales que a partir de la investigación preliminar se ha determinado, debería satisfacer la ***solución tecnológica*** que se adopte, de modo de garantizar los requisitos preestablecidos de seguridad, disponibilidad, flexibilidad, interoperabilidad y escalabilidad.

Esta lista de requerimientos no pretende ser una enumeración taxativa y acabada, ni un diseño detallado de las especificaciones funcionales de la PKI; sino un recorte de aquellos aspectos que se consideran más relevantes a tener en cuenta.

La misma, constituye una guía orientadora para evaluar a priori, y a los fines del estudio de factibilidad técnica, las distintas alternativas de implantación tecnológica que se postulan en la presente ingeniería de proyecto.

5.2.1. Seguridad de la clave privada de la CA

- Almacenamiento seguro mediante un dispositivo en hardware (HSM) de la clave privada de la CA que se ajuste al estándar FIPS 140-1 de nivel 3.
- Restricciones de Copyrigth que prevengan la distribución de la clave raíz de la CA.
- Reinicio de todos los servicios de la PKI luego de una caída del servidor de la CA sin compromiso de la clave de administrador ni otras claves maestras.
- Duplicado y recuperación, en caso de desastre, de la clave de la CA, con un sistema altamente seguro de puesta en común de información secreta entre múltiples partes, mediante la utilización de "k de n" tarjetas inteligentes.

5.2.2. Par de claves

- Posibilidad de generación centralizada de claves, backup de las claves privadas y la recuperación distribuida de claves.
- Esquemas de pares de claves duales: Alternativamente, se debe proveer a los usuarios dos pares de claves con fechas de expiración independientes: uno para firma y otro para cifrado. De este modo, se puede mantener un back-up (copia de resguardo) de las claves privadas de cifrado, de modo tal que documentos cifrados históricos puedan ser recuperados en el tiempo. La clave privada de firma sólo existirá durante la validez de un certificado emitido a un usuario final, de modo tal de garantizar no repudio.
- Posibilidad de que el administrador pueda especificar fechas de vencimiento independientes para la firma de la clave privada y la comprobación de la

clave pública, de modo que las comprobaciones puedan tener éxito después de que la clave de firma expira.

5.2.3. Protección de claves privadas

- Protección de las claves privadas de usuarios finales, servidores o dispositivos de red con por lo menos, un esquema basado en password. Dicho sistema debe mantener reglas estrictas en cuanto a la generación de password que indiquen longitud, formato, fecha de finalización, etc.). Estas reglas deben poder ser configurables por el administrador central. Dichas password no pueden ser almacenadas como texto en claro (sin cifrar) en ningún sitio, ni ser transmitidas como texto en claro por la red bajo ningún motivo.
- Soporte a la autenticación mediante: passphrase o PIN; dispositivos biométricos y smart cards.

5.2.4. Resguardo y recuperación de claves de cifrado

El resguardo y recuperación de claves de cifrado es muy importante para asegurar que la Administración Pública Provincial siempre será capaz de desencriptar la información que le es propia, manteniendo el control sobre la misma.

- Resguardo y recuperación de claves de cifrado.
- Recuperación de una clave de usuario para cifrado ante la pérdida de la misma.
- Recuperación del histórico de claves de un usuario ante la pérdida de una de las claves.
- Recuperación de claves mediante la presentación de m de n cerfiticados de administrados, de modo tal de garantizar el proceso de recuperación de claves.

5.2.5. Gestión de Certificados

- Interfaz web para que los usuarios finales puedan enviar solicitudes de enrolamiento, solicitudes de renovación, solicitudes de revocación, descargar las CRLs, etc.
- Administración automatizada que permita la autenticación y revocación transparente de usuarios o dispositivos, utilizando directamente sistemas administrativos o bases de datos preexistentes.
- Aprobación manual de solicitudes de emisión de certificados.
- Emisión de cerfiticados para SSL, S/MIME y Object signing.
- Soporte a la inclusión de extensiones propias y personalizadas a los certificados emitidos por la CA, sobre un modelo de información básico.
- Soporte a la emisión masiva de certificados.
- Posibilidad de exportar e importar certificados y, alternativamente su par de claves asociadas como un mensaje cifrado, mediante contraseña proporcionada por un responsable.

5.2.6. Revocación de Certificados

- Interfaz web para que los usuarios finales puedan enviar solicitudes de revocación de sus certificados personales.
- Actualización y emisión automática de la Lista de Certificados Revocados (CRL) inmediatamente después de que un certificado ha sido revocado, de modo de garantizar plena actualización del estado de los certificados.
- Posibilidad de descarga de la CRL por parte de los usuarios para incorporarla a sus aplicaciones y hacer validaciones de certificados revocados off-line.
- Logs o seguimiento de la frecuencia de actualización de las CRLs.
- Posibilidad de revocación de certificados expirados de modo tal que puedan ser incluidos en las listas para verificación de firmas históricas. Es decir posibilidad de incluir certificados expirados en las CRLs.
- Ante una revocación por compromiso de la clave, posibilidad de ingresar una fecha que indique la última fecha cierta en la que la clave se supo no

comprometida, de modo tal que esta información pueda ser tenida en cuenta por el usuario ante una comprobación de validez del certificado.

- Posibilidades de revocación manual (por parte del administrador) y automática.
- Posibilidad de revocación masiva de certificados.

5.2.7. Actualización de Clave y actualización de Certificados

- Interfaz web para que los usuarios finales puedan enviar solicitudes de renovación de sus certificados personales.
- Soporte a la actualización automática de certificados y claves de forma transparente al usuario final.
- Actualización simultanea del par de claves junto al certificado, de modo tal de asegurar la rotación de claves.
- Tiempo de vida de los certificados configurables de acuerdo a las políticas de seguridad que se definan.
- Almacenamiento automático en un archivo histórico de las claves privadas de cifrado cuando los usuarios actualizan su par de claves.

5.2.8. Repositorio de certificados / Base de datos de la CA

- Chequeo de la integridad de datos que asegure el mantenimiento adecuado de los datos de enrolamiento de los usuarios.
- Backup periódico de la base de datos de la CA fuera de horarios picos, con previo chequeo de la integridad de los datos que se resguardan.
- Encripción de la base de datos para almacenamiento seguro.

5.2.9. Mecanismos de gestión del servicio de directorios

- Servicio de directorio que permita administrar automáticamente certificados y listas de certificados revocados en directorios compatibles con LDAP.
- Publicación automática de los certificados emitidos en el servicio de directorio de la CA, de modo de asegurar la inmediata disponibilidad de los certificados para otros usuarios.

- Función de recuperación del directorio en caso de fallo.
- Integración de listas de certificados y listas de certificados revocados en directorios compatibles con LDAP.
- Soporte a la comunicación con múltiples servidores LDAP, para balancear la carga de trabajo, garantizar redundancia y proveer escalabilidad.

5.2.10. Certificación cruzada

La certificación cruzada es importante tanto dentro del dominio de control de la Administración Pública como con Autoridades Certificantes externas que sean validadas desde el punto de vista de una jerarquía de confianza. Esto tiene importantes implicancias tanto en los enfoques de interoperabilidad como de disponibilidad.

- Soporte a certificación cruzada con propósitos de lograr interoperabilidad y flexibilidad.
- Inclusión de extensiones personalizadas en la emisión de cerfiticados curzados generados por la CA.
- Revocación de certificados de CA cruzados, en caso de deterioro de la confianza o relación con la otra CA, e impacto inmediato de la revocación sobre los usuarios afectados.
- Aprobación de certificación cruzada mediante la presentación de m de n certificados de administrador.
- Posibilidad de que ante una caída de la CA raíz de la jerarquía, las CA subordinadas reestablezcan rápidamente su confianza en otro par de CAs.
- Tiempo de vida flexible para los certificados cruzados.

5.2.11. Gestión de reportes y pistas de auditoría

Mantener un registro administrativo de las acciones desarrolladas en la PKI es una característica fundamental que la solución debe satisfacer. El seguimiento de las transacciones en las que se basan los certificados se debe realizar a través de registros de auditoría, reportes y prácticas de seguridad auditables. Para ello se requiere:

- Generación auditable de la clave raíz .
- Historial completo de cada clave generada.
- Log de transacciones del o los administradores centrales.
- Reporte de certificados emitidos a una fecha y con una fecha de caducidad determinada.
- Logs y reportes exportables para ser integrados en otras aplicaciones mediante interfase ODBC o para ampliar facilidades de consulta (SQL query).
- Otros logs de transacciones tales como: habilitación y baja de usuarios, recuperación de certificados, cambios de nombres (DN) y certificados pendientes de aprobación.
- Posibilidad de programar (schedule) la generación de reportes.
- Logs o seguimiento de la frecuencia de actualización de las CRLs.

5.2.12. Configuración de políticas de acceso a la PKI

- Configuración de tiempo límite de login de un usuario a la PKI y sus servicios de usuario.
- Configuración de la cantidad de intentos fallidos de login.
- Configuración de intervalo de tiempo transcurrido antes de permitir un nuevo login.

5.2.13. Servicio de Time stamping:

Con propósitos de no repudio es deseable que la PKI preste el servicio de sello de fecha y hora asociado a la firma. Dado que no se puede confiar en el reloj de cada PC, este servicio debe ser brindado desde un servidor de Time Stamping. Es deseable que la solución sea capaz de prestar servicio de time stamping para firmas DSA y firmas RSA. Sería deseable también compatibilidad con tokens PKIX. Se deberán llevar además logs de transacciones y pistas de auditoría de las operaciones de time stamping.

5.2.14. Integración con aplicaciones comunes:

Los certificados emitidos deben poder incorporarse y ser usados en las aplicaciones clientes típicas tales como outlook, outlook express, lotus notes, IE, Netscape communicator, etc. Para garantizar esto la solución debe proveer integración abierta con la mayor cantidad de aplicaciones y servicios de Internet, basada en los estándares del mercado, como X509 v3, LDAP, PKCS#7, PKCS#10, PKCS#12 y PKIX.

5.2.15. Condiciones de interoperabilidad

- Interoperabilidad testeada con los proveedores de servicios de certificación más importantes a nivel mundial: IBM, Verisign, GlobalSEt, Entrust, etc.
- Soporte a múltiples conjunto de caracteres para lenguajes internacionales.
- Integración abierta con la mayor cantidad de aplicaciones y servicios de Internet, basada en los estándares del mercado, como X509 v3, LDAP, PKCS#7, PKCS#10, PKCS#12 y PKIX.
- Soporte integral de todos los tipos de certificados estándar, incluyendo SMIME, SSL y IPSec (este último solo se considera por si en un futuro se escala a servicios de transacciones de comercio electrónico seguras bajo el estándar SET).

5.2.16. Condiciones de escalabilidad

- Soporte a la comunicación con múltiples servidores LDAP, para balancear la carga de trabajo, garantizar redundancia y proveer escalabilidad.
- La solución debe proveer un mecanismo escalable de gestión de certificados revocados de modo tal que no haya degradación de performance cuando el número de usuarios aumenta.

5.3. Ajuste a estándares

A continuación se especifican los estándares de la industria a los que deberá ajustarse la solución tecnológica que se adopte para garantizar los re-

quisitos preestablecidos de seguridad, escalabilidad e interoperabilidad; así como también para cumplir con las condiciones legales impuestas en la Ley 25.506, su decreto reglamentario y demás disposiciones vigentes.

Característica o Servicio	Especificación de normas y estándares
Algoritmo de generación del par de claves	- 2048 bits (RSA) [PKCS#1] - 1024 bits (RSA/DSA)
Algoritmo de firma	- Md5withRSAEncryption con longitud de clave igual o superior a 1024 bits (RSA) - Sha1withDSAEncryption con longitud de clave igual o superior a 1024 bits (DSA)
Algoritmo simétrico de encriptado de clave privada	- TripleDES [X9.52] en sus distintos modos de operación CBC, CFB, OFB con longitudes de claves de 112 y 168 bits - IDEA con bloques de 128 bits e idénticos modos
Gestión de las solicitudes de certificados	- Las solicitudes desde el CL (Certificador Licenciado) hacia el Ente de Licenciamiento deben remitirse en formato DER o PEM (ISO25-1) - Las solicitudes desde los usuarios hacia el CL (Certificador Licenciado) deben ser remitidas en formato [PKCS#10] o alternativamente pueden utilizarse otros formatos o mecanismos que permitan generar la solicitud desde los navegadores de Internet, siempre y cuando se pueda garantizar que el solicitante posee la clave privada correspondiente a la clave pública incluida en la solicitud y que dichas claves han sido generadas con las condiciones impuestas en las especificaciones propuestas en el presente estudio. - Las solicitudes deben ser verificadas del modo que lo describe la sección

	2.3 (Proof of Possession POP of Private Key) en Internet X.509 Public Key Infraestructure Certificate Managemente Protocols [PKIX-CMP]
Gestión de Certificados	- Emisión de certificados con el formato establecido en la norma X.509 v3 según el estándar ISO/IEC/ITU X.509 cuyos datos y formatos se ajusten a lo requerido en el apartado 4.2.2.2. de la Resolución 194/98 - Los certificados deben soportar el uso de extensiones (Key usage, basic constraint) según la norma X.509 v3 - Los mecanismos de revocación de certificados deben ajustarse a la norma X.509 [PKIX1] - El formato de entrega de los certificados para la integración con distintas aplicaciones debe ser PEM o DER [ISO25-1] - Identificación única del certificado de un titular, en un formato compatible con la norma X.520 - El período de validez, debe consignar fecha y hora expresada en Coordinated Universal Time (UTC) - Identificación del emisor de un certificado, en un formato que se ajuste a la norma X.520
Gestión de certificados para Servidores	Soporte a la emisión y gestión de certificados para servidores de aplicaciones de Internet sobre el protocolo HTTPS u otros servicios utilizando el protocolo TLS o SSL v3
Gestión de la lista de Certificados Revocados (CRL)	Debe ajustarse a la norma X.509 v2
Logs de transacciones, Registros de Auditorías y Reportes	Debe llevar logs completos y registros de auditoría de todas las actividades y transacciones realizadas en el ámbito de la Autoridad de Certificación y Autoridad de Registro.

Servicios de Directorio	El servicio de directorio debe permitir insertar automáticamente certificados y listas de certificados revocados en directorios compatibles con el protocolo LDAP
Servicio de TimeStamp (TSA: Time Stamp Authority)	Compatible con el estándar definido en [PKIX-TS]
Servicio de Notariado	De acuerdo a la norma Internet X.509 Public Key Infraestructure Data Certification Server Protocols [PKIX-DCS]
Transmición de mensajes en aplicaciones de correo electrónico	Compatible con el estándar [SMIME]
Protocolos de transmisión en línea segura	1.[PKIX-TSL] (Transport Layer Security) 2.SSL versión 3

Tabla 1 – Definición de Estándares

5.4. Alternativas de adquisición de plataforma tecnológica

Se presentan a continuación dos ***soluciones tecnológicas*** alternativas para la implantación de una PKI acorde al diseño y especificaciones funcionales propuestas. Las mismas se analizan en sus dimensiones de hardware, software, protocolos de comunicación y de seguridad. Se ha priorizado también el ajuste a estándares internacionales que garantizan seguridad e interoperabilidad testeada.

5.4.1. Alternativa 1: Tercerización de la plataforma tecnológica de soporte a la PKI en una empresa de servicios PKI

Uno de los escenarios posibles, que no podemos dejar de considerar en el presente estudio de factibilidad, es la alternativa de delegar en una empresa de servicios PKI todo el soporte y gestión de la plataforma tecnológica necesaria para lograr una PKI operativa en los términos descriptos.

Existen en el mundo múltiples empresas especializadas en los servicios de certificación digital y firma digital, que se han constituido en la solución para múltiples organizaciones y Gobiernos. En los estudios preliminares se evaluaron las soluciones propuestas por Verisign Inc. (www.verisign.com) y Entrust Inc. (www.entrust.com) dos de las empresas más importantes a nivel mundial con presencia en los Gobiernos de Chile, España, Canadá y EE.UU. entre otros.

La siguiente figura ilustra el esquema de implantación de nuestra Autoridad Certificante y Autoridad de Registro, bajo un escenario de tercerización total de la infraestructura tecnológica.

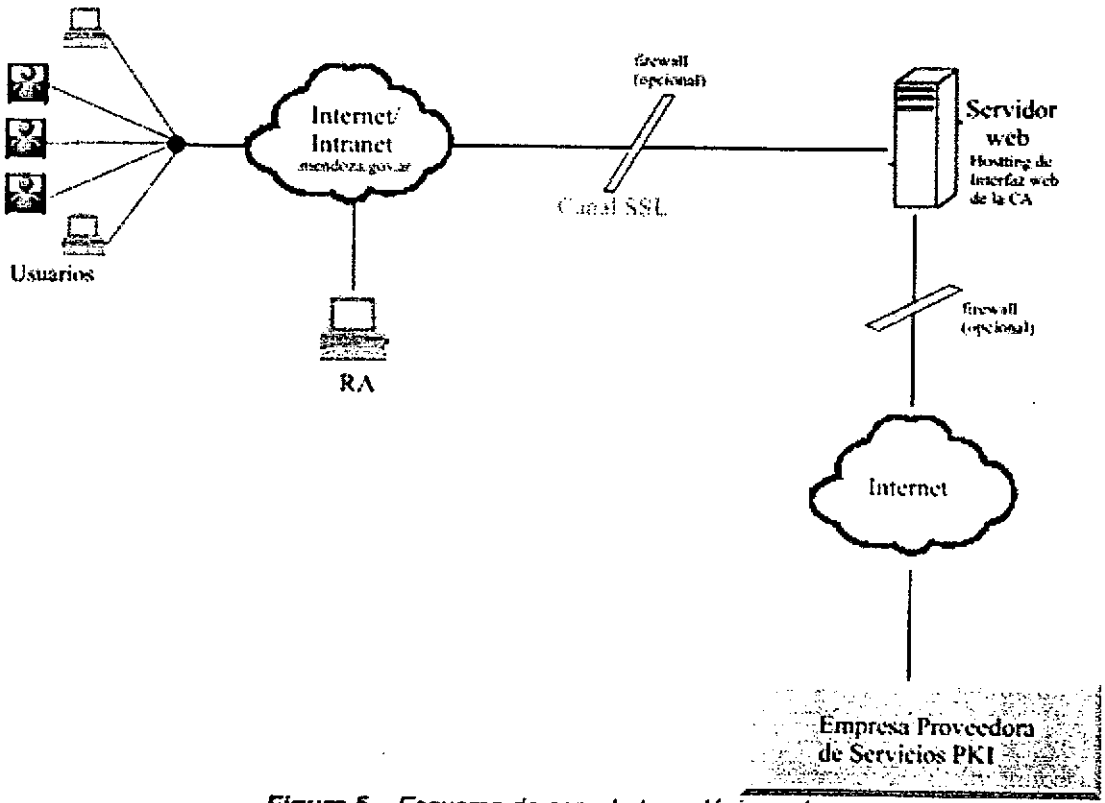


Figura 5 – Esquema de soporte tecnológico externo

Esta solución delega en una empresa externa todo el soporte tecnológico para la implantación de la Autoridad Certificante y funciones de Autoridad de

Registro, correspondiéndole contractualmente a dicha empresa garantizar la seguridad, disponibilidad permanente, interoperabilidad y escalabilidad de la infraestructura, así como también la construcción y gestión de planes de contingencia y recuperación ante desastres, en el marco de políticas de seguridad y procedimientos estandarizados mundialmente.

Bajo este esquema se provee a los administradores de la CA y RA provincial de una interfaz de administración remota, vía https (canal seguro) y asegurada mediante validación de cliente / servidor, que permite la configuración personalizada de los servicios de la PKI: Páginas de enrollamiento, gestión del CVC, gestión de las CRLs, configuración de políticas, administración de directorios, etc.

Las principal ***ventaja*** de este esquema de trabajo, es que en principio no se requieren inversiones especiales en equipamiento o conectividad fuera de las capacidades que hoy posee la provincia, puesto que solo se requiere hosting de las páginas de enrolamiento y administración del Ciclo de Vida de Certificados (CVC) junto a un Servidor Web para servirlas a los usuarios de la Intranet / Internet de Gobierno, y alternativamente un o dos dispositivos firewall. Todos elementos que hoy existen y se encuentran disponibles en la Administración Pública Provincial bajo los requerimiento técnicos de este tipo de implantación. Además se simplifican completamente las necesidades de Recursos Humanos capacitados y condiciones operativas para la administración de los servidores de la CA, Bases de Datos, directorios LDAP, mantenimiento de la seguridad, etc.

Sin embargo, esta propuesta presenta a nuestro criterio importantes ***desventajas*** de orden económico y técnico que no se pueden soslayar. En primer lugar, los costos de mantenimiento de los servicios externos son elevados y generan dependencia permanente de la empresa externa *(Ver Tabla 2 – Estimación de costos de outsourcing de la PKI)*. Por otra parte, consideramos poco confiable delegar todo el mantenimiento de la seguridad y los servicio de la PKI en una administración externa.

Cantidad de Certificados Gestionados	Costo estimado de mantenimiento anual para Certificados tipo X509 y S/Mime (En U$S)
	Costo Unitario U$S 12
200	2,400.00
500	6,000.00
1000	12,000.00
2000	24,000.00
10000	120,000.00
50000	600,000.00

Tabla 2 – Estimación de costos de outsourcing de la PKI

5.4.2. Alternativa 2: Implementación de una plataforma tecnológica propia

En este escenario definimos una ***vista lógica*** de los dispositivos y equipos que consideramos mínimamente necesarios para instrumentar la PKI propuesta de manera completa en las dependencias de la Gobernación de la Provincia de Mendoza. Proponemos también tres configuraciones alternativas de plataforma tecnológica para este modelo, con un análisis detallado de los costos, las debilidades y las fortalezas de cada una.

La siguiente figura ilustra el layout propuesto para la PKI provincial. En su lectura y análisis debe tenerse presente que el mismo propone un modelo de implementación concreta para el diseño propuesto en la *Figura 4 – Esquema de diseño preliminar propuesto para la PKI provincial* y que el ***criterio fundamental*** en su construcción ha sido lograr una estructura técnicamente confiable que garantice la seguridad, disponibilidad, eficiencia y escalabilidad de la solución con la mínima inversión posible.

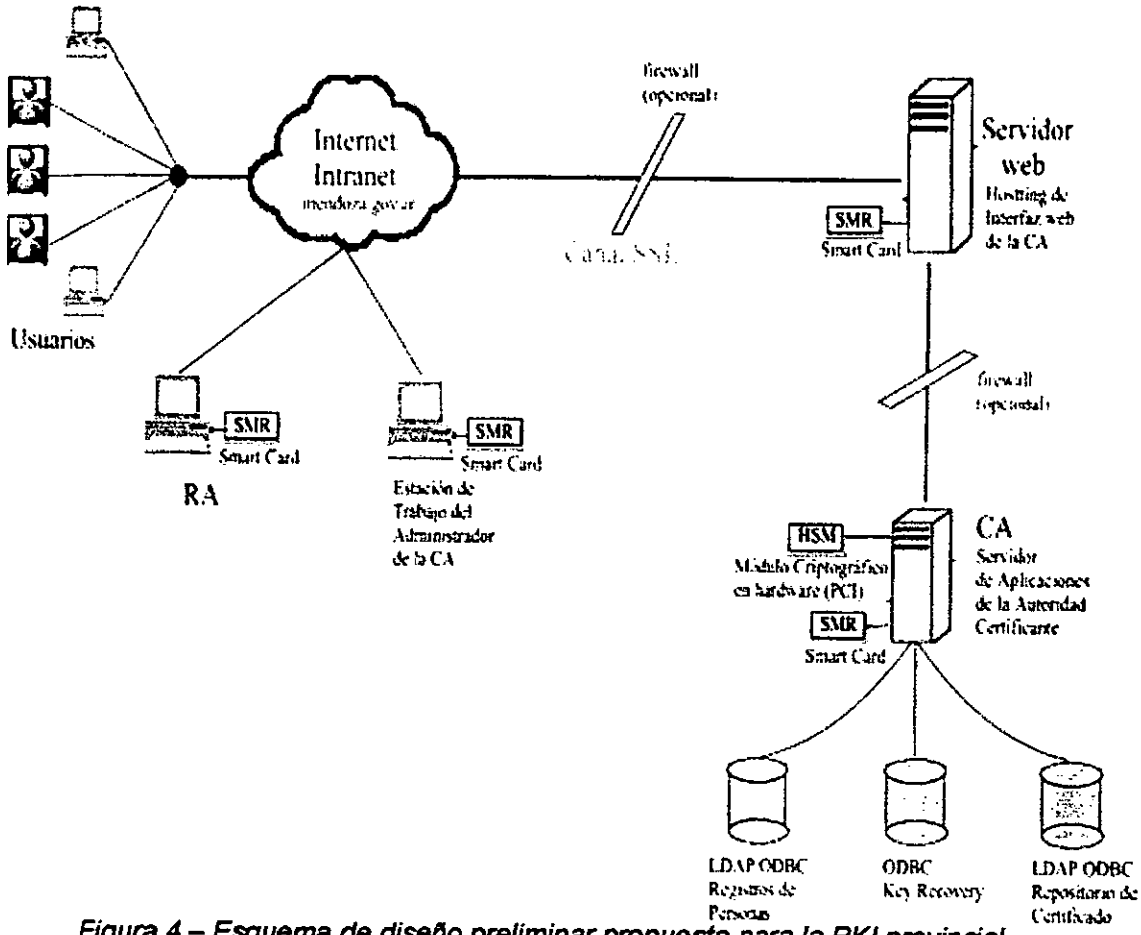


Figura 4 – Esquema de diseño preliminar propuesto para la PKI provincial

Exponemos a continuación tres alternativas de adquisición de plataforma tecnológica de soporte a este diseño PKI, las cuales varían en complejidad, calidad y costos.

Ver Configuraciones alternativas

Hoja de cálculo de
Microsoft Excel

Necesidades de Recursos Humanos

El abordaje de cualquiera de las soluciones técnicas que se han planteado para implementar la PKI provincial requiere la conformación de un equipo de personas técnicamente capacitado para administrarla de manera consistente y eficiente. Este equipo debería contar mínimamente con los siguientes perfiles.

- ***Administrador de servidores:*** administrador de los servidores implantados, encargado de gestionar la configuración del software de base y las aplicaciones que en el mismo se corren, el acceso de usuarios, las copias de seguridad de datos, el mantenimiento de los dispositivos periféricos y la seguridad lógica integral de todo el sistema.

- ***Administrador de Bases de Datos (DBA):*** encargado de administrar todas las aplicaciones vinculadas al almacenamiento de los datos que se mantienen en la PKI y su resguardo. En principio, estos repositorios serían el Registro de Personas, la base de datos para Recuperación de Claves en el esquema de par doble de claves (Key Recovery) y el Repositorio de Certificados.

- ***Administrador de la Autoridad de Registro (RA):*** Perfil con firma autorizada para desarrollar las funciones y procedimientos de Autoridad de Registro, tales como la aprobación de solicitudes de emisión, renovación y revocación de certificados, comprobación de bases de datos de personal, comprobaciones de datos de personas y equipos y todo lo concer-

niente a la autenticación de identidad y roles necesaria para otorgar y gestionar Certificados digitales.

- ***Administradores de la Autoridad Certificante (CA):*** Este perfil es crítico puesto que en él recaen las funciones principales de administración y mantenimiento de la Autoridad Certificante, sus aplicaciones asociadas y la garantía de cumplimiento de las políticas y procedimientos de seguridad establecidas para la misma. La o las personas que desarrollen este rol, individual o conjuntamente, deberán ser las únicas que tengan acceso físico y lógico a la clave privada de la CA, pilar fundamental de toda la seguridad de la infraestructura. Con ella podrán cumplimentar todas las funciones y operaciones definidas para la CA.

- ***Mesa de ayuda y soporte técnico:*** Es fundamental implementar un servicio permanente de soporte a usuarios, de modo tal de solucionar lo más rápidamente posible las dudas o inconvenientes que pudieran presentarse, tanto en la operación de las aplicaciones informáticas que usen los Certificados Digitales, como en el cumplimiento de procedimientos y ajuste a las políticas definidas por la CA.

- ***Web master:*** Teniendo en cuenta que se ha definido un formato de interfaz web para la interacción de los usuarios finales con la CA, se necesita un perfil capacitado para diseñar, construir y mantener las páginas web que constituirán dicha interfaz. Desde estas páginas una persona podrá en principio solicitar un Certificado Digital (Clase 1), solicitar la renovación o revocación de su Certificados, buscar y descargar Certificados de Terceras Personas, descargar un certificado de sitio o el certificado de la CA, consultar el servicio de directorios, descargar las Listas de Revocación de Certificados (CRLs), acceder al soporte técnicos, etc.

Una persona puede concentrar más de uno de estos roles, pero se recomienda que de acuerdo a un criterio de ***separación de funciones*** los siguientes perfiles sean desempeñados por personas diferentes:

El administrador de servidores, DBA, Administrador de RA y Administrador de CA deben ser personas distintas, con independencia funcional y jerárquica que desarrollen controles cruzados los unos sobre las actividades de los otros.

Es recomendable que la Administración de la CA esté distribuida entre dos o más personas con independencia funcional y jerárquica. Se recomienda también que la clave privada se integre conjuntamente con k de n tarjetas de acceso privadas de cada una de estas personas. Este criterio de seguridad es fundamental aún en la implementación de pequeña escala propuesta.

Las funciones de Autoridad de Registro pueden distribuirse entre distintas personas con firma autorizada, con el objetivo de distribuir la carga de trabajo. Esta distribución podría plantearse por distintos criterios, tales como: los usos de los certificados que gestionan, los sectores de la estructura de gobierno a los cuales están vinculados, etc.

Conclusiones y Sugerencias

Las siguientes conclusiones y sugerencias finales resultan de las investigaciones y pruebas preliminares realizadas; las cuales sustentan la información volcada en el presente documento.

Existen en el mercado múltiples configuraciones alternativas de equipamiento informático, aplicaciones de software, dispositivos de comunicaciones y de seguridad, que permiten implementar tecnológicamente una arquitectura PKI.

Las alternativas propuestas en la ingeniería de proyecto contemplan las especificaciones funcionales y técnicas deseables para una infraestructura técnicamente confiable, segura y escalable que brinde los servicios de certificación y firma digital a la comunidad del Gobierno de Mendoza. También consideran la adecuación de las soluciones a estándares abiertos. Existen hoy en día múltiples estándares asociados a las PKI. Debido a esto es muy importante contemplar que la solución que se adopte, se ajuste a determinados estándares y protocolos principalmente difundidos en la industria criptográfica de modo tal de garantizar condiciones de interoperabilidad, escalabilidad y seguridad. El ajuste a estándares es además un criterio fundamental para prevenir la rápida obsolescencia de la tecnología.

Desde el punto de vista técnico no recomendamos la alternativa de tercerización de la infraestructura tecnológica en una empresa de servicios PKI externa. Esta apreciación se sustenta en la dependencia que se genera de mecanismos y servicios tecnológicos, procedimientos y políticas, fijadas por terceras partes. Se debe tener en cuenta también, que en este caso se delega el manejo de los mecanismos que garantizan la seguridad y confidencialidad del sistema, pero no se delega la responsabilidad por las fallas de seguridad o disponibilidad que pudieran ocurrir.
Evaluando la relación costo / beneficio tampoco consideramos que la tercerización sea la alternativa más adecuada, ya que si bien soluciona la necesidad de una inversión inicial en tecnología, desaprovecha la economía de escala que se genera a medida que aumenta la cantidad de certificados gestionados por la PKI (Ver Tabla 2 – Estimación de costos de outsourcing de la PKI). Si consideramos la proyección de crecimiento que podría tener la infraestructura en la provincia, es económicamente inviable sostener en el tiempo esta alternativa.

Entre las alternativas de configuración propuestas para la implantación de la PKI en las dependencias de la Gobernación de la Provincia de Mendoza, se sugiere en primera instancia adoptar la tercera alternativa (Ver Configuración Alternativa 3). Esta recomendación se sustenta en que no requiere en principio inversión económica en software PKI, puesto que la solución propuesta es de código abierto y libre distribución. No obstante esto, satisface en gran medida las especificaciones funcionales y técnicas descriptas; y se ajusta a los estándares básicos propuestos en la legislación nacional, lo que garantiza posibilidades de escalarla progresivamente en el tiempo.

Luego de realizar una experiencia de gestión PKI primaria, se tendrá mayor información y conocimiento para proponer el diseño detallado de una infraestructura de mayor envergadura. Debe tenerse en cuenta en este sentido que el crecimiento no implica pérdida de la inversión en equipamiento realizada, ni conversiones inviables de los datos mantenidos en la jerarquía inicial, puesto que el ajuste a estándares descrito garantiza esta condición.

Al momento de implementar la solución concreta deberá tenerse presente que la Gestionabilidad de la PKI debe tener el mismo nivel de importancia que la seguridad, disponibilidad, interoperabilidad y escalabilidad. En este sentido deberán realizarse dedicados esfuerzos para lograr el equilibrio justo entre estos objetivos en ocasiones contrapuestos.

Finalmente es fundamental tener en cuenta, que el punto crítico para una implementación exitosa de estas tecnologías, es desarrollar las capacidades humanas para adquirirla y manejarla, tanto en el nivel de los especialistas técnicos encargados de diseñar, montar y poner en marcha la infraestructura como de los usuarios intermedios y finales de la misma.

En este último nivel de la jerarquía, los usuarios finales, es donde se deberá poner mayor énfasis al momento de desarrollar una plan de pruebas y puesta en marcha, contemplando un cuidadoso proceso de difusión y capacitación, de modo de garantizar el uso correcto de los certificados emitidos por la CA provincial.

III. Segundo informe Parcial: "Propuesta Organizacional de la Infraestructura"

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.

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).

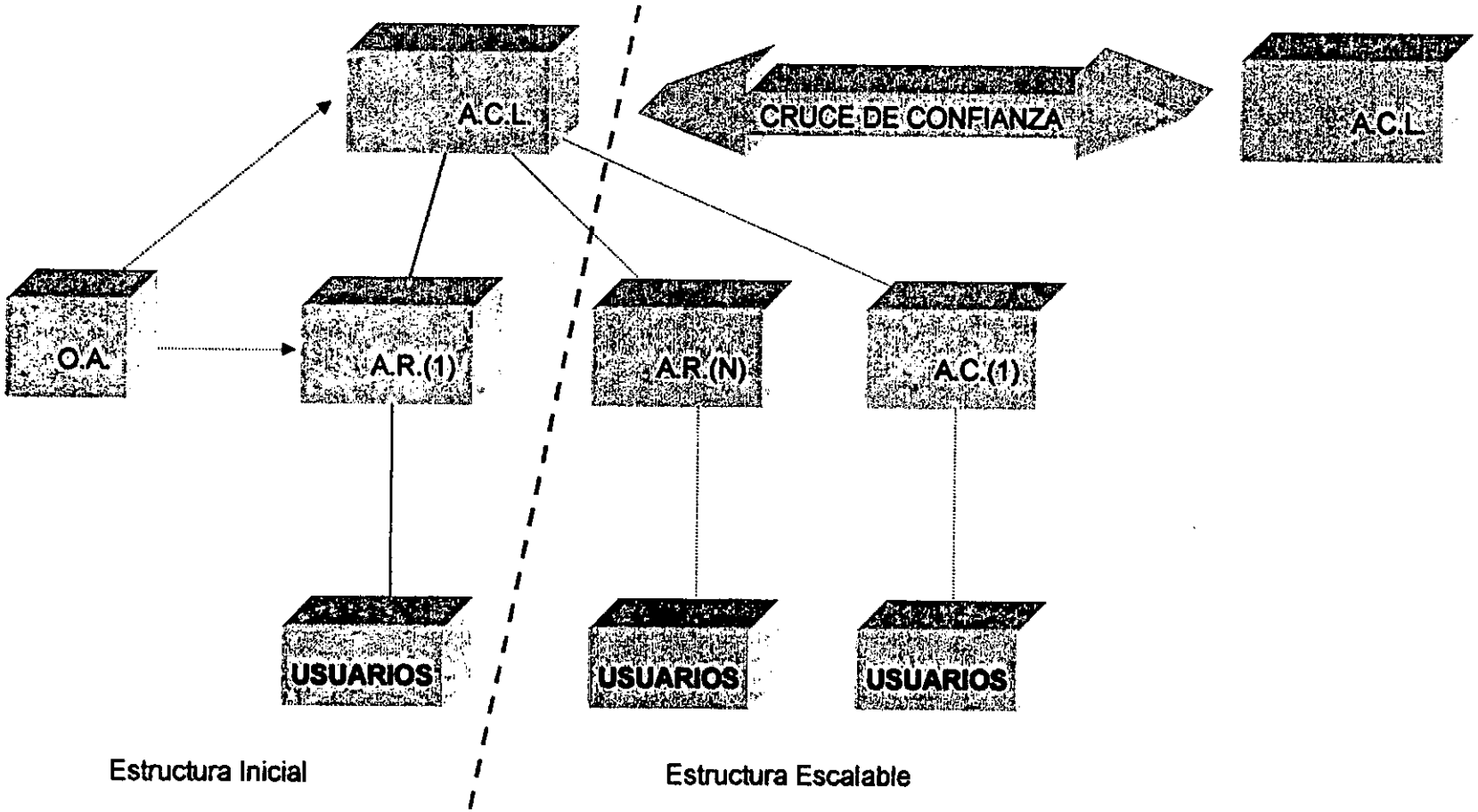


Figura 1 – Estructura inicial y escalabilidad

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 **orga-**

nismo 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 encuentran 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 Seguridad 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.

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, com-

petencia 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 Autoridad 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.

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.

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

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 dependen-

cias 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.

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.

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

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.

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.

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 ✔ Servicio de registración itinerante	✔ Responsable de la AR local ✔ Máxima autoridad del organismo al que pertenece el suscriptor ✔ Responsable de la AR local
2. ***registración Descentralizada***	✔ 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 aceptación. 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 incluyen, 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.

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 tipo 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 certificado 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 or-

ganismo 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 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 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.

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 efectuará 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 Seguridad, 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.

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.

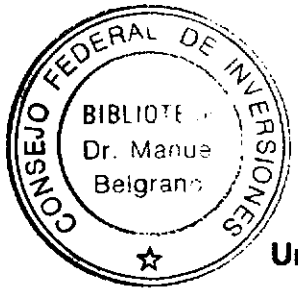
2-5- No disponibilidad del Oficial Certificador

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.



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 Pública 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

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/

IV. Tercer Informe Parcial: "Propuesta de normativa legal sobre firma digital para la provincia de Mendoza"

En función del panorama Nacional ya detallado y del absoluto convencimiento de los beneficios potenciales que la aplicación de estas tecnologías le traerán al gobierno provincial, hemos decidido en forma consonante con la filosofía de escalabilidad ya propuesta para nuestra Infraestructura de Firma Digital, comenzar legislando dentro de un marco general establecido por la Ley de Adhesión (Ver punto (a)) pero asegurar la viabilidad legal concreta en aplicaciones en escala a través del Decreto Reglamentario (Ver punto (b))

a) Ley de Adhesión.

Como primera medida, se estimo conveniente emitir la norma legal fundante del resto del andamiaje jurídico sobre la materia, engarzando en la posibilidad que contempla la legislación nacional vigente, ley 25.506, art. 50, que expresamente dispone: "*Invitación. Invítase a las jurisdicciones provinciales a instrumentar los instrumentos legales pertinentes para adherir a la presente ley.*".

Así las cosas, la provincia debe contar con la ley de adhesión, la cual no reviste mayores dificultades técnicas, sin perjuicio de las variables políticas que correspondan ser evaluadas, atento al alto nivel de innovación que implica la implementación de la materia *sub examine*.

La mencionada ley 25.506, si bien es de alcance nacional (regula materia contemplada por el C.C.) y por lo tanto en sentido estricto no necesita de adhesión, siendo obligatoria; deja abierta la posibilidad de adhesión a los fines de su instrumentalización.

Ello por cuanto la materia de fondo constituye facultades delegadas al gobierno nacional (art. 75 inc. 12), pero la materia administrativa es de competencia local.

Teniendo en cuenta estas consideraciones se elaboró un proyecto de adhesión que ya se encuentra en el circuito administrativo pertinente para luego ser sancionado con fuerza de Ley

Dicho expediente incluyó el siguiente dictamen legal:

Proyecto Ley de Adhesión de la Provincia a la ley nacional 25.506 de "Firma Digital".

La ley de referencia, en su art. 50, invita a las provincias a dictar los instrumentos legales pertinentes para adherir a la misma.

Así las cosas, es indudable que el Estado Provincial debe asumir un rol de liderazgo en la incorporación de la cultura digital en la sociedad mendocina.

Obviamente, la adhesión referida no es respecto de los primeros Capítulos, los cuales son ley nacional, de competencia delegada al estado nacional, y por lo tanto, no puede ser objeto en sentido estricto de una "adhesión". (cfr. Art. 75 inc. 12 CN)

Se advierte primeramente que, sobre la implementación de la Firma Digital en el orden local, cabe hacer algunas consideraciones.

En el orden local, los marcos legales posibles para implementar la Firma Digital ofrecen un plexo normativo tentativo, que pueden sintetizarse en las siguientes variantes:

Pueden dictarse normas administrativas, las cuales evidentemente son de naturaleza local (cfr. Art. 121 CN).

Esto tiene las lógicas desventajas derivadas de que no sería posible una aplicación total de la legislación nacional, pero sería un atenuante ante la realidad de que, por el momento, no se está en condiciones prácticas para dar total operatividad a la Firma Digital legislada.

Podría intentarse en todo caso la implementación de la firma electrónica, que no requiere mayores exigencias.

Por otro lado, no aparece prudente, ni práctica, ni jurídicamente atento a su dudosa legalidad, la creación de una Autoridad Licenciante local. Las derivaciones jurídicas pueden ser imprevisibles, y los conflictos y problemas que plantean en su análisis no aconsejan esta posibilidad (piénsese por ej., en los conflictos interprovinciales que podrían generarse, no tanto en el sentido del derecho público, sino en el terreno estrictamente privado).

Así las cosas, resulta entonces aconsejable el dictado de una ley de adhesión, en el marco mismo de la ley nacional, la cual traduciría efectivamente al menos una clara decisión política, creadora de obligaciones para el Estado Provincial, imponiendo deberes generales, análogos a los que la ley impone a la Administración Nacional.

De este modo, el Estado Provincial puede ir avanzando en la implementación de diversas políticas tendiente a la despapelización, ínter tanto se den las condiciones políticas, práctica y jurídicas exigidas por la ley nacional, sin entorpecer el avance acelerado que se advierte en el orden provincial.

También esto permite el dictado de normas provinciales, acordes con los progresos concretos y con las decisiones que tome la política local, ya sea mediante leyes formales (como sería posiblemente el caso de creación de una Autoridad Certificante Local Pública), o decretos o resoluciones según la materia y competencia específica, de acuerdo al producto que se desee aplicar.

Debe advertirse que una simple adhesión, de por sí no implica grandes cambios, pero orientada a la obligación de tomar medidas encaminadas al Estado Digital, conlleva al dictado de normas por parte del Poder Ejecutivo, por la cuales se arbitren los mecanismos necesarios al fin propuesto, lo cual, seguramente en una primera etapa, desencadene la necesidad del dictado de normas de carácter administrativo para avanzar en pasos concretos y posibles, ínter tanto se den las condiciones de cumplimiento total de la normativa nacional.

Como corresponde, los motivos concretos del proyecto, se agregan en la respectiva nota de elevación que antecede al articulado de la Ley de adhesión de Firma Digital.

MENDOZA,

NOTA N°

A la

HONORABLE LEGISLATURA DE LA PROVINCIA

S/R

Remito para su tratamiento proyecto de Adhesión de la Provincia a la ley nacional 25.506 de "Firma Digital".

Desde hace algunos años atrás se comenzó a diseñar y desarrollar el perfil de lo que será el "Estado Digital".

Loables han sido los esfuerzos realizados por el Estado Nacional, que culminaron felizmente con al sanción de la ley 25.506 de "Firma Digital".

Este cuerpo legal, en su art. 50, invita a las provincias a dictar los instrumentos legales pertinentes para adherir a la misma.

Así las cosas, es indudable que el Estado Provincial debe asumir un rol de liderazgo en la incorporación de la cultura digital en la sociedad mendocina. Algunos esfuerzos ya se realizaron, pero, indudablemente no son suficientes.

Con la aplicación de la Resolución N° 54 / 99 y del Decreto – Acuerdo N° 1806 del 5 de octubre de 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 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.

Además, los avances en materia de firma digital no son una iniciativa aislada sino que forman parte del Plan Provincial "Hacia el Gobierno Digital" trienio 2003/2005 cuyos objetivos son mejorar la calidad en la atención al público, a través de la incorporación de alternativas que promuevan la rapidez en el inicio y/o gestión de tramitaciones; promover la eficiencia en la gestión a través de la estandarización de los procedimientos y formularios utilizados para los trámites administrativos que tienen similares características y propiciar la disminución de costos en que debe incurrir la población al tener que trasladarse hasta una dependencia específica para realizar tramitaciones.

Dentro del marco de este plan el proyecto de Firma Digital forma parte del Programa de Incorporación de NTIC´s a la Gestión de Gobierno, el cual busca ampliar los servicios tecnológicos, a través de la introducción de nuevas formas y procesos internos en la administración del Estado, que permitan la integración de los sistemas de los diferentes servicios, compartir recursos y mejorar la Gestión interna de los mismos.

Es importante rescatar éstos antecedentes, porque la masificación del uso de Internet y de otras herramientas de las TI, sólo será posible cuando se bajen las barreras culturales y económicas que hoy imposibilitan alcanzar estas metas.

Al facilitar la autenticación a distancia entre partes que no necesariamente se conocen previamente, la firma digital constituye el mecanismo esencial para proveer seguridad y desarrollar la confianza en las redes abiertas. Esto le otorga un rol estratégico en el desarrollo del comercio electrónico en Internet.

Los beneficios de la firma digital no se reducen sólo al ámbito del comercio electrónico. Como también sucede en el ámbito nacional, nuestros organismos públicos están atiborrados de grandes cantidades de documentos en soporte papel que ocupan un significativo y costoso espacio de archivo en sus oficinas y que dificultan su informatización, lo que da como resultado un acceso a la información más lento y costoso.

Las exigencias legales referidas a la utilización del papel con firma manuscrita impiden la implementación de modernos sistemas informáticos mediante los cuales se podría acceder a documentos a distancia y a la información en forma inmediata.

En este orden de ideas, el presente proyecto impone al Poder Ejecutivo Provincial la obligación de promover el uso masivo de la firma digital de tal forma que posibilite entre otras cosas, el trámite de los expedientes por vías simultáneas, búsquedas automáticas de la información y seguimiento y control por parte del interesado, propendiendo a la progresiva despapelización del estado.

Por todo lo expuesto y detallado anteriormente es que se considera de vital importancia la sanción del presente proyecto para la progresiva utilización de la firma digital en el ámbito provincial, como así tender a una gradual despapelización del estado, enmarcado todo ello en una política orientada a una optimización del uso de los recursos del Estado en pos del logro de la reforma y modernización tendiente a lograr una alto grado de calidad de la prestación de servicios, en especial, aquellos que significan una interacción directa a través de la atención del público usuario.

DIOS GUARDE A V. H.

EL SENADO Y CÁMARA DE DIPUTADOS DE

LA PROVINCIA DE MENDOZA

SANCIONAN CON FUERZA DE LEY

Articulo 1° - Adhiérase la Provincia de Mendoza a la Ley 25.506 de "Firma Digital" sancionada por el Honorable Congreso de la Nación.

Art. 2°- Autorízase el empleo de la Firma Digital, en todas las dependencias del Poder Ejecutivo Provincial.

Art. 3°: El Poder Ejecutivo Provincial promoverá el uso masivo de la firma digital de tal forma que posibilite el trámite de los expedientes por vías simultáneas, búsquedas automáticas de la información y seguimiento y control por parte del interesado, propendiendo a la progresiva despapelización.

En un plazo máximo de 5 (cinco años) contados a partir de la entrada en vigencia de la presente ley, se aplicará la tecnología de firma digital a la totalidad de los decretos, resoluciones y decisiones administrativas en general, emanados de las jurisdicciones y entidades comprendidas en el art. 2° de la presente ley.

Art. 4°: El Poder Ejecutivo deberá reglamentar esta ley en un plazo no mayor a 180 (ciento ochenta) días de su publicación en el Boletín Oficial de la Provincia.

Art. 5° - Comuníquese al Poder Ejecutivo.

Al pasar el expediente por el estadio administrativo de la Asesoría Legal de la Gobernación, dicha dependencia emitió el siguiente dictamen:

Ref. Expte. N° 4163-U-03-00020

s/Proyecto de Ley.-

Se procura dictamen de esta Asesoría respecto al proyecto de Ley de Adhesión de la Provincia de Mendoza a la Ley Nacional N° 25.506/01 de Firma Digital sancionada por el Honorable congreso de la Nación, obrante a fs. ¼ de autos.

A fs. 5/7 obra dictamen legal del Dr. Julio Alvarez quien aconseja como instrumento legal pertinente para la implementación de la Firma Digital en el orden local, la adhesión a la Ley Nacional.

En líneas generales se comparte la opinión del citado letrado, razón por la cual ésta asesoría no tiene objeciones que formular al proyecto de ley.

Analizado el mismo consideramos oportuno hacer las siguientes consideraciones:

1) El art. 1° formula la adhesión de la Provincia de Mendoza a la Ley N° 25.206.

Respecto a ello entendemos que debería especificarse si la adhesión es total, o parcial y exclusivamente en lo pertinente.

Ello por cuanto de los términos del artículo siguiente se deduce que el empleo de la firma digital se autoriza únicamente en las dependencias del Poder Ejecutivo Provincial siendo que la Ley N° 25.506 establece un ámbito de aplicación más amplio comprendiendo a las jurisdicciones y entidades comprendidas en el art. 8° de la Ley N° 24.156, es decir todo el sector Público Nacional.

Se sugiere a modo de colaboración y teniendo en cuenta otras leyes de adhesión, consultadas como antecedentes, la siguiente redacción del artículo

1°: "De conformidad a lo establecido por el art. 50 de la Ley N° 25.506 de Firma Digital, adhiérase la Provincia de Mendoza a la mencionada Ley, declarándose de aplicación a la Jurisdicción Provincial sus disposiciones en lo pertinente y con las limitaciones establecidas en el artículo siguiente"

2) Asimismo debería especificarse si las tecnologías y previsiones de la Ley Nacional se utilizarán en el ámbito interno y en relación con los administrados, y siempre de acuerdo con las condiciones que se establezcan en la reglamentación a que hace referencia el art. 4° del proyecto en cuestión.

Tal observación se realiza a fin de delimitar con precisión el ámbito de aplicación y el alcance en el orden local, siendo fundamental para la implementación la reglamentación del Poder Ejecutivo Provincial.

Al respecto el art. 37 del Decreto N° 2628/02, reglamentario de la Ley N° 25.506 dispone: *"Despapelización del Estado. Sin perjuicio de la aplicación directa de la ley en lo relativo a la validez jurídica de la firma electrónica, de la firma digital y de los documentos digitales, la implementación de las disposiciones de la ley y del presente decreto para la digitalización de procedimientos y trámites internos de la Administración Pública Nacional, de las Administraciones Públicas Provinciales, y de los Poderes Legislativos y Judiciales del orden nacional y provincial, así como los vinculados a la relación de las mencionadas jurisdicciones y entidades con los administrados, se hará de acuerdo a lo que fijen reglamentariamente cada uno de los Poderes y Administraciones. "*

3) En el art. 3° último párrafo pensamos que debería ajustarse la terminología en lo que refiere a..."emanados de la jurisdicciones y entidades comprendidas en el art 2°...". Dicha expresión debería ser remplazada, a nuestro criterio, por la siguiente:..."emanados de la dependencias comprendidas en el art. 2°..."

4) Quisiéramos señalar que en el orden local, el Código]Fiscal en su art. 120 modificado, prevé la utilización de la firma impresa por medios electrónicos e intervenida mediante el sistema de timbrado, cuando lo apruebe expresamente la repartición responsable de la emisión y la Resolución 60/00 aprueba que la firma impresa en las boletas de deuda que emita la DGR a partir del 21/09/2000, se efectúe por medios electrónicos y sea intervenida mediante el sistema de timbrado.

5) Finalmente consideramos que debería solicitarse dictamen de la Asesoría de Gobierno.

Asesoría Legal
Mendoza, 22 de Julio del 2003
Dictamen N° 305/03

Atentos a estas observaciones, la consultoría del proyecto Firma Digital hizo descargo de la siguiente manera:

Ref.:Expte. 4163-U-03-00020 s/ Proyecto de Ley.

Respecto del dictamen obrante a fs. 9-11 del expte. de referencia, expreso lo siguiente.

- En primer lugar, debe considerarse la coincidencia de opiniones con la asesora interviniente, atento a que –como dice el mismo dictamen- *"en líneas generales se comparte la opinión del citado letrado, razón por la cual esta Asesoría no tiene objeciones que formular al proyecto de ley"* (subrayado nuestro)

- En referencia a la consideraciones que seguidamente pasa a exponer el profesional, me permito efectuar algunas reflexiones, sin dejar de señalar que podría existir cierta contradicción entre decir que *"no tiene objeciones que formular"*, y por otro lado efectuar observaciones las cuales, aunque aparentemente formales, pueden implicar un cambio en la decisión que adopta el proyecto. En este caso, la observación no sería jurídica, sino una apreciación política diversa.

- Efectuamos algunas consideraciones, en el mismo orden tratado por el mencionado asesor:

1) Demás está decir que la adhesión no puede ser sino en lo pertinente. Tratándose de una ley bastante compleja, obviamente la adhesión no puede ser sobre los aspectos referidos a la validez de la firma digital en sí, lo cual es materia cuya competencia pertenece al Congreso (art. 75 inc. 12 CN), y por lo tanto no es concebible una adhesión sobre dichos aspectos. El asesor preopinante entiende que habría una falta de perfecta correlación entre el art. 1° y el 2° del Proyecto. Pone como argumento el hecho de que la ley 25.506 establece un ámbito de aplicación más amplio que en el proyecto en cuestión. El argumento no es pertinente, por cuanto la aplicación en el orden concreto, no puede ordenarse en ámbitos sobre los cuales no existe competencia nacional, como son las administraciones provinciales (Cfr. arts. 75 inc. 12 , 5 y 122 CN). Vale decir que así como la Nación puede establecer un ámbito de aplicación, lo propio puede hacer cada Provincia, siendo ésta quien lo determinará, de acuerdo a lo que considere conveniente, por razones prácticas, políticas, etc. Debe advertirse que existen muchas barreras culturales sobre esta materia, por lo cual perfectamente cada estado provincial puede elegir una aplicabilidad escalonada o paulatina del empleo de la firma digital; lo cual no es incompati-

ble con la adhesión (Infraestructura, etc.) Pero reitero, esto es competencia exclusiva de cada provincia. Aún así, no veo inconveniente es la reforma propuesta, advirtiendo solamente que amplía el ámbito de aplicación, lo cual solamente puede significar una decisión política distinta, pero no por existir objeción alguna en la decisión originalmente propuesta. Adviértase, por último, que la normativa citada por el Asesor, se encuentra en el Capítulo "Disposiciones Complementarias" de la Ley.

2) Tampoco consideramos apropiada la segunda observación. Se trata de un proyecto de Adhesión, y no creo ni técnica y prácticamente apropiado, incluir normas de carácter reglamentario en la ley. Tampoco alcanzo a comprender acabadamente la observación formulada. Más bien creo que el asesor interviniente ha incurrido en un error al confundir *"el ámbito interno y en relación con los administrados"*, con *"actos de efectos directos"* (nuestro acto administrativo, del art. 28 ley 3909). Efectivamente, si fuera esto último, tendría más sentido la observación, aunque de todas maneras esa restricción convendría efectuarla por norma de inferior rango, y por razones prácticas coyunturales, cuidando de no alterar el espíritu de la ley. Finalmente, me permito advertir que en el orden nacional, es el mismo Decreto citado por la asesora, la norma que determina que *"la implementación de las disposiciones de la ley ... se hará de acuerdo a lo que fijen reglamentariamente cada uno de los poderes y Administraciones"* (Públicas Provinciales).

3) Respecto de esta observación, se trata de cuestiones terminológicas, pudiendo seguirse por la que se considere más conveniente.

4) En relación a esta 4° consideración, tampoco la entendemos apropiada, además de no ser pertinente al tema *sub examine*, atento a que creemos se ha caído en una confusión entre la firma electrónica, la firma efectuada por medios electrónicos, y la firma digital, con efectos y naturaleza jurídica por ende distinta.

5) Finalmente, respecto a la solicitud de dictamen a Asesoría de Gobierno, deberá evaluarse esa posibilidad en el marco del Decreto 3152/88. (Cfr. Dictamen 993/91 Asesoría de Gobierno. Instrucciones que deben guiar la intervención del Asesor de Gobierno en las Actuaciones Administrativas).

En síntesis. Entendemos que las observaciones no son sustanciales, salvando lo referido al ámbito y alcance, pero no por razones jurídicas sino por distinta evaluación política.

Parece más apropiada una autorización más acotada, sin perjuicio que por distinta percepción de la realidad política, se decide una autorización más amplia.

Por último, le expreso que es nuestra opinión, la conveniencia de ir avanzando de manera gradual en la implementación de la firma digital. Debe tenerse presente que el camino recorrido en el orden nacional ha sido lento, aún no concluido, y requirió el dictado de abundante normativa, provisoria alguna; amén de decir que es escasa la experiencia en otras administraciones locales. Por ello, resulta prudente ir avanzando de manera escalonada, pero segura, evitando pretender la sanción de normas que no se condicen con la realidad sociológica y cultural, elemento de hecho que debe considerarse a la hora de legislar, en una visión trialista del derecho.

El proyecto en cuestión seguramente es pasible de innumerables mejoras, pero las observaciones realizadas entendemos que no son sus-

tanciales, y algunas de ellas, tampoco pertinente. No veo inconveniente en tomar los cambios formales propuestos, pero conociendo que pueden implicar una decisión política diferente.

Creemos que la Unidad que Ud. dirige, es el organismo gubernamental apropiado para decidir los alcances de la ley, por contar con todos los elementos necesarios para poder evaluar prudentemente el caso, atento al avance registrado en el orden local, y conociendo las limitaciones que todavía existen en el orden nacional.

El proyecto originario optó por una autorización más restringida, precisamente por una evaluación tomada con los diversos responsables del área, quienes se encuentran en mejores condiciones que un técnico en derecho, para poder elegir lo posible, dejando de lado quizá lo mejor, pero inviable o difícil de concretar, evitando de esta manera, que proyectos nunca alcancen sanción, y si la alcancen, sea letra muerta por imposibilidad de cumplimiento.

Por ello, sin perjuicio de modificaciones formales, puede mantenerse el proyecto original, atento, como dijo la misma asesora, que no existen mayores *"obieciones que formular al proyecto de ley"*.

Pero el sentido práctico aconseja el dictado de una norma provincial de adhesión, a la mayor brevedad posible, por cuanto los avances locales lo exigen, aceptando finalmente o no las modificaciones formales sugeridas. La misma seguramente será perfectible, pero necesaria para avanzar a paso seguro en el desarrollo de un Gobierno Digital, siendo en este caso, la Provincia verdadera pionera en este terreno.

b) Decreto Reglamentario.

Así las cosas, el gobierno provincial debe proceder a emitir la norma correspondiente –decreto reglamentario de la ley de adhesión- a fin hacer operativa la norma básica.

VISTO el Decreto Nº 1672 del 24 de agosto de 2001, y la ley nacional 25.506., y

CONSIDERANDO:

Que la necesidad de optimizar la actividad de la Administración Pública Nacional adecuando sus sistemas de registración de datos, tendiendo a eliminar el uso del papel y automatizando sus circuitos administrativos, amerita la introducción de tecnología de última generación, entre las cuales se destacan aquellas relativas al uso de la firma digital y de la firma electrónica, susceptible de la misma o superior garantía de confianza que la firma ológrafa;

Que la Ley 25.506 de ha constituido un avance significativo y trascendente en tal dirección, al reconocer el empleo de la firma digital y de la firma electrónica y su eficacia jurídica en las condiciones que establece la misma;

Que se considera necesario estimular la difusión de las citadas tecnologías a través del dictado de una norma de jerarquía superior, que promueva la extensión del uso de la firma digital a todo el ámbito del Sector Público Provincial;

Que la tecnología aquí propuesta ya ha sido incorporada en la legislación de otros países con positiva repercusión tanto en el ámbito privado como público;

Que el mecanismo de la firma digital cumple con la condición de no repudio, por la cual resulta posible probar inequívocamente que una persona firmó efectivamente un documento digital y que dicho documento no fue alterado desde el momento de su firma, siempre que su implementación se ajuste a los procedimientos exigidos por la normativa vigente;

Que el Poder Ejecutivo ha enviado a la Honorable Legislatura un proyecto de ley de adhesión de la provincia a la ley 25.506 de Firma Digital;

Que intertanto se den las condiciones tanto nacionales como provinciales para la completa aplicación del régimen de firma digital en la Provincia, resulta conveniente avanzar en la implementación de la firma electrónica en el

ámbito del Poder Ejecutivo Provincial, atento a que la misma exige tecnologías que la provincia está en condiciones de aplicar;

Que en el orden jurídico, la firma electrónica difiere de la digital en los aspectos referidos al régimen probatorio. (art. 5° ley 25.506);

Que la presente normativa fue concebida con el propósito de crear una alternativa válida a la firma ológrafa para el ámbito del Poder Ejecutivo Provincial;

Que resulta conveniente, en virtud del grado de especialidad alcanzado en materia de Gobierno Digital, que se designe como autoridad de Aplicación del presente decreto, a la UNIDAD DE REFORMA DEL ESTADO, dependiente del Sr. Gobernador de la Provincia (art. 2° Dec. 1672/01);

Que dada su índole, se ha considerado conveniente y necesario que la autorización del empleo de la tecnología de la firma electrónica en el ámbito del Poder Ejecutivo Provincial se sujete a un término de vigencia, que permita evaluar, a partir de su efectiva utilización, tanto su funcionamiento en las diferentes jurisdicciones cuanto el grado de confiabilidad y seguridad del sistema;

Que en mérito a tales circunstancias se prevé expresamente en la presente normativa la elaboración, por la Autoridad de Aplicación, de un informe acerca de los resultados del empleo de la firma electrónica a fin de que, sobre la base de las conclusiones emergentes, proponga al PODER EJECUTIVO PROVINCIAL las medidas tendientes a fijar un régimen definitivo en la materia;

Que asimismo y con idéntico fundamento, se delega en la UNIDAD DE REFORMA DEL ESTADO la facultad de prorrogar, por una única vez, el plazo del Artículo 1° del presente Decreto.

Por ello,

EL GOBERNADOR DE LA PROVINCIA

D E C R E T A:

Artículo 1°: Autorízase por el plazo de dos años, a contar del dictado de los manuales de procedimiento y de los estándares aludidos en el artículo 5° del presente Decreto, el empleo de la firma electrónica en la instrumentación de los actos internos del Sector Público Nacional, que no produzcan efectos jurídicos individuales en forma directa. En el régimen del presente Decreto la firma electrónica tendrá los efectos regulados por la ley 25.506 de firma digital.

Artículo 2°: Los términos de este decreto tendrán los alcances definidos en el Glosario que como Anexo integra el presente Decreto.

Artículo 3°: Las disposiciones del presente Decreto serán de aplicación en todo el ámbito del Poder Ejecutivo Provincial.

Artículo 4°: Las distintas jurisdicciones del Poder Ejecutivo Provincial deberán arbitrar los medios que resulten adecuados para extender el empleo de la tecnología de la firma electrónica, en función de los recursos con los que cuenten y en el más corto plazo posible.

Artículo 5°: Dispónese que la Unidad de Reforma del Estado, dependiente del Sr. Gobernador de la Provincia, sea la Autoridad de Aplicación del presente Decreto, estando facultada, además, para dictar los manuales de procedimiento, y los estándares tecnológicos aplicables a las claves, los que deberán ser definidos en un plazo no mayor de CIENTO OCHENTA (180) DIAS corridos, y cuyos contenidos deberán reflejar el último estado del arte. Las jurisdicciones del Poder Ejecutivo Provincial deberán informar a la Autoridad de Aplicación, con la periodicidad que ésta establezca, las aplicaciones que concreten de la tecnología autorizada por el presente Decreto.

Artículo 6°: Ciento ochenta (180) días corridos antes de la finalización del plazo establecido en el artículo 1°, la autoridad de aplicación definida en el artículo 5 del presente Decreto deberá elaborar y remitir al Señor Gobernador de la Provincia un informe acerca de los resultados que la aplicación del sistema autorizado hubiere tenido en las respectivas jurisdicciones. Asimismo, propondrá al Poder Ejecutivo el régimen definitivo a adoptar en la materia.

Artículo 7°: Deléguese en la Unidad de Reforma del Estado la facultad de prorrogar, por una única vez, el plazo establecido en el Artículo 1° del presente Decreto.

Artículo 8°: Comuníquese, publíquese, dése al Registro Oficial y archívese.

De esta manera queda configurado el marco legal pensado para la implementación de la firma digital en la Provincia de Mendoza, sin perjuicio de las eventuales modificaciones o normativa anexa que se dicte a la medida de la evolución del proyecto.

V. INFORME FINAL:
"Prueba Piloto y Propuesta de Implementación"

1-Introducción

En el marco del proyecto Firma Digital Mendoza y de acuerdo con el Plan de Actividades propuesto, se presentan a continuación, el desarrollo de la actividad y de las tareas que la integran, identificada como número 5 dentro del mismo:

Identificar del universo de procedimientos en el ámbito del Gobierno de la Provincia aquellos que por sus características sean susceptibles a la aplicación de firma digital.

Fundamentar y proponer la aplicación de la herramienta sobre un procedimiento factible.

Generar una Propuesta de implementación en la Provincia de Mendoza en función de condiciones particulares.

Superando el alcance del presente proyecto y por la excelente repercusión que ha tenido en el ámbito provincial, se presentan aquí no sólo las actividades anteriormente señaladas, sino que también describiremos en forma detallada la implementación exitosa de la primera prueba piloto de Firma Digital realizada en el Sitio www.edemocracia.mendoza.gov.ar y el desarrollo de la AC-Urme, la Autoridad Certificante de la Unidad de Reforma y Modernización del Estado con los circuitos administrativos en los que ha sido testeada.

Además, presentamos en éste informe el desarrollo de la página web del proyecto de Firma Digital ya disponible para navegación en www.firmadigital.mendoza.gov.ar

2-Prueba Piloto "Firma digital en e-democracia"

El sitio edemocracia se ha concebido como una herramienta que permite la participación de los ciudadanos en los procesos democráticos, creando relaciones entre los actores sociales, incluido el propio gobierno.

Las Tecnologías de la Información y la Comunicación ocupan un papel central para fomentar el entramado cívico y asociativo, generando nuevas comunidades reales o virtuales, nuevos espacios que incrementen la participación y la reflexión cívico política.

Toda comunidad digital que pretenda constituir un espacio abierto de comunicación y participación, creíble y confiable, requiere de la responsabilidad y compromiso de sus actores sobre la información que publican; y de la garantía que dicha información se comunica como fue concebida por sus autores, sin cambios ni alteraciones. **La firma digital es el medio que provee estas garantías en edemocracia.**

Destinatarios y usos

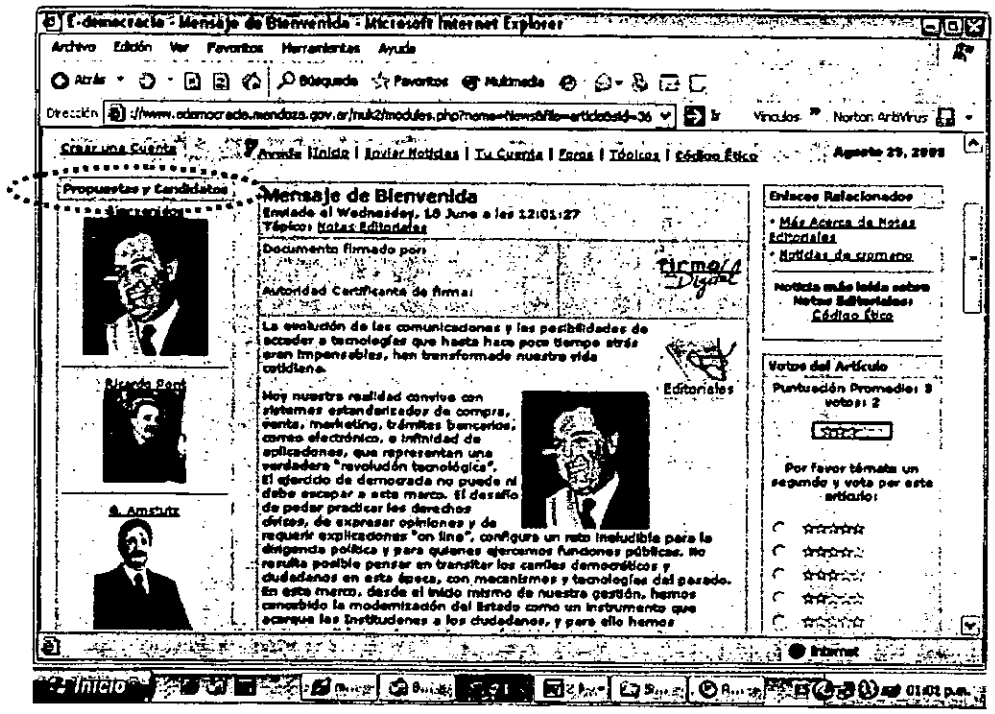
Los participantes del sitio e-democracia, quienes tienen la posibilidad de contar con Certificados Digitales validados por la Unidad de Reforma y Modernización del Estado y con ellos **firmar sus artículos proporcionándoles las garantías que otorga la firma hológrafa**. Es decir asegurando la identidad del autor y la integridad de la información publicada.

Desarrollo

Esta primera prueba constituye un avance muy importante para nuestro proyecto que desde un principio, no incluía la implementación de una prueba piloto. Varios factores se conjugaron para lograr que la provincia de Mendoza contara tan rápidamente con la primera implementación de firma digital:

- *La **excelente repercusión** del proyecto en el ámbito provincial.*
- *Los **desarrollos realizados por los técnicos** de este proyecto para la aplicación de firma en particular*
- ***El convenio celebrado con Certisur** S.A. por el cuál la implementación de la Prueba Piloto cuenta con el respaldo de Certificados de Firma Digital de reconocido prestigio mundial emitidos por Verisign y sin costo alguno para la provincia.*
- ***La difusión del proyecto** a través del Coloquio "Hacia el Gobierno Digital" organizado por la Unidad de Reforma del Estado, en donde se trataron temas relacionados por personalidades reconocidas del medio. Las distintas notas realizadas por los medios de comunicación mendocinos y el artículo publicado el diario de tirada nacional "El Cronista Comercial" el día 20 de Octubre del corriente.*

El sitio se encuentra disponible para consulta en www.edemocracia.mendoza.gov.ar en donde se puede ver el avance de ésta Prueba Piloto a través de las publicaciones firmadas digitalmente en la parte de propuestas de los candidatos.



Procedimientos y funcionamiento interno

Autoridad Certificante de la
Secretaria Administrativa Legal y Técnica del Gobierno de Mendoza
Unidad de Reforma y Modernización del Estado

Procedimientos de Validación para
la Emisión de Identificadores Digitales.

El presente documento describe el procedimiento de validación que la Unidad de Reforma y Modernización del Estado de la Secretaria Administrativa Legal y Técnica del Gobierno de Mendoza aplica a los fines de emitir los certificados digitales Class 2 dentro de la VeriSign Trust Network.

Este procedimiento es de aplicación para la emisión de Certificados Digitales Class 2 sólo para los participantes del sitio

www.edemocracia.mendoza.gov.ar , allí podrán publicar toda la información relacionada a los procesos electorales provinciales y municipales quedando debidamente registrados ante la Secretaria Administrativa Legal y Técnica del Gobierno de Mendoza.

Este documento ha sido redactado con la asistencia del personal de CertiSur y cualquier modificación sobre el mismo debe ser notificada a CertiSur con anterioridad; a fin de determinar que sean cumplidos los requisitos mínimos exigibles para la emisión de un certificado Class 2 dentro de la VeriSign Trust Network.

Procedimiento para Certificados Iniciales

Solicitud

Toda persona que desee obtener un Certificado Digital deberá primero completar y luego imprimir la nota solicitud web ubicada en www.firmadigital.mendoza.gov.ar, la página de Firma Digital de la Unidad de Reforma y Modernización del Estado de la Secretaria Administrativa Legal y Técnica del Gobierno de Mendoza, la cual incluye los siguientes datos:

De los suscriptores

a.Datos personales

•Nombre y apellido.

•Tipo y Número de documento.

•Dirección de correo electrónico PERSONAL

b.Declaración Jurada

La nota solicitud Web debe ser impresa, datada y firmada por el interesado.

Una vez realizada esta tarea deberá comunicarse con la Unidad de Reforma para que un operario (que debe ser integrante de la Unidad de Reforma y Modernización del estado), vaya a visitarlo.

El operario de la Unidad de Reforma del Estado verificará

De los suscriptores

1)Que el DNI, LC o LE corresponde a la persona

2)Que dicha persona es aquella cuyos datos figuran en la nota solicitud Web por él presentada. A tal fin debe cotejar los datos del documento con los que figuran en el formulario impreso por el solicitante.

A continuación el operario solicita fotocopia del documento de identidad del solicitante e inicíala la misma en prueba de conformidad.

Una vez finalizado el proceso de autenticación, se le hará entrega al solicitante de un sobre cerrado conteniendo el Código Personal Único 1.

El operario entregará toda la información al Administrador de la Autoridad Certificante de la Unidad de Reforma y Modernización del Estado de la Secretaria Administrativa Legal y Técnica del Gobierno de Mendoza.

El Administrador deberá verificar que la información recibida de manos del operario se encuentre correctamente datada y firmada

Si todas las validaciones son correctas, deberá enviar al solicitante, a la dirección de correo electrónico indicada en la nota solicitud Web el Código Personal Único 2.

El solicitante debe entrar al sitio web de CertiSur y completar la solicitud

Validación

1. La Unidad de Reforma y Modernización de la Secretaria Administrativa Legal y Técnica del Gobierno de Mendoza almacena la información provista por el solicitante, durante el periodo de tiempo indicado en el CPS para certificados de Clase 2.

La validación de la información y documentación será realizada por personas autorizadas por la Secretaria Administrativa Legal y Técnica del Gobierno de Mendoza a tal fin.

El administrador debe:

a.Verificar que los datos de la solicitud nota web coincidan con los datos de la nueva solicitud de certificado ingresada con el PIN 1 y el PIN 2.

b.Verificar que el Código Personal Único 1 coincide con el entregado a la persona en el momento de la visita del operario.

c.Verificar que el Código Personal Único 2 coincide con el enviado a dicha persona a su casilla de correo electrónico personal.

d.La dirección de correo electrónico es validada en el proceso de envío del Código Personal Único 2

2.En caso de faltar alguna documentación o de que la documentación no esté completa contactarse con el solicitante para pedirle la documentación faltante y asentar esta situación en el legajo

3.Si existe algún error en la información contenida en la solicitud, ésta deberá ser rechazada y se deberá informar al solicitante el motivo del rechazo y asentar esta situación en el legajo.

Generación de los Códigos Personales Únicos

1.El Administrador generará dos Códigos Personales Únicos (PIN) por cada uno de los potenciales solicitantes de certificados digitales. Dichos códigos deben ser mantenidos en secreto en poder solamente del Administrador y copias de cada uno de ellos debe ser enviada al solicitante del certificado.

a.El Administrador generará, por medio de un proceso, un primer código único (denominado PIN1) que el solicitante debe utilizar al momento de ingresar la solicitud de Certificado Digital sobre la página Web. Dicho código debe ser entregado en sobre cerrado al solicitante, al momento de presentar el formulario nota solicitud Web.

b.El segundo código único (denominado PIN2) será enviado por correo electrónico a la dirección que figura en el formulario nota solicitud Web.

Emisión y retiro del Certificado

Una vez que el Administrador ha validado los datos y estos se corresponden con el procedimiento indicado anteriormente procede a la aprobación del mismo.

El sistema genera automáticamente un mensaje de correo electrónico enviado a la dirección consignada en la solicitud conteniendo un tercer código único (identificado como código de retiro) que el usuario utiliza para retirar el certificado aprobado.

Este procedimiento se debe realizar desde la misma computadora donde se completó la solicitud.

Procedimiento para la Renovación de Certificados

(SOLO PARA EL CASO DE PASAR A PRODUCCIÓN)

Solicitud

En el Control Center se configurará el sistema para que automáticamente se le envíe un mail al Usuario notificando el vencimiento del certificado con 30 días de anticipación. Dicho usuario ingresará directamente al sitio de la MPKI Lite y autogestionará el proceso de renovación presentando el certificado a vencer.

Validación

El administrador del sistema, ingresará periódicamente al sitio para constatar si existen nuevas solicitudes de renovación de certificados. Personal autorizado controlará que la documentación presentada oportunamente siga vigente.

En caso de estar correcto, se procederá a autorizar el pedido de renovación desde el Control Center, A continuación, el usuario; accederá por medio de un navegador a la página de la Secretaria Administrativa Legal y Técnica del Gobierno de Mendoza, opción "RENOVAR" y realizará el procedimiento allí indicado. Una vez realizado correctamente el sistema enviará automáticamente un mensaje con un código que le permitirá al usuario retirar el Certificado correspondiente.

Para cada solicitud se llenará la "Planilla de seguimiento para renovación de certificados" que corresponda durante el periodo de tiempo indicado en el CPS para certificados de Clase 2.

Procedimiento para la Revocación de Certificados

Solicitud

La revocación de Certificados se debe realizar on line utilizando la Frase de Comprobación correspondiente.

En caso que el usuario no recuerde esta Frase deberá presentar una NOTA DE REVOCACION ante la Unidad de Reforma y Modernización del Estado de la Secretaria Administrativa Legal y Técnica del Gobierno de Mendoza, conteniendo todos los datos del Certificado (nombre del titular, dirección de correo electrónico, número de documento de identidad, etc.). Una vez recibida esta NOTA DE REVOCACIÓN y verificados los datos, el Administrador podrá revocar el Certificado y habilitar el usuario a solicitar uno nuevo.

Una vez recibida la suscripción, el Administrador procederá a validar los datos según lo detallado en este procedimiento.

Revocación Manual

El usuario accederá por medio de un navegador a la página de la Unidad de Reforma y Modernización del Estado de la Secretaria Administrativa Legal y Técnica del Gobierno de Mendoza, y seleccionará la opción "REVOCAR", debiendo posteriormente ingresar su nombre o dirección de correo electrónico.

El sistema para continuar la operación le solicitará la frase de comprobación.

ANEXO I. INSTRUCCIONES PARA SOLICITUD E INSTALACIÓN DE CERTIFICADOS DIGITALES

Cómo solicitar un certificado digital en la Unidad de Reforma y Modernización del Estado de la Secretaria Administrativa Legal y Técnica del Gobierno de Mendoza

Toda persona que desee obtener un Certificado Digital debe presentar ante la Unidad de Reforma y Modernización del Estado de la Secretaria Administrativa Legal y Técnica del Gobierno de Mendoza el formulario "Certificados Digitales Altas / Bajas". Contra entrega del mismo, recibirá un sobre conteniendo el PIN 1. Posteriormente, se le enviará a la dirección de correo electrónico personal, el PIN 2.

Con esta información el solicitante deberá:

1.Acceder por medio de un navegador a la pagina de solicitud indicada por el Banco

<<https://onsite.certisur.com/services/SecretaraiAdministrativaLegalyTecnicadelGobiernodeMendozaUnidaddeReformayModernizaciondelEstado/digitalidCenter.htm>>,opción SOLICITUD" y completar el formulario online

a.Datos Personales

•Nombre y apellido.

•Dirección de correo electrónico.

•Tipo y Número de documento.

b.PIN 1: entregado contra la presentación de formulario

c.PIN 2: enviada a la casilla de correo electrónico personal

2.Una vez presionado el botón Continuar, deberá aguardar la recepción de un mensaje de correo electrónico, indicando los pasos a seguir.

Cómo retirar e instalar un certificado?

Una vez que el Administrador haya finalizado el proceso de validación, el solicitante recibirá un correo electrónico y las instrucciones para retirar el certificado. Con esa información el solicitante debe:

1.Acceder por medio de un navegador a la pagina de solicitud indicada por el Banco

<<https://onsite.certisur.com/services/SecretaraiAdministrativaLegalyTecnicadelGobiernodeMendozaUnidaddeReformayModernizaciondelEstado/digitalidCenter.htm>>,opción "RETIRAR DIGITAL ID"

2.Ingresar el PIN enviado en el mensaje

3.Al presionar el botón "Aceptar" instalará el certificado digital y finalizará el proceso.

Infraestructura y desarrollo tecnológico

Para documentar la infraestructura y desarrollo tecnológico que soportó la firma digital en el sitio e-democracia se deben abordar tres ejes fundamentales de la tarea.

1. Autoridad Certificante
2. Certificados Digitales
3. Desarrollo de Aplicaciones

1. Autoridad Certificante

La necesidad de contar con Certificados Digitales confiables para la comunidad y para los actores del sitio e-democracia, llevó a la Unidad de Reforma a celebrar un convenio con la empresa Certisur S.A. socio estratégico para el Cono Sur de de Verisign Trust Network; líder mundial en tecnologías de clave pública. Este convenio permitió la constitución de una Autoridad Certificante de firma dependiente de la Secretaría Administrativa, Legal y Técnica de la Gobernación, lo que constituyó el instrumento primario y fundamental para el desarrollo de la experiencia.

Dicha AC, gestionada por los expertos de la Unidad de Reforma y Modernización del Estado, ha emitido Certificados Digitales Clase 2 en la jerarquía de confianza de la VeriSign Trust Network para los precandidatos y candidatos

a Gobernador y a Intendentes departamentales de la Provincia de Mendoza que han publicado sus propuestas en el sitio www.edemocracia.mendoza.gov.ar, de acuerdo al manual de procedimientos acordado para tal fin.

2. Certificados Digitales

La empresa CertiSur proveyó la infraestructura tecnológica y de seguridad necesaria para la gestión del CVS de los certificados digitales y el asesoramiento técnico necesario para los desarrollos implicados en la experiencia. Esta actividad la realizó ante el requerimiento de los técnicos del Gobierno de Mendoza de implementar un esquema de prueba de los productos que la empresa provee como soluciones tecnológicas en el eje de Gobierno, de modo tal de tener información completa y pertinente para la comparación de alternativas en el presente estudio de factibilidad. Tanto la implementación de la AC, como la emisión y gestión de certificados tuvo costo cero para la provincia en el marco del convenio.

Es importante destacar que los certificados emitidos cumplen holgadamente con los requisitos técnicos previstos en la Ley 25.506, su decreto reglamentario y la Res. 194/98 que regula los aspectos vinculados al soporte tecnológico de la firma digital. También satisfacen los estándares de la industria.

Las características principales de los mismos son:

- *Certificados X509. v3*
- *Algoritmo de firma: MD5RSA*
- *Clave pública: RSA (1024 bits)*
- *Uso de la clave: Firma digital*
- *Punto de Distribución de la CRL: URL=http://pilotonsitecrl.verisign.com/OnSitePublic/LatestCRL.crl*
- *Algoritmo de identificación: Sha1*
- *Certificados exportables a formatos pem-encode, der y pfx*

3. Desarrollo de Aplicaciones

El proceso de firma de las propuestas implicó un desarrollo específico adaptado a las necesidades del weblogs (PHP Nuke) sobre el cuál se implementó e-democracia.

Para instrumentar la firma digital de las propuestas debió modificarse el código original de los módulos de publicación y edición de noticias de PHP Nuke, incluyendo en el mismo procedimientos y funciones que invocaban los métodos de firma y verificación provistos por el control Capicom v 2.0, software de libre distribución provisto por Microsoft Corp.

Capicom es un control ActiveX que brinda a los desarrolladores una interface COM a la API Microsoft CryptoAPI y que provee objetos y métodos para implementar firma digital desde SmartCards o desde claves de software, cifrado de datos con criptografía de clave pública, gestión del almacén de certificados y gestión de la información contenida en los certificados, entre otras funcionalidades

El algoritmo de firma se aplicó a la concatenación de los campos Title, Text y BodyText del formulario de edición de noticias provisto por PHP Nuke a sus editores, en adelante ***texto en claro.***

La ***firma obtenida*** por la aplicación del algoritmo, codificada en ***Code-Base 64*** se almacenó junto al ***texto en claro*** en la base de datos que gestiona el weblog. Esto implicó también modificaciones a la estructura de BD de PHP Nuke y la gestión del impacto de estas modificaciones en todo el código del weblog.

Así mismo, se construyeron funciones para codificar en Code-Base 64 el ***certificado digital*** asociado a la firma. Dicha representación se almacenó también junto a la firma y al texto en claro en la BD del weblog.

En síntesis el desarrollo obtenido funciona del siguiente modo:

"la ***firma digital*** de un ***texto*** se construye a partir de la aplicación de procedimientos apropiados, disparados ante la presencia del evento ***"Firmar Digitalmente"*** en la publicación o edición de una noticia/propuesta; y se almacena junto al texto firmado y al Certificado pertinente en la BD de PHP Nuke. Cualquier modificación posterior a dicho texto en claro devela automáticamente la inconsistencia entre el texto modificado y la firma almacenada. De esta forma se garantiza la integridad de la información. La presentación del Digital Id asociado a la firma y su verificación provee las garantías de autoría necesarias, con lo cuál se cierra el proceso".

Las características principales del desarrollo son:

- *Lenguaje de programación de aplicaciones: PHP – VBScript – Funciones PHP/OpenSSL*
- *Motor de BD: MySQL*
- *Librerías y ytilidades: Capicom 2.0*
- *Gestión del almacén de certificados: Implementado a través de Capicom 2.0*
- *Algoritmo de firma: MD5RSA*
- *Representación de la firma: Binario codificado en Base64*
- *Representación del Certificado: Exportado a DER, codificado en Code-Base-64*

Esta iniciativa permitió

- garantizar la autoría e integridad de las propuestas publicadas en e-democracia

- probar y evaluar un circuito completo de implementación de la tecnología de firma digital
- difundir la aplicación de las tecnologías de firma digital y criptografía de clave pública a los visitantes del sitio edemocracia
- contribuir a la formación de especialistas en PKI

Tutoriales

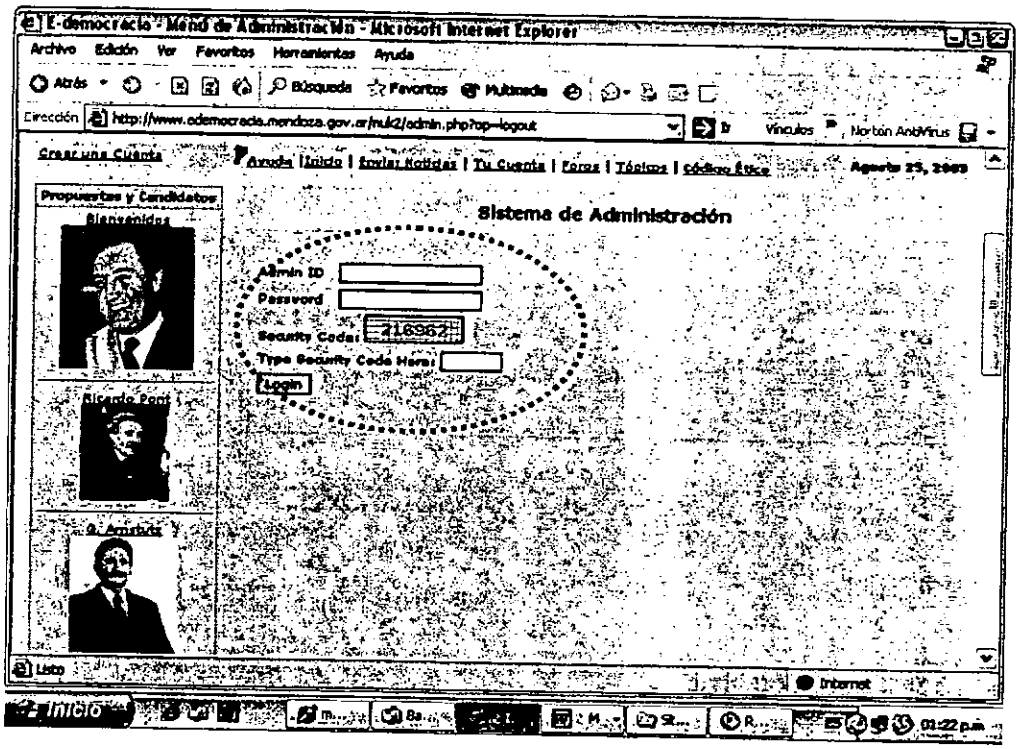
Los siguientes documentos fueron elaborados con el objeto de apoyar a los usuarios en el proceso de subir y firmar digitalmente de las propuestas publicadas por los candidatos:

Cómo publicar y firmar digitalmente su propuesta ?

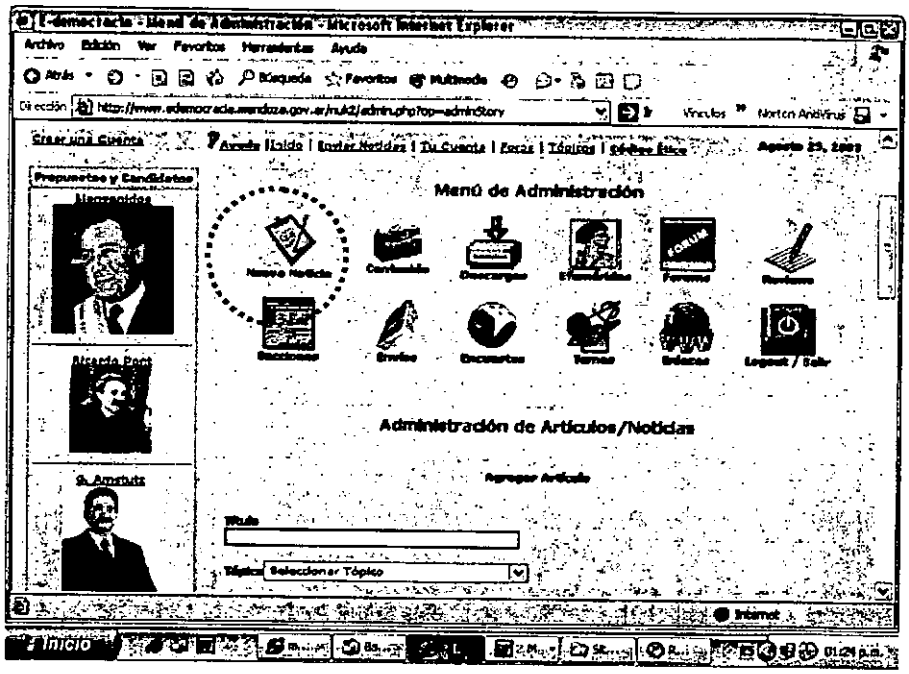
Básicamente siga el siguiente procedimiento **para publicar por primera vez y firmar digitalmente** su publicación:

1. Ingrese al Sitio www.edemocracia.mendoza.gov.ar y haga clic en candidatos

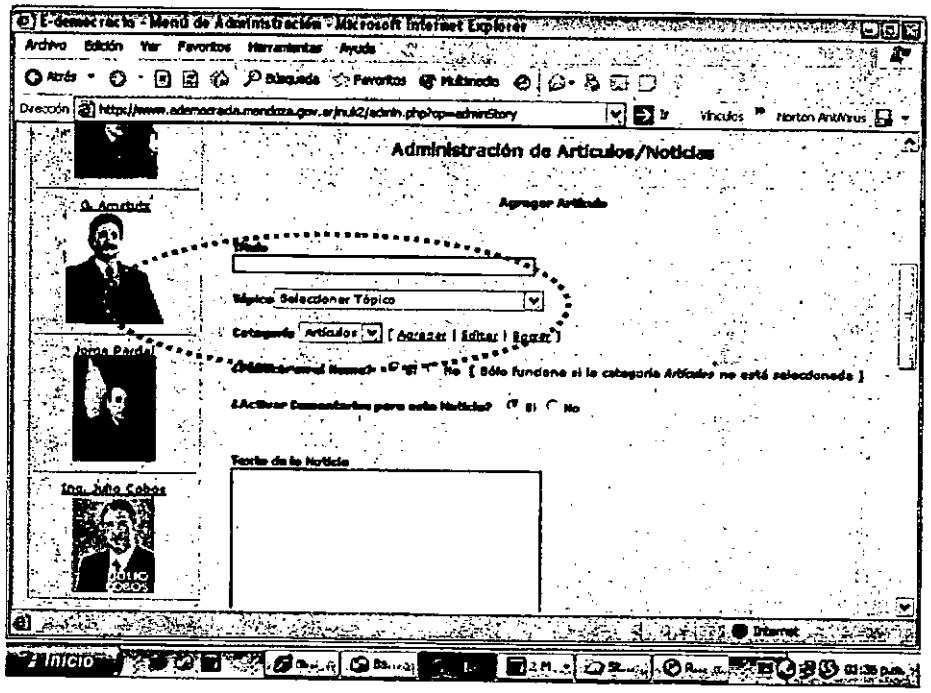
2. En la siguiente pantalla ingrese:
   a. Su usuario (Admin. ID)
   b. Su clave (Password)
   c. Y el código de seguridad que se ve en el recuadro titulado Security Code



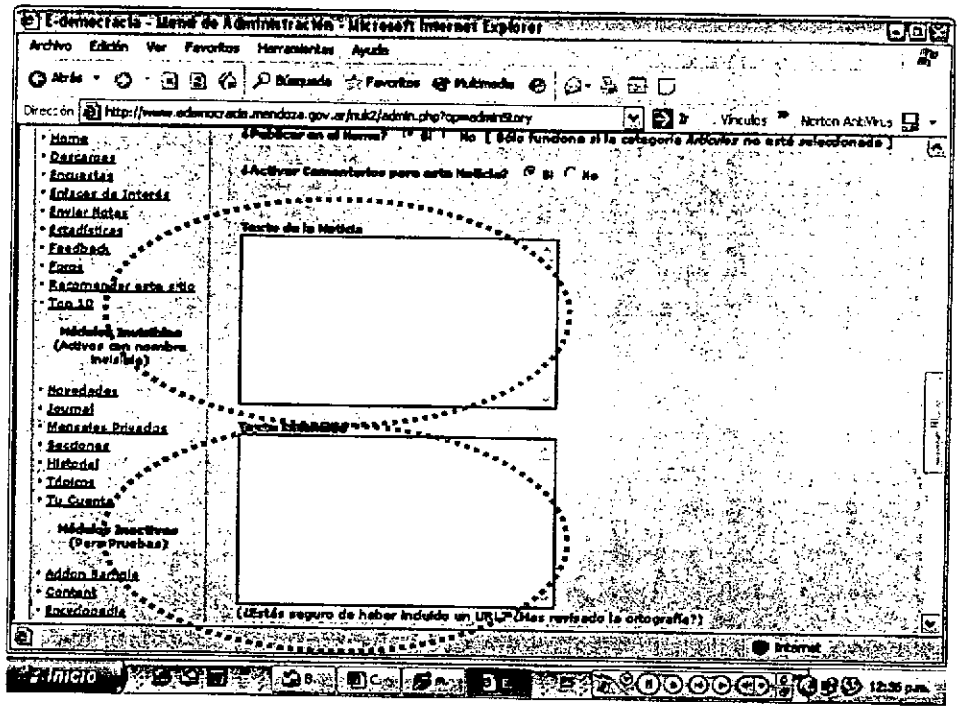
3. A continuación escriba el texto en la interfaz que se le presenta al hacer click en nueva noticia:



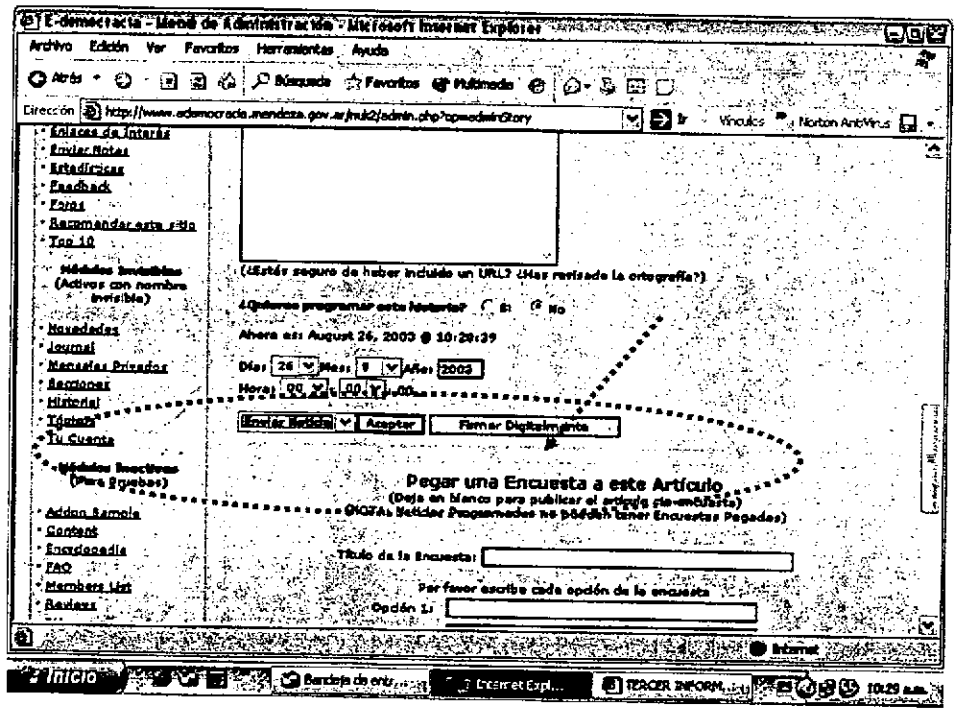
Coloque **título y seleccione tópico**

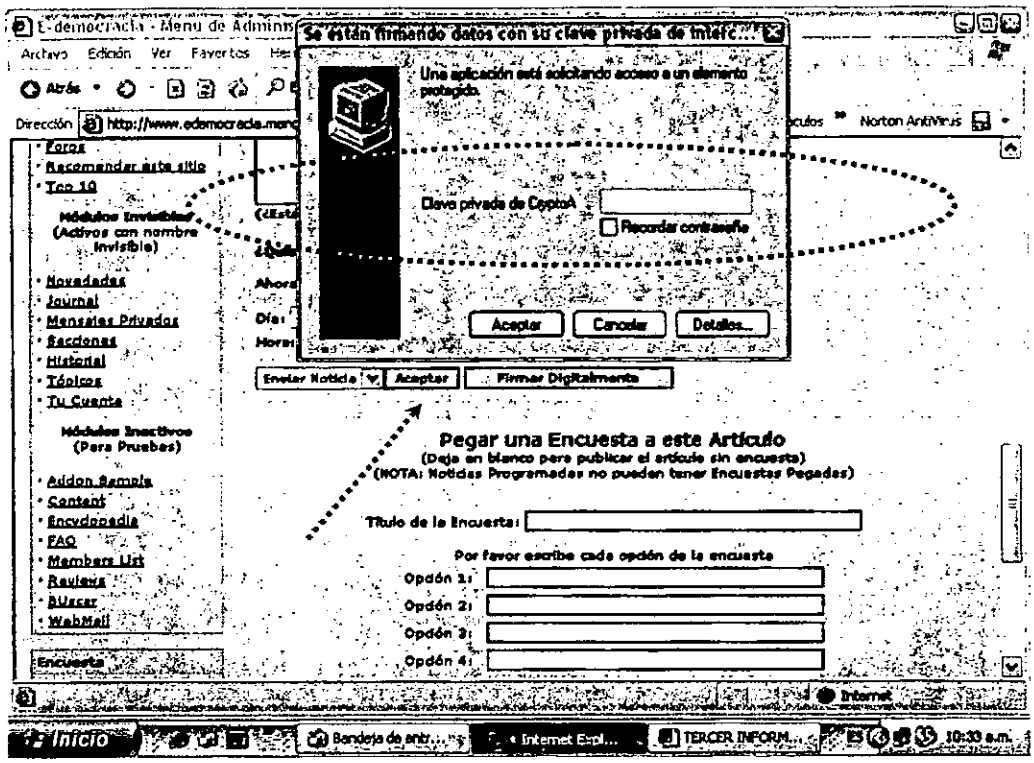


Agregue el texto introductorio en el primer cuadro y el texto extendido en el segundo



4. Para concluir elija enviar noticia y firme digitalmente su publicación asegurando las garantías de integridad y autoría.





Por último, no olvide apretar **el botón aceptar.**

Gracias por su publicación!

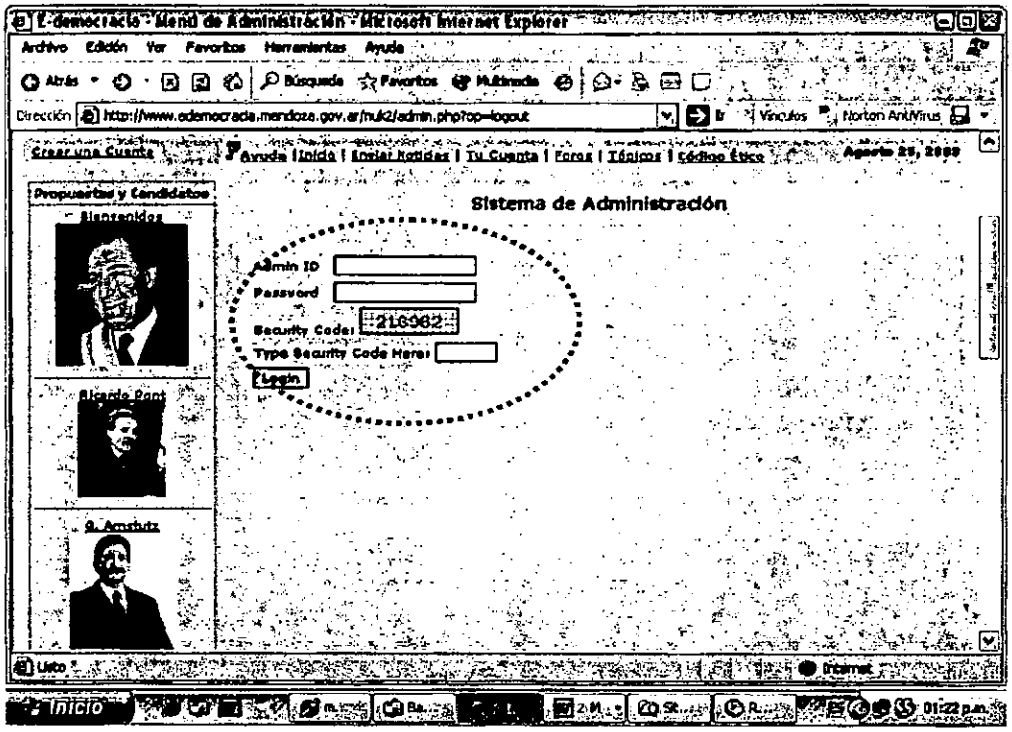
REFORMA
& MODERNIZACION DEL ESTADO

Cómo editar y firmar digitalmente su propuesta ya publicada?

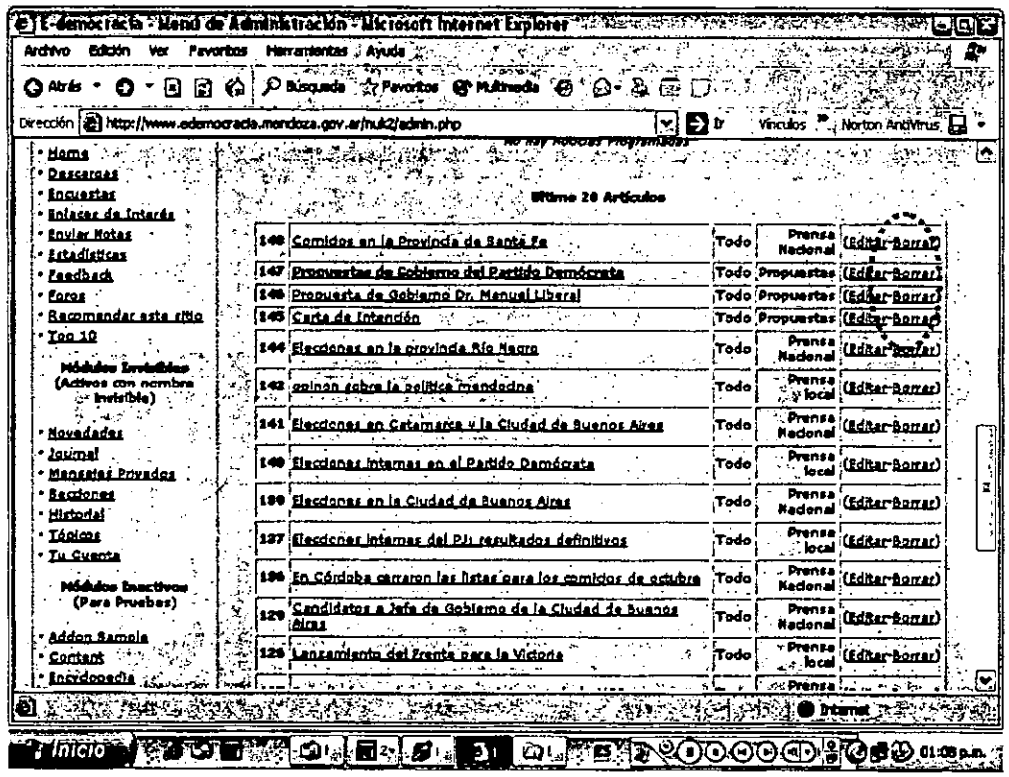
Básicamente siga el siguiente procedimiento **para editar y volver a firmar digitalmente** una publicación ya existente:

5. Ingrese al Sitio www.edemocracia.mendoza.gov.ar y haga clic en candidatos

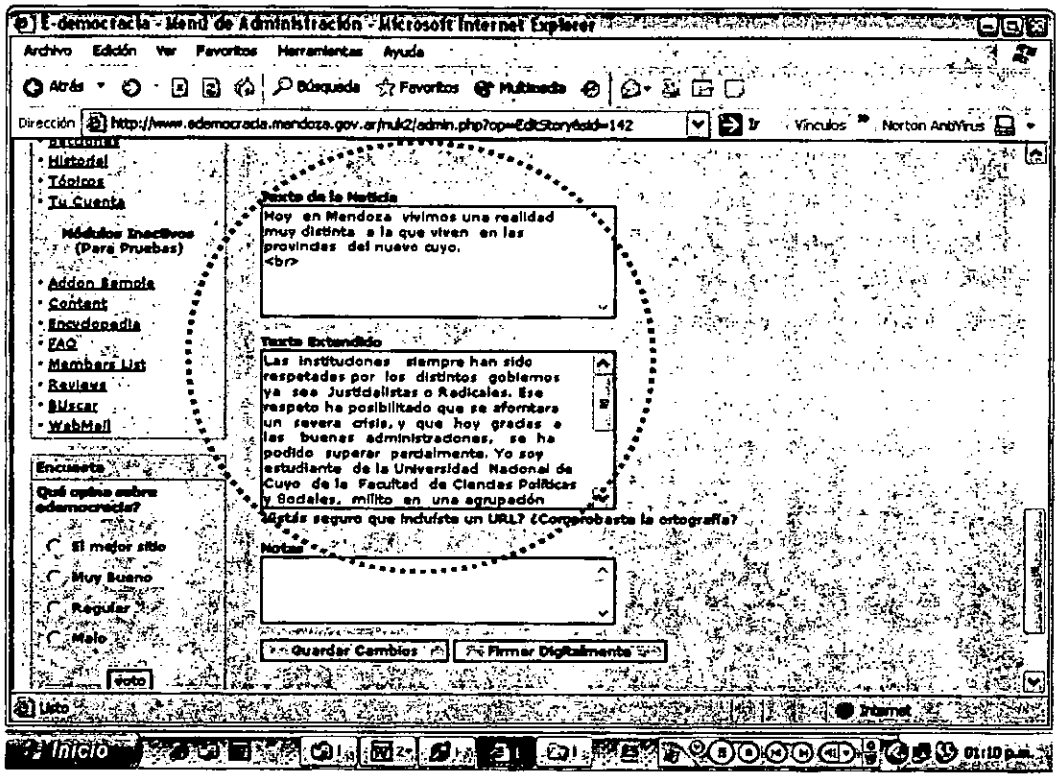
6. En la siguiente pantalla ingrese:
   a. Su usuario (Admin. ID)
   b. Su clave (Password)
   c. Y el código de seguridad que se ve en el recuadro titulado Security Code



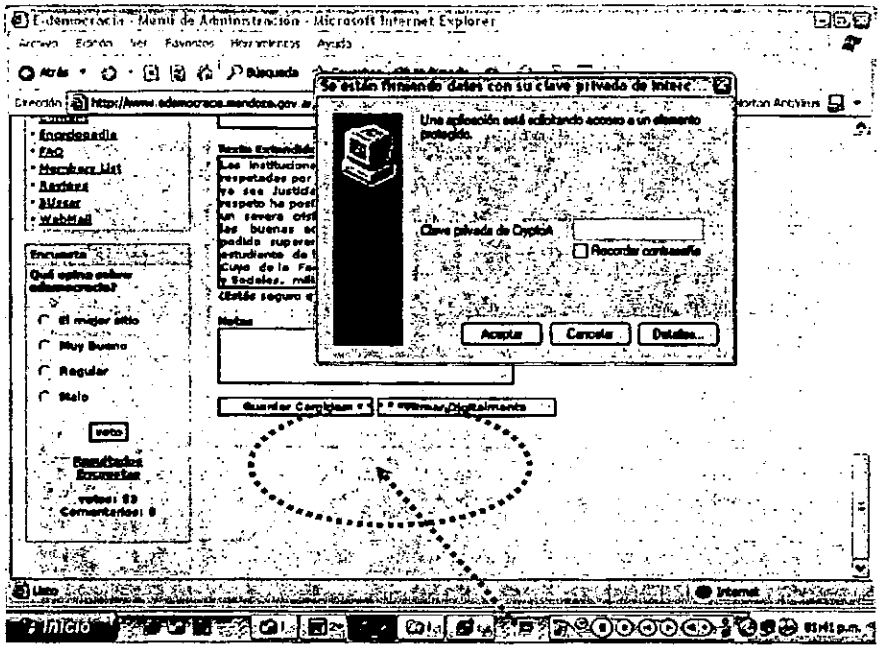
7. A continuación localice la propuesta que desea arreglar o completar y seleccione **Editar**



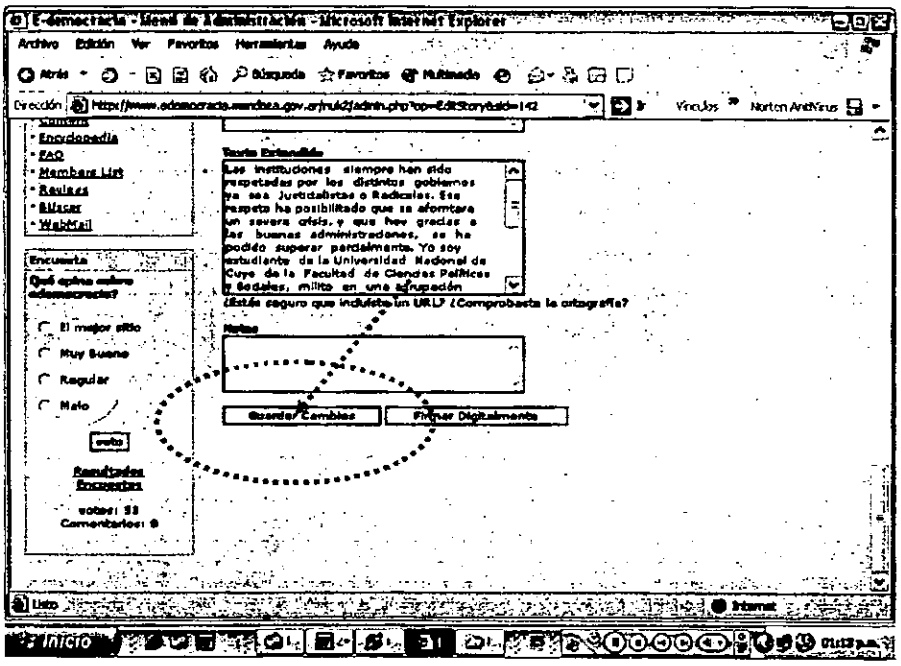
Realice los cambios que desee.....



8. **Firme digitalmente** su publicación editada asegurando las garantías de integridad y autoría.



9. Por último, **no olvide guardar los cambios realizados.**



3-Creación de la AC-URME Autoridad Certificante de la Unidad de Reforma y Modernización del Estado

En la tarea de instrumentar ***prototipos PKI*** y ponerlos en funcionamiento con circuitos de prueba, de modo de poder evaluar comparativamente el rendimiento de distintas alternativas desde sus características económicas, operativas y técnicas, en base a métricas y consideraciones fundadas en la experiencia; se ha implementado en el ***marco del proyecto de firma digital*** y con ***tecnología propia del Gobierno de la Provincia*** de Mendoza, la ***AC-Urme Autoridad Certificante de la Unidad de Reforma y Modernización del Estado***.

La AC-Urme constituye una Infraestructura de Clave Pública (PKI) diseñada para implementar y difundir el uso de los Certificados Digitales y la firma digital en el ámbito del Gobierno de Mendoza, a los fines de brindar los siguientes servicios:

- Correo electrónico seguro, firma digital y no repudio.
- Autenticación de identidad: de Servidores (sitio seguro) y de clientes (control de acceso).
- Canal Seguro (SSL).
- Secure Desktop – Cifrado de archivos (acuerdo de clave privada mediante clave pública).
- Secure e-forms: firma digital y seguridad para formularios basados en web.
- Seguridad de aplicaciones sobre intranets y extranets.

Por sus características topológicas, técnicas y operativas, se define como una infraestructura de clave pública de ***pequeña escala***[1] con amplias posibilidades de ***escalabilidad*** y excelentes condiciones de interoperabilidad.

La implantación inicial consta de:

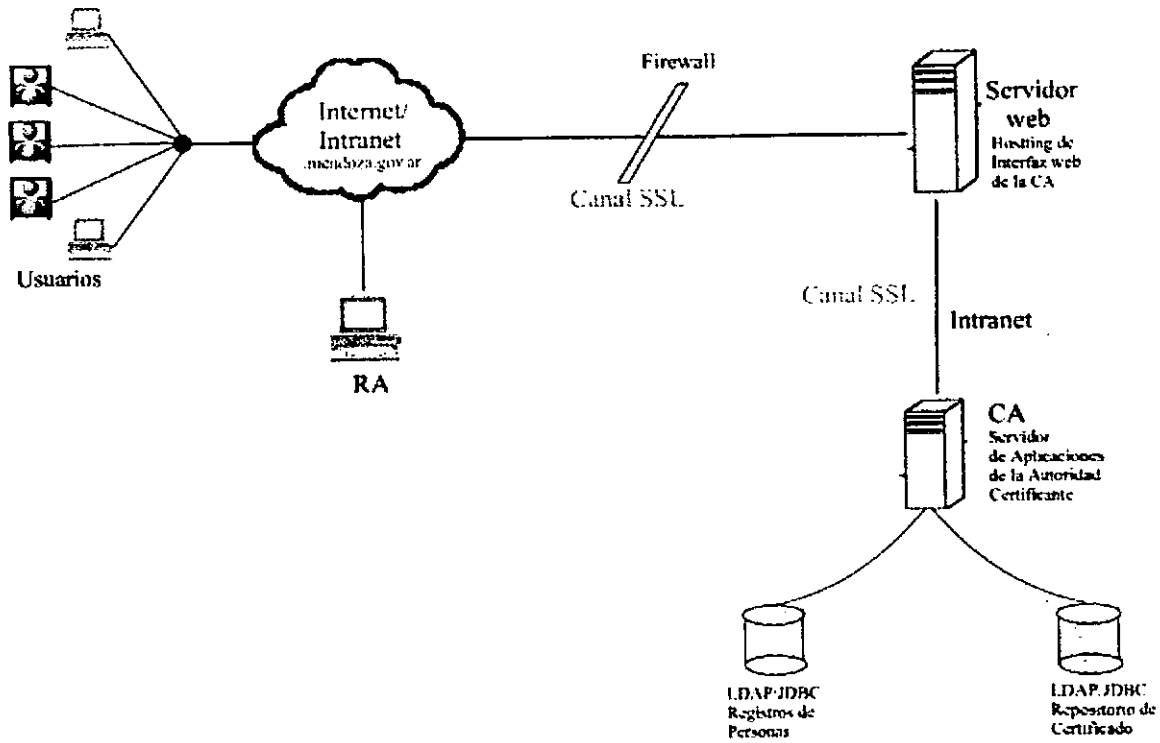
- ***Una Autoridad Certificante (AC-Urme):*** que permite el manejo del ciclo de vida de certificados , a través de la solicitud, aprobación, renovación, auditoría y revocación de certificados
- ***Una Autoridad de Registro (AR-Urme):*** que permite desarrollar funciones, tales como aprobación de certificados, remisión de solicitud aprobada a la CA, auditoría, manejo de las solicitudes de revocación y otras; de manera distribuida entre un número ilimitado de administradores, asegurando la separación de roles.

Y prevé un **modelo de escalabilidad jerárquico** con las siguientes características:

- Posibilidad de agregar nuevas Autoridades de Registro, eventualmente con funciones distribuidas por Organismo de Gestión o Ministerio; o alternativamente por tipo de certificados que gestionan.
- Posibilidad de subordinar a una CA Raíz, otras Autoridades Certificantes que se ajusten a Políticas, estándares y procedimientos consistentes. Esto tiene por objetivo, proveer al modelo de mecanismos de división de la carga de trabajo, mejora de performance, actualización tecnológica, distribución de roles, aseguramiento de la disponibilidad del sistema, etc.

[1] Por ***pequeña escala***, entendemos una PKI que pueda gestionar eficientemente un rango de entre ***500*** y ***1000*** certificados emitidos a usuarios finales; y un rango de entre ***20*** y ***40*** certificados de servidor

La siguiente figura ilustra el layout de la AC-Urme, tal como funciona actualmente. El ***criterio fundamental*** en su construcción ha sido lograr una estructura técnicamente confiable que garantice seguridad, disponibilidad, eficiencia y escalabilidad de la solución con la mínima inversión posible.



La misma se basa fundamentalmente en software de libre distribución, aprovechando la potencialidad de los sistemas Linux y su integración natural con la plataforma J2EE.

Su gran ventaja, es que tanto el software de base como el software de gestión PKI (EJBA) satisfacen los requisitos planteados por los estándares na-

cionales e internacionales sin demandar grandes inversiones económicas y de recursos humanos.

Se debe tener claro, no obstante, que con el espíritu de proponer una solución de prueba sin costo económico, se redujeron en esta propuesta las especificaciones de los servidores y dispositivos de almacenamiento y servidores redundantes, el motor de base de datos, los módulos criptográficos en hardware (HSM) y el uso de smart-cards. Todas estas características pueden luego ser agregadas en caso de que la PKI escale.

En función de una valoración de los requerimientos de espacio físico, condiciones de conservación y medidas de seguridad física necesarias para la instalación de los servidores y dispositivos de comunicaciones, se instalaron los equipos en las dependencias de la Gobernación, con una estrecha vinculación a las oficinas de la Unidad de Reforma del Estado de la provincia.

En base a las pruebas realizadas se considera que la infraestructura instalada constituye un sistema técnicamente confiable, ajustado a los estándares tecnológicos y operativos propuestos en el marco regulatorio de la actividad (Res. 194/98); por la Autoridad de Aplicación (Jefatura de Gabinete de Ministros); y a los estándares internacionales.

En términos operativos creemos que es la solución ideal para una primera experiencia de implantación PKI, garantizando confiabilidad, confidencialidad, integridad y disponibilidad.

Circuitos de prueba implementados

Los certificados emitidos por la AC-Urme han sido utilizados en:

- pruebas de firma de correo electrónico
- pruebas de cifrado de datos
- pruebas de firma de e-forms

Como desarrollos particulares se citan:

- Implementación de sitio seguro con autenticación de cliente para la interfase de administración web de la AC-Urme.
- Implementación de sitio seguro con validación de cliente para el sitio www.tramite.mendoza.gov.ar , interfase de administración de la Guía Orientadora de Trámites que mantiene la provincia.
- Implementación de sitio seguro para la página web del proyecto de firma digital http://www.firmadigital.mendoza.gov.ar

4-Estrategia para la Identificación de Procedimientos Aptos

Casi cualquier número de transacciones electrónicas puede requerir los niveles de seguridad que provee una PKI, sin embargo es importante hacer una adecuada elección del alcance y los ámbitos de aplicación de los servicios de criptografía asimétrica para lograr ahorros y no incurrir en sobrecostos de implementación

Criterios de selección de circuitos administrativos

- Trámites con alta frecuencia de repetición a cargo de la misma oficina, ente o persona.
- Circuitos que requieren autenticación de las partes involucradas
- Circuitos administrativos que enlazan importantes distancias geográficas
- Circuitos basados en gran cantidad de papeleo
- Circuitos administrativos de transferencia de información con exigencias de oportunidad

Criterios de selección de transacciones aptas para ser firmadas digitalmente

- Aquellas que requieren efectiva autenticación de personas o entes involucrados en la transacción
- Aquellas que implican traslado de fondos
- Aquellas que autorizan subsidios o prestaciones sociales de ayuda
- Aquellas que se definan en las políticas y manuales de procedimientos de la Autoridad Certificante

Criterios de selección de transacciones aptas para ser encryptadas

- Aquellas que contengan información estrictamente confidencial
- Aquellas que contengan información que no debe estar disponible públicamente sin filtros previos

Tales pautas serán el marco conceptual a tener en cuenta a la hora de seleccionar y priorizar los circuitos en los que se desarrollarán aplicaciones de firma digital. Además, debemos tener en cuenta que para fijar estos criterios de selección de circuitos, se han tenido en cuenta las características de éstos que se relacionan directamente con los potenciales beneficios y ahorros que la aplicación de la tecnología puede producir.

5-Propuesta Aplicación Resoluciones/Fundamentación

A continuación proponemos un diseño preliminar para el desarrollo e implantación de un circuito administrativo que permita la redacción, revisión, firma, gestión y consulta, de normas y resoluciones de la Secretaría Administrativa, Legal y Técnica de la Gobernación con soporte digital.

Esta actividad tiende a identificar y describir una solución tecnológica que con el uso de la firma digital permita:

- prescindir totalmente del soporte impreso de las normas, con el efecto del ahorro producido por el proceso de despapelización
- agilizar el proceso de redacción, revisión y firma de las normas, aprovechando los beneficios que las nuevas tecnologías aportan para el acceso y traspaso de la información y el trabajo colaborativo.
- optimizar las formas de organización y vinculación, sistematización, consulta y distribución de normas legales, sin perder garantías en cuanto a la integridad del texto resolutivo y la autoría de sus firmas

Atendiendo a estas premisas proponemos:

1. **Reformular el circuito** administrativo de producción de resoluciones para la Secretaría Administrativa, Legal y Técnica, de modo tal que no se involucren copias en papel de la norma, traspasos reiterativos de información entre oficinas y se eliminen cuellos de botella o tiempos muertos en el proceso de emisión y difusión de la norma legal.
2. Implementar un **repositorio digital** de resoluciones con posibilidades de consulta en línea sobre la Intranet de Gobierno.
3. Instrumentar un esquema de **implementación en paralelo** con el circuito actual de modo de efectuar análisis comparativos que aporten una valoración justa de los ahorros o mejoras que se logren

6-Sitio web del Proyecto

Se ha desarrollado el sitio web del proyecto de Firma Digital disponible para consulta e interacción en www.firmadigital.mendoza.gov.ar . El sitio cuenta con toda la información acerca del **Proyecto**, la **Legislación** sobre la materia, las **Alianzas estratégicas** desarrolladas, los contenidos explicativos de la **prueba piloto** en e-democracia, un apartado de **preguntas frecuentes** y conceptos básicos, un repositorio con **descargas de interés**, una **zona segura** a la que sólo pueden acceder las personas que posean certificados y por último la posibilidad de pedir asesoramiento y apoyo en la **zona de soporte.**