G/U.151
L19
III
$536 - a Vila
44708

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

firma Digital

INFORME FINAL

CONSEJO FEDERAL DE INVERSIONES
BIBLIOTECA
Dr. Manuel Belgrano

CONSEJO FEDERAL DE INVERSIONES
CONSULTOR: LIC. PABLO GUILLERMO LIOY
Fecha de impresión 28/06/2004 10:30

ÍNDICE

RESUMEN DE CONTENIDOS

Se presentan a continuación, a modo de Informe Final, las actividades y tareas desarrolladas en el marco de planificación del proyecto de Firma Digital Mendoza.

Los contenidos ya presentados en informes anteriores se presentan resumidos y sintetizados por importancia, para obtener una versión más detallada de los temas por favor remitirse a los informes precedentes.

El resumen de las actividades realizadas es el siguiente:

1. ***Implementación de experiencia piloto de Sitio Seguro:***

   - Relevamiento del circuito operativo de carga de información
   - Explicitación de la necesidad puntual
   - Determinación de mejoras
   - Desarrollo de documentación explicativa de sitio seguro para ser incluida (como servicio de información al ciudadano) en el sitio de la Guía de Trámite
   - Determinaciones sobre la provisión de certificados
   - Capacitación de los referentes de la guía
   - Instalación de protocolos y configuración de los servidores web de la Guia de Trámite
   - Gestión/emisión de certificados de servidor y de usuarios finales para el sitio de la Guía de Trámite, para sus interfaces de administración y carga y para los referentes de la misma.
   - Desarrollo un plan de pruebas e instrumentación de las pruebas previstas
   - Implementación efectiva de sitio seguro
   - Evaluación de Resultados

2. ***Implementación de un prototipo de PKI:***

   - Evaluación de herramientas de libre distribución para el desarrollo o implementación de aplicaciones PKI

- Explicitación del modelo PKI para la constitución de una CA con una RA de pequeña escala para la provincia de Mendoza
- Desarrollo de un Prototipo del diseño preliminar haciendo uso de la tecnología seleccionada. El prototipo debe ser capaz de realizar funciones básicas de una CA y de una RA: Emisión de certificados, gestión del CVS de certificados, gestión de CRL, etc.; bajo las condiciones de interoperabilidad, seguridad y escalabilidad preestablecidas en el Estudio de Factibilidad para una PKI de pequeña escala.
- Documentación del diseño prototipado.
- Diseño de una interface web para el prototipo que permita a usuarios finales gestionar el CVS de sus certificados de manera remota de acuerdo a procedimientos y políticas establecidas.
- Diseño de un plan de pruebas y ejecución
- Evaluación de resultados.
- Desarrollo de políticas de certificación específicas en función de las experiencias piloto implementadas
- Desarrollo de manual de funciones y procedimientos para la gestión del CVS de los Certificados y la administración de las experiencias piloto implementadas
- Análisis de normas técnicas y estándares internacionales de licenciamiento de Autoridades Certificantes

3. ***Implementación de experiencia piloto en el Circuito de Resoluciones:***

- Relevamiento de procedimientos actuales de redacción, corrección, firma y archivo de resoluciones
- Explicitación de necesidades puntuales
- Determinación de mejoras sustanciales
- Determinaciones sobre la provisión de certificados

- Diseño global: propuestas alternativas para el circuito administrativo de resoluciones con aplicación de la tecnología de firma digital.
- Diseño detallado: identificación detallada de los procedimientos y aplicaciones tecnológicas que deberán desarrollarse e implementarse para instrumentar el nuevo circuito administrativo de resoluciones
- Desarrollo: desarrollo de aplicaciones informáticas que sustenten el archivo y gestión digital de resoluciones y la firma digital de las mismas
- Capacitación de los empleados administrativos y funcionarios que intervienen en el circuito
- Plan de Pruebas: diseño y ejecución de un plan de pruebas sobre las aplicaciones informáticas y la estructura procedimental que soporta al circuito
- Implantación: implementación en paralelo, contemplando la digitalización y firma del archivo histórico de resoluciones y la puesta en marcha de los nuevos procedimientos.
- Evaluación de Resultados

4. ***Diseño e implementación de un Plan de Difusión:***

- Identificación de Agentes y Organismos relacionados
- Análisis de Alternativas y medios de difusión
- Diseño de iniciativas de difusión
- Puesta en practica de iniciativas
- Evaluación de Resultados

5. ***Constitución en (RA) Autoridad de Registro Provincial:***

- Identificación de experiencia piloto en la que se usarán los certificados de la ONTI
- Determinación de Funciones de la RA

- •Designación de Oficiales de Registro
- •Determinación de Responsabilidades
- •Diseño de manuales
- •Puesta en Marcha de la Autoridad de Registro
- •Administración de la RA

6. ***Participar y promover la creación y reformulación de normativas relacionadas:***

   - •Tareas de seguimiento y allanamiento del proceso de aprobación del proyecto de Ley de Adhesión a la Ley Nacional de Firma Digital
   - •Promoción de decretos desarrollados y propuestos en el proyecto antecedente de Firma Digital
   - •Promoción y participación en la reformulación de normativas existentes en función de reingenierías de trabajo administrativo provocadas por la aplicación de la nueva tecnología de Firma Digital

7. ***Identificar nuevos ámbitos de aplicación de la tecnología de Firma Digital:***

   - •Aplicación de la Estrategia de Identificación de Procedimientos aptos
   - •Enriquecimiento de la estrategia
   - •Creación de espacios de documentación y respuesta a las necesidades de aplicación de la tecnología desde la propia demanda local
   - •Formulación de nuevas propuestas de implementación de experiencias piloto

8. ***Actividades de Transferencia Tecnológica para la implementación del programa de gobierno digital del CFI en las provincias***

- Preparación de materiales de difusión y presentaciones para eventos de acuerdo con la necesidad particular
- Asistencia en los procesos de transferencia de experiencias brindando asesoramiento técnico y desarrollando documentación de apoyo según el plan establecido por el CFI

Los nuevos contenidos correspondientes a lo planificado para el informe final corresponden a la culminación de la actividad 3,4,5 y la actividad 6, 7y 8.

De esta manera se cumple con los objetivos propuestos para el proyecto y con las líneas de acción planteadas:

LÍNEA DE IMPLEMENTACIÓN DE EXPERIENCIAS PILOTO

Actividades:

Implementación de experiencia piloto de Sitio Seguro: concientes de la transversalidad de nuestro proyecto con las iniciativas de e-government, hemos otorgado seguridad a la carga de contenidos por parte de los referentes de la Guía de Trámites.

Implementación de experiencia piloto en el Circuito de Resoluciones: de acuerdo con la propuesta de aplicación plasmada en el Informe Final del proyecto de Firma Digital precedente, hemos implementado firma digital en el circuito de aprobación de resoluciones de la Secretaría Administrativa Legal y Técnica.

LÍNEA DE INVESTIGACIÓN Y DESARROLLO

Actividades

Implementación de un prototipo de PKI: cuyo antecedente fue el diseño de una Infraestructura de Clave Pública de certificación realizada en el proyecto Firma Digital precedente y a los efectos de bajar a la realidad dicho desarrollo teórico, hemos desarrollado e implementado un prototipo de infraestructura de clave pública a través de una Autoridad Certificante de Firma Digital

LÍNEA DE FORTALECIMIENTO Y CRECIMIENTO DE PROYECTO

Diseño e implementación de un Plan de Difusión: se trató de fortalecer nuestro proyecto acercando la tecnología de firma digital a los distintos agentes relacionados en el ámbito provincial

Constitución en Autoridad de Registro de la ONTI: la celebración de un convenio con la Oficina Nacional de Tecnologías de la Información, Organismo avanzado en materia de firma digital y designado como Autoridad Certificante de la Administración Pública Nacional, nos permitió recibir transferencia tecnológica valiosa para nuestro proyecto y constituimos en una Autoridad de Registro que valide la emisión de certificados para ser usados en experiencias piloto en la Administración Pública Provincial.

Participación, creación y reformulación de normativas relacionadas: determinadas por el subestudio de factibilidad legal realizado y las que surgieron de las implementaciones concretas.

Identificación de nuevos ámbitos de aplicación de la tecnología de Firma Digital: hemos aplicado la Estrategia de Identificación de Procedimientos aptos fijada en el proyecto precedente, como así también estamos respondiendo a las necesidades de las dependencias interesadas en la aplicación de ésta tecnología en sus circuitos y sistemas de información de la demanda local.

INFORME FINAL

I. IMPLEMENTACIÓN DE EXPERIENCIA PILOTO SITIO SEGURO

Siguiendo la tendencia de generar interrelaciones entre los proyectos y aprovechar la sinergia que ellas aportan, el equipo de firma digital ha desarrollado el sistema de Sitio Seguro para el esquema de carga de la Guía de Trámites.

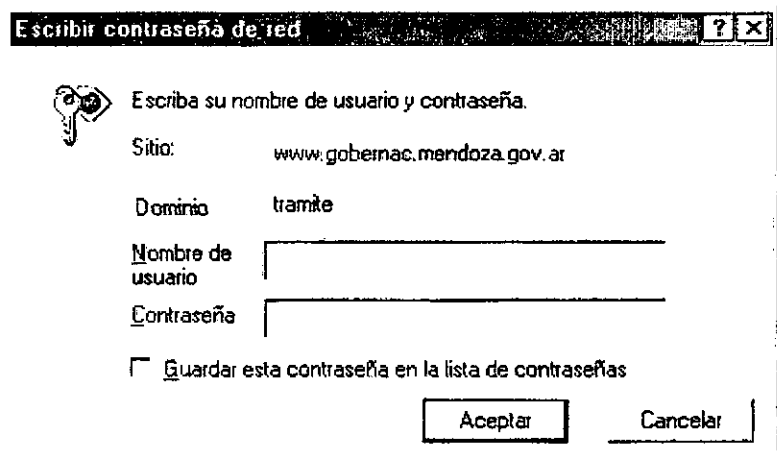
Hablamos de un "Sitio Seguro" cuando nos referimos a un lugar virtual confiable en Internet, perteneciente a una empresa u organización que lo mantiene en línea por medio de un servidor de www (World Wide Web).

Cuando una persona se conecta a un sitio seguro, el servidor presenta un certificado emitido y firmado por la Entidad Emisora de Certificados.

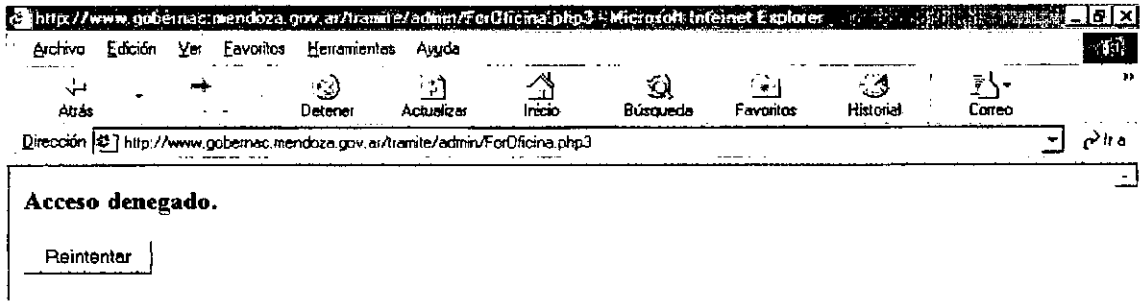
A. Relevamiento del Circuito operativo de carga

Descripción del procedimiento actual:

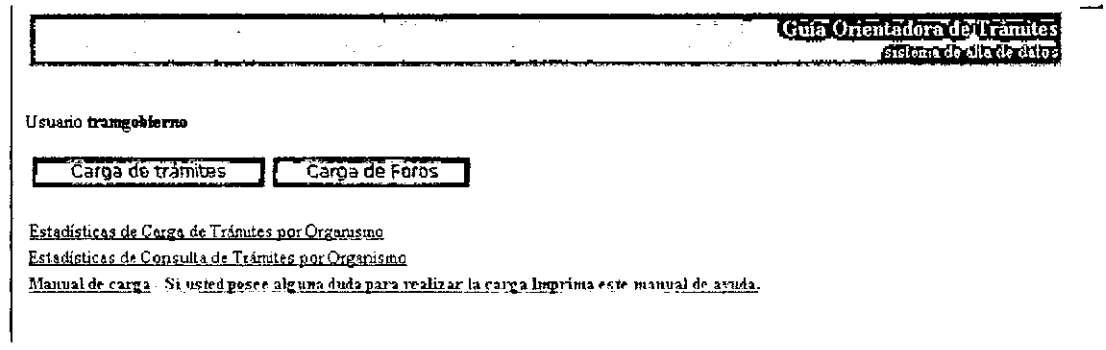
1. **Referente:** Para comenzar la carga de Trámites debe ingresar a: www.tramite.mendoza.gov.ar/admin/usuarios.php3 y en la ventana "Ingresar al Sistema", debe colocar el nombre de usuario **y la** contraseña **asignada.**



2. **Sistema**: si el usuario o la clave no son correctos el sistema lo indicará mediante una página, especificando que se cometió un error. Dando la posibilidad al usuario a volver a ingresar por medio del botón Reintentar que se muestra en dicha página.



3. **Referente:** luego de ingresar correctamente al sistema, presiona botón **Carga de Trámites** y continúa con el procedimiento específico de carga.



Se trata de un procedimiento distribuido, autónomo y totalmente descentralizado para la carga de datos en la que la designación de los responsables se hace en un primer momento y luego debe confiarse en el acceso remoto de los mismos asegurando su identidad a través de medios lógicos de autenticación. Un reto verdaderamente difícil para los mecanismos de autenticación electrónica tradicionales.

Desventajas de un sistema login password

Cuando usamos un típico sistema de usuarios y contraseñas, como el usado actualmente por la Guía, tenemos un nivel de identificación de usuarios débil, es decir, nos encontramos en el umbral de la seguridad para sistemas

informáticos y dadas las condiciones y variables del entorno puede resultar adecuado o no. Tales conclusiones deberán surgir de la consideración del tipo de información que se está intercambiando con el sistema y la valoración de las posibles acciones que se puedan realizar en pos de quebrar la seguridad que éste método sugiere en función de la evolución del poder computacional disponible. Dichos planteos los resolveremos más adelante, por ahora debemos tener claro que el método utilizado actualmente no garantiza:

- ***Identificación unívoca***: el usuario no sabe que está ingresando a su sitio o a una réplica.
- ***Confidencialidad***: la información puede ser interceptada.
- ***Integridad:*** los datos pueden llegar incompletos y con posibilidad de error.
- ***No repudio:*** la información no es digitalmente firmada probando así que fue enviado por cierta persona evitando el rechazo de la misma.

Sin duda son éstas falencias las que se han tenido en cuanta al momento de determinar mejoras en la seguridad del sistema.

B. Explicitación de la necesidad puntual

Retomamos aquí, el desafío planteado en el apartado anterior de determinar claramente cuáles son las necesidades de seguridad que el sistema demanda y cuáles son los fundamentos de la aplicación de Sitio Seguro en la Guía de Trámites.

Estrategia para identificación de procedimientos aptos

Sometimos al circuito de carga de la Guía de Trámites a consideración de nuestra "Estrategia para la Identificación de Procedimientos Aptos", ya que consideramos 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.

Según los "Criterios de selección de circuitos administrativos" de nuestra estrategia, las conclusiones fueron:

- ***Circuitos administrativos de transferencia de información con exigencias de calidad en la información:*** resulta uno de los objetivos primordiales de la "Guía de Trámites" asegurar la calidad de sus contenidos en términos de información fidedigna, actualizaciones oportunas y responsabilidad de los referentes por la carga. No resulta ilógico además, pedir que dicha información no pueda ser alterada mientras viaja al servidor que la almacena para luego ofrecerla al ciudadano.

- ***Circuitos que requieren autenticación de las partes involucradas:*** si lugar a dudas, el circuito de carga de los referentes responsables de ésta tarea necesita autenticación unívoca de las partes. Asegurando que las únicas personas que pueda acceder a los contenidos de la Guía son aquellas que fueron designadas para esa tarea. Desde el otro lado, garantizando a los referentes de carga que la información que están transmitiendo es recibida por el sistema de la Guía y no por otro.

- ***Circuitos administrativos que enlazan importantes distancias geográficas:*** la extensión territorial que abarca el circuito de carga resulta importante. Nos encontraremos municipalidades como la de Malargüe que se encuentran alejadas por más de 350 kilómetros de nuestra Unidad de Reforma, la aplicación de técnicas criptográficas en las instancias del procedimiento, como por ejemplo la autenticación remota de los referentes, soluciona muchos problemas de la no presencialidad y ahorra considerables costos de traslado y tiempo.

- ***Circuitos que incluyen información estrictamente confidencial:*** este criterio no hace alusión al circuito de carga, sino más bien tiene en cuenta

la seguridad de los datos que los usuarios de la guía mandan vía web para la realización de tramitaciones on-line. Datos que no pueden ser publicados sin el consentimiento expreso de sus propietarios

Necesidades puntuales

Nuestra necesidad es la de dotar al sistema de carga de la Guía de Trámites de seguridad en la autenticación y el intercambio de los datos provenientes de los usuarios autorizados para la carga y de la información contenida en la base de datos, mediante métodos de encriptación que aseguran la identidad de las partes involucradas y el traslado seguro de los datos transmitidos.

En concreto debemos asegurar:

- **Protección de los sistemas de transferencia o transporte.** En este caso debemos garantizar, en el diseño del sistema la transferencia segura de la información de forma transparente al usuario final. Ejemplos de este tipo de planteamientos serían el establecimiento de un nivel de transporte seguro, de un servicio de transmisión de datos seguro.
- **Gestión de claves:** Éste es un tópico de capital importancia, al que se aplica el uso de la criptografía y debe estar resuelto antes de que el usuario esté en condiciones de enviar un solo bit seguro. En el caso de las claves secretas el problema mayor consiste en mantener su privacidad durante su distribución, en caso de que sea inevitable su envío de un punto a otro. En el caso de clave pública, los problemas tienen que ver con la garantía de que pertenecen a su titular y la confianza en su vigencia (que no haya caducado o sido revocada).
- **Autenticación del cliente:** representa la necesidad de la identificación inequívoca del referente por parte del el servidor al cual está accediendo y, se pueda garantizar categóricamente que la persona designada responsable de la carga es quién está modificando la base de datos de trámites.

- ***Identificación unívoca del servidor***: desde el otro lado necesitamos asegurarle al referente que está ingresando a su sitio y no a una réplica.
- ***Confidencialidad***: resulta de vital importancia garantizar que la información que se le carga al sistema llegue a la base de datos de una manera segura, evitando bajo todo punto de vista la interceptabilidad de la información
- ***Integridad:*** evitar la posibilidad de que los datos pueden llegar incompletos y con posibilidad de error.
- ***No repudio:*** debemos probar que la información cargada ha sido enviada por cierta persona evitando el rechazo de la misma, para asegurar los atributos de calidad buscados por la Guía de Trámites en sus contenidos.

Entonces, la constitución de un SITIO SEGURO consiste en la seguridad en la comunicación a través de redes, especialmente Internet, consistente en prevenir, impedir, detectar y corregir violaciones a la seguridad durante la transmisión de información, más que en la seguridad en los ordenadores, que abarca la seguridad de sistemas operativos y bases de datos. Consideraremos la información esencialmente en forma digital y la protección se asegurará mayormente mediante medios lógicos, más que físicos.

Los mecanismos básicos pueden agruparse de varias formas para proporcionar los servicios previamente mencionados. Conviene resaltar que los mecanismos poseen tres componentes principales:

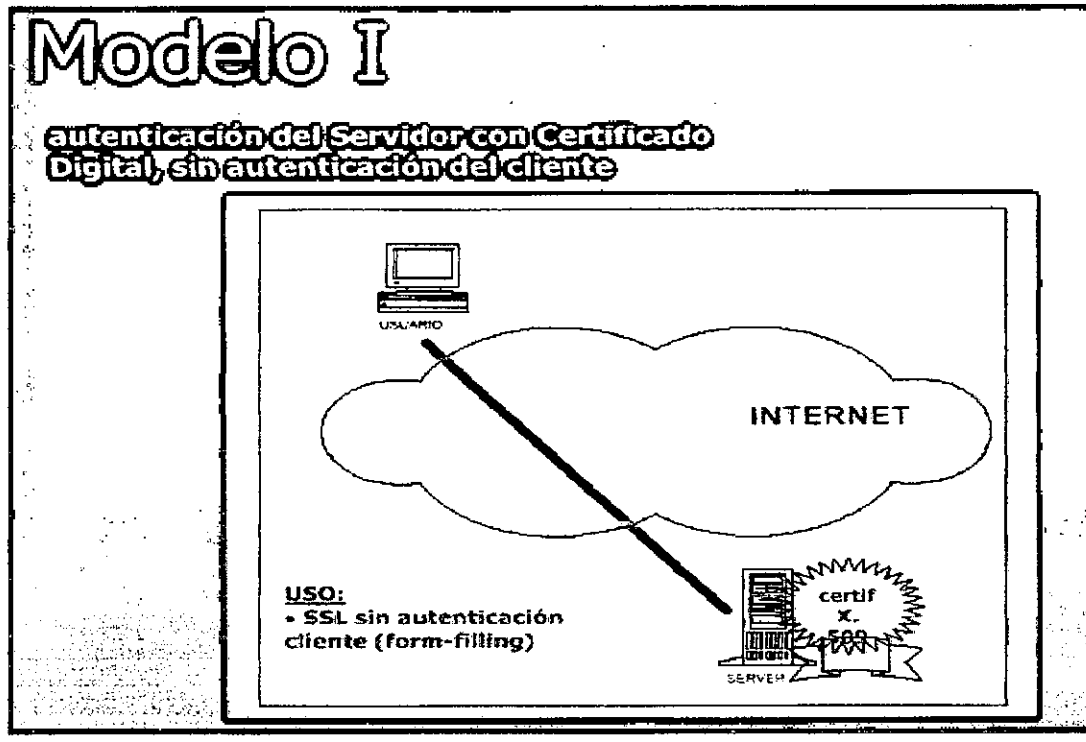
- Una información secreta, como claves y contraseñas, conocidas por las entidades autorizadas.
- Un conjunto de algoritmos, para llevar a cabo el cifrado, descifrado, hash (desmenuce de un mensaje compilado) y generación de números aleatorios.
- Un conjunto de procedimientos, que definen cómo se usarán los algoritmos, quién envía qué a quién y cuándo.

Asimismo es importante notar que los sistemas de seguridad requieren una gestión de seguridad. La gestión comprende dos campos bien amplios:

- Seguridad en la generación, localización y distribución de la información secreta, de modo que sólo pueda ser accedida por aquellas entidades autorizadas.
- La política de los servicios y mecanismos de seguridad para detectar infracciones de seguridad y emprender acciones correctivas.

C. Determinación de mejoras

Concretamente existen dos modelos para mejorar la seguridad del sistema a través de la implementación de Sitio Seguro:



Modelo I: En el primer modelo la aplicación de ésta tecnología proporciona:

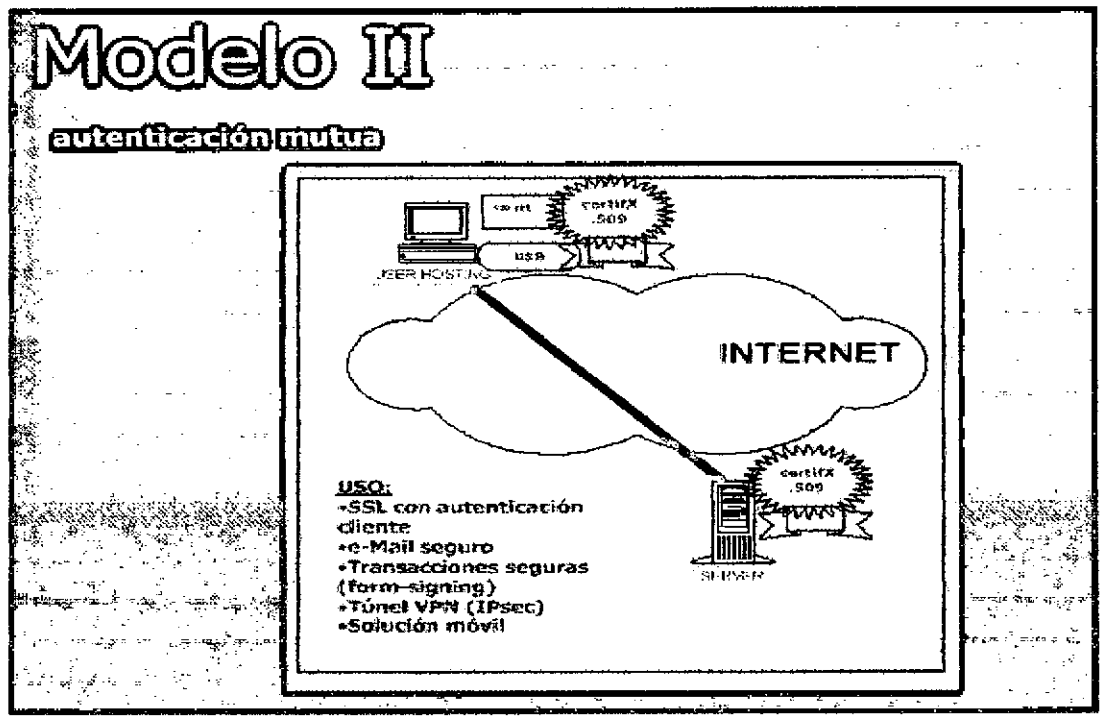
- **Autenticación mutua entre el servidor seguro:** el cliente tiene la garantía de estar *hablando* con el servidor al que accede.

- **Privacidad en el intercambio de información:** sólo el cliente y el servidor seguro conocen lo que viaja por la red. Nadie distinto a ellos podrá leer la información que intercambien. Ahora que se ha establecido un canal de transmisión seguro SSL, es posible el intercambio de datos. Cuando el servidor o el cliente desea enviar un mensaje al otro, se genera un digest (utilizando un algoritmo de hash), encriptan el mensaje y el digest y se envía, cada mensaje es verificado utilizando el digest.

"Este modelo será usado para la transmisión de datos confidenciales de los usuarios de e-trámite de la Guía de Trámites con el objeto de proveer una serie de garantías", *a saber:*

- ***Identificación unívoca***: Constituye una mejora fundamental al momento de aportarle al usuario la total seguridad de que sus datos están siendo ingresados por el sitio Guía de Trámites y no en una réplica del mismo.
- ***Confidencialidad***: la información que viaje desde el usuario a la Base de Datos no podrá ser interceptada. Constituye una mejora radical en la seguridad en el traspaso de datos mediante herramientas de encriptado de información. Contribuye al aseguramiento de la integridad y veracidad de la información.
- ***Integridad:*** los datos envidos por usuarios llegarán completos y sin posibilidad de error, ya que la tecnología garantiza la verificación de la integridad de los mensajes mediante la aplicación de una función de hash. Cualquier diferencia, pérdida de datos, o modificación de los datos originales enviados será alertada por el sistema.

De esta forma, todos los datos provenientes de los usuarios que realizan trámites a través de la Guía se resguardan, mediante métodos de encriptación que aseguran la integridad y confidencialidad de la información que viaja por la web.



Modelo II: En el segundo modelo la aplicación de ésta tecnología proporciona:

- **Autenticación mutua entre el servidor seguro y el cliente.** El servidor sabe con total seguridad quien es el cliente que esta al otro lado y el cliente tiene la garantía de estar *hablando* con el servidor al que accede.
- **Privacidad en el intercambio de información.** Sólo el cliente y el servidor seguro conocen lo que viaja por la red. Nadie distinto a ellos podrá leer la información que intercambien. Ahora que se ha establecido un canal de transmisión seguro SSL, es posible el intercambio de datos. Cuando el servidor o el cliente desea enviar un mensaje al otro, se genera un digest (utilizando un algoritmo de hash), encriptan el mensaje y el digest y se envía, cada mensaje es verificado utilizando el digest.

***"Este es el modelo que se ha elegido para el circuito de carga de información por parte de los referentes de la Guía de Trámites con el objeto de proveer una serie de garantías"**, a saber:*

- ***Identificación unívoca***: Constituye una mejora fundamental al momento de aportarle al referente la total seguridad de que sus datos están siendo ingresados por el sitio Guía de Trámites y no en una réplica del mismo, por otro lado garantiza la identidad del referente que está cargando información ante el Sitio Guía de Trámites, aporte fundamental a la calidad de los contenidos on-line.
- ***Confidencialidad***: la información que viaje desde el referente a la Base de Datos no podrá ser interceptada. Constituye una mejora radical en la seguridad en el traspaso de datos mediante herramientas de encriptado de información. Contribuye al aseguramiento de la integridad y veracidad de la información.
- ***Integridad:*** los datos envidos por los referentes llegarán completos y sin posibilidad de error, ya que la tecnología garantiza la verificación de la integridad de los mensajes mediante la aplicación de una función de hash. Cualquier diferencia, pérdida de datos, o modificación de los datos originales enviados será alertada por el sistema.
- ***No repudio:*** la información es digitalmente firmada por el referente probando así que fue enviada por este y por nadie más, responsabilizándolo por la calidad de la información cargada y por la oportunidad en las actualizaciones que se realicen

De esta forma, todos los datos provenientes de los usuarios autorizados para la carga y la información contenida en la base de datos se resguardan, mediante métodos de encriptación que aseguran la identidad de las personas autorizadas a realizar modificaciones en los datos.

Hemos pasado de un sistema de identificación débil a un sistema de identificación fuerte, calificado mundialmente como uno de los más seguros hasta el momento.

D. Desarrollo de documentación explicativa de Sitio Seguro

El siguiente documento forma parte de la información disponible en la Guía de Trámites y tiene como objetivo explicar el funcionamiento de la tecnología de Sitio Seguro.

Con esto se espera difundir el uso de la herramienta a través de sus características y utilidades promoviendo la conciencia en el usuario del cuidado de la seguridad de sus datos en Internet

Sitio Seguro en la Guía de Trámites

Como norma general y mientras no se advierta de lo contrario, cuando usted rellena un formulario y pulsa el botón enviar, está enviando toda la información en forma de datos a través de la red. Datos que son transmitidos de servidor en servidor hasta llegar a su destinatario y que pueden ser interferidos o robados antes de llegar a su destino.

Por eso se hace necesaria la utilización de tecnologías que permitan salvaguardar la privacidad de sus datos.

El protocolo SSL permite la autenticación de servidores, la codificación de datos y la integridad de los mensajes. Con SSL sus comunicaciones en Internet serán transmitidas en formato codificado. De esta manera, la información que envíe llegará de manera privada y no será manipulada. Además, usted tendrá la seguridad de que está ingresando al sitio de la Guía de Trámites y no a una réplica.

¿Qué significa SSL?

Son las siglas inglesas correspondientes a Secure Sockets Layer. El protocolo SSL fue desarrollado por Netscape para permitir confidencialidad y autenticación en Internet.

SSL opera como una capa adicional entre Internet y las aplicaciones

De acuerdo con la convención establecida, la dirección de las páginas Web que requieren una conexión SSL comienza con https: en lugar de http:

"La Guía de Trámites garantiza que todos los procesos de captación y transferencia de información facilitada por los usuarios y referentes es transferida mediante el protocolo de seguridad SSL Secure Sockets Layer (servidor seguro) desde su navegador hasta nuestros servidores"

¿Cómo funciona un servidor seguro?

Para establecer una comunicación segura utilizando SSL se deben de cumplir una serie de requisitos:

1. Cuando un usuario accede a la Guía de Trámites a través de su dirección url segura https://www.tramite.mendoza.gov.ar se establece la conexión y el navegador solicita una conexión segura. Una vez se ha hecho la solicitud, el cliente y el servidor empiezan a negociar la conexión SSL.

2. Como el servidor al que accede es un servidor seguro, este responderá afirmativamente a la solicitud, enviándole un certificado electrónico de tipo RSA.

3. Después de recibir este certificado el navegador lo desempaquetará con la clave de la autoridad de certificación, ya integrada en el software, obteniendo de este modo la clave según el algoritmo RSA.

4. Por último, el navegador genera una clave de encriptación simétrica y se la envía encriptada al servidor (con su clave pública). A partir de este momento, tanto el navegador como el servidor pueden establecer una comunicación segura basada en esta clave simétrica, que ambos y sólo ellos conocen.

"Las claves simétricas son generadas aleatoriamente en cada sesión, por lo cual no hay posibilidad de que estas sean conocidas por eventuales hackers"

¿Cómo puedo saber si realmente estoy en un servidor seguro?

Es sencillo saber si hemos conectado con un servidor seguro. En primer lugar, la dirección de URL comienza por https:// en vez de http:// (a esta dirección se accede, a veces, sin intervención del usuario, debido a que se pulsa una palabra clave que la lleva incorporada, o bien intencionadamente cuando se desea acceder a un servidor en modalidad segura). Además, en la mayoría de los visualizadores tendremos una indicación de que la conexión segura se ha establecido.

Una llave o un candado cerrado en la parte izquierda (Netscape), o bien, un candado cerrado en la parte derecha (Explorer y Navigator). En el caso de Opera, aparece en la parte superior izquierda.

Iconos identificativos de los navegadores más usados:

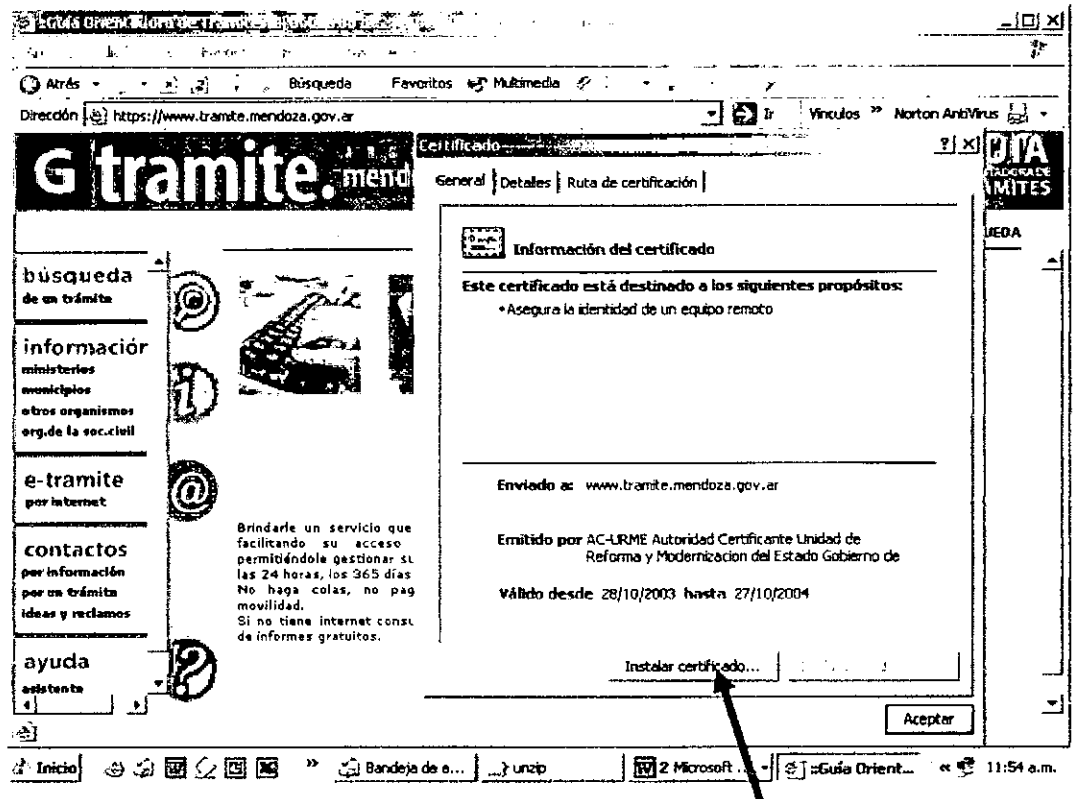
Explorer

Netscape

Navigator

Opera

Además, es importante comprobar que el certificado de seguridad otorgado es válido y vigente haciendo clic en el icono del candado:



Ahora bien, si usted confía en la Autoridad Certificante que emitió el certificado y además el certificado no ha caducado, haga clic en **instalar certificado**

Consejo!!!

Los sitios auténticos utilizan certificados del servidor de la red SSL para ofrecer comunicaciones seguras por desciframiento todos los datos a y desde el sitio. Siempre examine el certificado de un sitio antes de incorporar cualquier información.

Nunca ofrezca información confidencial por Internet sin ningún tipo de protección, especialmente si son números de tarjeta de crédito.

Muy Importante!!!

En el caso de la Guía de Trámites la dirección segura a través de la que se ejecutan todos los formularios es **https://www.tramites.mendoza.gov.ar** y el certificado ha sido otorgado por la **Autoridad Certificante de la Unidad de Reforma y Modernización del Estado de la Provincia de Mendoza (AC-URME).**

E. Determinaciones sobre la provisión de certificados

Provisión de Certificados Digitales

Habitualmente, resulta una decisión muy importante determinar cuál será el agente que emitirá y gestionará los certificados que se piensan aplicar a una experiencia piloto determinada. En su momento, cuando se implementó la experiencia piloto en e-democracia, las circunstancias particulares de la aplicación demandaban el uso de certificados digitales de alta confianza y renombre para la sociedad ya que:

- Era la primer experiencia piloto que se implementaba en la provincia de Mendoza

- Los certificados iban a ser usados en un circuito semiabierto, es decir, la provisión de los certificados alcanzaba a ciudadanos (candidatos a las elecciones)

- Las plataformas políticas eran publicadas y el proyecto de firma digital debía asegurarles garantías de integridad a sus autores y de autoría a los ciudadanos que ingresaban al sitio. Además el candidato que firmaba su propuesta, se hacía responsable ante la sociedad de cumplirla.

Cualquier falla en el sistema hubiera perjudicado fuertemente la credibilidad de una tecnología poco difundida e indirecta o directamente la imagen del candidato político que publicaba

- La planificación de una infraestructura provincial se encontraba en pleno proceso de planificación e investigación, por parte de los integrantes de este proyecto y por lo tanto, no se estaba en condiciones de afrontar las responsabilidades por la emisión y gestión de certificados.

Los factores precedentes impulsaron la celebración de un convenio entre la Unidad de Reforma del Estado y la Compañía Certisur S.A, representante de la prestigiosa Verisign en Latinoamérica. A través de este convenio el proyecto de firma digital 2003 contó con la infraestructura de una empresa de nivel mundial para la provisión de los certificados que serían usados en la experiencia piloto de e-democracia, que se ajustaban perfectamente a las demandas particulares de la aplicación.

Actualmente, el escenario y las condiciones particulares de la experiencia piloto de Sitio Seguro en la Guía de Trámites determinan la consideración de factores diferentes a la hora de tomar una decisión respecto de la provisión de certificados, a saber:

- El equipo de la Unidad de Reforma ha desarrollado un fuerte know how gracias a la experiencia piloto desarrollada en e-democracia

- Paralelamente, las investigaciones sobre la tecnología disponible para el montaje de una Infraestructura de Clave Pública han alcanzado una considerable madurez
- La planificación y el diseño organizacional realizado durante el proyecto de firma digital 2003 proporciona una base conceptual robusta

- El circuito de carga de la Guía de Trámites puede considerarse como un esquema cerrado de implementación, dónde la provisión de los certificados alcanza a agentes ubicados dentro de la estructura organizativa de la Administración Pública Provincial

- El avance en la normativa inherente al respaldo legal de la tecnología de firma digital, tanto a nivel nacional con la designación del nuevo organismo que hará las veces de Autoridad de Aplicación, como a nivel provincial con la Ley de adhesión provincial.

Por lo antedicho, el equipo del proyecto de firma digital ha decidido afrontar la provisión y gestión de certificados para la experiencia piloto de Sitio Seguro en la Guía de Trámites a través del **Prototipo de Infraestructura de Clave Pública AC-URME**, cuyas funciones básicas ya se encuentran implementadas, faltando desarrollos periféricos que no afectaran el correcto funcionamiento de la experiencia de Sitio Seguro.

F. Capacitación de los referentes de la guía

Se ha realizado la capacitación, en forma personalizada, de los referentes de la guía de trámites en el uso del nuevo sistema de seguridad de Sitio Seguro para el circuito de carga de trámites.

La capacitación consistió en una serie de jornadas individuales en las que en algunos casos se citó al referente en la Unidad de Reforma y en otros el equipo de firma digital se trasladó al propio lugar de carga del referente.

Nociones básicas sobre Sitio Seguro

¿Cómo instalar un Certificado Digital?

Acceso de referentes a la Guía de Trámites

Acceso de referentes a la Guía de Trámites

Para establecer una comunicación segura con la Guía de Trámites utilizando SSL se deben de cumplir una serie de pasos. Cada vez que un referente carga un nuevo trámite a la base de datos debe seguir el siguiente procedimiento:

Descripción del procedimiento

El presente procedimiento supone que el referente ya ha instalado en su computadora, y por lo tanto en su navegador de Internet (browser) su Identificador Digital (Certificado emitido por la AC-URME: Autoridad Certificante de la unidad de Reforma y Modernización del Estado), tal como se explica en el documento ¿Cómo instalar un Certificado Digital?.Cabe señalar que una vez hecho esto, el referente sólo deberá realizar el primer paso del procedimiento dejando el resto a cargo del sistema.

1. **Referente:** accede a la Guía de Trámites a través de su dirección url segura https://www.admtramite.mendoza.gov.ar, establece la conexión y el navegador solicita una conexión segura.

2. **Servidor Guía de Trámites:** dado que es un servidor seguro, responderá afirmativamente a la solicitud, enviándole un certificado electrónico de tipo RSA emitido por la AC-URME.

3. **Browser del Referente**: Después de recibir este certificado el navegador lo desempaquetará con la clave de la autoridad de certificación, ya integrada en el software, obteniendo de este modo la clave según el algoritmo RSA.

4. **Servidor Guía de Trámites:** el servidor solicita al referente que se identifique a través de su identificador digital personal (Certificado emitido por la AC-URME). En algunos casos cuando hay más de un certificado instalado en la máquina del referente, este deberá optar por el Certificado Digital para acceso a la Guía de Trámites.

5. **Servidor Guía de Trámites:** verifica la identidad del referente que solicita el acceso comprobando la validez del Certificado Digital instalado en su computadora. En el caso que el referente no posea el Identificador Digital que le fue otorgado o no sea el identificador correcto, se le deniega el acceso y el procedimiento concluye.

6. **Browser del Referente**: Por último, el navegador genera una clave de encriptación simétrica y se la envía encriptada al servidor (con su clave pública). A partir de este momento, tanto el navegador como el servidor pueden establecer una comunicación segura basada en esta clave simétrica, que ambos y sólo ellos conocen.

7. **Referente**: realiza la carga del trámite de acuerdo con el procedimiento de carga habitual del sistema.

G. Instalación de protocolos y configuración de servidores web

Para lograr la implementación de sitio seguro se trabajó en la instalación y configuración de tres componentes o aspectos básicos en los servidores de la Guía:

1. el Protocolo SSL y sus servicios
2. los Certificados de Servidor correspondientes
3. la configuración apropiada del Web Server para dar soporte SSL utilizando los certificados de servidor disponibles

Cabe aclarar que se no se necesitó instalación del protocolo SSL en los clientes, puesto que está embebido en la mayor parte de los browsers, tales como IE, Netscape Comunicator, etc.

Plataforma tecnológica del Servidor

- S.O. RedHat Linux 9.0
- WebServer: Apache Http Server
- SSL: mod-ssl
- Certificados: X509 v3 – PEM encoded

H. Gestión/emisión de certificados

Como se ha mencionado previamente, el desarrollo de sitio seguro proporciona seguridad usando una combinación del protocolo SSL (Secure Sockets Layer) y certificados digitales. SSL maneja las comunicaciones encriptadas y la mutua autentificación entre navegadores y el servidor seguro. Los certificados SSL proporcionan autentificación para el servidor seguro.

Ante la alternativa de trabajar con certificados autofirmados; se decidió utilizar los certificados que podía emitir la AC-URME (Autoridad Certificante de la Unidad de Reforma y Modernización del Estado), aún en su carácter de prototipo, con dos objetivos.

1. Probar los servicios del software PKI implementado y sus desarrollos complementarios, en una aplicación concreta y con un marco procedimental determinado.
2. Instaurar la necesidad de contar con una Autoridad Certificante a la hora de emprender este tipo de desarrollos. Esto tiende a generar conciencia de que es la Autoridad Certificante quien proporciona garantías concernientes a la identidad de la organización que provee el sitio web.

A continuación se presenta a modo de marco general, el ***procedimiento informático*** que debe desarrollarse para obtener un Certificado Digital firmado por una Autoridad Certificante (AC). Este procedimiento que algunas veces es transparente al usuario, es el que en general proponen la mayoría de la empresas líderes en Certificación Digital y los documentos de trabajo más aceptados en la industria. Así mismo, es totalmente coherente con los requisitos establecidos por la Ley 25.506 y sus normas complementarias.

1. El solicitante o suscriptor crea, haciendo uso de alguna herramienta proveedora de servicios criptográficos, un par de claves encriptadas, pública y privada.

2. Una vez creado el par de claves, el solicitante genera una petición de certificado basada en la clave pública. La sintaxis detallada de esta petición o CSR está descripta por el Estándar PKCS#10. La petición contiene información sobre el suscriptor. En el caso de que éste sea un servidor habrá datos referentes al dominio, responsables y hosting del mismo.

3. El solicitante deberá entonces enviar la petición de certificado o CSR, junto con los documentos que prueben su identidad a una AC que resulte confiable para los usos a los que estará determinado el Certificado.

4. La Autoridad Certificante, a través de su Autoridad de Registro posiblemente, cumplimentará los procedimientos establecidos para verificar la identidad del suscriptor.

5. Una vez cumplimentadas las verificaciones pertinentes, la Autoridad Certificante firmará y enviará al suscriptor o responsable del sitio su certificado digital.

6. Luego los suscriptores deberán instalar los Certificados en su browser o en su servidor (en el caso de un certificado SSL) y utilizarlos para manejar transacciones seguras.

Presentado este marco general, documentamos a continuación detalladamente, el procedimiento informático que se siguió para emitir los Certificados SSL y los Certificados de Referentes de la Guía:

Los Certificados utilizados en la implementación de sitio seguro para la Guía de Trámite y su interfase de administración son Certificados X.509 con

Extensiones SSL firmados por la AC-URME y generados en formato PEM-encoded.

Su estructura y contenido, ajustadas a las especificaciones de un X.509 v3, a la recomendación RFC 3280 y al diseño preliminar de los certificados emitidos por la AC-URME.

I. Desarrollo de un plan de pruebas e instrumentación

Se realizaron pruebas para evaluar la operatoria completa del Sitio Seguro en función del modelo de comportamiento esperado. En función de los resultados se realizaron los ajustes necesarios en la configuración del web Server y en el formato de los Certificados emitidos.

J. Implementación efectiva de Sitio Seguro

Al 24/12/03 se han desarrollado y ejecutado todas las actividades que, de acuerdo con los puntos anteriores del presente informe, significaron la implementación efectiva del Sistema de Sitio Seguro en la Guía de Trámites del Gobierno de la Provincia de Mendoza.

K. Evaluación de Resultados

Indicadores Críticos

Experiencia piloto Sitio Seguro
(Mediciones realizadas al 24/12/03)

Indicadores Cualitativos	Métricas y Resultados
Satisfacción de los usuarios: # Quejas y Reclamos	No se han registrado quejas por el sistema de Sitio Seguro
Marco legal: Documentación de la experiencia	Procedimientos de emisión y solicitud de certificados (En desarrollo) Política de certificación (En desarrollo)
Alcance: Participación de los sectores relacionados	Ministerio de gobierno Ministerio de Hacienda Ministerio de Economía Ministerio de Ambiente y Obras Públicas Instituto Provincial de la vivienda Ministerio de Justicia y Seguridad

Indicadores Cuantitativos	Métricas y Resultados
Eficiencia:	
% de certificados emitidos correctamente	100 % (7 personales y 1 de servidor)
# de fallas del sistema	0 (No se produjeron fallas)
# de interrupciones del servicio	0 (El servició estuvo disponible 365/7)
Asistencia:	
# de actores capacitados	7 (siete) referentes de la guía de trámites
# de asistencias otorgadas	8 (siete) Acciones de asistencia técnica
% de asistencias exitosas	100%
Uso del Sistema:	
% de utilización de servicios	95% de accesos con certificado
(sobre el total de referentes con Certificado)	5% de accesos login password
# de comunicaciones seguras establecidas	53
Acciones correctivas detectadas	**Acciones correctivas implementadas**
No se han detectado hasta la fecha	Ninguna

Calificación ponderada final

Implementación exitosa de la experiencia piloto

II. IMPLEMENTACIÓN DE UN PROTOTIPO DE PKI

A. Evaluación de herramientas de libre distribución

El criterio general que se adoptó para seleccionar el software PKI, fue optar por aquella herramienta que soportara la mayor cantidad de características funcionales, con los mínimos requerimientos de desarrollos complementarios y con las mejores condiciones en cuanto a:

- simplificación de la complejidad de diseño y desarrollo, instalación y puesta a punto.
- portabilidad de código
- soporte de tecnologías asociadas
- interoperabilidad
- escalabilidad

Atentos a este criterio general, concluimos en la conveniencia de utilizar EJBCA, puesto que representa, dentro de las opciones evaluadas, la mejor opción para prototipar una Autoridad Certificante de pequeña escala como la descripta.

B. Explicitación del modelo PKI

De acuerdo con los conceptos plasmados en el estudio de factibilidad precedente a la continuidad de este proyecto, se consideró estratégico otorgarle al espectro de criptografía de clave pública la planificación de 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"

Es por eso que para el año 2004 consideramos la implementación de un prototipo de PKI atendiendo dos razones de corte estratégico:

- Sentar un importante precedente provincial que nos permita fundamentar un futuro licenciamiento de la Autoridad Certificante de la Unidad de Reforma y Modernización del Estado (en adelante AC-URME)
- Posicionarnos con una infraestructura propia que nos permita la provisión y gestión de certificados de forma totalmente independiente

Misión del prototipo

Securizar las transacciones electrónicas de la Administración Pública Provincial en un entorno de prueba, proveyendo claves y gestionando eficientemente certificados confiables, para lograr las preciadas garantías de autenticación, integridad, confidencialidad y no repudiación.

Objetivos

Nuestra definición de un Prototipo de Infraestructura de Clave Pública (AC-URME) de propósito general para la provincia de Mendoza sustenta los siguientes objetivos:

•Probar y determinar los alcances de la tecnología disponible

•Evaluar la implementación de una infraestructura propia de Firma Digital a través de un prototipo con alcances reales

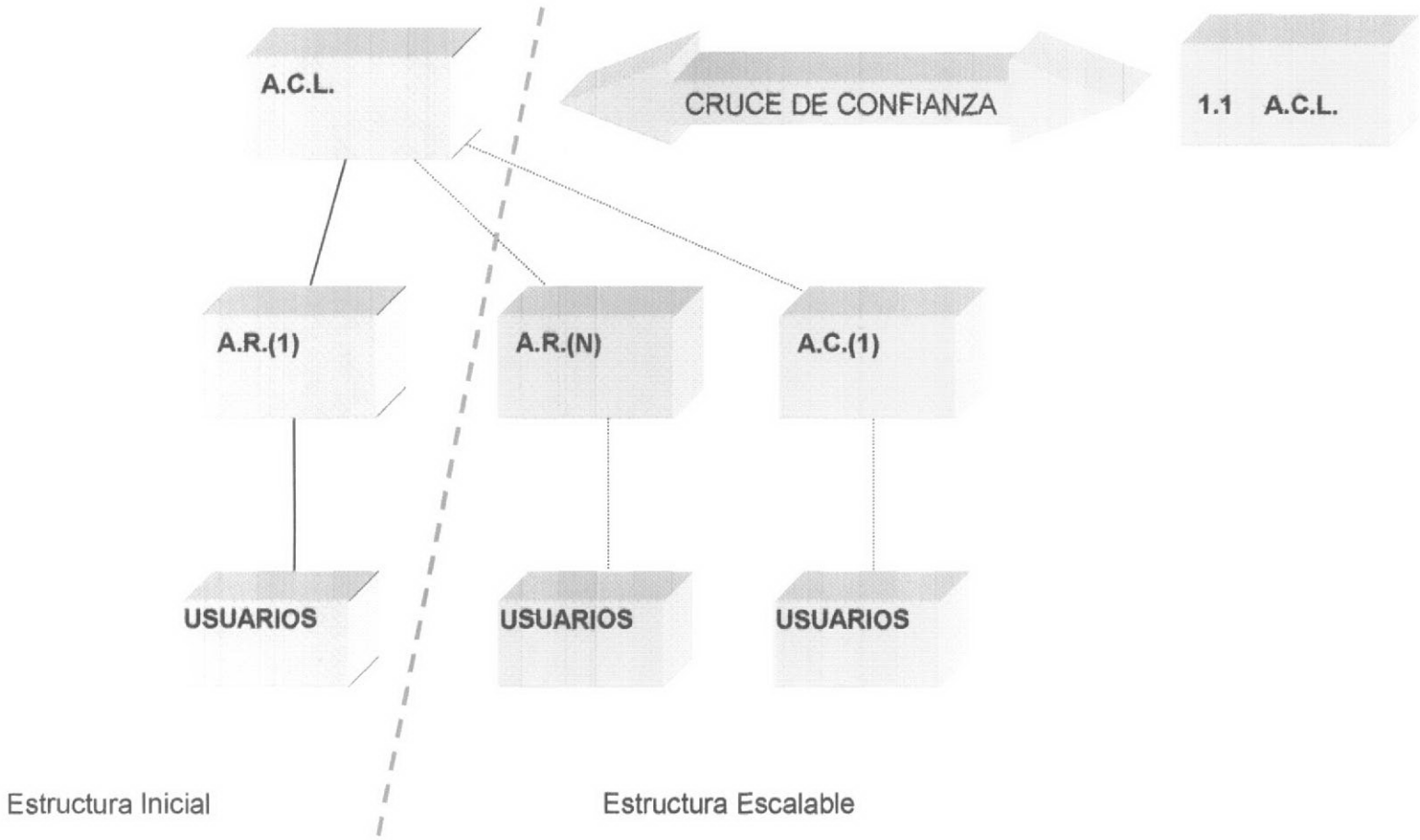
•Posibilitar, desde una perspectiva administrativa y técnica, la utilización de servicios de firma digital de una variedad de aplicaciones piloto en la Administración Pública Provincial, atendiendo a nociones de eficiencia, optimización y despapelización del Estado

Estructura formal

Ha sido nuestro objetivo plasmar aquí la organización estructural que le daremos a nuestra implementación prototipo de la AC-URME. Es conveniente señalar que en su diseño se materializan las premisas planteadas en el estudio de factibilidad sobre condiciones de interoperabilidad y de escalabilidad realizadas en el proyecto antecedente.

Por consiguiente en la figura 1 se muestra tanto la estructuración inicial del prototipo, como también la tendencia ordenada y gradual de crecimiento planificad del mismo (Sombreado).

Figura 1 – Estructura inicial del prototipo AC-URME y escalabilidad



Consejo Federal de Inversiones
Lic. Pablo Guillermo Lioy
"Firma Digital

Modelo de Escalabilidad del prototipo

Como se puede ver en la figura 1 nuestra definición del prototipo 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.

▪El futuro licenciamiento de la Autoridad Certificante para dejar su condición de prototipo y obtener la plena validez de los certificados que emite y gestiona.

Alcance General de la Infraestructura

La infraestructura del prototipo 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 y dependencias del Poder Ejecutivo Provincial, dentro del marco de las experiencias piloto que se realicen.

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 nuestro prototipo AC-URME desarrolle y experimente 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

C. Desarrollo del Prototipo AC-URME

EJBCA – SOFTWARE PKI

Los desarrollos de la AC-URME se estructuran sobre el software PKI EJBCA. EJBCA es básicamente una API java, de libre distribución y código abierto, mantenida y actualizada como un proyecto Sourcefoge www.sourceforge.net, que provee componentes para el desarrollo de todos los servicios básicos de una AC; con amplias posibilidades de escalabilidad puesto que puede ser utilizada como una aplicación standalone o integrada en cualquier aplicación J2EE.

Como se vio en la evaluación de herramientas alternativas, las principales características que justificaron el uso de esta herramienta:

- licencia Open Source (LGPL)
- construida sobre tecnología J2EE
- arquitectura basada en componentes flexibles que pueden ser incorporados o no en desarrollos particulares
- permite crear una jerarquía con múltiples niveles de CAs
- soporte al Enrroll individual o emisión batch de certificados
- soporte a certificados en formatos PKCS#12, PEM o DER
- APIs y herramientas diversas para el desarrollo de una interfase web de administración del CVS.
- GUI de administración web, asegurada a través de autenticación fuerte
- soporte a múltiples niveles de administradores con privilegios específicos y grupos de usuarios basados en perfiles
- profiles configurables para diferentes tipos de certificados y perfiles de usuario

- manejo de certificados bajos los estándares X509 y PKIX (RFC3280).
- manejo de CRLs (Certificate Revocation List) de acuerdo al estándar X509 v2
- generación programada y automática de CRL
- soporte a puntos de distribución de la CRL basada en URL de acuerdo a la recomendación RFC3280
- clases para notificación por email de nuevos usuarios agregados por la RA.
- almacenamiento de certificados y CRLs en múltiples motores de Bases de Datos
- soporte a la publicación LDAP de certificados y CRLs.
- soporte SCEP (Simple Certificate Enrollment Protocol)
- Soporte OCSP (Online Certificate Status Protocol)

Construcción de Profiles de Certificados

Un profile de Certificado define la configuración y contenidos que tendrán los Certificados emitidos bajo ese perfil. De acuerdo a lo propuesto en el diseño detallado de los contenidos mínimos de Certificados, se definieron los siguientes profiles para el prototipo AC-URME:

- ***CA:*** Define los contenidos mínimos y extensiones de Certificados de una Autoridad Certificante potencial en la jerarquía AC-URME.
- ***ROOTCA:*** Define los contenidos mínimos y extensiones del Certificado Raíz de la Autoridad Certificante principal de la AC-URME.
- ***ENDUSER:*** Define los contenidos mínimos y extensiones de los Certificados que se emitan a Personas físicas.
- ***SERVIDOR:*** Define los contenidos mínimos y extensiones de los Certificados SSL que emita el prototipo AC-URME.

- ***PRUEBA:*** Este profile se creó a los efectos de probar distintas alternativas de configuración de Certificados y su comportamiento frente a distintas aplicaciones. Su único objetivo es la realización de pruebas técnicas y no se emitirán para uso en aplicaciones reales bajo este profile.

La definición de estos perfiles se concretó a través de las herramientas de configuración que provee la interface web de configuración del software PKI.

Con la tecnología PKI de base previamente instalada, y los aspectos fundamentales de diseño debidamente configurados se abordó el desarrollo y puesta a punto de los módulos de emisión, renovación y revocación de certificados, seguimiento de transacciones y emisión de la CRL. Documentamos a continuación las características más relevantes de cada desarrollo.

Cabe aclarar que los usuarios o las entidades que solicitan certificados quedan registrados en la base de datos central del Prototipo AC-URME. Esta base de datos reúne información de identificación de usuarios registrados, certificados emitidos, renovados o revocados y toda transacción realizada sobre el prototipo. De este modo se articula sobre un repositorio central de información la operación de todos los circuitos involucrados en la gestión del ciclo de vida de certificados.

Emisión de Certificados

Se desarrollaron procedimientos para la emisión individual de certificados bajo los siguientes perfiles:

- Certificado de CA
- Certificado de RootCA
- Certificado de Usuario final – Enduser
- Certificado de Servidor

- Certificado de Prueba

Para certificados de Usuario Final y de Prueba, se desarrollaron también mecanismos de generación batch, de lotes de Certificados, de acuerdo a información de registro suministrada por Bases de Datos.

La emisión de certificados requiere los siguientes pasos:

- El usuario o entidad solicitante completa la Solicitud de emisión de Certificado sobre su par de claves.
- La Autoridad de Registro, previa verificación de identidad de acuerdo a los procedimientos descritos en el Manual de Procedimientos, aprueba la solicitud con su firma y la remite a la Autoridad Certificante en formato PKCS#10.
- la Autoridad Certificante emite el Certificado de acuerdo al CSR PKCS#10 y bajo el perfil adecuado.
- Los certificados emitidos se distribuyen a partir de la interface web del prototipo o en algún medio de almacenamiento magnético: disquetes, CDs, etc.

Los certificados emitidos son automáticamente publicados en el directorio LDAP del prototipo AC-URME.

El módulo soporta los siguientes formatos de codificación del certificado: P12, JKS y PEM.

Renovación de Certificados

El procedimiento de renovación provoca la emisión de un nuevo Certificado para el mismo par de claves. Tanto el certificado anterior como su renovación quedan almacenados en la base de datos y accesibles desde la interfase de Administración web del prototipo.

No se han impuesto controles de fechas para la renovación, el único requisito imponible es que el estado del suscriptor esté habilitado para con-

cretar la renovación. Es decir que se haya configurado a *new* su estado, operación que solo está permitido para el administrador de la CA.

El proceso de revocación cambia el estado de un Certificado de *Generated* a *Revoked*, previa recepción de solicitud del suscriptor, de informe de la RA o por operación del administrador de la CA.

El cambio de estado a *revoked* provoca la inclusión inmediata del certificado en la próxima CRL generada por la CA.

Así mismo, se almacena en la base de datos central del prototipo AC-URME y en la extensión *reason code* de la entrada correspondiente al certificado en la CRL, información sobre el motivo de la revocación dentro de las siguientes posibilidades:

- Compromiso de clave
- Compromiso de CA
- Compromiso de RA
- Cambio de datos de entidad
- Cese de operaciones
- Redefinición de privilegios
- Motivo no especificado

Seguimiento de Transacciones

A partir de la información almacenada en la base de datos del prototipo y de los logs de transacciones del aplication web server, se construyó un script de seguimiento de transacciones que permite obtener la siguiente información:

- logins de administrador
- revocación de certificados
- cambio de privilegios de CA-administrador
- cambio de privilegios de RA
- creación de CRL
- creación de certificados
- edición de profiles de certificados

- revocación de certificados
- renovación de certificados
- definición de usuarios
- actualización de datos de usuarios
- eliminación de usuarios
- notificaciones
- edición de parámetros de configuración
- eventos desconocidos
- eventos de error:
    - en logins de administrador
    - en revocación de certificados
    - en transacciones sobre los datos de usuarios
    - intentos de acceso no autorizados
    - en la creación de CRL
    - en la emisión de certificados
    - en cambios de configuración de preferencias de administrador
    - en cambios en la edición de profiles de certificados
    - en querys a la base de datos
    - en notificaciones

Emisión de CRLs

Se desarrollaron para el prototipo las rutinas de ***emisión de CRL*** configurado para activarse automáticamente cada 24 hs. y ***descarga de la última CRL*** emitida en formato .crl (extensiones Crypto Shell) disponibles para ser incorporadas en browsers como IE o Netscape.

El diseño de la CRL se ajusta al estándar X509 v2, siguiendo las recomendaciones publicadas por la Oficina Nacional de Tecnologías Informáticas – ONTI y la *RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"*.

Dado que se trata de un prototipo, no se han incluido en el desarrollo de CRL todas las extensiones propuestas en el diseño, sino sólo la extensión *reason code* dada su importancia a los efectos de la realización de pruebas.

D. Documentación del Diseño Prototipado

Se documenta a continuación las tareas vinculadas con la instalación y configuración primaria de EJBCA en el servidor de prueba, su customización de acuerdo al diseño global de la AC-URME; y los primeros desarrollos realizados sobre este producto.

Esta documentación tiende a informar los aspectos más relevantes de la instalación, sin que sea posible realizar, en el contexto del presente informe, un abordaje pormenorizado de todos los detalles.

Plataforma instalada en el Servidor AC-URME

- Sistema Operativo: Linux Red Hat 8.0
- Base de Datos: PostgreSQL 7.2
- Aplication Server: JBOSS 3.2.0_Tomcat 4.1.24
- CA Autority: EJBCA 2.0.1

Instalaciones previas

Previo a la instalación del software de la CA Autority, se deben instalar los siguientes productos. Se documentan los puntos más relevantes de su configuración para un funcionamiento elemental; y las direcciones web desde donde se pueden descargar los productos y su documentación.

- ***Plataforma java - J2EE (Java II – Enterprise Edition)***. Como software de base a todo el desarrollo es necesario instalar la plataforma Ja-

va II. Se deberán configurar como mínimo las variables de entorno *JAVA_HOME, CLASSPATH* y *PATH*. www.javasoft.com / www.sunjava.com

- ***AplicationServer – JBOSS 3.2.1. con Tomcat 4.1.1.*** – EJBCA se desarrolla sobre el open source J2EE Aplication Server JBoss con un motor Servlet embebido, en nuestro caso Tomcat. JBoss debe descomprime en un directorio cuyo nombre no tenga espacios. Con su configuración inicial se puede levantar el servidor y testear su funcionamiento en modo localhost navegando la dirección http://127.0.0.1:8080 – Inicialmente da error porque no tiene ningún contexto configurado. Se debe configurar la variable de entorno *JBOSS_HOME* de modo que apunte al directorio raíz donde se instaló el AplicationServer. www.jboss.org

- ***Apache ant*** – Herramienta java utilizada para la compilación de las aplicaciones. Se debe configurar la variable de entorno *ANT_HOME* de modo que apunte al directorio donde se instaló la aplicación. Agregar ${ANT_HOME/bin} al paso del sistema. Puede testearse su correcto funcionamiento ejecutando el comando *prompt ant –help* en el prompt.

Otras dependencias que son incluidas junto al software son:

- ***Bouncycastle:*** Para sus servicios criptográficos y la creación de certificados y CRLs, EJBCA usa el open source JCE crypto provider de Bouncy Castle. Este software no requiere instalación particular por cuanto se provee junto a EJBCA como bcprovidk 14-1.19-.jar y bcmail-jdk14-1.19. La versión incluida en EJBCA 2.0 es 1.19. www.bouncycastle.org

- ***Log4J:*** Este producto provee el seguimiento de transacciones – logs de transacciones- sobre JBOSS. Es un proyecto de Apache Software Foundation . La versión provista por el release de EJBCA utilizado es la 1.2.7. www.ant.apache.org , www.jakarta.apache.org

- ***JUnit:*** Esta herramienta se utiliza para el desarrollo de test automatizados. EJBCA la utiliza para correr el runtest inicial de la instalación u otro tipo de pruebas particulares que pueden ser diseñadas. La versión utilizada es 3.7. y esta licenciada bajo una IBM Public License. www.junit.org

- ***OpenLDAP:*** Directorio LDAP de código abierto provisto por el grupo OpenLDAP. www.openladp.org

Instalación Primaria de la CA Autority – EJBCA 2.0.1

Se resumen a continuación los pasos básicos seguidos en la instalación primaria del software EJBCA.

1. Descomprimir el archivo ***ejbca2_0_tar.gz*** en un directorio.
2. Compilar la aplicación con la herramienta ***ant. Ant*** es un producto que opera sobre el archivo de configuración *build.xml* compilando las aplicaciones Java descriptas por este archivo.
3. Construir la documentación de EJBCA con ***ant javadoc***
4. Ejecutar ***ant deploy.*** Esta herramienta monta los servicios de la CA Authority sobre el AplicationServer JBOSS.
5. Ejecutar ***ant keystore*** esto copia el keystore primario (almacén de certificados de prueba) *(src/ca/keystore/server.p12)* al directorio $JBOSS_HOME/conf
6. Levantar los servicios del servidor JBOSS
7. Correr el test preliminar sobre la herramienta con el script ***runtest.sh***

8. Inicializar la CA para operación corriendo el script ***ca.sh init.*** Este script emite la primera CRL y ajusta algunos parámetro de operación inicial.

Configuración el servicio de directorios LDAP

Para publicar certificados y CRLs en un directorio LDAP, se instaló en primera instancia el paquete OPEN LDAP www.openldap.org, elegido entre las alternativas posibles como el servicio de directorio a utilizar.

Configuración de la Interfase de Administración WEB RA - ADMIN

La interfase de administración web permite administrar EJBCA remotamente mediante una conexión SSL (128 bits) con autenticación de Cliente. El Administrador de la AC-URME posee por tanto un Certificado de ***Super-Admin*** que le permite acceder a esta herramienta.

Puesta en marcha - iniciación primaria de la AC-URME

Hasta aquí se describió la instalación del software de base para la Autoridad Certificante y la configuración del mismo de acuerdo al conjunto de herramientas tecnológicas y servicios que se decidió utilizar para el desarrollo de la AC-URME.

Vamos a documentar ahora, los primeros pasos dados en la puesta en marcha de la AC-URME. Es decir, el procedimiento informático seguido para la creación de la CA y la RA de acuerdo al diseño PKI propuesto, la emisión del Certificado de la CA y la emisión de la primera CRL.

1. Crear el keystore de la CA raíz de la AC-URME, utilizando el script *ca.sh*

./ca.sh makeroot "C=**AR**, O=**Gobierno de Mendoza**, OU = Secretaria Administrativa Legal y Tecnica del Gobierno de Mendoza, OU = Unidad de Reforma y Modernizacion del Estado, CN = AC-URME Autoridad Certificante Unidad de Reforma y Moder-

nizacion del Estado Gobierno de Mendoza" 1024 365 null $JBOSS_HOME/server/default/deploy/conf/server.p12 *******

El comando anterior crea la estructura para la CA Raíz de la PKI, su par de claves y su certificado. Se ha utilizado una longitud de clave de 1024 bits (RSA) y se ha dado validez de un año para el Certificado. El repositorio del Certificado es *server.p12*

Nota: Los nombres y directorios referenciados para los repositorios de certificados y otros datos se han dado a modo de ejemplo, pero no revelan nominaciones reales con el objetivo de preservar la seguridad de la AC-URME.

2. Editar el archivo de configuración *src/ca/ca/META-INF/ejb-jar.xml* para reflejar los valores asignados al Keystore y al KeyStorePass
3. Ejecutar el comando *ant keystore* para montar sobre JBOSS la nueva configuración.
4. Inicializar la CA luego de haber generado la clave del rootCA ejecutando el script *./ca.sh init*

PKIX requiere que la CRL esté siempre disponible aunque esté vacía. Por ello la CA debe ser inicializada corriendo el script *ca.sh init* luego de que el rootCA ha sido creado.

Certificados AC-URME

Una vez inicializada, la Autoridad Certificante ya está en condiciones de emitir Certificados. A partir de este momento deben definirse aspectos del **diseño detallado** de la AC-URME, tales como los **perfiles de usuario** a Certificar, los **procedimientos y políticas de Certificación** y el formato e información general de **Certificado** que emitirá la CA.

El diseño propuesto adhiere al contenido de los siguientes documentos:

- RFC 3039 "Internet X.509 Public Key Infraestructure Qualified Certificates Profile"
- RFC 3280 "Internet X.509 Public Key Infraestructura Certificate and Certificate Revocation List (CRL) Profile"
- RFC 3279 "Algorithms and Identifiers for the Certificate and Certificate Revocation List (CRL) Profile"
- Textos preliminares de los documentos referidos al proceso de licenciamiento de certificadores publicados por la ONTI – Oficina Nacional de Tecnologías de la Información dependiente de la Subsecretaría de la Gestión Pública de la Jefatura de Gabinete de Ministro
- Especificaciones de diseño

Extensiones de certificados

Se consideran en este apartado las Extensiones de Certificados que según la RFC 3280 y en consonancia con los textos preliminares del proceso de licenciamiento publicados por la ONTI se ha decidido incorporar como mínimo en los Certificados emitidos por la AC-URME

Las extensiones a incluir en los Certificados Emitidos por la AC-URME son:

- ✓ *BasicConstraint*
- ✓ *KeyUsage*
- ✓ *CRLDistributionPoint*
- ✓ *SubjectKeyIdentifier*
- ✓ *CertificatePolicies*
- ✓ *AutorityKeyIdentifier*
- ✓ *ExtendedKeyUsage*
- ✓ *SubjectAlternativeName*

NO CRÍTICAS

Serán marcadas como no críticas las siguientes extensiones

Authority Key Identifier

Descripción: Proporciona un mecanismo para identificar unívocamente la clave pública correspondiente a la clave privada utilizada para firmar un certificado por la AC. Esto es útil fundamentalmente cuando el Certificador tiene múltiples claves de firma y múltiples certificados en uso; ya que contribuye a la construcción de la ruta de certificación. Es útil también para localizar claves que han expirado, con fines de verificación de firmas a largo plazo, en las cuales se necesita la validación de la cadena para firmas de certificados, cuando todos los certificados y claves en la cadena puedan haber expirado. Esta extensión, está compuesta por tres campos: *KeyIdentifier*, *authorityCertIssuer*, *authorityCertSerialNumber*. La clave de CA específica se puede identificar mediante la especificación de un valor para el campo *keyIdentifier* de esta extensión o mediante el uso de una combinación de los campos del número de serie del certificado CA (*authorityCertSertial Number*) y el nombre de CA *(authorityCertIssuer)*. Se pueden usar ambos mecanismos, pero la forma *keyIdentifier* permite una identificación más específica cuando se construyen rutas de certificación y es por esto que se ha decidido utilizar este mecanismo en la ACURME.

Contenido Certificados AC-URME: Para todos los certificados emitidos por la AC-URME sean estos para personas físicas, jurídicas o servidores se utilizará el OCTECT STRING asignado en la extensión *Subject Key Identifier* del Certificado rootCA de la AC-URME en el campo *KeyIdentifier* de la Extensión *AuthorityKeyIdentifier*. Es claro que en el caso del Certificado de rootCA coincidirán los valores de las extensiones *Subject Key Identifier* y *Authority Key Identifier*.

SubjectKeyIdentifier

Descripción: Proporciona un mecanismo para identificar certificados que contienen una clave pública particular. Esto es útil fundamentalmente cuando el Certificador o una entidad destino, tiene múltiples certificados en uso, algunos de los cuales contienen la misma clave pública (en el caso de las renovaciones por ejemplo). En este último caso, todos los certificados asociados a una misma clave pública, deberían tener el mismo valor para la extensión *SubjectKeyIdentifier.*

Esta extensión, está compuesta por el campo: *KeyIdentifier* el cual contiene un número, derivado en general de la clave pública, que sirve como identificador único para esa clave pública. La AC-URME, de acuerdo a la RFC 3280, opta por utilizar el Hash SHA-1 (160 bits) calculado sobre la Clave Pública para construir este valor. Para facilitar la construcción de la ruta de certificación, esta extensión DEBE estar presente en cualquier certificado de Autoridad Certificante, es decir, en todos aquellos certificados que tengan el campo *ca=TRUE* en la extensión crítica *basicconstraint.* El valor del campo *KeyIdentifier* de la extensión *SubjectKeyIdentifier* en el certificado de CA deberá ser el valor del campo *KeyIdentifier* en la extensión *AuthorityKeyIdentifier* de todos los certificados emitidos por esta CA. Se sugiere también que esta extensión esté presente en todos los certificados de entidad destino.

Contenido Certificados AC-URME: La AC-URME, de acuerdo a la RFC 3280, asignará al campo *KeyIdentifier* de esta extensión el Hash SHA-1 (160 bits) calculado sobre la Clave Pública contenida en el Certificado. Es decir el Hash SHA-1 sobre la clave pública contenida en el campo *subjectPublicKeyInfo* del Certificado

Certificate Policies

Descripción: Define el OID con que se registra la política de certificación a la que se ajusta la emisión de certificados de una AC. El OID y el documento digital que contiene la política DEBEN ser declarados ante el órgano de control y la extensión *"CertificatePolicies"* DEBE declarar la URI donde el documento estará disponible.

La extensión *"CertificatePolicies"* DEBE incluir toda la información sobre la política necesaria para la validación del certificado. Si la información sobre la política se incluye en la extensión *"QCStatements"* entonces esta información DEBE definirse en las políticas indicadas. Esta extensión DEBE estar presente en todos los certificados.

Contenido Certificados AC-URME: OID susceptible de ser registrado ante la ONTI para identificar la política de certificación. En este caso y por tratarse de un prototipo con fines experimentales, se respetará el formato de construcción del OID, aunque no se concrete la registración.

Subject Alternative Name

Descripción: permite asociar identidades adicionales al titular de un certificado. Las opciones definidas incluyen una dirección del correo electrónico, un nombre DNS, una dirección IP, y un identificador uniforme de recurso (URI).

Contenido Certificados AC-URME: Se completará con datos alternativos cuando sea necesario en el contexto de una aplicación particular.

Extended Key Usage

Descripción: indica uno o más propósitos para los que la clave pública del certificado puede ser utilizada, además o en lugar de los propósitos básicos

indicados en la extensión *"KeyUsage"*. Esta extensión DEBE ser utilizada al menos en los siguientes casos:

Certificados para firma de respuestas OCSP DEBEN incluir el valor "id-kpOCSPSigning" (1.3.6.1.5.5.7.3.9)

Certificados para servicios de certificación digital de fecha y hora DEBEN incluir el valor "id-kp-timeStamping" (1.3.6.1.5.5.7.3.8)

Contenido Certificados AC-URME: El prototipo deberá contemplar las siguientes alternativas para las *Extended Key Usage* cuando se considere necesario:

- Autenticación del servidor (1.3.6.1.5.5.7.3.1)
- Autenticación del cliente (1.3.6.1.5.5.7.3.2)
- Correo seguro (1.3.6.1.5.5.7.3.4)
- Seguridad IP del sistema final (1.3.6.1.5.5.7.3.5)
- Seguridad IP del usuario de seguridad (1.3.6.1.5.5.7.3.7)

CRLDistributionPoint

Descripción: Indica cómo se obtiene la información de CRL. Se debe considerar una CRL estándar, que contiene todos los Certificados revocados que no han expirado. Esta extensión DEBE estar presente en TODOS los certificados emitidos. Esta extensión NO DEBE ser crítica.

Contenido Certificados AC-URME: Se incorporará una entrada en la extensión por cada punto de distribución donde los usuarios puedan verificar el estado de Certificados revocados contra una CRL. Sobre esta extensión volveremos en detalle al momento de documentar el diseño de la CRL.

EXTENSIONES CRÍTICAS

Dado que los certificados serán utilizados primariamente con propósitos de validación de firma digital, de acuerdo a lo establecido por la RFC 3280, serán marcadas como críticas las siguientes extensiones:

BasicConstraint

Descripción: Permite identificar si el certificado es de una Autoridad Certificante, en cuyo caso el atributo booleano ***ca*** de esta extensión debe ser *TRUE*. En el caso de que el titular del certificado sea una entidad final en la jerarquía, el atributo ***ca*** debe figurar en *FALSE*. Esta extensión también incluye el atributo ***PathLenConstraint***, al que se presta atención cuando estamos frente a un Certificado de Autoridad Certificante. Este atributo se usa para establecer la longitud máxima de la ruta de certificación que la CA permite. Es decir, indica el número de Certificados (o de saltos intermedios – los extremos no se cuentan) que como máximo se pueden seguir en una ruta de certificación hasta llegar a una entidad final. La ausencia de este campo en cualquier certificado en la cadena, indica que la ruta puede tener cualquier longitud. Un valor de 0 indica que la CA especificada en el campo *subject* puede expedir únicamente certificados para entidades destino y no puede expedir certificados para otras CA.

Importante: Si el atributo ***ca*** esta en *FALSE* entonces el atributo ***keyCertSign*** de la extensión crítica ***key usage*** debe estar también en *FALSE*, indicando así que una entidad final no tiene posibilidad de firmar certificados. De igual forma si el atributo ***ca*** esta en *TRUE* entonces el atributo ***keyCertSign*** de la extensión ***key usage*** debe estar en *TRUE*

Contenido Certificados AC-URME: Para los certificados de entidad final, sean estos personas físicas, jurídicas o equipos se incluirá la extensión, aunque según la RFC 3280 no es obligatorio. En este caso, será ***ca=FALSE*** y no se incluirá el campo ***PathLenConstraint.*** Para el certificado

rootCA se incluirá la extensión marcada como crítica y será ***ca=TRUE***, ***PathLenConstraint=0.*** Esto crea un modelo directo, limitado; pero más controlado que entendemos funcionaría adecuadamente en una primera instancia de la AC-URME. Un valor diferente de cero permite la construcción de modelos jerárquicos más escalables, en donde las CA sucesivas pueden extender la confianza mediante la certificación a otras CA. Sin embargo, el impacto de decisiones futuras por terceros se vuelve mucho menos claro en este esquema y entendemos que en una primera experiencia de constitución de la AC-URME, es conveniente restringirla a un modelo directo.

Key Usage

Descripción: Define el propósito (por ejemplo: cifrado, firma, firma de CRL, firma de Certificados) para el cual se puede usar la clave pública contenida en el certificado. Según la RFC 3280 esta extensión debe incluirse en todos los certificados que contengan claves públicas con fines de verificación de firma, de verificación de otros certificados o de CRLs; y puede marcarse como crítica o no crítica. La extensión está compuesta de 9 campos de bit que según como estén asignados con valor 0 (no activo) o 1 (activo) definen las configuraciones posibles de uso de la clave. Estos son:

digitalSignature (0)
nonRepudiation (1)
keyEncipherment (2)
dataEncipherment (3)
keyAgreement (4)
keyCertSign (5)
cRLSign (6)
encipherOnly (7)
decipherOnly (8)

- Cuando el bit *digitalSignature* (firma digital) se activa identifica que la clave se usa con fines de firma digital, diferentes de la firma de Certificados y CRL.

- Cuando el bit *nonRepudiation* (aceptación – no repudio) se activa, la clave se usa para ofrecer un servicio de aceptación o no repudio. Un tercero puede utilizar esta clave brindando una forma de servicio notarial, en la cual se verifica la firma de una entidad destino, para prevenir una posterior negación de que la firma se usó.

- Cuando el bit *keyEncipherment* (clave de cifrado) se activa, la clave se usa para cifrar otras claves o información de seguridad. Cuando se especifica, se puede restringir para indicar que la clave de cifrado sólo se puede usar *encipherOnly* (sólo cifrar) o *decipherOnly* (solo descifrar). Estas restricciones también se aplican al acuerdo de claves *keyAgreement*.

- Cuando el bit *dataEncipherment* (cifrado de datos) se activa, la clave se usa para cifrado de datos. Las claves no están cubiertas por este tipo de clave.

- Cuando el bit *keyAgreement* (acuerdo de clave) se activa, la clave se usa en el proceso de establecer o llegar a un acuerdo sobre cuál es la clave que se debe usar para operaciones futuras. Esto se usa en general en el establecimiento de sesiones seguras en la red.

- Cuando el bit *keyCertSign* (clave para firma de certificado) se activa, la clave se usa para verificar firmas en certificados de clave pública. Esta configuración sólo es válida en certificados de CA, es decir aquellos que tienen el atributo *ca=TRUE* en la extensión *Basic Constraint*.

- Cuando el bit *cRLSign* (firma de CRL) se activa, la clave se usa para verificar la firma de la CA en una lista de revocación de certificados.

PKIX recomienda que esta extensión se marque como crítica. Esto implica que la clave se puede usar únicamente para los propósitos que se hayan designado; ya que al marcar la extensión como crítica, la CA esta indicando que la clave se está certificando sólo para esos propósitos. Esto es un aspecto importante si surgen temas de responsabilidad cuando una clave se usa para otros fines. Si la extensión se marca como no crítica, se ubica en el estado de un campo de advertencia. La clave se puede usar para otros propósitos a discreción del usuario del certificado.

Contenido Certificados AC-URME: En principio y salvo que un profile de certificado particular así lo requiera, esta extensión será marcada como crítica en los certificados emitidos por la AC-URME. Tendrá la siguiente configuración de carácter general de acuerdo a los distintos perfiles de Certificados.

Para Certificados de Certificadores:

0	*digitalSignature*	0
1	*nonRepudiation*	0
2	*keyEncipherment*	0
3	*dataEncipherment*	0
4	*keyAgreement*	0
5	*keyCertSign*	1
6	*cRLSign*	1
7	*encipherOnly*	0
8	*decipherOnly*	0

Para Certificados de proveedores de servicios de firma digital que emiten información de estado de certificados (por ej.: CRLs, OCSP)

0	*digitalSignature*	0
1	*nonRepudiation*	1*
2	*keyEncipherment*	0
3	*dataEncipherment*	0
4	*keyAgreement*	0
5	*keyCertSign*	0
6	*cRLSign*	1*
7	*encipherOnly*	0
8	*decipherOnly*	0

* Se debe activar en caso de que emitan CRLs u OCSP respectivamente

Nota: No se prevé que el prototipo AC-URME emita en principio certificados a proveedores de este tipo de servicios.

Para Certificados de otros proveedores de servicios de firma digital

0	*digitalSignature*	0
1	*nonRepudiation*	1
2	*keyEncipherment*	0
3	*dataEncipherment*	0
4	*keyAgreement*	0
5	*keyCertSign*	0
6	*cRLSign*	0
7	*encipherOnly*	0
8	*decipherOnly*	0

Nota: No se prevé que el prototipo AC-URME emita en principio certificados a proveedores de este tipo de servicios.

Para Certificados de personas físicas y jurídicas:

0	*digitalSignature*	1
1	*nonRepudiation*	1
2	*keyEncipherment*	0
3	*dataEncipherment*	0
4	*keyAgreement*	0
5	*keyCertSign*	0
6	*cRLSign*	0
7	*encipherOnly*	0
8	*decipherOnly*	0

Para Certificados de Servidor

0	*digitalSignature*	1
1	*nonRepudiation*	1
2	*keyEncipherment*	1
3	*dataEncipherment*	1
4	*keyAgreement*	0
5	*keyCertSign*	0
6	*cRLSign*	0
7	*encipherOnly*	0
8	*decipherOnly*	0

Cabe aclarar que la configuración precedente se ajusta a los requerimientos de los documentos preliminares publicados por la ONTI.

Abordamos en esta etapa el diseño detallado de la Lista de Certificados Revocados que emitirá la AC-URME.El diseño propuesto adhiere al contenido de los siguientes documentos:

- RFC 3280 "Internet X.509 Public Key Infraestructura Certificate and Certificate Revocation List (CRL) Profile"
- RFC 3279 "Algorithms and Identifiers for the Certificate and Certificate Revocation List (CRL) Profile"
- Textos preliminares de los documentos referidos al proceso de licenciamiento de certificadores publicados por la ONTI – Oficina Nacional de Tecnologías de la Información dependiente de la Subsecretaría de la Gestión Pública de la Jefatura de Gabinete de Ministros.

E. Diseño de interface web para el prototipo AC-URME

En el informe anterior, documentamos el diseño global propuesto para la interfase web del prototipo AC-URME. En este contexto, describimos el conjunto de ***contenidos*** y ***aplicaciones*** que deben desarrollarse para lograr en la práctica el ***diseño conceptual*** propuesto y presentamos el ***diseño de imagen*** para el sitio *www.acurme.mendoza.gov.ar*, en el cual se esquematiza la forma de navegabilidad y la distribución de acceso a los contenidos y servicios.

Abordamos en esta etapa el diseño detallado de la dimensión de ***Servicios*** que la interfase web debe proveer a los suscriptores para una ágil gestión del CVS de sus Certificados. Es decir, proveemos las especificaciones de los módulos:

- Solicitar Certificado
- Instalar Certificado Raíz
- Buscar Certificado
- Renovar Certificado
- Revocar Certificado
- Descargar CRL

Presentamos a continuación las especificaciones propuestas para cada uno de estos espacios web con lo que se completa la etapa de diseño de la interfase web para el prototipo AC-URME.

Solicitar Certificado

El módulo de solicitud de certificados debe implementar, en aquellos aspectos que puedan resolverse de manera remota, el procedimiento de solicitud de certificados descrito en el *Manual de Procedimientos,* incluyendo generación del par de claves y descarga e instalación en el cliente del certificado de la ACURME. Así mismo, debe mantener absoluta concordancia con lo dispuesto en la *Política de* Certificación. En particular se debe incluir en este espacio web:

1. Descripción de los usos de los certificados de acuerdo a la Política de Certificación.
2. Acceso visible al documento de la Política de Certificación y Manual de Procedimientos.
3. Identificación de quiénes pueden solicitar certificados de usuario final, de persona jurídica o de servidor.
4. Acuerdo del suscriptor, anexo a su solicitud.
5. Formularios web de solicitud de acuerdo al tipo de certificado.
6. Instructivos y ayuda para completar los formularios de solicitud.
7. Descripción de la información complementaria a presentar por el suscriptor en forma personal, adjunta a su solicitud, si corresponde.

Los contenidos y desarrollos del módulo deben estar estructurados de forma de guiar al suscriptor para que cumplimente los siguientes pasos:

- Instalación del Certificado raíz de la jerarquía, certificado de la AC-URME.
- Aceptación del acuerdo del suscriptor.

- Llenado y envío del formulario de Solicitud de Certificado.
- Recepción de la confirmación de "Recepción de Solicitud"
- Recepción del "Mail de Verificación" de solicitud.
- Confirmación por respuesta del "Mail de verificación".
- Acreditación de identidad
- Recepción del Mail de Notificación de emisión de certificado
- Verificación y descarga del certificado

Instalar Certificado Raíz

Este módulo debe proveer la descarga e instalación automática en el navegador del cliente, del certificado raíz de la jerarquía – Certificado de la AC-URME. Esta operación resulta indispensable para que el navegador u otras aplicaciones clientes reconozcan los certificados emitidos por la AC-URME como certificados válidos.

Se debe proveer alternativamente en este módulo de documentación de ayuda al suscriptor, para la instalación del certificado raíz en aplicaciones clientes típicas como navegadores de Internet y gestores de correo electrónico. Así mismo se deberá proveer la Huella Digital (fingerprint) del Certificado de Root CA de la AC-URME con el fin de que los suscriptores puedan verificar su autenticidad.

Buscar Certificado

Como se especificó en el diseño del prototipo, se debe proveer un repositorio público de certificados emitidos por la AC-URME, de manera que los certificados *de clave pública* estén disponibles para ser descargados por usuarios en general en el momento que lo necesiten.

El módulo debe proveer como mínimo búsqueda por:

- ***DN: Distinguished Name*** con que fue emitido el certificado

- ***Email:*** Email que se registró en la solicitud del certificado para el caso de certificados emitidos a personas físicas y/o jurídicas.

Renovar Certificado

Este módulo debe instrumentar el procedimiento de renovación de certificados descrito en el *Manual de Procedimientos,* para aquellos suscriptores que posean un certificado vigente emitido por la AC-URME. Así mismo, debe mantener absoluta concordancia con lo dispuesto en la *Política de* Certificación en cuanto a plazos y condiciones de renovación.

El módulo debe implementar un método de *renovación automática,* ejecutado desde un browser cliente que tenga instalado el Certificado vigente del suscriptor.

En particular se debe incluir en este espacio web:

1. Acceso visible al documento de la Política de Certificación y Manual de Procedimientos.
2. Identificación de quiénes pueden solicitar la renovación de sus certificados.
3. Formularios web de solicitud de renovación de acuerdo al tipo de certificado.
4. Instructivos y ayuda para completar los formularios de solicitud de renovación.
5. Descripción de la información complementaria a presentar por el suscriptor en forma personal, adjunta a su solicitud, si corresponde.

Los contenidos y desarrollos del módulo deben estar estructurados de forma de guiar al suscriptor para que cumplimente los siguientes pasos:

1. Llenado y envío del formulario de Solicitud de Renovación.
2. Recepción de la confirmación de "Recepción de Solicitud"
3. Recepción del "Mail de Verificación" de solicitud.
4. Confirmación por respuesta del "Mail de verificación".
5. Recepción del Mail de Notificación de emisión de certificado
6. Verificación y descarga del certificado

Revocar Certificado

Este módulo debe instrumentar el procedimiento de revocación remota de certificados descrito en el *Manual de Procedimientos,* para aquellos suscriptores que posean un certificado válido emitido por la AC-URME. Así mismo, debe mantener absoluta concordancia con lo dispuesto en la *Política de* Certificación.

En particular, solo podrá revocar remotamente un certificado el titular del certificado a revocar a través de un método de *revocación automática*, ejecutado desde un browser cliente que tenga instalado el Certificado vigente del suscriptor.

En particular se debe incluir en este espacio web:

6. Acceso visible al documento de la Política de Certificación y Manual de Procedimientos.
7. Identificación de las condiciones bajo las cuáles se puede solicitar la revocación remota de certificados.
8. Formularios web de solicitud de revocación de acuerdo al tipo de certificado.
9. Ayuda para completar los formularios de solicitud.

Los contenidos y desarrollos del módulo deben estar estructurados de forma de guiar al suscriptor para que cumplimente los siguientes pasos:

1. Elegir el tipo de certificado a revocar: persona física o jurídica, certificado SSL.
2. Completar la solicitud de revocación consignado el motivo por el cuál se revoca el certificado:
   a. Pérdida del soporte del certificado y claves
   b. Posible compromiso de la clave
   c. Abandono del puesto de trabajo
   d. Errores graves en información del certificado
   e. Cambio de datos fundamentales
   f. Otros.

Descargar CRL

Este módulo debe proveer acceso directo a la descarga de la Lista de Certificados Revocados (CRL) emitida diariamente por la AC-URME. El archivo con la CRL descargado debe proveerse en formato de extensiones Crypto Shell para que pueda ser fácilmente instalado en los clientes de correo, browsers u otras aplicaciones específicas.

F. Diseño y ejecución de un Plan de Pruebas

Documentamos a continuación el ***Conjunto de Pruebas*** al que fue sometido el prototipo AC-URME.

Descripción de la Prueba	Objetivo de la Prueba	Ejecución de la Prueba	Resultados/Conclusiones
Testear adaptabilidad del software PKI al estándar X509 v3 y PKIX (RFC3280)	Evaluar características básicas de EJBCA de acuerdo al diseño prescripto para el prototipo	▪ Se configuraron distintos perfiles de Certficados y se emitieron certificados bajo estos perfiles y en distintos formatos. ▪ Se importaron los certificados emitidos en aplicaciones como Outlook Express, Outlook, IE y Netscape. ▪ Se emitieron distintas versiones de CRL ▪ Se importaron las CRL emitidas en Outlook. ▪ Se accedió a través de funciones criptográficas a la información de los campos de los certificados emitidos, de acuerdo a la estructura propuesta por el estándar X509 v3.	El prototipo respeta el estándar X509 y las recomendaciones de la RFC3280.
Testear que bases de datos soporta el software PKI, para almacenar Certificados emitidios y CRLs.	Evaluar flexibilidad del software PKI para trabajar con distintos repositorios de Certificados	▪ Se configuró el software PKI para operar con MySQL, Hypersonic y PostgreSQL. ▪ Bajo cada una de estas configuraciones se corrió un	El software operó correctamente con los tres motores de base de datos. Se decidió la implementación final sobre PostreSQL por sus características de seguridad y administración de grandes volúmenes de datos.

Descripción de la Prueba	Objetivo de la Prueba	Ejecución de la Prueba	Resultados/Conclusiones
		script de prueba que creaba e inicializaba una Root-CA, creaba usuarios, emitía certificados y CRLs. • Se evalúo la correcta operación de la base de datos ante estas transacciones.	
Testear creación de una root CA con múltiples niveles de CAs.	Dimensionar posibilidades de escalabilidad futura	Se creó una Root-CA con dos CAs dependientes y una RA por cada CA creada. Se corrió el Script de creación de usuarios, certificados y CRLs para cada una de estas entidades y se comprobó su funcionamiento con distintos administradores y características.	No se encontraron problemas de ejecución ni en la creación de las Autoridades Certificantes, ni en los procesos de certificación testeados.
Testear emisión de Certificados por enrrolamiento individual.	Evaluar interfase web de enrolamiento	Se emitieron 5 certificados de prueba haciendo uso de la interfase web de enrolamiento.	Debieron modificarse algunos aspectos vinculados al momento de generación del par de claves y generación de la CSR en formato PKCS#10
Testear diferentes configuraciones de profile de Certificado, para distintos tipos de usuarios y aplicaciones.	Medir ajuste del prototipo a las especificaciones de diseño planteadas para el perfil de Certificados	Se configuraron 5 alternativas diferentes de profile de Certificados, variando en cada caso: • la configuración de campos del DN (Distinguished Name) • las extensiones incluidas • extensiones críticas y no críticas • la longitud y algoritmos de	Pudieron emitirse satisfactoriamente distintos certificados de acuerdo a los profiles configurados. Los datos incluidos en el DN (Distinguished Name) y otros campos, tanto como las extensiones y su nivel de procesamiento se ajustaron exactamente a la definición de cada profile asociado. Las pruebas de generación de claves fueron igualmente satisfactorias.

Descripción de la Prueba	Objetivo de la Prueba	Ejecución de la Prueba	Resultados/Conclusiones
		generación de claves Se emitieron dos certificados de prueba en formato PKCS#12, por cada uno de estos profiles. Se comprobó el contenido de los certificados emitidos de acuerdo a la configuración de perfil.	
Testear formatos de exportación de certificados soportados (PKCS12 , PEM, JKS)	Evaluar caracterIsticas de interoperabilidad del prototipo	Se emitieron 6 certificados de prueba, con datos ficticios: • 3 Certificados SSL, en formatos PKCS12, PEM y JKS • 3 Certificados de Entidad Final, en formatos PKCS12, PEM y JKS Para los Certificados SSL: • Se comprobó el correcto funcionamiento del certificado emitido en formato PEM-Encoded con la configuración SSL de un web-server Apache. • Se comprobó el correcto funcionamiento del certificado emitido en formato JKS con la configuración SSL del web-server Jakarta-Tomcat. • Se comprobó la conversión	Todas las pruebas de uso y conversión entre formatos de representación de Certificados tuvieron resultados satisfactorios. No obstante se recomienda siempre que sea posible, que el Certificado se emita en el formato de representación en el que se va a utilizar de acuerdo a la aplicación particular, debido a la complejidad asociada a lograr conversiones correctas entre formatos.

Descripción de la Prueba	Objetivo de la Prueba	Ejecución de la Prueba	Resultados/Conclusiones
		entre formatos de certificados con funciones de php-openssl y con librerías java. Para los certificados de entidad final: • Se importaron los certificados emitidos en formato PKCS#12 en los repositorios de certificados de Outlook Express, Outlook, IE 5.0, IE 6.0 y Netscape Comunicator 4.1 • Se firmaron formularios web, con la ayuda de la API Microsoft CAPICOM, con los certificados emitidos en formato PEM-Encoded. • Se comprobó la validación de cliente en un esquema de sitio seguro implementado en el web-server Jakarta-Tomcat con el certificado emitido en formato JKS. Se comprobó la conversión entre formatos de certificados con funciones de Openssl y APIs java.	
Testear proceso batch para emisión de certificados.	Evaluar mecanismos de emisión masiva	Se realizó la emisión de un lote de 40 certificados de usuario final en formato P12, por proceso batch, haciendo uso del	Los certificados fueron en su totalidad, correctamente emitidos. Las transacciones asociadas fueron debidamente registradas en la base de datos y en los logs

CONSEJO FEDERAL DE INVERSIONES

Descripción de la Prueba	Objetivo de la Prueba	Ejecución de la Prueba	Resultados/Conclusiones
		script provisto a tal efecto.	de transacciones.
Probar la creación de CRLs usando agendas de procesos.	Medir ajuste del prototipo a las especificaciones de diseño planteadas para la Política de Certificación	Se configuró el prototipo para que emitiera la CRL automáticamente cada 24 hs. Se generaron y revocaron certificados de prueba durante 10 días para evaluar el comportamiento de la emisión de CRLs.	A través del seguimiento de las CRLs emitidas y logs de transacciones del prototipo, se comprobó el correcto funcionamiento de los scripts de emisión y descarga de CRL. Así mismo las CRLs emitidas y los certificados revocados, fueron sistemáticamente importados dentro del manejador de certificados del browser IE 6.0, a partir de lo cual se evaluó su correcto funcionamiento.
Testear tipos y longitudes de claves que soporta el software PKI, tanto para la clave privada de la CA como para los certificados. (RSA 1024, 2048 bits, DSA y Diffie-Helman).	Medir ajuste a la Política de Certificación Evaluar características de interoperabilidad del prototipo	Se generaron tres Se generaron 3 Certificados en tres pruebas de creación de autoridad certificante.	El prototipo soporta claves RSA 1024 y 2048. La generación de claves DSA requiere de la construcción de scripts especiales.
Probar la emisión de Certificados con distintos algoritmos de firma md5withRSAEncryption, Sha1RSA y otros contemplados en la RFC3279.	Medir ajuste del prototipo a las especificaciones de diseño planteadas para el perfil de Certificados y la Política de Certificación. Evaluar características de interoperabilidad del prototipo.	Se intentó la configuración de profiles para la emisión de certificados con distintos algoritmos de firma: • Sha1 with RSA Encryption • Md5withRSAEncrytpion	El prototipo soporta la emisión directa de certificados firmados con el algoritmo SHA1 with RSA Encryption. Si bien la documentación del software PKI de base y las API javas asociadas mencionan la posibilidad de firmar certificados con Md5WithRSAEncryption, se debe desarrollar un módulo alternativo para incorporar esto en la definición de profiles de Certificados.
Testear funcionamiento de la extensión *KeyUsage* en	Evaluar seguridad en el comportamiento de los	Se realizaron pruebas de:	Ambos intentos emitieron el mensaje de advertencia y error esperado.

Descripción de la Prueba	Objetivo de la Prueba	Ejecución de la Prueba	Resultados/Conclusiones
Certificados emitidos.	Certificados emitidos de acuerdo a la Política de Certificación.	Intento de firma de email con un certificado que no incluía en su extensión *KeyUsage* la entrada de firma de email. Intento de cifrado de email con un certificado que no incluía en su extensión *KeyUsage* el envío de correo seguro.	

G. Evaluación de Resultados

Sistema de medición

Es importante señalar que una PKI es una infraestructura de seguridad electrónica, y una infraestructura ante la ausencia de procesos de aplicación específicos no produce ningún resultado. Por consiguiente, nuestro enfoque primario se centra en los procesos específicos de aplicaciones particulares, en función de los innumerables procesos que potencialmente una PKI puede apalancar.

Nos basaremos en medidas generales y medidas particulares con las que, razonablemente, podamos cuantificar las dimensiones que son de nuestro interés, a saber:

Medidas Generales y particulares

La siguiente tabla define los indicadores generales utilizados para medir el rendimiento de la PKI con enfoque en los procesos de las aplicaciones específicas. Cabe señalar que la tabla debe adaptarse a las medidas particulares que determinen las circunstancias diferenciales de cada aplicación.

Experiencia piloto .....
(Mediciones realizadas al .....)

Indicadores Cualitativos	**Métricas y Resultados**
Satisfacción de los usuarios:	
# Quejas y Reclamos	
Temática de reclamos	.....
Beneficios diferenciales	.....
Marco legal:	
Documentación de la experiencia	.....
Alcance:	
Participación de los sectores relacionados	.....
Indicadores Cuantitativos	**Métricas y Resultados**
Eficiencia:	
% de certificados emitidos correctamente	
# de fallas del sistema	
# de interrupciones del servicio	
Tiempos comparados	
Ahorros generados	.....
Asistencia:	
# de actores capacitados	
# de asistencias otorgadas	
% de asistencias exitosas	.....

Uso del Sistema:
% de utilización de servicios
(sobre el total de suscriptores) .....

Acciones correctivas detectadas	Acciones correctivas implementadas
.....	.....

Calificación ponderada final

.....

H. Desarrollo de Políticas de Certificación

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

Ac-Urme

1 INTRODUCCIÓN

1.1 Resumen

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 y sus funcionarios y agentes que soliciten la emisión de certificados de clave pública de acuerdo con las políticas particulares de emisión. 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.

1.2 Participantes y aplicabilidad

Esta política es aplicable por:

La Autoridad Certificante de la Unidad de Reforma del Estado (en adelante AC-URME) que otorga certificados a favor de los funcionarios y agentes pertenecientes a los organismos o dependencias del Poder Ejecutivo de la Administración Pública Provincial.

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

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.

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.

Certificador

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: firmadigital@mendoza.gov.ar

Personalmente o por correo:

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

Autoridad de Registro

Se utilizará una Autoridad de Registro local (Residente en el mismo lugar físico de la Ac-Urme) utilizadas por el Certificador en el proceso de recepción de solicitudes de emisión de certificados, identificación y autenticación de los solicitantes de certificados y recepción y validación de solicitudes de revocación.

Titulares de certificados

Podrán recibir certificados emitidos por el Certificador:

- Personas Físicas: funcionarios y agentes del Poder Ejecutivo Provincial

- Personas Jurídicas: organismos o dependencias del Poder Ejecutivo Provincial entes autárquicos, organismos provinciales y municipales
- Equipamientos: servidores pertenecientes al equipamiento afectado al Poder Ejecutivo Provincial
- Aplicaciones: aplicaciones utilizadas en circuitos administrativos del PE Provincial

Aplicabilidad

Los certificados que emita el Certificador estarán disponibles para los siguientes usos o aplicaciones en general y de de acuerdo con las circunstancias particulares de la aplicación a la que se circunscriban

- 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

1.3 Contactos

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:

firmadigital@mendoza.gov.ar

Personalmente o por correo:

Provincia de Mendoza

Casa de Gobierno

Peltier 351 4° Piso Cuerpo Central

CP 5500

2 RESPONSABILIDADES DE PUBLICACION Y REPOSITORIO

2.1 Obligaciones

Obligaciones del Certificador

- Recibir una solicitud de emisión de certificado digital, firmada digitalmente con los correspondientes datos de verificación de firma digital del solicitante.
- Emitir certificados digitales de acuerdo a lo establecido en sus políticas de certificación, y de acuerdo con:
- Lo previsto en la normativa provincial propuesta
- Los estándares tecnológicos adoptados por la Provincia.
- Identificar inequívocamente los certificados digitales emitidos.
- 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.
- Revocar los certificados digitales por él emitidos en los siguientes casos:
- A solicitud del titular del certificado digital.
- 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.

- 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.
- Por condiciones especiales definidas en su política de certificación.
- 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.
- 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.
- Cumplir cabalmente con las políticas de certificación acordadas con el titular y con su Manual de Procedimientos.
- 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.
- 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.

- Disponer de un servicio de atención a titulares y terceros, que permita evacuar las consultas y la pronta solicitud de revocación de certificados.
- Garantizar el acceso permanente, eficiente y gratuito de los titulares y terceros al repositorio de certificados revocados.
- 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.
- Mantener a disposición permanente del público las Políticas de Certificación y el Manual de Procedimientos correspondiente.
- Mantener actualizados los repositorios de certificados revocados por el período establecido en sus políticas de certificación.
- 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.
- 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.
- Poner a disposición del solicitante de un certificado digital toda la información relativa a su tramitación.
- 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.

- 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 auditoria de que hubiera sido objeto, su manual de procedimientos y toda información que determine la autoridad de aplicación nacional.
- Informar en las políticas de certificación si los certificados digitales por él emitidos requieren la verificación de la identidad del titular.
- 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.
- Abstenerse de generar, exigir, tomar conocimiento o acceder bajo ninguna circunstancia a la clave privada del suscriptor.
- Mantener el control exclusivo de sus propios datos de creación de firma digital e impedir su divulgación.
- 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.
- Proteger el acceso y el uso de la clave privada mediante procedimientos que exijan la participación de más de una persona.
- Operar utilizando un sistema técnicamente confiable de acuerdo con lo que determine la autoridad de aplicación nacional.
- Garantizar la confiabilidad de los sistemas de acuerdo con los estándares tecnológicos adoptados por la Provincia.
- Garantizar la existencia de sistemas de seguridad física y lógica que cumplimenten las normativas vigentes.
- Utilizar con exclusividad los sistemas que cumplan las funciones de certificación con ese propósito, sin que se les asigne ninguna otra función.
- 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.

- 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.
- Mantener la confidencialidad de toda información que no figure en el certificado digital.
- Mantener la documentación respaldatoria de los certificados digitales emitidos, por diez (10) años a partir de su fecha de vencimiento o revocación.
- Publicar en el Boletín Oficial aquellos datos que la autoridad de aplicación nacional determine.
- 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.
- Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas.
- Registrar las transacciones realizadas, a fin de identificar el autor y el momento de cada una de las operaciones.
- 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.
- 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.
- Informar inmediatamente al ente licenciante sobre cualquier cambio en los datos relativos a su licencia.
- Informar a la autoridad nacional de aplicación de modo inmediato la ocurrencia de cualquier evento que comprometa la correcta prestación del servicio.

- 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
- Emplear personal idóneo que tenga los conocimientos específicos, la experiencia necesaria para proveer los servicios ofrecidos y en particular, competencia en materia de gestión, conocimientos técnicos en el ámbito de la firma digital y experiencia adecuada en los procedimientos de seguridad pertinentes.
- Disponer de recursos humanos y tecnológicos suficientes para operar de acuerdo a las exigencias establecidas en la normativa provincial propuesta.
- Disponer de los recursos financieros adecuados al tipo de actividad de certificación que desarrolla, acorde con los niveles de responsabilidad derivados de la misma.
- 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.
- Constituir domicilio legal en la Provincia de Mendoza.
- Cumplir con toda otra obligación emergente de su calidad de titular de la licencia adjudicada por el ente licenciante.
- Generar en un ambiente seguro las firmas digitales propias y todos los servicios para los cuales solicite licencia.
- Cumplir con lo previsto en sus políticas y procedimientos de certificación.
- Garantizar la continuidad de las operaciones mediante un Plan de Contingencia actualizado y aprobado.
- Respetar el derecho del titular del certificado digital a no recibir publicidad de ningún tipo por su intermedio, salvo consentimiento expreso de éste.
- Cumplir las normas y recaudos establecidos para la protección de datos personales.

Obligaciones de la Autoridad de Registro

- La recepción de las solicitudes de emisión de certificados.

- La validación de la identidad y autenticación de los datos de los titulares de certificados.
- La validación de otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue la Autoridad Certificante Licenciada.
- La remisión de las solicitudes aprobadas a la Autoridad Certificante Licenciada con la que se encuentre operativamente vinculada.
- La recepción y validación de las solicitudes de revocación de certificados; y su direccionamiento a la Autoridad Certificante Licenciada con el que se vinculen.
- La identificación y autenticación de los solicitantes de revocación de certificados.
- 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.
- El cumplimiento de las normas y recaudos establecidos para la protección de datos personales.
- 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.

Obligaciones del titular del certificado

- Mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, e impedir su divulgación.
- Utilizar un dispositivo de creación de firma digital técnicamente confiable.
- 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.
- 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.

Obligaciones de terceros usuarios

- La obligatoriedad de aceptar los términos de la Política de Certificación o del documento "Acuerdo con terceros usuarios".
- La obligatoriedad de rechazar la utilización del certificado para fines distintos a los previstos en la Política de Certificación que lo respalda o en el documento de "Acuerdo con terceros usuarios".
- La obligatoriedad de verificar la validez, revocación o suspensión del certificado utilizando la información de estado de revocación adecuada.
- La falta de cumplimiento de estas obligaciones por parte del tercero parte no exime las responsabilidades del Certificador y del titular del certificado que pudieran resultar.

Obligaciones del servicio de repositorio

- 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 auditoria de que hubiera sido objeto, su manual de procedimientos y toda información que determine la autoridad de aplicación;
- Garantizar el acceso permanente, eficiente y gratuito de los titulares y terceros al repositorio de certificados revocados.
- Mantener actualizados los repositorios de certificados revocados por el período establecido por el Ente Administrador.
- Cumplir las normas y recaudos establecidos para la protección de datos personales.
- La obligatoriedad de implementar los recursos necesarios para garantizar la seguridad de los datos almacenados, desde el punto de vista técnico y legal.

2.2 Responsabilidades

Ley 25.506

ARTICULO 38. - El certificador que emita un certificado digital o lo reconozca en los términos del artículo 16 de la presente ley, es responsable por los daños y perjuicios que provoque, por los incumplimientos a las previsiones de ésta, 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.

Artículo 39: Limitaciones de responsabilidad.

ARTICULO 39. - Los certificadores licenciados no son responsables 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 ley; 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.

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.

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.

Limitaciones de responsabilidad: el certificador licenciado no es responsable en los siguientes casos:

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.

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.

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.

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.

Contar con personal idóneo y confiable, con antecedentes profesionales acordes a la función desempeñada.

Responder a los pedidos de informes por parte de un tercero respecto de la validez y alcance de un certificado digital emitido por él.

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.

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.

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.

2.3 Interpretación y Legalidad-Legislación aplicable

Ley Nacional de Firma Digital N° 25.506

Decreto Reglamentario Nacional 2628/02

Proyecto Provincial de adhesión a la Ley Nacional Ref.:Expte. 4163- U-03-00020

2.4 Publicación y Repositorios

Publicación de información del Certificador

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.

Frecuencia de publicación

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.

Controles de acceso a la información

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.

2.5 Auditorías

Se aplica artículo 21 inc. k) de la Ley 25.506:

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.

Se aplica el artículo 20 del Decreto 2628/02

Conflicto de intereses. Para garantizar la objetividad e imparcialidad de la actividad de auditoría no podrán desempeñarse en la prestación de servicios de auditoría aquellas entidades o personas vinculadas con prestadores de servicios de certificación, lo que será establecido en el Pliego Estándar de Precalificación de Entidades de Auditoría previsto en el artículo 18 del presente decreto.

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.

2.6 Confidencialidad

Información confidencial

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.

Información no confidencial

- Contenido de los certificados y de las listas de certificados revocadas
- Información sobre personas físicas o jurídicas que se encuentre disponible en certificados o en directorios de acceso público
- Políticas de Certificación y Manual de Procedimientos del Certificador
- Versiones públicas de la Política de Seguridad del Certificador

Publicación de información sobre la revocación o suspensión de un certificado

Se deberá considerar la información sobre la revocación o suspensión de un certificado como información no confidencial.

3 IDENTIFICACIÓN Y AUTENTICACIÓN

3.1 Registro inicial

Los procesos a seguir son los siguientes:

Registración Centralizada

Identificación de datos por la Autoridad de Registro local

Todo suscriptor de un certificado debe iniciar el trámite de solicitud ingresando al sitio web de la AC-URME www.firmadigital.com.ar. 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.

Datos identificatorios:

Datos Personales

Apellido y Nombre

Dirección de Correo Electrónico

Tipo y Número de Documento

Título

Localidad

Datos del ente al que pertenece

Cargo/Función

Oficina

Dependencia

Ministerio/Organismo

3.2 Categorías de Certificación por niveles de confianza:

la presente política admite la distinción de los procesos de validación de los datos identificatorios del suscriptor por categorías. Cada categoría representa un nivel de confianza en la verificación de los datos del suscriptor, a saber:

Categoría A

Se trata de la categoría con más bajo nivel de confianza en la cuál se realizan verificaciones de la cuenta de correo del suscriptor y de sus datos personales contra la Base de datos de Recursos Humanos. No requiere la presencia física del Suscriptor y no se le pide documentación adicional salvo que el oficial de registro así lo disponga

Categoría B

En esta categoría se realizan las mismas verificaciones de la Categoría A, además se le pide la siguiente documentación:

Solicitud de Certificado Impresa y Firmada conteniendo los siguientes datos personales:

Documento de identidad (original y fotocopia) y el Código de Identificación del requerimiento.

Y se realizan las siguientes verificaciones:

Que el documento corresponde a la persona presente.

Que dicha persona es aquella cuyos datos figuran en la Solicitud de Certificado presentada. A tal fin debe cotejar los datos del documento con los que figuran en la mencionada Solicitud.

Que la firma hológrafa de la Solicitud de Certificado corresponda con la del documento

Categoría C

Se realizan las mismas verificaciones que en la Categoría B pero además se pide y se verifica una 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 que se especifica:

Nombre y Apellido

Documento de Identidad (DNI u otro de validez nacional)

Jurisdicción/Organismo/Dependencia/Cargo

Categoría D

Constituye la categoría de máximo nivel de Confianza en la cuál se lleven a cabo las verificaciones de la Categoría C pero en presencia del Escribano de Gobierno que certifica y deja constancia de todo lo actuado en el proceso de validación

3.3 Normativa

El Certificador debe cumplir con lo establecido en:

El artículo 21 inc. a) de la Ley 25.506

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

y el artículo 34 inc. e) del Decreto 2628/02 relativos a la información a brindar a los solicitantes.

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 República Argentina y los medios a los que el suscriptor puede acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema o presentar sus reclamos.

3.4 Necesidad de Nombres Significativos

Las distintas denominaciones que se utilicen para cada tipo de certificado deben ser como mínimo:

Para personas físicas:

commonName: DEBE corresponder con el nombre que figura en el documento de identidad del titular (DNI, Pasaporte, ...)

organizationalUnitName y organizationName: PUEDEN ser utilizados para guardar la información relativa a la Organización a la cual el titular se encuentra asociado (deben respetar los criterios definidos para los atributos "organizationName" y "organizationalUnitName" de personas jurídicas u Organismos Públicos). El tipo de asociación entre el organismo y el titular debe ser evaluado a partir de la política de certificación

Para personas jurídicas:

commonName: en caso de existir DEBE corresponder a la unidad operativa suscriptora del certificado (ej. Gerencia de Compras)

organizationalUnitName: PUEDE contener a las unidades operativas relacionadas con el suscriptor

organizationName: DEBE coincidir con la inscripción en IGJ

Para Organismos Públicos:

commonName: en caso de existir DEBE corresponder a la unidad operativa suscriptora del certificado (ej Dpto. de Mesa de Entradas)

organizationalUnitName y organizationName: DEBEN corresponder con la denominación oficial del organismo

3.5 Unicidad de nombres

El nombre distintivo debe ser único a cada suscriptor (puede haber más de un certificado con igual nombre distintivo si corresponde al mismo suscriptor).

3.5.1 Reconocimiento, autenticación y rol de las marcas registradas

Se podrán registrar marcas como nombres distintivos siempre que se demostrare ser titular de registro de las mismas conforme lo determina la ley 22.362 y la normativa específica del Instituto Nacional de la Propiedad Industrial, para lo cual se

deberá exhibir el título de registro correspondiente o bien la licencia que autoriza al uso de dicha marca..

3.5.2 Autenticación de la identidad de personas físicas

Se describirán los procedimientos de autenticación de la identidad de los titulares de los certificados de personas físicas en el Manual de procedimientos correspondiente y complementario a la presente Política de Certificación.

Deben considerarse obligatoriamente las exigencias reglamentarias impuestas por:

El artículo 21 inc i) de la Ley 25.506

Mantener la documentación respaldatoria de los certificados digitales emitidos, por diez (10) años a partir de su fecha de vencimiento o revocación.

El artículo 21 inc f) de la Ley 25.506

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.

El artículo 34 inc. i) del Decreto 2628/02

Abstenerse de generar, exigir, tomar conocimiento o acceder bajo ninguna circunstancia a la clave privada del suscriptor.

El artículo 34 inc. m) del Decreto 2628/02 relativo a la protección de datos personales.

Cumplir las normas y recaudos establecidos para la protección de datos personales.

3.6 Requerimiento de revocación

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.

4 CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS

4.1 Requerimiento de certificado

Los requisitos y procedimientos operativos establecidos por el Certificador para recibir los requerimientos de certificados están disponibles en el Manual de Procedimientos complementario a esta Política de Certificación. Estos procedimientos deberán ser cumplidos por el Certificador o por la Autoridad de Registro operativamente vinculada y por los solicitantes de certificados.

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.

El proceso de solicitud puede ser iniciado solamente por el interesado, quien debe acreditar fehacientemente su identidad o por el representante autorizado de la persona jurídica solicitante

4.2 Emisión del certificado

Los requisitos y procedimientos establecidos por el Certificador para la emisión del certificado y para la notificación de dicha emisión al solicitante se encuentran disponibles en Manual de Procedimientos complementario a esta Política de Certificación

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.

4.3 Aceptación del certificado

Los requisitos y procedimientos referidos a la publicación del certificado y a la aceptación del mismo por su titular se detallan en el Manual de Procedimientos complementario a esta Política de Certificación

4.4 Suspensión y Revocación de Certificados

El Certificador debe asegurar que los certificados sean revocados de una manera oportuna basada en una solicitud de revocación de certificado autorizada y validada.

4.4.1 Causas de revocación

Las obligaciones establecidas en el artículo 19 inc. e) de la Ley 25.506

Revocar los certificados digitales por él emitidos en los siguientes casos, entre otros que serán determinados por la reglamentación: 1) A solicitud del titular del certificado digital. 2) Si determinara que un certificado digital fue emitido en base a una información falsa, que en el momento de la emisión hubiera sido objeto de verificación. 3) Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros. 4) Por condiciones especiales definidas en su política de certificación. 5) Por resolución judicial o de la autoridad de aplicación.

Las obligaciones establecidas en el artículo 23 del Decreto 2628/02

Revocación de certificados. Se deberán revocar los certificados digitales emitidos en los siguientes casos:

a) A solicitud del titular del certificado digital

b) Si se determina que un certificado digital fue emitido en base a una información falsa que en el momento de la emisión hubiera sido objeto de verificación.

c) Si se determina que los procedimientos de emisión y/o verificación han dejado de ser seguros.

d) Por condiciones especiales definidas en las Políticas de Certificación.

e) Por Resolución Judicial o de la Autoridad de Aplicación debidamente fundada.

f) Por fallecimiento del titular.

g) Por declaración judicial de ausencia con presunción de fallecimiento del titular.

h) Por declaración judicial de incapacidad del titular.

i) Si se determina que la información contenida en el certificado ha dejado de ser válida.

j) Por el cese de la relación de representación respecto de una persona.

4.4.2 Autorizados a solicitar la revocación

Las personas autorizadas para solicitar la revocación de un certificado son las siguientes:

- Titular del certificado
- Responsable autorizado que efectuara el requerimiento, en el caso de certificados de personas jurídicas
- Persona jurídica titular del certificado a través de un funcionario debidamente autorizado
- Personas habilitadas por el titular de certificado a tal fin.
- Certificador o la Autoridad de Registro operativamente vinculada.
- Autoridad de Aplicación de la Infraestructura de Firma Digital establecida por la Ley 25.506.
- Autoridad judicial competente

4.4.3 Procedimientos para la solicitud de revocación

Clases de revocación

- 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.

- Revocación obligatoria

Un suscriptor debe solicitar la inmediata revocación de su certificado:

Cuando se produzcan cambios en la información que el certificado contiene o ésta se desactualice.

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.

Cuando cese su vínculo laboral con el organismo, dependencia o institución.

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

A solicitud del suscriptor cuando se verifiquen los procedimientos de recepción y validación establecidos en el Manual de Procedimientos.

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.

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.

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

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.

Si se verifica cualquier otro supuesto que se contemple en el Manual de Procedimientos.

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 anterior

4.4.4.- Plazo para la solicitud de revocación

La solicitud de revocación debe efectuarse en forma inmediata cuando se presente alguna de las circunstancias previstas en el apartado 4.4.1.

El servicio de recepción de solicitudes de revocación deberá estar disponible en forma permanente (7x24 horas) cumpliendo con lo establecido en el artículo 34 inc. f) del Decreto 2628/02.

El plazo máximo entre la recepción de la solicitud y el cambio de la información de estado del certificado, indicando la revocación, puesta a disposición de los terceros usuarios debe ser a lo sumo de 72 hs

El Certificador responsable de la Política de Certificación deberá responder plenamente por los daños causados por el uso de un certificado en el período transcurrido entre la recepción de la solicitud de revocación y la publicación de la lista de certificados revocados

4.4.4 Frecuencia de 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.

4.4.5 Requisitos para la verificación de la lista de certificados revocados

Los terceros usuarios deberán validar el estado de los certificados, mediante el control de la lista de certificados revocados.

Asimismo, la autenticidad y validez de la lista de certificados revocados también deberá ser confirmada mediante la verificación de la firma digital del Certificador que la emite y de su período de validez.

El Certificador está obligado a cumplir con lo establecido en el artículo 34 inc. g) del Decreto 2628/02

Garantizar el acceso permanente, eficiente y gratuito de los titulares y terceros al repositorio de certificados revocados.

4.4.6 Disponibilidad en línea del servicio de revocación y verificación del estado del certificado

El Certificador posee disponible un servicio de revocación de certificados en línea y de verificación de su estado. La verificación del estado de un certificado podrá efectuarse directamente ante el Certificador por medio del acceso a la lista de certificados revocados o de otros medios de verificación de estado en línea.

El Certificador debe poner a disposición de los terceros usuarios:

- la información relativa a las características operacionales de los servicios de verificación de estado
- la disponibilidad de tales servicios y cualquier política aplicable en caso de no disponibilidad
- cualquier característica opcional de tales servicios
- el apartado anterior.

4.5 Procedimientos de Auditoría de Seguridad

Se incluirán referencias a los temas vinculados a la auditoría del Certificador desarrollados en su Manual de Procedimientos.

Se especificará entre otros:

- Tipos de eventos registrados (logs de auditoría).
- Frecuencia de su procesamiento y archivo
- Período de conservación
- Métodos de protección contra borrado o modificación
- Procedimientos de resguardo de logs de auditoría
- Sistema de recolección de datos de auditoría
- Notificación de eventos significativos
- Informes de vulnerabilidad

4.6 Archivo de registros

4.6.1 Información a ser archivada

La AC-URME debe conservar información acerca de:

Solicitudes de certificados y toda información que avale el proceso de identificación.

Solicitudes de revocación de certificados

Certificados emitidos y listas de certificados revocados.

Archivos de auditoría.

Toda comunicación relevante entre la AC-URME y los suscriptores.

4.6.2 Plazo de conservación

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

4.6.3 Protección de archivos

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

4.6.4 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.

4.7 Plan de recuperación ante desastres

4.7.1 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.

4.7.2 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.

4.8 Cese de Actividades del Certificador

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.

5 CONTROLES DE SEGURIDAD FÍSICA, FUNCIONALES Y PERSONALES

5.1 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.

5.2 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.

5.3 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.

5.4 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.

5.5 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.

5.6 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.

6 CONTROLES DE SEGURIDAD TÉCNICA

6.1 Generación e instalación de claves

6.1.1 Generación del par de claves

El par de claves debe ser generado únicamente por el titular del certificado, permaneciendo su clave privada en todo momento bajo su absoluto y exclusivo control.

El medio de generación y almacenamiento de la clave privada utilizada en la generación de la firma debe asegurar que:

La clave privada sea única y su confidencialidad se encuentre debidamente garantizada

No pueda ser deducida y se encuentre protegida contra réplicas fraudulentas realizadas con las tecnologías disponibles a la fecha

Pueda ser eficazmente protegida por su titular contra su utilización ilegal, de acuerdo a la aplicabilidad del certificado.

El transporte entre el dispositivo de generación y el de almacenamiento se realice en forma segura

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.

6.1.2 Entrega de la privada al suscriptor

Deberán considerarse obligatoriamente las exigencias reglamentarias impuestas la Ley 25.506 art. 21 inc. b) y el Decreto 2628/02 art. 34 inc. i).

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

Abstenerse de generar, exigir, tomar conocimiento o acceder bajo ninguna circunstancia a la clave privada del suscriptor.

6.1.3 Entrega de la clave pública al emisor del certificado

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

- No pueda ser cambiada durante la transferencia.
- El remitente posea la clave privada que corresponde a la clave pública transferida.
- 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.

6.1.4 Tamaño de claves

- Deben respetarse las siguientes longitudes mínimas de claves:
- Para certificados de Certificador o de información de estado de certificados: 2048 bits.
- Para certificados utilizados en servicios relacionados a la firma digital (certificación de hora digital, almacenamiento seguro de documentos electrónicos, etc.): 2048 bits.
- Para certificados de responsables de Autoridades de Registro que sean utilizados para aprobar solicitudes, renovaciones, revocaciones, etc.: 1024 bits.
- Para certificados de usuario (personas físicas o jurídicas): 1024 bits.

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

- Los tipos de algoritmos de firma aceptables.
- 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.

6.1.5 Generación de claves por hardware o software

Deben respetarse las siguientes exigencias mínimas:

- Las claves criptográficas del Certificador deben ser generadas por dispositivos homologados FIPS 140 nivel 3 o equivalentes.
- Las claves criptográficas utilizadas para la firma de información de estado de certificados o servicios relacionados a la firma digital deben ser generadas en dispositivos FIPS 140 nivel 2 o equivalente.
- Las claves criptográficas que los usuarios responsables de la Autoridad de Registro utilicen para aprobar solicitudes, renovaciones, revocaciones, etc. deben ser generadas en dispositivos FIPS 140 nivel 2 o equivalente.

6.2 Protección de la clave privada

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

6.2.1 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.

6.2.2 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.

6.2.3 Otros aspectos del manejo de claves

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.

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.

6.2.4 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.

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.

6.2.5 Estándares para módulos criptográficos

Deben respetarse las siguientes exigencias mínimas:

- Las claves criptográficas del Certificador deben ser generadas y almacenadas en dispositivos homologados FIPS 140 nivel 3 o equivalentes.
- Las claves criptográficas utilizadas para la firma de información de estado de certificados o servicios relacionados a la firma digital deben ser generadas y almacenadas en dispositivos FIPS 140 nivel 2 o equivalente.
- Las claves criptográficas que los usuarios responsables de la Autoridad de Registro utilicen para aprobar solicitudes, renovaciones, revocaciones, etc. deben ser generadas y almacenadas en dispositivos FIPS 140 nivel 2 o equivalente.

6.2.6 Control "N de M" de clave privada

El control de la utilización de las claves criptográficas del Certificador debe estar dividido de forma tal que sea necesaria la presencia de al menos 2 personas distintas (o N personas distintas de un total de M posibles, con $N \geq 2$).

6.3 Perfil de la lista de certificados revocados

Las listas de certificados revocados correspondientes a la presente Política de Certificación deberán ser emitidas conforme con lo establecido en el estándar ITU X.509 y deben cumplir con las indicaciones establecidas en el apartado "3 - Perfil de

CRLs" del documento "Perfil Mínimo de Certificados y Listas de Certificados Revocados"

I. Desarrollo de Manual de Funciones y procedimientos

Procedimientos fundamentales para el funcionamiento operativo del prototipo PKI.

Procedimientos de Emisión y Validación de Certificados Digitales Iniciales

Introducción:

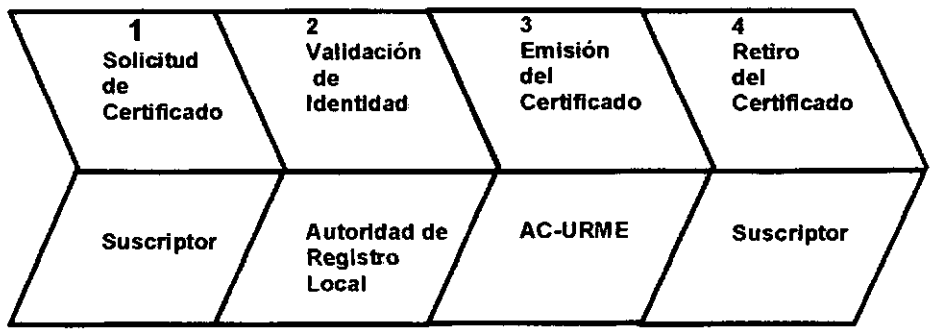
Los siguientes procedimientos describen el conjunto de pasos realizados por la Autoridad Certificante de la Administración Pública de la Provincia de Mendoza cuyas funciones son ejercidas por la Unidad de Reforma y Modernización del Estado de la Secretaría Administrativa Legal y Técnica de la Gobernación (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.

Se puede esquematizar en las siguientes etapas:

Secuencia Sintética del Proceso

(Arrow chart)

Etapas



Principal sector interviniente

Objetivo:

A través de la redacción de estos procedimientos se busca formalizar las tareas que lo conforman y fortalecer el diseño estructural de la AC-URME. Además se busca asegurar la correcta prestación de servicios de provisión de certificados y validación de identidad atendiendo a la satisfacción de los usuarios

Alcance:

Los procedimientos son de aplicación para la emisión de Certificados Digitales en el ámbito del Poder Ejecutivo Provincial y las extensiones que determinen convenios celebrados con otras entidades

Definición de Roles

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

1. Operador Técnico de la AC-URME
2. Responsable de la Autoridad de Registración de la AC-URME
3. Oficial Certificador de la AC-URME
4. Sustitutos de los anteriormente mencionados
5. 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.

1. Funciones del Operador Técnico de la AC-URME

- Administrar los recursos informáticos que integran la estructura de la AC-URME.
- Habilitar la intervención digital del Responsable de la Autoridad de Registración y del Oficial Certificador en los procesos de emisión y revocación de certificados

- Archivar las copias de resguardo generadas por el sistema y la copia del software de la AC-URME
- Implementar y cumplir los procedimientos de seguridad.

2. *Funciones del Responsable de la Autoridad de Registración local*

- Recibir las solicitudes de nuevos certificados para suscriptores.
- Verificar los datos de identidad y de competencia del solicitante.
- Aprobar la emisión del certificado solicitado.
- Aprobar la revocación de certificados
- Archivar la información respaldatoria.

3. *Funciones del Oficial Certificador*

- Ser el depositario de la clave privada de la AC-URME.
- Firmar digitalmente los certificados de los suscriptores.
- Firmar digitalmente las listas de certificados revocados (CRLs).

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

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.

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.

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.

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.

Referencias:

Los siguientes procedimientos han sido realizados teniendo en cuenta los estándares internacionales de CPS (Certification Policy Statement), así como también aquellos procedimientos fijados por Autoridades Certificantes reconocidas dentro de las mejores prácticas a nivel nacional e internacional.

Descripción de los Procedimientos:

Categoría A

Solicitud de Emisión del Certificado

1. ***Suscriptor:*** todo suscriptor de un certificado 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 *(Ver G-Registros)*, generar su propio par de claves y remitir todo el conjunto de datos en formato PKCS#10 a la AC-URME.

Validación de Identidad del suscriptor (Categoría A)

Los pasos a seguir para la identificación de los suscriptores de certificados diferirán en función de las distintas categorías de Validación admitidos por la AC-URME (*Ver G-Registros)*.

2. ***Autoridad de Registración Local:*** recibe la solicitud web y automáticamente envía una mail por el cual el suscriptor 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.

3. ***Suscriptor:*** recibe el mail y lo responde confirmando su efectiva recepción

4. ***Autoridad de Registración local:*** recibe la réplica del mail completando así la verificación de la cuenta de correo, en caso de no recibirla finaliza el procedimiento. A continuación procede a la verificación de los datos restantes contenidos en la solicitud web comparándolos con los del correspondiente Legajo de Personal

5. ***Autoridad de Registración local:*** una ves cumplida la etapa de validación de la identidad del suscriptor de acuerdo con los pasos anteriores, el Responsable de la Autoridad de Registración local puede:

   - 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 puede solicitar cualquier tipo de documentación adicional que considere necesaria a efectos de cumplimentar el proceso de identificación y debe informar al suscriptor acerca de los elementos necesarios para finalizar satisfactoriamente el proceso de validación de su identidad. El suscriptor 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.
   - Aprobar la emisión del certificado y continuar con el paso 6

6. ***Oficial Certificador:*** recibe la aprobación, verifica el cumplimiento de las distintas instancias del proceso y firma el nuevo certificado informando al suscriptor acerca de su emisión a través de un mensaje de correo electrónico firmado digitalmente que contiene un PIN que usará para retirar su certificado. En forma inmediata procede a publicar el nuevo certificado emitido en un repositorio público.

7. ***Suscriptor:*** recibe el correo electrónico con las instrucciones para retirar su certificado y haciendo uso del PIN y del Código de Identificación de la Solicitud retira su Certificado Digital de la interface web de la AC-URME.

Descripción del Procedimiento:

Categoría B

Solicitud de Emisión del Certificado

1. ***Suscriptor:*** todo suscriptor de un certificado debe iniciar el trámite de solicitud ingresando al sitio web de la AC-URME. Debe completar e imprimir el formulario de solicitud de certificado, incluyendo sus datos identificatorios (agregar datos), generar su propio par de claves y remitir todo el conjunto de datos en formato PKCS#10 a la AC-URME.

Validación de Identidad del suscriptor (Categoría B)

Los pasos a seguir para la identificación de los suscriptores de certificados diferirán en función de las distintas categorías de Validación admitidos por la AC-URME (*Ver G-Registros)*.

2. ***Autoridad de Registración Local:*** recibe la solicitud web y automáticamente envía una mail por el cual el suscriptor 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.

3. ***Suscriptor:*** recibe el mail y lo responde confirmando su efectiva recepción

4. ***Autoridad de Registración local:*** recibe la réplica del mail completando así la verificación de la cuenta de correo, en caso de no recibirla finaliza el procedimiento. A continuación procede a la verificación de los datos restantes contenidos en la solicitud web comparándolos con los del correspondiente Legajo de Personal

5. ***Suscriptor:*** conviene con el responsable de la Autoridad de Registración Local un encuentro presencial para el cual debe contar con la siguiente documentación:
    - Solicitud de Certificado Impresa y Firmada conteniendo los siguientes datos personales:
    - Documento de identidad (original y fotocopia) y el Código de Identificación del requerimiento.

6. ***Autoridad de Registración Local:*** El Responsable de la Autoridad de Registración local verificará:
    - Que el documento corresponde a la persona presente.
    - Que dicha persona es aquella cuyos datos figuran en la Solicitud de Certificado presentada. A tal fin debe cotejar los datos del documento con los que figuran en la mencionada Solicitud *(Ver G-Registros)*
    - Que la firma hológrafa de la Solicitud de Certificado corresponda con la del documento}

    - 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 paso 1).

    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 Solicitud de Certificado presentada, en prueba de conformidad. Posteriormente, procederá a archivar toda la documentación de respaldo.

7. ***Autoridad de Registración local:*** una ves cumplida la etapa de validación de la identidad del suscriptor de acuerdo con los pasos anteriores, el Responsable de la Autoridad de Registración local puede:

- 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 puede solicitar cualquier tipo de documentación adicional que considere necesaria a efectos de cumplimentar el proceso de identificación y debe informar al suscriptor acerca de los elementos necesarios para finalizar satisfactoriamente el proceso de validación de su identidad. El suscriptor 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.
- Aprobar la emisión del certificado y continuar con el paso 6

8. ***Oficial Certificador:*** recibe la aprobación, verifica el cumplimiento de las distintas instancias del proceso y firma el nuevo certificado informando al suscriptor acerca de su emisión a través de un mensaje de correo electrónico firmado digitalmente que contiene un PIN que usará para retirar su certificado. En forma inmediata procede a publicar el nuevo certificado emitido en un repositorio público.
9. ***Suscriptor:*** recibe el correo electrónico con las instrucciones para retirar su certificado y haciendo uso del PIN y del Código de Identificación de la Solicitud retira su Certificado Digital de la interface web de la AC-URME.

Descripción del Procedimiento:

Categoría C

Solicitud de Emisión del Certificado

1. ***Suscriptor:*** todo suscriptor de un certificado debe iniciar el trámite de solicitud ingresando al sitio web de la AC-URME. Debe completar e imprimir el formulario de solicitud de certificado, incluyendo sus datos identificatorios *(Ver G-Registros)*, generar su propio par de claves y remitir todo el conjunto de datos en formato PKCS#10 a la AC-URME.

Validación de Identidad del suscriptor (Categoría C)

Los pasos a seguir para la identificación de los suscriptores de certificados diferirán en función de las distintas categorías de Validación admitidos por la AC-URME (*Ver G-Registros)*.

2. ***Autoridad de Registración Local:*** recibe la solicitud web y automáticamente envía una mail por el cual el suscriptor 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.

3. ***Suscriptor:*** recibe el mail y lo responde confirmando su efectiva recepción

4. ***Autoridad de Registración local:*** recibe la réplica del mail completando así la verificación de la cuenta de correo, en caso de no recibirla finaliza el procedimiento. A continuación procede a la verificación de los datos restantes contenidos en la solicitud web comparándolos con los del correspondiente Legajo de Personal

5. ***Suscriptor:*** conviene con el responsable de la Autoridad de Registración Local un encuentro presencial para el cual debe contar con la siguiente documentación:

    - Solicitud de Certificado Impresa y Firmada conteniendo los siguientes datos personales:

    - 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) Ministerio/Organismo/Dependencia/Cargo

- Documento de identidad (original y fotocopia) y el Código de Identificación del requerimiento.

6. ***Autoridad de Registración Local:*** El Responsable de la Autoridad de Registración local verificará:
   - Que el documento corresponde a la persona presente.
   - Que dicha persona es aquella cuyos datos figuran en la nota y en la Solicitud de Certificado presentada. A tal fin debe cotejar los datos del documento con los que figuran en la Solicitud de Certificado y la mencionada nota *(Ver G-Registros)*. Verificará que la misma haya sido certificada por la Mesa de Entradas, Salidas y Archivo del organismo.
   - 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 paso 1).
   - Que la firma hológrafa de la Solicitud de Certificado corresponda con la del documento

   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, la Solicitud de Certificado y la Nota presentada, en prueba de conformidad. Posteriormente, procederá a archivar toda la documentación de respaldo.

7. ***Autoridad de Registración local:*** una ves cumplida la etapa de validación de la identidad del suscriptor de acuerdo con los pasos anteriores, el Responsable de la Autoridad de Registración local puede:

   - 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 puede solicitar cualquier tipo de documentación adicional

que considere necesaria a efectos de cumplimentar el proceso de identificación y debe informar al suscriptor acerca de los elementos necesarios para finalizar satisfactoriamente el proceso de validación de su identidad. El suscriptor 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.

- Aprobar la emisión del certificado y continuar con el paso 6

8. ***Oficial Certificador:*** recibe la aprobación, verifica el cumplimiento de las distintas instancias del proceso y firma el nuevo certificado informando al suscriptor acerca de su emisión a través de un mensaje de correo electrónico firmado digitalmente que contiene un PIN que usará para retirar su certificado. En forma inmediata procede a publicar el nuevo certificado emitido en un repositorio público.
9. ***Suscriptor:*** recibe el correo electrónico con las instrucciones para retirar su certificado y haciendo uso del PIN y del Código de Identificación de la Solicitud retira su Certificado Digital de la interface web de la AC-URME.

Descripción del Procedimiento:

Categoría D

Solicitud de Emisión del Certificado

1. ***Suscriptor:*** todo suscriptor de un certificado debe iniciar el trámite de solicitud ingresando al sitio web de la AC-URME. Debe completar e imprimir el formulario de solicitud de certificado, incluyendo sus datos identificatorios *(Ver G-Registros)*, generar su propio par de claves y remitir todo el conjunto de datos en formato PKCS#10 a la AC-URME.

Validación de Identidad del suscriptor (Categoría D)

Los pasos a seguir para la identificación de los suscriptores de certificados diferirán en función de las distintas categorías de Validación admitidos por la AC-URME *(Ver G-Registros)*.

2. ***Autoridad de Registración Local:*** recibe la solicitud web y automáticamente envía una mail por el cual el suscriptor 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.

3. ***Suscriptor:*** recibe el mail y lo responde confirmando su efectiva recepción

4. ***Autoridad de Registración local:*** recibe la réplica del mail completando así la verificación de la cuenta de correo, en caso de no recibirla finaliza el procedimiento. A continuación procede a la verificación de los datos restantes contenidos en la solicitud web comparándolos con los del correspondiente Legajo de Personal

5. ***Suscriptor:*** conviene con el responsable de la Autoridad de Registración Local un encuentro presencial para el cual debe contar con la siguiente documentación:

    - Solicitud de Certificado Impresa y Firmada conteniendo los siguientes datos personales:

    - 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) Ministerio/Organismo/Dependencia/Cargo

- Documento de identidad (original y fotocopia) y el Código de Identificación del requerimiento.

6. ***Autoridad de Registración Local:*** El Responsable de la Autoridad de Registración local verificará:
   - Que el documento corresponde a la persona presente.
   - Que dicha persona es aquella cuyos datos figuran en la nota y en la Solicitud de Certificado presentada. A tal fin debe cotejar los datos del documento con los que figuran en la Solicitud de Certificado y la mencionada nota *(Ver G-Registros)*. Verificará que la misma haya sido certificada por la Mesa de Entradas, Salidas y Archivo del organismo.
   - 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 paso 1).
   - Que quede constancia de todo lo actuado por la Escribanía de Gobierno.

   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, la Solicitud de Certificado y la Nota presentada, en prueba de conformidad. Posteriormente, procederá a archivar toda la documentación de respaldo.

7. ***Autoridad de Registración local:*** una ves cumplida la etapa de validación de la identidad del suscriptor de acuerdo con los pasos anteriores, el Responsable de la Autoridad de Registración local puede:

   - 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 puede solicitar cualquier tipo de documentación adicional

que considere necesaria a efectos de cumplimentar el proceso de identificación y debe informar al suscriptor acerca de los elementos necesarios para finalizar satisfactoriamente el proceso de validación de su identidad. El suscriptor 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.

- Aprobar la emisión del certificado y continuar con el paso 6

8. ***Oficial Certificador:*** recibe la aprobación, verifica el cumplimiento de las distintas instancias del proceso y firma el nuevo certificado informando al suscriptor acerca de su emisión a través de un mensaje de correo electrónico firmado digitalmente que contiene un PIN que usará para retirar su certificado. En forma inmediata procede a publicar el nuevo certificado emitido en un repositorio público.
9. ***Suscriptor:*** recibe el correo electrónico con las instrucciones para retirar su certificado y haciendo uso del PIN y del Código de Identificación de la Solicitud retira su Certificado Digital de la interface web de la AC-URME.

Registros:

Solicitud de Emisión del Certificado

Datos a completar

1. Datos Personales
    - Apellido y Nombre
    - Dirección de Correo Electrónico
    - Tipo y Número de Documento
    - Título
    - Localidad
2. Datos del ente al que pertenece
    - Cargo/Función
    - Oficina
    - Dependencia
    - Ministerio/Organismo

Categorías de Certificación por niveles de confianza

A) Se trata de la categoría con más bajo nivel de confianza en la cuál se realizan verificaciones de la cuenta de correo del suscriptor y de sus datos personales contra la Base de datos de Recursos Humanos. No requiere la presencia física del Suscriptor y no se le pide documentación adicional salvo que el oficial de registro así lo disponga

B) En esta categoría se realizan las mismas verificaciones de la Categoría A, además se le pide la siguiente documentación:

- Solicitud de Certificado Impresa y Firmada conteniendo los siguientes datos personales:
- Documento de identidad (original y fotocopia) y el Código de Identificación del requerimiento.

Y se realizan las siguientes verificaciones:

- Que el documento corresponde a la persona presente.
- Que dicha persona es aquella cuyos datos figuran en la Solicitud de Certificado presentada. A tal fin debe cotejar los datos del documento con los que figuran en la mencionada Solicitud.
- Que la firma hológrafa de la Solicitud de Certificado corresponda con la del documento

C) Se realizan las mismas verificaciones que en la Categoría B pero además se pide y se verifica una 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 que se especifica:

- Nombre y Apellido
- Documento de Identidad (DNI u otro de validez nacional)
- Jurisdicción/Organismo/Dependencia/Cargo

D) Constituye la categoría de máximo nivel de Confianza en la cuál se lleven a cabo las verificaciones de la Categoría C pero en presencia del Escribano de Gobierno que certifica y deja constancia de todo lo actuado en el proceso de validación

Adjuntos o anexos

Anexo I

Cómo solicitar un certificado digital a la AC-URME Autoridad Certificante de 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 AC-URME el formulario "Certificados Digitales Altas / Bajas" ubicado en la interface web.

Contra entrega del mismo, recibirá un correo electrónico conteniendo su correspondiente Código Identificatorio. Posteriormente, se le enviará a la dirección de correo electrónico personal un PIN que le permite el retiro de su Certificado.

Anexo II

Cómo retirar e instalar un certificado?

Una vez que la Autoridad de Registro Local 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 interface web de la AC-URME opción "RETIRAR CERTIFICADO DIGITAL "
2. Ingresar el Código de Identificación de su solicitud
3. Ingresar el PIN de retiro de Certificado
4. Al presionar el botón "Aceptar" instalará el certificado digital y finalizará el proceso.

''Es importante señalar que estos procedimientos son suficientes para el desempeño del prototipo de la AC-URME, sin embargo, de acuerdo con las nuevas disposiciones se han incluido procedimientos adicionales en las Políticas de Certificación (Ver apartado II.f.)"

J. Análisis de normas técnicas y estándares de licenciamiento

Consideramos de gran importancia guiar el desarrollo de nuestras actividades en el ámbito del proyecto de Firma Digital, de acuerdo con las normas técnicas y estándares de licenciamiento para Autoridades Certificantes. En este orden de ideas, la implementación del prototipo PKI debe estar regida por las normas, requerimientos y requisitos que son condición necesaria para superar con éxito los procesos de Licenciamiento.

La Oficina Nacional de Tecnologías Informáticas (ONTI), dependiente de la Subsecretaría de la Gestión Pública de la Jefatura de Ministros; reconocida por el Decreto 1028/2003 como la encargada de definir las normas y procedimientos reglamentarios del régimen de firma digital definido en la Ley N° 25.506; ha elaborado los textos preliminares de los documentos referidos al proceso de licenciamiento de los certificadores:

- Disposición estableciendo el marco normativo aplicable al otorgamiento y revocación de las licencias de firma digital a otorgarse a los certificadores.

Anexos de la disposición:

- Procedimiento de Licenciamiento.
- Requisitos Mínimos para Políticas de Certificación.
- Perfil Mínimo de Certificados y Listas de Certificados Revocados.

Dichos documentos y sus referencias a estándares internacionales han sido utilizados en las determinaciones y especificaciones de nuestra Infraestructura de Firma Digital.

Además, la ONTI ha puesto a consideración pública dichos textos preliminares de los documentos referidos al proceso de licenciamiento de los certificadores. Los mismos pueden descargarse desde la dirección http://www.pki.gov.ar . Una vez redactadas sus versiones finales, estos documentos constituirán la base normativa que deberán cumplir los certificadores para la obtención de carácter de certificador licenciado.

El equipo de Firma Digital en Mendoza, autores del presente informe, ha colaborado en el proceso de consulta pública de los documentos enviando sus aportes.

III. IMPLEMENTACIÓN DE EXPERIENCIA EN EL CIRCUITO DE RESOLUCIONES

A. Relevamiento del procedimiento actual

Hemos relevado aquí el procedimiento general de redacción, corrección, firma y archivo por el cual pasan todas las resoluciones de la Subsecretaría Administrativa Legal y Técnica

Descripción del procedimiento actual:

1. Oficina de Origen: envía expediente con requerimiento de dictado de resolución por Mesa de Entradas.

2. Mesa de Entradas: recepciona y envía expediente con el requiriendo de dictado de resolución oportunamente originado en diversas oficinas de la Gobernación, para que sea revisado por despacho.

   Tipos de contenido de Resolución

   - Sumarios
   - Adicionales de Sueldo
   - Modificaciones de Presupuesto
   - Renuncias
   - Pago de Facturas y Gastos
   - Contratos de Locación de Servicios

3. Despacho: estudia y controla que el expediente cumpla con los requisitos necesarios para dar proceso al armado de la Resolución que correspondiere en cada caso. En caso de no cumplir con los requisitos lo observa, y lo devuelve a Mesa de Entradas para que se subsanen las observaciones realizadas. En caso de que el expediente esté correcto continúa con paso 5.

4. Mesa de Entradas: devuelve expediente a la Oficina de Origen para que se subsanen las observaciones y se repite el ciclo (desde paso 1).

5. Despacho: Una vez que el expediente cumple con todos los requisitos para el caso particular procede a armar el proyecto de resolución que se adjunta al expediente y se manda a supervisión.

6. Supervisión: realiza el análisis y la valoración legal del texto de la resolución y del expediente. Si es necesaria alguna modificación, aclaración o rectificación, lo observa y lo devuelve a Despacho o a la Oficina de Origen que corresponda. Caso contrario manda expediente a la Dirección de Administración para que siga su curso (paso 8)

7. Despacho u Oficina de origen : da curso a las observaciones correspondientes y una vez satisfechas devuelve el expediente a Supervisión y se repite el ciclo administrativo (Desde paso 6)

8. Dirección de Administración: revisa el texto de la resolución contenido en el expediente. Si es necesario realiza observación y en este caso devuelve el expediente a Despacho o a la Oficina de Origen. Si no es necesaria observación alguna, le da visto bueno a través de sello marginal y Firma del director de Administración, a continuación pasa el expediente a la Secretaría Administrativa, Legal y Técnica (Paso 10)

9. Despacho u Oficina de Origen: da curso a las observaciones correspondientes y una vez satisfechas devuelve el expediente a Dirección de Administración y se repite el ciclo administrativo (Desde paso 8)

10. Secretaría Administrativa Legal y Técnica: recibe el expediente y revisa el texto de la resolución. En caso de existir alguna observación devuelve le expediente a Despacho u a la Oficina de Origen y se repite el ciclo administrativo (Desde paso

8). De no existir modificación alguna promulga la resolución a través de la firma del Secretario titular y la devuelve a Despacho para su numeración.

11. Despacho: recibe el expediente con el texto de la resolución ya firmado y procede a numerar la norma de acuerdo con su correlatividad por año y a cargar dicha información en un índice interno. Archiva los originales y distribuye copias a las dependencias afectadas por el alcance de la nueva resolución.

    Si afecta al área de Comunicación Social o de Contabilidad 2 copias.
    Si afecta el área de Personal 6 copias
    Si afecta la Dirección General de Servicios 5 copias

12. Despacho: en caso que en la resolución se indique la leyenda "comuníquese publíquese y archívese" se envía copia de resolución para ser publicada en el Boletín Oficial y se carga en el índice interno.

Características particulares

El procedimiento anteriormente descripto posee una serie de particularidades que deben analizarse detenidamente:

- El volumen de Resoluciones que siguen el circuito por año es un promedio de trescientas (300)
- Intervienen dos (2) Funcionarios con firma autorizada, uno de ellos es el Director General de Administración y el otro es el titular de la Subsecretaria
- Existe una serie de relaciones entre las distintas resoluciones: derogación, refrendo (transferencia), modificación, ampliación, rectificación. Vale decir, están conectadas entre sí.
- La vigencia en el tiempo de una resolución es perdurable salvo que exista una derogación

- Actualmente existe un índice interno de resoluciones que contiene los siguientes datos: carátula, número (correlativo por año), resumen, fecha y publicación en el B.O.
- El archivo de resoluciones se encuentra dividido en un Archivo local, ubicado en despacho y un Histórico, ubicado en el archivo histórico.
- Existe una marcada necesidad de Consulta de resoluciones por parte de los funcionarios y oficinas de gobernación.
- El circuito de resoluciones posee relaciones o cruces con los siguientes circuitos: proyectos de leyes, leyes, memorándum, notas, decretos, acuerdos, oficios del Poder Judicial.

B. Explicitación de la necesidad puntual

Determinaremos claramente aquí, cuáles son las necesidades que Firma Digital puede satisfacer de manera óptima en el circuito de resoluciones y cuáles son los fundamentos de la aplicación.

Estrategia para identificación de procedimientos aptos

Hemos sometimos el circuito de Resoluciones a consideración de nuestra "Estrategia para la Identificación de Procedimientos Aptos", ya que consideramos 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.

Según los "Criterios de selección de circuitos administrativos" de nuestra estrategia, las conclusiones fueron:

- Trámites con alta frecuencia de repetición a cargo de la misma oficina, ente o persona: en efecto, el procedimiento de resoluciones, como ya vimos, posee tales características

- Circuitos que requieren autenticación de las partes involucradas: en este caso concreto se requiere la firma digital de las personas responsables de la promulgación de los textos resolutivos
- Circuitos basados en gran cantidad de papeleo: resulta verdaderamente costoso el actual sistema de distribución de fotocopias de las resoluciones a los sectores involucrados
- Circuitos administrativos de transferencia de información con exigencias de oportunidad: se evalúa conveniente agilizar el circuito de resoluciones a través de la implementación del nuevo sistema

Necesidades puntuales

Del estudio detallado del circuito de resoluciones se identificaron las siguientes necesidades:

- Necesidad de agilizar los pasos que implican firmas de visto bueno y promulgación de las resoluciones
- Necesidad de conservar en un archivo general las resoluciones debido a sus características de perdurabilidad en el tiempo
- Necesidad de medios de conservación con mayor resistencia al paso del tiempo
- Necesidades de consulta de resoluciones por parte de funcionarios y oficinas de gobierno
- Necesidad de mejora en la accesibilidad y disponibilidad de la información
- Necesidad de relacionar la información
- Necesidad de asegurar la autenticidad de la información detallada en la resolución
- Necesidad de garantizar la integridad de la información
- Necesidad de garantizar el no repudio de la información

C. Determinación de mejoras

Nuestro modelo de implementación de Firma Digital en el circuito de resoluciones se orienta, en función de las necesidades identificadas, a la **creación de un repositorio digitalizado de resoluciones con garantías de Firma Digital.**

Cabe señalar, que nuestra idea de repositorio excede el alcance de su denominación, ya que es nuestro propósito acercarnos a la definición de una biblioteca digital de resoluciones. Es decir un "conjunto de recursos de información en formato digital, insertos en un contexto organizacional que procura la selección, evaluación, registro y sistematización para su disponibilidad y que permite – mediante Tecnologías de información, el acceso local o a distancia por parte de una comunidad de usuarios locales o remotos".

Mejoras puntuales

Para describir las mejoras y beneficios que introduce nuestra aplicación debemos describir las propias de un Repositorio Digital y las propias de un Repositorio Digital con Firma Digital.

Repositorio Digital

- Mayor acceso y disponibilidad de la información sin dependencia de barreras temporales, geográficas y espaciales.
- Ahorro en costos de papelería y de transferencia
- Posibilidades de búsqueda por criterios
- Información actualizada
- Información centralizada
- Información segura y perdurable en el tiempo
- Posibilidades de relacionar la información entre sí
- Despapelización del Estado
- Agilización de los procesos de consulta
- Mejoras en la calidad de la información
- Liberación de espacios físicos de archivo de papel
- Liberación de tiempos en tareas manuales

Repositorio Digital con Firma Digital

Esta mejora implica que los textos de las resoluciones no serán firmados en forma hológrafa y luego digitalizados, sino que los mismos responsables de la promulgación suplantarán su firma manuscrita por una Firma Digital en los textos resolutivos que irán directamente al repositorio digital. Con lo cual los textos resolutivos digitalizados tendrán un genuino **valor legal.**

En este sentido Firma Digital proveerá a la información incluida en el repositorio digital de las siguientes garantías:

- ***Integridad:*** los textos de las resoluciones firmados digitalmente por los responsables estarán completos y sin posibilidad de error, ya que la tecnología garantiza la verificación de la integridad de la resolución mediante la aplicación de una función de hash. Cualquier diferencia, pérdida de datos, o modificación de los datos originales será alertada por el sistema.

- ***Autenticidad y autoría:*** se puede contar con la absoluta seguridad sobre el valor de verdad del texto resolutivo ya que, a diferencia de un repositorio común, el texto resolutivo se encontrará firmado digitalmente por los responsables de su promulgación. Esto es posible gracias a que la verificación de la Firma se encuentra disponible para aquellas personas que ingresen a consultar el repositorio, a través de la clave pública del propio firmante.

- ***No repudio:*** debido a las garantías anteriores, la información es digitalmente firmada posee valor legal en el repositorio. Es decir, no se tiene sólo una imagen de una norma en Internet, sino que lo que se tiene es la propia norma digitalizada y firmada digitalmente por los responsables de su promulgación, con lo cual su responsabilidad por lo que firmaron y se encuentra en el repositorio es plena.

De esta forma, los textos resolutivos contenidos en la base de datos, se resguardan mediante métodos de criptografía asimétrica que aseguran la integridad y autoría de las resoluciones y la identidad de las personas que las promulgaron.

D. Determinaciones sobre la provisión de certificados

Es una decisión muy importante determinar cuál será el agente que emitirá y gestionará los certificados que se piensan aplicar a una experiencia piloto determinada.

Actualmente, el escenario y las condiciones particulares de la experiencia en el circuito de resoluciones determinan dos posibilidades de similares características tecnológicas a la hora de tomar una decisión respecto de la provisión de certificados

- Provisión de certificados por parte de la AC-ONTI (Autoridad Certificante de la Oficina Nacional de Tecnologías Informáticas), organismo que se encontraría dispuesto a emitir certificados bajo el estándar x.509 v3 a favor de las personas que lo solicitaren en el marco de las experiencias piloto de firma digital de la Unidad de Reforma Mendoza.

- Provisión de certificados por parte de la AC-URME (Prototipo de Autoridad Certificante de la Unidad de Reforma y Modernización del Estado), certificados diseñados en función del estándar x.509 v3 y de confiabilidad probada en la implementación de Sitio seguro en la Guía de trámites

Por lo antedicho, el equipo del proyecto de firma deberá tomar en cuenta factores legales, políticos y técnicos al momento de la implementación en el circuito de resoluciones para decidir el origen de los certificados a proveer a los usuarios.

E. Diseño global

En la etapa de diseño global evaluamos distintas alternativas de 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.

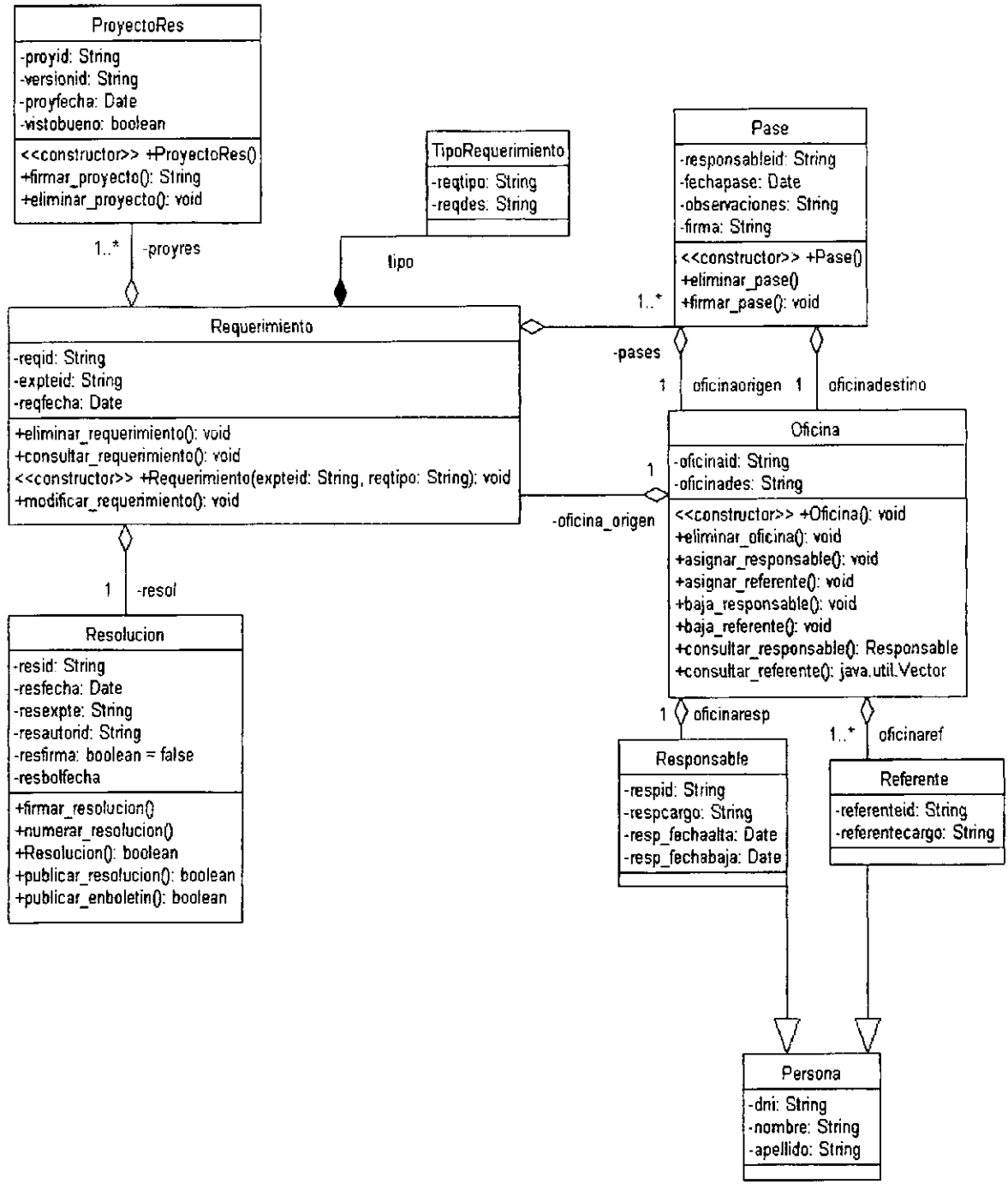
Esta actividad tiende a identificar y describir una solución tecnológica que con el uso de la firma digital permita:

- 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 pensamos en:

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.

El siguiente *diagrama de clases*[1] describe un modelo global para la informatización del circuito de resoluciones descrito, con aplicación de la firma digital.



[1] *Diagrama de Clases: herramienta de diseño de sistemas perteneciente a UML (Unified Modeling Language). Ver Diseño Detallado.*

Las clases *Requerimiento, Pase y ProyectoRes* son las entidades centrales para el manejo de todos los pasos previos a la firma y publicación de la Resolución. La clase Resolución modela el comportamiento de las normas ya aprobadas en el sistema. El resto de las clases dan soporte al manejo de responsables y firmas autorizadas sobre resoluciones.

Si bien es factible desarrollar este modelo, la posibilidad de implementarlo exitosamente se debilita frente a la necesidad de adjuntar en cada pase, el expediente vinculado al texto resolutivo. Este expediente que se encuentra en soporte impreso y que constituye un elemento fundamental en el circuito de producción de la norma, condiciona múltiples aspectos en la implementación integral del modelo, tales como:

- No se elimina el cuello de botella provocado por el paso de carpetas de expediente entre oficinas.
- No se puede agilizar la función de la mesa de entrada, que sigue siendo concentradora de cualquier movimiento de expedientes que se produzca.
- Impide eliminar las firmas sobre soporte impreso.
- Se produce una separación difícil de manejar entre las resoluciones con soporte digital y los expedientes en soporte impreso.
- Confunde y desmotiva a los actores que intervienen en el circuito, ya que agregarían el procesamiento de los documentos, pases y requerimientos digitales a su actual manejo de expedientes, sin ver claramente los beneficios del cambio.

Por estos motivos, decidimos acotar el desarrollo a la construcción de un repositorio digital de resoluciones con firma digital, descartando, en principio, la informatización de los pasos previos a la producción del texto resolutivo final. Esta simplificación del modelo permitirá cumplir de igual modo la mayoría de los objetivos propuestos, con menores riesgos en la implementación y con mayores perspectivas de éxito y aceptación de los usuarios. En líneas generales permitirá:

- Probar la aplicación de la firma digital, de una manera más simple y directa.
- Eliminar las copias impresas de la Resolución que circulan luego de que la misma se firma y publica.
- Contar con un repositorio público de resoluciones que pueda ser accedido desde la Intranet de Gobierno.

El recorte propuesto sobre el modelo global no rescinde la posibilidad de que progresivamente se puedan ir agregando nuevos módulos al sistema hasta lograr el circuito completo con soporte digital; pero es menos ambicioso en los alcances propuestos para una primera etapa.

En otro orden de cosas, proponemos no acotar el diseño a un repositorio de resoluciones para la Secretaría Legal y Técnica, sino a desarrollar un repositorio digital de normas legales que pueda ser adaptado con mínimos esfuerzos a distintas oficinas y tipos de normas legales en el ámbito de la administración pública. Es por esto que no hablaremos ya de circuito o aplicación de resoluciones, sino de aplicación de normas, como una manera de referenciar este sistema más amplio. El diseño detallado describe más profundamente el modelo propuesto.

F. Diseño detallado

El diseño detallado de una aplicación informática reúne el conjunto de herramientas que permiten especificar claramente las características que deberán respetarse en la fase de desarrollo. Estas herramientas deben ajustarse a un modelo de diseño particular, con sustento teórico, de modo tal que cualquier programador o ingeniero en software pueda hacer una interpretación precisa de los requerimientos planteados.

Para documentar las especificaciones del Repositorio Digital de Normas Legales con firma digital, decidimos ajustarnos a un modelado conceptual orientado a objetos y bases de datos, utilizando para ello diagramas UML. El Lenguaje de Modelado Unificado (UML - Unified Modeling Language) es un lenguaje gráfico para visualizar, especificar y documentar cada una de las partes que comprende el desa-

rrollo de software. UML entrega una forma de modelar cosas conceptuales como son las entidades y actores que intervienen en el circuito administrativo, además de cosas concretas al desarrollo como lo son escribir clases en un lenguaje determinado, esquemas de base de datos y componentes de software reutilizable.

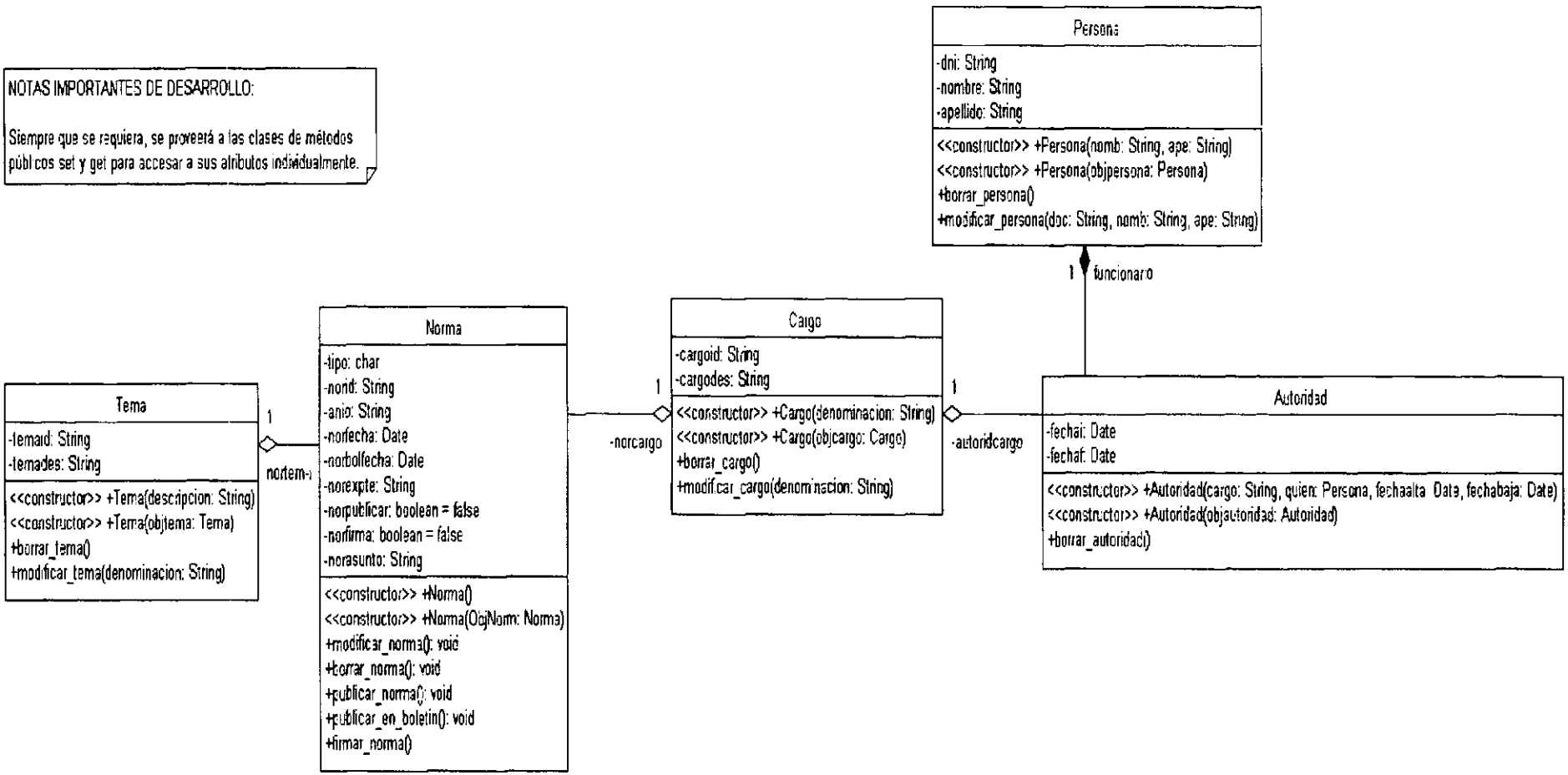
En este sentido construimos en primer lugar el ***Diagrama de Clases*** del modelo de Normas Legales, instrumento fundamental para especificar las clases que deberán programarse con sus principales atributos y servicios.

Complementariamente diseñamos el modelo de base de datos que sustentará el repositorio haciendo uso de un ***ERD (Diagrama o Modelo de Entidad Relación).*** Esta herramienta permite mostrar las tablas y relaciones que contendrá la Base de Datos de Normas con detalle de sus campos, claves primarias, índices, etc.

Se prevé en el diseño propuesto, un desarrollo ajustado a una arquitectura de ***tres capas*** que fortalezca el concepto de *separación* entre los componentes de software que administran la gestión de datos, los que componen la lógica de procesos y aquellos que definen la interfase con el usuario. Un modelo de tres capas promueve una programación ordenada y de calidad, garantizando facilidad de mantenimiento, encapsulamiento y módulos de software altamente reutilizables.

En cuanto a la estrategia de implantación, el diseño adhiere al modelo cliente-servidor, en el cual los usuarios accedan a través de una interfase web a los datos en el repositorio central mantenido por el motor de base de datos y gestionado por los módulos que operan del lado del servidor. Esto garantiza amplio acceso a los servicios del sistema desde cualquier puesto de trabajo sin necesidad de contar con instalaciones particulares en cada una de las máquinas clientes.

Diagrama de Clases



G. Desarrollo de aplicaciones informáticas que sustenten el archivo y gestión digital de resoluciones y la firma digital de las mismas

Se ha completado en esta etapa las tareas de desarrollo del Repositorio Digital de Normas Legales con firma digital en función de las especificaciones de diseño documentadas en el informe anterior.

Presentamos a continuación los aspectos fundamentales del desarrollo, la descripción de los módulos que componen el software y su interrelación.

Plataforma – Bajo costo, portabilidad y escalabilidad

El desarrollo se ajusta a un modelo de tres-capas e implementa una arquitectura Cliente-Servidor. Del lado del servidor se requiere el motor de base de datos PostgreSQL 7.3 al cual se accede a través de un conector JDBC, la plataforma J2EE y cualquier servidor de aplicaciones web que interprete código JSP (*Java Server Pages*) y Servlets Java. En particular se ha utilizado para el desarrollo el *Application Server Jakarta-Tomcat 4.1.*, pero cualquier otro que cumpla los requisitos es aceptable. Del lado del cliente, sólo se necesita un browser de Internet y algún plugin de firma digital de documentos PDF.

Se debe destacar que el desarrollo sobre plataforma J2EE garantiza la portabilidad del software a entornos Linux o Windows; y que además tanto la plataforma java, como el motor de base de datos y el application server requeridos en el servidor, son software de libre acceso.

Interfase web total

Tanto el módulo de consultas al Repositorio, como los módulos de Gestión de Datos utilizan *interfase web* con el usuario. Esto posibilita:

- Libre acceso a la aplicación y sus servicios desde cualquier puesto de trabajo conectado a la Intranet de Gobierno sin necesidad de instalación previa de aplicaciones cliente.
- Carga de la complejidad del lado del servidor, con la ventaja de que los usuarios pueden consultar o gestionar el repositorio desde un cliente delgado (Arquitecturas 486, Pentium ,etc.). Costo cero en inversión en Hardware.
- Mayores posibilidades de escalabilidad
- Costo cero en licencias de software cliente.
- Mantenimiento y resolución de problemas centralizado
- Menor esfuerzo de Capacitación y aprendizaje intuitivo de los usuarios.

Código Fuente

La programación hace uso de los siguientes lenguajes:

- Consultas y transacciones sobre el motor de base de datos: *ANSI-SQL*
- Procedimientos almacenados en la base de datos: *PL/SQL*
- Servlets y Clases: *Java (J2EE)*
- Interface web: *JSP, Javascript, HTML*

Seguridad y Acceso

El *módulo de consultas* al repositorio es de acceso público a cualquier usuario de la Intranet de Gobierno o eventualmente de Internet. La seguridad en las consultas se implementa:

- A nivel de base de datos: utilizando un usuario público con privilegios exclusivos de consulta.
- A nivel de los documentos consultados con la tecnología de firma digital.

El *módulo de gestión de datos* – altas, bajas y modificaciones al repositorio- es de acceso exclusivo a usuarios con privilegios de administración u operación

sobre el sistema. La seguridad en el acceso a las aplicaciones y transacciones sobre la base de datos se implementa a través de:

- Control de privilegios de usuarios en la conexión a la base de datos.
- Sitio seguro con validación de certificado de cliente en el *Application Server.*

Tolerancia a fallas y gestión de errores

Las fallas y errores que pueden producirse en tiempo de ejecución *(por ej.: por problemas de conexión, locks sobre la base de datos, transacciones no autorizadas, caída del application server, etc.)* se gestionan bajo el concepto de ***manejo de excepciones***. Esto implica que el sistema genera una excepción ante un error o falla que es tratada por un manejador de excepciones especialmente diseñado para tratar este tipo de errores. De esta forma se separa el código de manejo de errores, del código que atiende a la lógica principal del desarrollo, facilitando su comprensión y mantenimiento posterior. Así mismo, un cuidadoso manejo de excepciones implica en nuestro desarrollo una mayor tolerancia a fallas, objetivo de diseño fundamental en un sistema que pretende estar on-line 24x7x365.

Formato de los documentos Digitales

Aunque el desarrollo no condiciona en principio el formato de los documentos digitales que puede almacenar el repositorio, se sugiere y así se lo indica para la etapa de implementación del proyecto, que se utilicen documentos en formato .pdf, dado que este formato constituye un estándar para la publicación de documentos en Internet.

Firma Digital de documentos

En esta primera versión del desarrollo, la firma digital de los documentos requiere que el cliente instale en su desktop algún plugins de firma digital de documentos .pdf. Se prevé desarrollar un servlet para una versión posterior, que

permita agregar esta funcionalidad a la aplicación de lado del servidor, liberando a los clientes de la necesidad de instalaciones complementarias.

Estructura del Desarrollo

El desarrollo se estructura en dos módulos principales: las ***consultas al repositorio*** y la ***gestión de datos*** sobre el repositorio.

Módulo: Gestión de Datos

Las altas, bajas y modificaciones sobre datos almacenados en el repositorio se realizan a través de ***5 componentes*** interrelacionados cuyo desarrollo responde a especificaciones de diseño planteadas en el *Modelo de Base de Datos* y en el *Diagrama de Clases* que documentamos en etapa de diseño detallado.

- **ABM de Autoridades:** Cada norma almacenada en el repositorio debe estar firmada por una Autoridad Responsable cuyos datos y certificados digitales deben ser correctamente mantenidos y actualizados. Este componente web implementa las altas, bajas y modificaciones a la tabla que mantiene y controla toda la información vinculada a autoridades.

- **ABM de Cargos:** Cada persona que firma una norma está asociada a un cargo o función en un período determinado. Este componente implementa la administración de la información vinculada a la estructura organizacional y la asignación de personas en cargos.

- **ABM Temas:** Como criterio organizador cada norma se asocia a un tema en particular. El componente de ABM Temas permite parametrizar la tabla de temas de modo que el repositorio pueda configurarse de acuerdo a necesidades puntuales de clasificación de información en cada implementación.

- **ABM de Actualizaciones:** Una norma reciente puede relacionarse con otras a través de algún tipo de actualización que la misma impone sobre sus antecedentes. En general los tipos de relación de actualización son: "*modifica*", "*deroga*", "*ratifica*", etc. Con el objeto de parametrizar los tipos de relación entre normas de modo de garantizar la construcción de un mapa de relación que permita seguir todo el historial de un documento, se mantiene en el sistema una tabla de *Actualizaciones*. Este componente implementa la administración de esta tabla y sus vinculaciones con la tabla de *Relación entre normas*.

- **ABM de Normas:** Este componente gestiona la tabla principal de normas almacenadas en el repositorio. Esta tabla reúne toda la información descriptiva de las normas así como también el documento digital asociado a cada una. A través de este componente, usuarios autorizados pueden cargar nuevas normas al repositorio, modificar datos asociados a una norma o dar de baja algunos documentos, con los debidos controles sobre la información almacenada.

Documentamos a continuación las validaciones y controles fundamentales que el desarrollo impone sobre la gestión de datos:

Validación y controles implementados en la interface web:

- Edición de formularios de acuerdo a especificaciones del diccionario de datos.
- Correcta selección de opciones y parámetros.
- Correcta vinculación de procesos y selección de menús.
- Manejo de sesiones.
- Manejo de mensajes de error y advertencia.

Validaciones y controles implementados a nivel de código java:

•Manejo de excepciones SQL, del servidor de aplicaciones, etc.

•Correcta gestión de fechas, períodos y conversión de formatos.

•Gestión de parámetros web, validación de campos nulos.

•Conversión adecuada de tipos de datos.

Validaciones a nivel de base de datos: A través de la validación de integridad referencial y procedimientos almacenados se garantiza que:

- No pueda eliminarse una autoridad si está asociada a alguna norma en el sistema.
- No pueda eliminarse un cargo si tiene autoridades vinculadas al cargo.
- No pueda eliminarse una norma si está vinculada a otras normas en el sistema.
- No puedan registrarse dos personas en un mismo cargo en un mismo período, ni en períodos superpuestos de alguna forma.
- No puedan almacenarse normas con fecha de publicación en el boletín anterior a la fecha de emisión.
- No puedan eliminarse actualizaciones que vinculen normas.
- No puedan vincularse normas inexistentes.
- No pueda eliminarse un tema que tiene normas asociadas.
- Se carguen adecuadamente todos los datos requeridos como obligatorios para una norma, una autoridad, un cargo o un tema.
- Se gestione sin errores el número de Expte. Vinculado a la norma.

Módulo de Consulta

El módulo de Consulta consta de tres componentes: consulta básica, consultas avanzadas y reportes.

Consultas Básicas: Este componente permite a los usuarios consultar normas en el repositorio por los siguientes criterios:

a. Número de la norma.
b. Fecha de emisión.
c. Fecha de publicación en el Boletín Oficial.
d. Autoridad que la firma.

Ante cualquier consulta realizada se devuelven los datos descriptivos de la o las normas que satisfacen el criterio de búsqueda especificado y se da acceso a los documentos digitales.

Este módulo es de acceso público a cualquier usuario de la Intranet de Gobierno.

Consultas Avanzadas: Este componente permite refinar búsquedas y consultas de documentos ***combinando*** según las necesidades del usuario los siguientes criterios:

a. Número de la norma.
b. Fecha de emisión.
c. Fecha de publicación en el Boletín Oficial.
d. Autoridad que la firma.
e. Cargo o función que la emite.
f. Tema asociado.
g. Descriptores o palabras incluidas en el abstract de la norma.
h. Normas comprendidas en un período determinado.
i. Normas relacionadas a una norma en particular.

De esta manera se pueden imponer filtros compuestos en las consultas a la Base de Datos para ampliar o restringir el conjunto de resultados.

Este módulo es de acceso público a cualquier usuario de la Intranet de Gobierno.

Reportes: Este componente permite a usuarios autorizados configurar distintos modelos de reportes sobre los registros y documentos almacenados en el repositorio. No se brinda aquí un conjunto de reportes predefinidos, sino una interfase web para que los usuarios puedan definir dinámicamente los datos a incluir en sus reportes de acuerdo a la combinación de criterios de consulta y selección de campos.

H. Capacitación

La capacitación de los empleados y funcionarios involucrados en el circuito se abordó desde dos dimensiones igualmente importantes. Por un lado la capacitación operativa en el uso de las herramientas informáticas y los cambios en los procesos habituales de gestión, firma y consulta de normas legales. Por otro, la formación acerca de los alcances tecnológicos y legales de la firma digital; y la concientización sobre las ventajas comparativas que la introducción de esta tecnología tiene sobre la gestión. En ambas dimensiones se entendió que la capacitación constituía una herramienta fundamental para garantizar el éxito de la experiencia y que debía ser utilizada para generar confianza, difundir y provocar entusiasmo contagioso entre todos los actores involucrados en el circuito.

Tomando en cuenta estas consideraciones, se diseño la siguiente planificación que condujo las actividades de capacitación.

Diseño de la capacitación

Objetivos

- Generar habilidades de administración y uso del repositorio digital de normas legales con firma digital.
- Involucrar y comprometer a los destinatarios en el sostenimiento y desarrollo del repositorio.

- Favorecer la apropiación de la tecnología de firma digital.

Destinatarios

Empleados y funcionarios involucrados en el circuito de producción, gestión y firma de normas legales en el ámbito de la Secretaría Administrativa, Legal y Técnica.

6.3.1 *Aprendizajes Acreditables*

Se pretende que los capacitados adquieran los siguientes conceptos y actitudes:

- Compromiso por la tarea.
- Importancia de la gestión para optimizar la gestión, conocimiento y utilización de la normativa legal.
- Criterio común en la atención de problemas.
- Dominio de la interfase web del repositorio.
- Correcta comprensión de los parámetros del sistema.
- Utilización cotidiana de salidas y consultas como método de control.
- Correcta utilización de firmas digitales y certificados digitales.

Contenidos

- Modelo lógico y funcional del repositorio.
- Estructura conceptual del sitio web: zonas pública y segura.
- Aplicación y alcances de la firma digital y certificados digitales al digesto.
- Obtención de Certificados digitales.
- Seguridad SSL en el sistema y autenticación de clientes.
- Parametrización inicial.
- Administración del módulo temas.
- Administración del módulo vínculos.
- Administración de los módulo autoridades y cargos.
- Administración del módulo de normas.

- Carga y firma de documentos digitales.
- Consultas al sistema en zona segura.
- Consultas al sistema en zona pública.

Carga horaria del módulo

12 hs. reloj.

Actividades/Recursos/Tiempos

Contenido Conceptual	*Estrategias/Actividades*	*Recursos*	*Tiempos*
•Modelo lógico y funcional del repositorio. •Estructura conceptual del sitio web: zonas pública y segura.	Presentación inicial de los capacitadotes, de los objetivos de la capacitación y las expectativas de logro / Dinámica de Grupos. Presentación de la interfase web / Presentación y exploración del sitio.	•papelería •Intranet •Sitio web del repositorio	2 hs. - Tarde
•Aplicación y alcances de la firma digital y certificados digitales al digesto. •Obtención de Certificados digitales. •Seguridad SSL en el sistema y autenticación de clientes.	Exposición teórica Pruebas de accesos a la zona segura con Certificados válidos y no válidos / Juego de roles. Realización de la solicitud de Certificados digitales. Obtención, descarga e instalación de certificados digitales en las máquinas de los responsables.	•presentación powerpoint •Certificados Digitales de prueba •Autoridad de Registro de la ONTI	4 hs. – Mañana
•Administración del módulo temas. •Administración del módulo vínculos. •Administración de los módulo autoridades y cargos.	Abordaje de casos prácticos. Uso guiado de la interfase de administración del repositorio.	•Intranet •Sitio web del repositorio •Resoluciones de la Secretaría Administrativa Legal y Técnica, en formato impreso y digital •Certificados digitales de los	2 hs. - Tarde

		responsables	
•Administración del módulo de normas. •Carga y firma de documentos digitales.	Abordaje de casos prácticos. Uso guiado de la interfase de administración del repositorio.	•Intranet •Sitio web del repositorio •Resoluciones de la Secretaría Administrativa Legal y Técnica, en formato impreso y digital •Certificados digitales de los responsables	4 hs. - Mañana
•Consultas al sistema en zona segura. •Consultas al sistema en zona pública.	Abordaje de casos prácticos. Uso guiado de la interfase de administración del repositorio.	•Intranet •Sitio web del repositorio •Resoluciones de la Secretaría Administrativa Legal y Técnica, en formato impreso y digital •Certificados digitales de los responsables	2 hs. - Tarde

Evaluación

Para evaluar el cumplimiento de los objetivos propuestos para la capacitación se emplearán distintos indicadores de control y uso del sistema durante la etapa de implementación, tales como:

- Seguimiento del uso apropiado del sistema.
- Interpretación de parámetros, elementos de datos y solución de casos problema.
- Evolución de los volúmenes de carga de documentos digitales al repositorio.
- Seguimiento de consultas de operadores del sistema.

Resultados de la capacitación

El curso se realizó satisfactoriamente y de acuerdo a la planificación detallada. Se capacitaron 3 personas de la oficina de despacho, el Secretario Administrativo, Legal y Técnico; y el Director de Administración.

Cuando se avance en la carga y firma de documentos, se prevé realizar una presentación institucional que difunda los alcances de la aplicación en el ámbito de la Administración Pública.

I. Plan de Pruebas

Documentamos a continuación el ***Conjunto de Pruebas*** que se realizaron sobre las aplicaciones informáticas del repositorio digital de normas legales. Estas pruebas se realizaron previo a comenzar las instancias de capacitación e implementación, de forma tal de detectar a priori posibles fallas a nivel de interfase, integridad de datos o control de acceso. Cabe aclarar que las pruebas instrumentadas tenían como principal objetivo garantizar un adecuado grado de ***tolerancia a fallas*** del sistema, tanto en los aspectos vinculados a la plataforma de hardware y software, como a las fallas que pueden producirse por errores humanos en su operación.

Descripción de la Prueba	Objetivo de la Prueba	Ejecución de la Prueba	Resultados/Conclusiones
Control de acceso de usuarios	Validar los esquemas de control de acceso a nivel de usuarios, de forma de garantizar que sólo ingresen a la zona segura del sistema usuarios autorizados.	▪Intento de acceso a la zona segura por canal http no seguro. ▪Emisión de Certificados Digitales de prueba. ▪Inclusión de Certificados de prueba en el repositorio de Certificados del sitio seguro. ▪Intentos de ingreso con Certificados válidos. ▪Intentos de acceso con Certificados no válidos.	Se comprobó el correcto funcionamiento de los esquemas de control de acceso con autenticación de cliente en el sitio seguro.

		▪Comprobación de access-logs.	
Manejo de sesiones y logs de transacciones	Comprobar la correcta apertura, mantenimiento y cierre de las sesiones iniciadas en los browsers clientes. Verificar la correcta registración en logs de transacciones de sesiones iniciadas y su duración, con fines de seguimiento y auditoría.	▪Apertura de múltiples sesiones desde un mismo cliente. ▪Cierre de sesiones desde una ventana de browser, manteniendo otras conexiones abiertas. ▪Apertura de sesiones desde distintos clientes, con el mismo usuario. ▪Apertura de sesiones y cierre de aplicaciones sin cerrar sesión. ▪Seguimientos y comprobación de logs mantenidos por el Application Server JBOSS y por logs de transacciones del motor de base de datos.	Se comprobó el correcto funcionamiento de los esquemas de mantenimiento de sesiones. El sistema maneja adecuadamente la apertura de múltiples sesiones y el cierre de conexiones abiertas.
Conexión a la base de datos	Medir la tasa de fallas en intentos de conexión al motor de base de datos y el correcto manejo de excepciones por fallas de conexión.	▪Disparo de múltiples solicitudes de conexión simultáneas. Prueba de volumen. ▪Introducción explícita de errores en los parámetros de conexión para generar excepciones y medir esquemas de tolerancia a fallo. ▪Intentos de conexión cuando el motor de Base de Datos se encuentra fuera de servicio. Control de excepciones. ▪Pruebas de conexión sobre distintos drivers JDBC.	No se detectaron fallas de conexión en condiciones normales de operación del motor de base de datos. Fue exitoso el establecimiento de conexiones concurrentes. Frente a fallas forzadas del motor o los parámetros de conexión se comprobó el correcto disparo, captura y manejo de excepciones por parte de la aplicación.
Manejo de excepcio-	Garantizar el	▪Introducción explícita	Se identificaron puntos de

nes	correcto manejo de errores en el sistema.	de fallas y errores en puntos de control de código y en esquemas operativos de la plataforma, para generar excepciones SQL, excepciones en peticiones al Application Server y excepciones en la construcción de objetos.	control en los módulos ABM de Normas, ABM de Autoridades y ABM de Temas, en los cuáles no se había instrumentado correctamente la captura de excepciones y el manejo de errores. Se corrigió el código y se repitió la corrida de pruebas con resultados exitosos.
Validación de Integridad Referencial	Validar coherencia, consistencia e integridad referencial a nivel de diseño de base de datos.	Se realizaron transacciones sobre el sistema con un conjunto de datos de prueba diseñado específicamente para validar las comprobaciones de integridad que el mismo realiza de acuerdo al Modelo de Entidades y Relaciones planteado. Tales pruebas incluyeron: ▪Intentos de eliminar una autoridad mientras está asociada a alguna norma en el sistema. ▪Intentos de eliminar un cargo mientras existen autoridades vinculadas al cargo. ▪Intentos de eliminar una norma cuando está vinculada a otras normas en el sistema. ▪Intentos de registrar dos personas en un mismo cargo en un mismo período, y en períodos superpuestos de alguna forma. ▪Intentos de almacenar normas con fecha de publicación en el boletín anterior a la	Se identificaron aspectos de la ejecución de querys en cascada sobre las tablas que no habían sido tenidos en cuenta y que afectaban la consistencia de información. Se instrumentaron cambios en el modelo de base de datos y en el código de la aplicación para controlar estas situaciones.

		fecha de emisión. ▪Intentos de eliminar actualizaciones que vinculen normas. ▪Intentos de vincular normas inexistentes. ▪Intentos de eliminar un tema que tiene normas asociadas. ▪Intentos de update con datos faltantes sobre los campos requeridos como obligatorios para una norma, una autoridad, un cargo o un tema. ▪Verificación de funcionamiento sobre procedimientos almacenados	
Mensajes de error y advertencia.	Comprobar la claridad y pertinencia de los mensajes de error y/o advertencia	▪Establecimiento de puntos de control sobre el código de manejo de excepciones. ▪Revisión sobre la sintaxis de mensajes. ▪Corridas de pruebas con conjuntos de datos erróneos para forzar la aparición de mensajes. ▪Ejecución de pruebas aleatorias, para testear el correcto manejo de errores y su identificación mediante mensajes.	Se comprobó la pertinencia en la aparición de mensajes de error y advertencia. Se corrigieron errores de redacción sobre los textos de mensajes para favorecer su correcta interpretación.
Control de concurrencia a nivel de transacciones sobre la Base de Datos	Validar la consistencia de información frente a la ejecución de transacciones concurrentes	▪Seteo del motor de base de datos con distintos modelos de control de concurrencia, según lo propone el estándar ANSI-SQL ▪Disparo de transacciones concurrentes.	La aplicación demostró una gestión consistente de datos bajo el esquema más restrictivo de control de concurrencia (Read Committed Isolation Level), por lo que podemos garantizar un adecuado manejo transaccional de los datos.

		▪Selección del modelo apropiado para garantizar seguridad y consistencia en transacciones concurrentes.	
Edición de formularios de acuerdo a especificaciones del Diccionario de Datos	Comprobar el correcto funcionamiento de la interfase de usuario a nivel de gestión de formularios web.	▪Comprobaciones sobre la correcta selección de opciones y parámetros. ▪Comprobaciones sobre la gestión de parámetros web y su transferencia entre páginas. ▪Validaciones sobre campos nulos. ▪Comprobaciones sobre formatos de fecha, períodos e internacionalización. ▪Verificación de acciones frente a eventos <TAB> <CLICK> <MOUSEOVER> <ONLOAD> <ONFOCUS>	Se identificaron fallas en la programación de eventos <TAB> y <ONFOCUS> y faltas de verificación de campos nulos en algunos formularios. Todas las fallas identificadas fueron adecuadamente corregidas.
Prueba de menús	Comprobar la correcta vinculación de procesos y selección de menús	▪Comprobación puntual de cada acceso, mensajes de guía y titulaciones. ▪Navegación programada de la aplicación por rutas de menús alternativos.	La prueba fue exitosa en todos sus aspectos.

CONSEJO FEDERAL DE INVERSIONES
BIBLIOTECA
Dr Manuel
Belgrano

J. Implementación

Concretada la etapa de pruebas se emprendió la implementación efectiva del repositorio de resoluciones en el ámbito de la Secretaría Administrativa Legal y Técnica.

Implementar un sistema, no implica únicamente instalar el software y capacitar al personal, sino adecuar la estructura organizacional, los procesos administrativos y operativos, los controles, las políticas, los procedimientos y hasta la propia aplicación informática a los cambios que la introducción del nuevo sistema acarrea.

Teniendo en cuenta lo dicho y dadas las características de experiencia piloto que este desarrollo posee, es importante definir los objetivos y alcances de la implantación, por cuanto aportará a la comprensión de las actividades realizadas y su proyección futura.

Objetivo: Ejecutar pruebas de funcionalidad e iniciar el funcionamiento del repositorio digital de normas legales en el ámbito de la Secretaría Administrativa Legal y Técnica.

Alcance: La implementación inicial aspira a la puesta en marcha de la dinámica de sistemas, logrando el mejor impacto sobre las personas y procesos involucrados.

En esta instancia se realizaron las siguientes actividades:

1. ***Definiciones finales sobre la metodología de implementación y puesta en marcha***

Por los alcances legales de los certificados de firma digital involucrados en el proceso y por ser una experiencia preliminar, se decidió en esta instancia, adoptar una metodología de implementación en ***paralelo*** al circuito actual, proyectando

a futuro un abandono gradual del mantenimiento de copias impresas de la norma. Esta forma de implementación, permitirá además medir el impacto de la introducción del nuevo circuito en comparación con las prácticas habituales.

Otro punto fundamental para la implementación implicó decidir cómo se manejaría el archivo histórico de normas y que conjunto de normas se incluirían en el digesto digital en primera instancia. En este sentido se decidió incluir el archivo completo desde el año 2000, digitalizando imágenes de las normas impresas y firmando las imágenes digitales. En fechas anteriores al 2000, solo se incluirán las normas vinculadas a otras normas cargadas al sistema, eventualmente firmadas por un fedatario de copia fiel.

Desde la fecha de inicio de la implementación en adelante, los documentos cargados al sistema serán documentos digitales convertidos a formato PDF (Formato de Documento Portátil) y firmados digitalmente.

Por último se diseñaron los parámetros que constituirían la configuración inicial del repositorio: selección de temas, vínculos posibles, períodos válidos, firmas autorizadas, etc.

2. Asignación de recursos y responsables

Se designaron 2 empleados de la oficina de Despacho dependiente Secretaría Administrativa Legal y Técnica como responsables de la sistematización y carga del repositorio. Estas personas se desempeñaron durante la etapa de implementación, con el soporte permanente del equipo de desarrollo y bajo el control de la Jefa de Despacho y del Secretario Administrativo.

Para el proceso de carga inicial se dispuso de los siguientes recursos, además del servidor donde corre la aplicación.

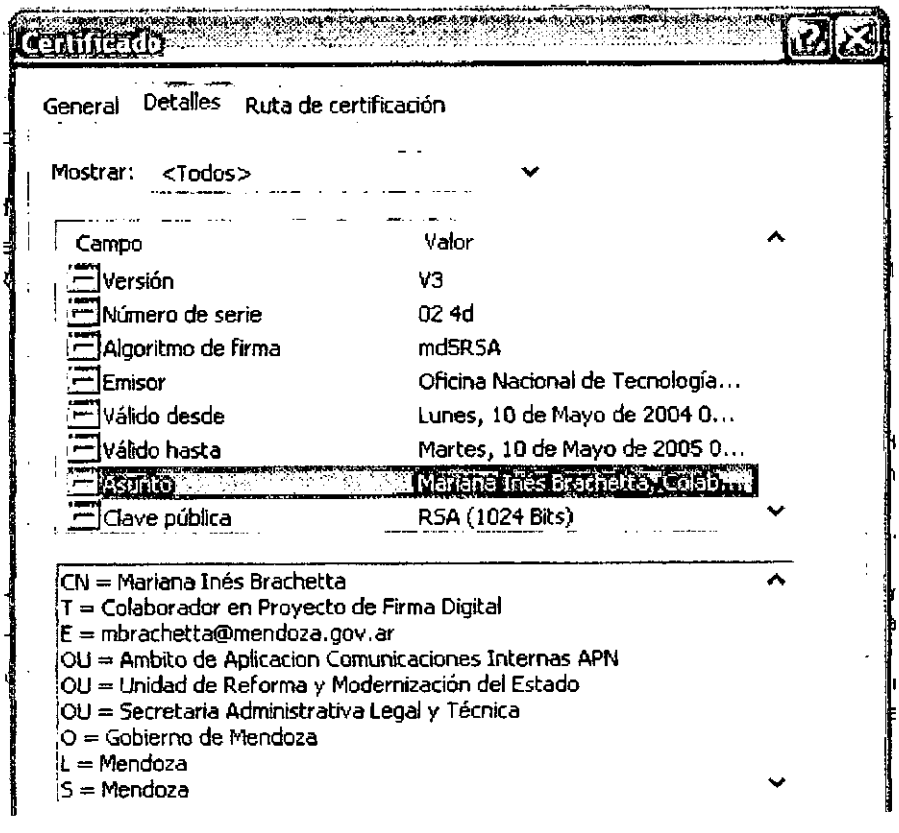
- 2 PC con sistema operativo Windows 98.
- 1 Scanner.
- Certificados Digitales.

- CDs. Para backup.

Este equipamiento no requirió inversión alguna debido a que constituyen recursos de los que dispone la oficina de Despacho.

3. Provisión de Certificados de firma digital a responsables

A través de la Autoridad de Registro de la ONTI, constituida en la Unidad de Reforma y Modernización del Estado, se proveyó de Certificados Digitales con capacidades de firma digital a los responsables de la carga y administración del repositorio, así como también a las autoridades con firma autorizada (Secretario Administrativo, Legal y Técnico - Director de Administración). En esta primera etapa se emitieron 5 certificados digitales a tal efecto. Se adjunta a continuación una imagen del Certificado de Administrador de Sitio.



4. ***Capacitación de responsables***

Se realizó un adiestramiento intensivo de los responsables de acuerdo al plan especificado, tanto en los aspectos operativos del sistema, como en la toma de conciencia sobre la mejora de procesos y principios básicos introducidos por el circuito digital.

5. ***Puesta en marcha del proceso de digitalización, carga del archivo de resoluciones e inicio de la dinámica de sistemas***

Una vez capacitados los responsables se inició el proceso de parametrización inicial del sistema, digitalización de normas y carga preliminar de datos. El esfuerzo en esta etapa, de acuerdo al objetivo de implementación planteado, no radicó en el volumen de datos y documentos sistematizados, sino en la puesta en marcha y ajuste de la dinámica de sistemas, de forma tal de garantizar la continuidad e independencia de su ciclo de vida en el tiempo.

6. ***Soporte continuo y retroalimentación al sistema***

Las etapas de capacitación y puesta en marcha, constituyen en toda implementación oportunidades de prueba funcional del sistema. De estas etapas, se obtiene en general retroalimentación para los diseñadores y desarrolladores, en función de la experiencia que aportan los actores involucrados en su operación y uso.

En nuestro caso particular, la interacción permanente de los expertos del proyecto de firma digital con los responsables designados para la tarea, aportó a: la selección de los parámetros iniciales, cubrir dudas operativas que surgieron durante la etapa de carga inicial y fundamentalmente a identificar necesarios ajustes sobre el desarrollo de la herramienta informática y el circuito operativo.

K. Evaluación de Resultados

Describimos a continuación el sistema de evaluación de resultados que se aplicará al repositorio digital. El modelo reúne un conjunto de indicadores y aspectos observables que permitirán identificar las ventajas comparativas del circuito digital y obtener conclusiones válidas sobre la experiencia.

Es importante señalar que el diseño respeta el enfoque del modelo general de evaluación de resultados, propuesto para el proyecto de firma digital y la infraestructura PKI, con un enfoque particular a los procesos específicos de la presente aplicación.

Este modelo se basa en métricas con las que, razonablemente, se puedan cuantificar las dimensiones que son de nuestro interés.

La siguiente tabla define los indicadores generales utilizados para medir el rendimiento de la aplicación.

Experiencia piloto Repositorio de Normas Legales con firma digital
Instrumento de Evaluación

Indicadores Cualitativos	Métricas y Resultados
Satisfacción de los usuarios: •Temática de reclamos Resistencia al cambio Grado de aceptación de funcionarios •Grado de aceptación del personal de planta •Solicitudes de transferencia tecnológica	
Beneficios diferenciales: •Despapelización •Reducción de gastos en fotocopias •Disponibilidad	

- •Evolución de consultas personales
- •Ahorros de tiempo

Marco legal:

- •Impacto en normativa interna

Alcance:

- •Participación de los sectores relacionados
- •Difusión pública

Indicadores Cuantitativos	Métricas y Resultados
Eficiencia:	
•% de certificados emitidos correctamente	
•Nro. de consultas exitosas / Total de consultas mensuales	
•Nro. de consultas fallidas / Total de consultas mensuales	
•% de fallas de sistema	
•% de interrupciones del servicio	
•Tiempos comparados	
•Ahorros generados	
Asistencia:	
•Número de visitas de soporte mensuales	
•Nivel de reclamos atendidos mensuales	
Uso del Sistema:	
•Cant. de consultas mensuales	
•Cant. de verificaciones de certificación	
•% de utilización de servicios (sobre el total de actores involucrados)	
Calificación ponderada final	
.....	

IV. DISEÑO E IMPLEMENTACIÓN DE UN PLAN DE DIFUSIÓN

A. Identificación de Agentes y Organismos Relacionados

En el ámbito externo relacionado con Tecnología se pretende generar acciones de difusión sobre temas relacionados con la Firma Digital. Resulta de vital importancia para el desarrollo y maduración de la Tecnología, generar espacios comunes y compartidos de trabajo e investigación que dan lugar a la formación de un cúmulo de conocimientos.

Concretamente se han identificado dos instituciones objetivo:

- (UTN) Universidad Tecnológica Nacional
- (ITU) Instituto Tecnológico Universitario

Por otro lado en el ámbito interno se debe profundizar las acciones de difusión y los usos y beneficios de la Tecnología de Firma Digital. Si bien el potencial de alcance de las aplicaciones es muy amplio, hemos identificado ciertas dependencias internas de la Administración Pública que por circunstancias particulares como el grado de utilización de las Tic´s y el tipo de trabajo que realizan resultan más propensas a la adopción de la Tecnología. A continuación se hace una enumeración no excluyente de las dependencias objetivo para este proyecto.

- (DGE) Dirección General de Escuelas
- Ministerio de Justicia y Seguridad
- Ministerio de Gobierno
- Subsecretaría de Desarrollo Social

B. Análisis de Alternativas y Medios de difusión

De la consideración de los medios de difusión que se encuentran al alcance para cumplir con los objetivos de este Plan, proponemos la utilización de los siguientes:

- La pagina oficial del proyecto www.firmadigital.mendoza.gov.ar
- Envío de mails informativos (mailing)
- Realización de eventos

- Reuniones informativas
- Disertaciones

C. Diseño de Iniciativas de Difusión

Página web-Mailing: se prevé el envío masivo de un mail de difusión que invita a navegar la página del proyecto y ofrece la colaboración activa del equipo de firma digital en el desarrollo de aplicaciones o proyectos relacionados:

Asunto: Invitación-Unidad de Reforma

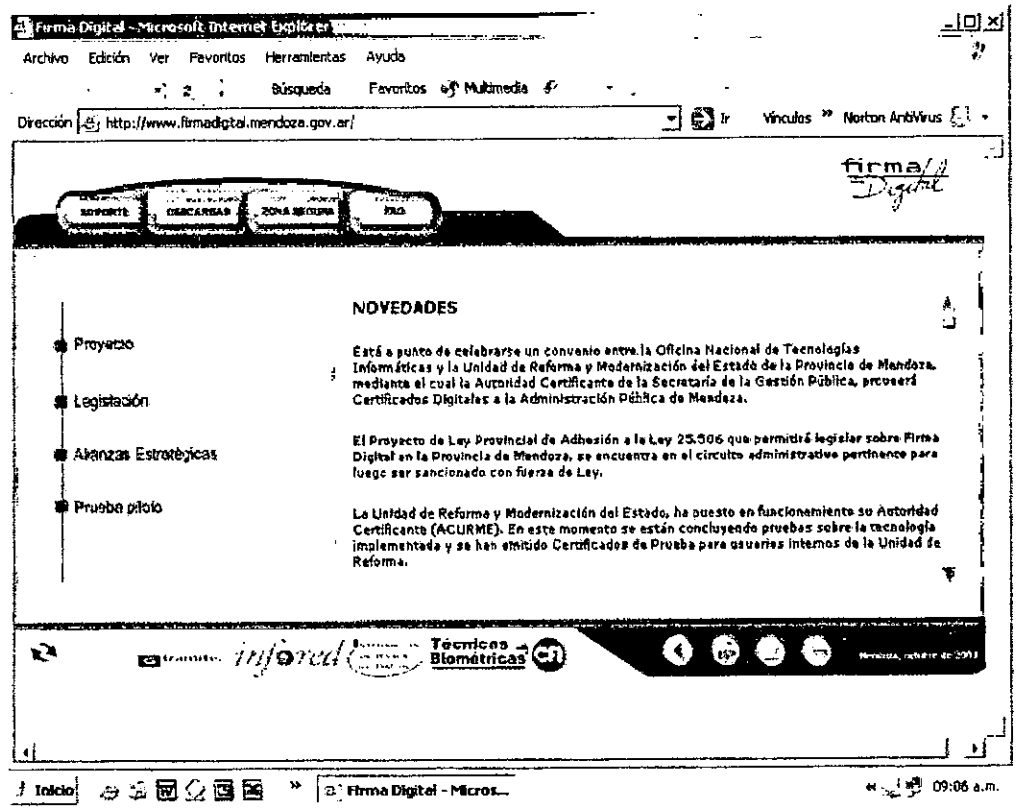
Firma Digital (www.firmadigital.mendoza.gov.ar)

La misión de nuestro proyecto es **difundir y facilitar** el uso de tecnología de firma digital en el ámbito de la Administración Pública Provincial.

En tal sentido, uno de nuestros principales objetivos es prestar **asesoramiento y apoyo** a proyectos relacionados con la tecnología de firma digital.

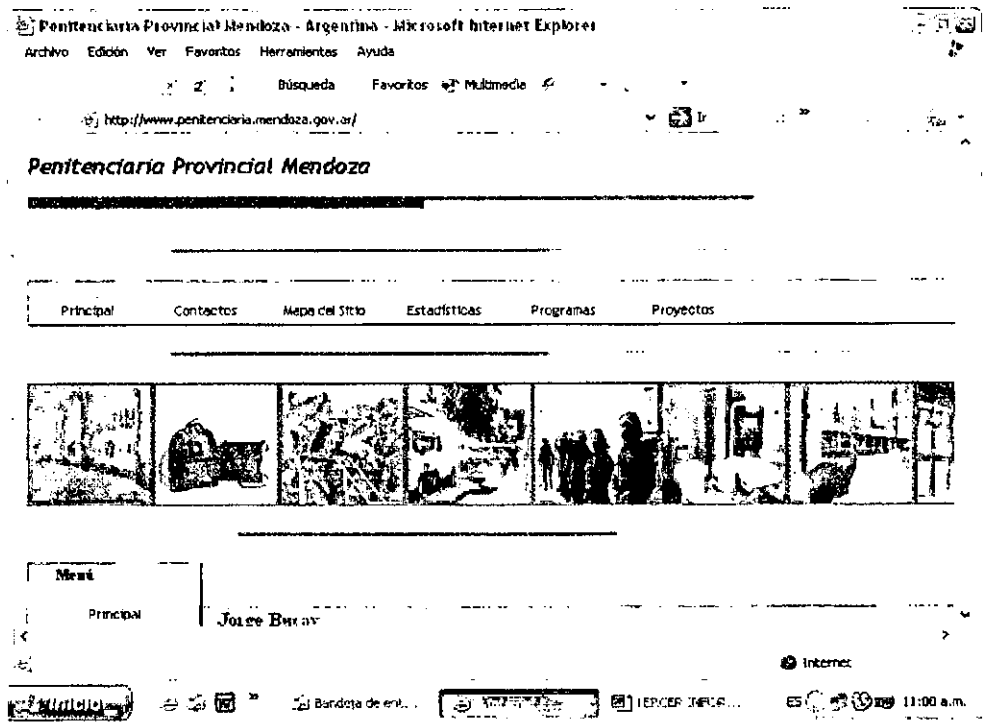
Convencidos de su impacto en los procesos de **despapelización** del Estado, de **reducción de gastos y tiempos** y por ser condición necesaria para asegurar **transparencia y confiabilidad** de cualquier iniciativa de Gobierno Digital lo invitamos a visitar nuestra **página web** www.firmadigital.mendoza.gov.ar, donde usted podrá interiorizarse acerca de esta herramienta y **enviarnos su inquietud o necesidad** de contar con las garantías que la firma digital puede proveer en los circuitos críticos de su repartición

Cabe señalar que nuestra página web cuenta con apartados de información donde el navegante puede interiorizarse en el proyecto y encontrar información relevante sobre el uso de la tecnología de firma digital.

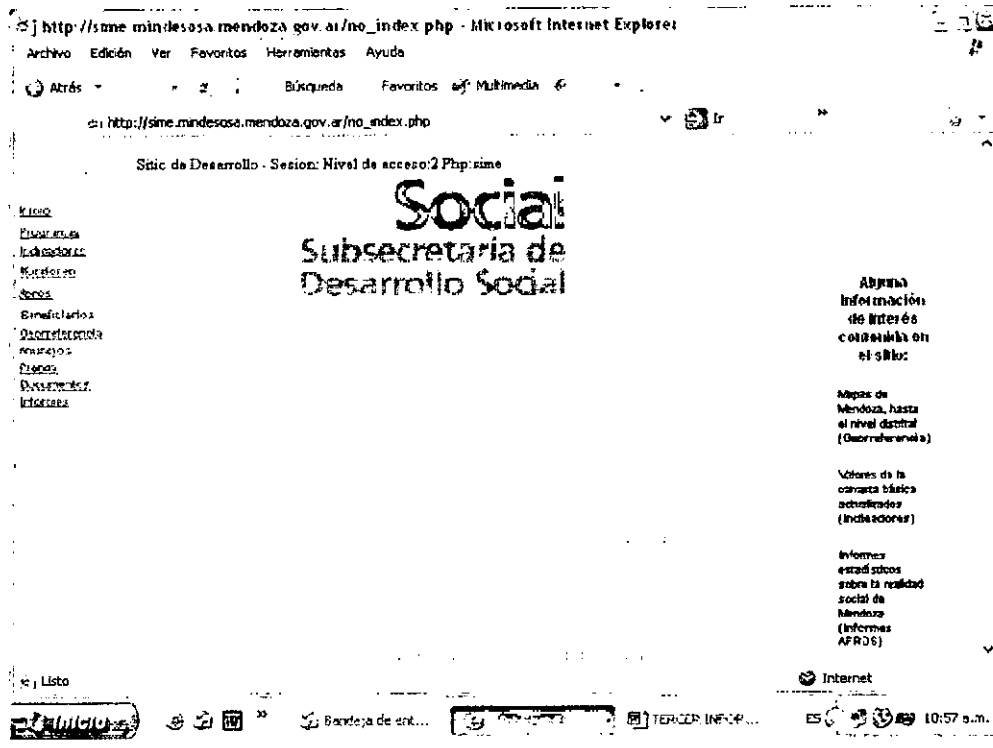


Reuniones Informativas: Se planea la realización de charlas informativas sobre distintos temas con los principales exponentes de las dependencias objetivos señaladas en apartados anteriores, a saber:

- (DGE) Dirección General de Escuelas: se prevé la realización de una reunión informativa sobre el uso de la tecnología con el Director General Lic. Victor Correas
- Ministerio de Justicia y Seguridad: reunión a concertar con el encargado del Área de Cómputos de Penitenciaria Provincial, el Sr Marcelo Lavizari sobre aplicaciones de seguridad basadas en tecnología de firma digital en el Sistema de Mesa de entrada.



- Ministerio de Gobierno: reuniones informativas sobre la experiencia piloto de "Resoluciones" en la Secretaría Administrativa Legal y Técnica con el Subsecretario Dr Claudio Romano y el Director de Administración Sr Adelmo Pesce.
- Subsecretaría de Desarrollo Social: reunión informativa a realizar con los responsables del sitio en la Intranet de gobierno sobre aplicaciones de Sitio Seguro.



- (UTN) Universidad Tecnológica Nacional: se prevé la realización de una reunión con el responsable del área informática el Ing. Luis Borrego

Disertaciones: se realizará una charla teórico-práctica acerca de los fundamentos de la criptografía de clave pública y sus principales usos en el Instituto Tecnológico Universitario (ITU)

D. Puesta en practica de iniciativas

Página web – Mailing: se realizó el envío masivo del mail diseñado en el apartado anterior a todas las cuentas de correo de gobernación con el dominio @mendoza.gov.ar.

Reuniones informativas

- (DGE) Dirección General de Escuelas: se realizó una reunión con el Director General Lic. Victor

Correas en la que se expusieron temas relacionados con la aplicación de tecnologías de Firma digital. Las conclusiones fueron muy satisfactorias, quedando planteada la necesidad concreta de dotar de seguridad a las comunicaciones internas del Ministerio.

- Ministerio de Justicia y Seguridad: se llevo a cabo una reunión con el Área de Cómputos de la Penitenciaría Provincial, en la que se manifestó la voluntad de firmar un convenio de transferencia tecnológica de firma digital para dotar al sistema de mesa de entrada de mayor seguridad.
- Ministerio de Gobierno: se llevaron a cabo reuniones informativas y explicativas sobre el uso de aplicaciones con firma digital en la Dirección de Administración de la Gobernación
- Subsecretaría de desarrollo social: se prevé la realización de nuevas reuniones con ésta dependencia para precisar la necesidad de aplicar sitio seguro al portal o bien diseñar un circuito de actualizaciones por correos firmados digitalmente.
- (UTN) Universidad Tecnológica Nacional: de acuerdo con la petición realizada por el sector de informática de la institución se prevé la realización de charlas informativas sobre firma digital dirigidas al alumnado regular.

Disertaciones:

- Se llevo a cabo una charla informativa dirigida al alumnado del Instituto Tecnológico Universitario, en la primera parte se dieron los fundamentos de la criptografía de clave pública y luego

se realizó un taller práctico en el que se mostró el uso de certificados digitales para firma digital.

A continuación adjuntamos la presentación usada en la charla.

PresentaciónITU.pdf

- Participamos en calidad de expositores en la "Jornada Nacional Interdisciplinaria de Firma Digital y Documento Electrónico" en el Colegio Público de Abogados de la Capital Federal junto a reconocidos expositores en la materia.

A continuación adjuntamos la presentación usada en la charla.

FirmaAbogados.pdf

E. Evaluación de Resultados

Se han recopilado en este apartado y se presentan a continuación, los resultados de la puesta en práctica de las iniciativas de difusión.

Página web – Mailing: ha existido un aumento en el número de navegantes de la página web de firma digital registrado luego del envío masivo de mails de difusión. Así también hemos recibido más consultas sobre temas relacionados con la firma digital de corte tanto técnico, como de aspectos legales. Si bien es una iniciativa que ha dado sus frutos, consideramos que se deben aumentar esfuerzos de difusión en el mismo sentido.

Un ejemplo de tales consultas, es la siguiente solicitud de soporte llenada por el solicitante que se despliega de la solapa de "soporte" de nuestro sitio web:

DATOS DEL SOLICITANTE

==========

Entidad Solicitante: utn regional mendoza

Oficina:

Responsable: José Eduardo Roldán

Contacto Sr./Sra.: José Eduardo Roldán

E-mail de contacto: jercom777@hotmail.com

Telefono: 4486758

NECESIDAD DE SOPORTE

==========

Investigación sobre firma digital

OTROS DATOS

==========

Experiencia previa: ninguna

Medio de vinculacion: web

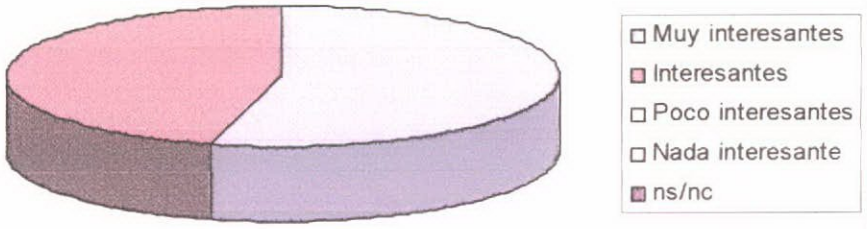
Reuniones informativas

Esta iniciativa de difusión orientada más hacia el ámbito interno de la Administración Pública Provincial ha resultado por demás satisfactoria, ya que, además de lograr los efectos buscados de sensibilización de las dependencias administrativas objetivo, se lograron esbozar posibilidades claras de implementación de la tecnología de firma digital.

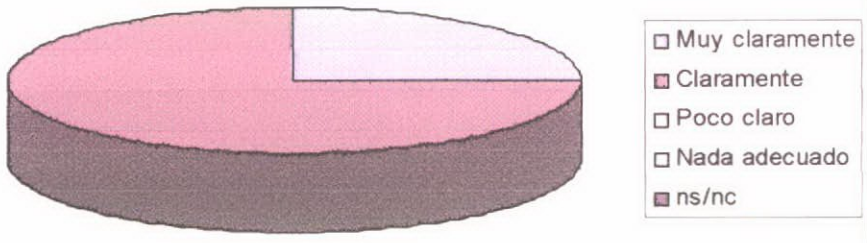
Disertaciones:

Elaboramos un cuestionario evaluativo que repartimos entre los miembros del auditorio del Instituto Tecnológico Universitario y obtuvimos los siguientes resultados:

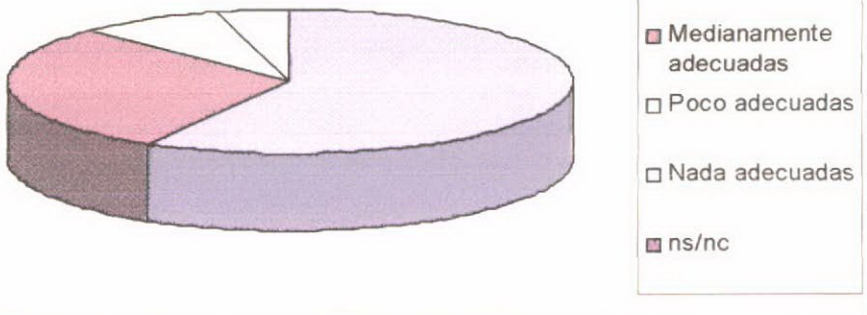
Los contenidos abordados te parecieron....



Consideras que las ideas se explicaron...



El material aportado y las actividades realizadas te parecieron...



Además en auditorio se manifestó muy interesado en profundizar en los siguientes temas:

- Alcances de la garantía de los certificados
- Recibir más información sobre criptografía
- Seguridad y transporte
- Confianza del usuario
- Aplicaciones a nivel usuario
- Sitio seguro

V. Constitución de una Autoridad de Registro Provincial (RA)

A través del convenio de colaboración mutua y transferencia tecnológica firmado con la Oficina Nacional de Tecnologías Informáticas(ONTI), la Unidad de Reforma y Modernización del Estado se ha constituido en Autoridad de Registro Provincial del citado organismo. Dicho título habilita a nuestra oficina a validar la información de requerimientos de certificados digitales que la ONTI emitirá a favor de organismos, funcionarios y agente provinciales. Estos certificados serán utilizados en ciertas aplicaciones locales a definir por el equipo de firma digital de la Provincia de Mendoza.

A. Identificación de la experiencia piloto en la que se usarán los certificados ONTI

Se manifestó que "el escenario y las condiciones particulares de la experiencia en el circuito de resoluciones determinan dos posibilidades de similares características tecnológicas a la hora de tomar una decisión respecto de la provisión de certificados"

- Provisión de certificados por parte de la AC-ONTI (Autoridad Certificante de la Oficina Nacional de Tecnologías Informáticas)

- Provisión de certificados por parte de la AC-URME (Prototipo de Autoridad Certificante de la Unidad de Reforma y Modernización del Estado)

Atendiendo al avanzado grado de desarrollo del Prototipo de Autoridad Certificante de la Unidad de Reforma y Modernización del Estado AC-URME, el equipo del proyecto de firma ha decidido proveer a los usuarios de la experiencia de Resoluciones de cerificados diseñados en función del estándar x.509 v3 y de confiabilidad probada en la implementación de Sitio seguro en la Guía de trámites. Sin embargo, se prevé también, la utilización de certificados emitidos por la AC-ONTI atendiendo a la disponibilidad de los mismos a la fecha de realización del presente informe final.

B. Determinación de Funciones de la RA

Básicamente las funciones a cumplir por una autoridad de registro son las siguientes:

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.

C. Designación de Oficiales de Registro

Los oficiales de registro serán las personas encargadas de llevar a cabo las tareas mencionadas en el apartado anterior.

La designación se llevó a cabo a través de una Resolución de nombramiento de los responsables de la Autoridad de Registro (titular y suplente). **Resolución 71 del 9 de marzo del 2004.**

Dicha resolución fue refrendada por decreto del Gobernador de la Provincia. **Decreto 602 del 12 de abril.**

D. Determinación de Responsabilidades

Se debe poner de manifiesto que el incumplimiento de las obligaciones derivadas de la función asignada a los oficiales de registro genera responsabilidad personal. Por lo tanto los oficiales asumen el compromiso de:

- Dar cumplimiento a los procedimientos establecidos en el convenio y las normas reglamentarias sobre firma digital.
- Mantener el control de sus claves privadas e impedir su divulgación.
- Solicitar la inmediata revocación de sus certificados en caso de compromiso de la clave privada.
- Resguardar el secreto de las claves privada aún en caso de que el certificado se encuentre expirado.
- Solicitar la inmediata revocación de sus certificados en caso de producirse algún cambio en sus situaciones laborales que implique la discontinuidad de la función como Responsable de la Autoridad de Registro.
- Comunicar en forma inmediata y fehaciente a la Autoridad Certificante la desvinculación laboral o funcional con el organismo que me ha designado como Responsable de la Autoridad de Registro.
- Mantener actualizados los certificados emitidos
- Permitir las auditorías y controles necesarios para garantizar la seguridad de la operatoria del sistema.
- Mantener el archivo y resguardo de la información.

Asimismo, firmaron un acuerdo de responsabilidad en el que declararon conocer que toda la información que reciben, administran, almacenen y mantengan bajo su control en relación al desempeño de la función de Responsable de la Autoridad de Registro, reviste el carácter de secreta y se encuentra amparada bajo las leyes 24.766 y 25.326.

Y además que en relación a la citada información, declararon que se encuentran prevenidos respecto de la confidencialidad de la misma, y que deben abstenerse de usarla y revelarla.

E. Diseño de manuales

De acuerdo con lo que dispone el convenio celebrado en su artículo tercero la Provincia debe adherir a lo dispuesto en la Política Certificación y el Manual de Procedimientos de la Autoridad Certificante de la Oficina Nacional de Tecnologías de la Información (Disposición ONTI Nº 5/02), disponible en http://ca.pki.gov.ar/policy.html

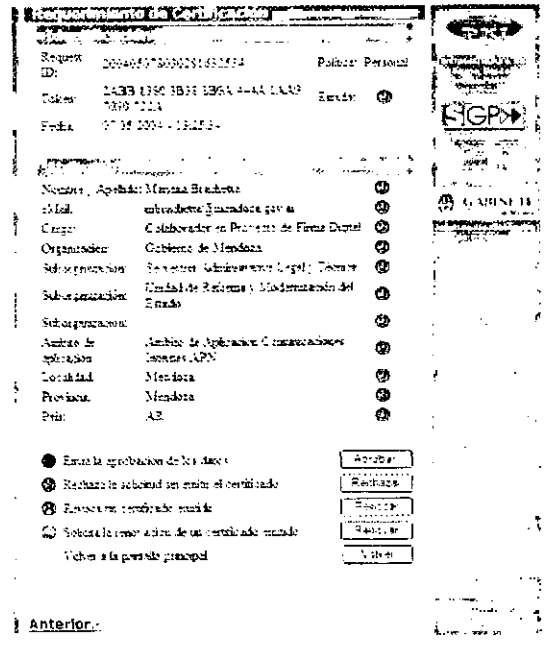
F. Puesta en Marcha de la Autoridad de Registro

A la fecha de presentación de este informe, ya se han dispuesto las acciones para que la Autoridad de Registro se encuentre en pleno funcionamiento. En tal sentido, las pantallas que sostienen tal afirmación se presentan en el siguiente apartado.

G. Administración de la RA

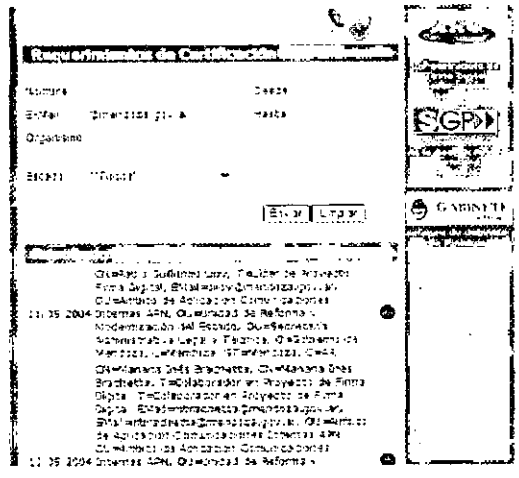
De acuerdo con las responsabilidades definidas para la Autoridad de Registro de Firma digital se están llevando a cabo las actividades propias, a saber:

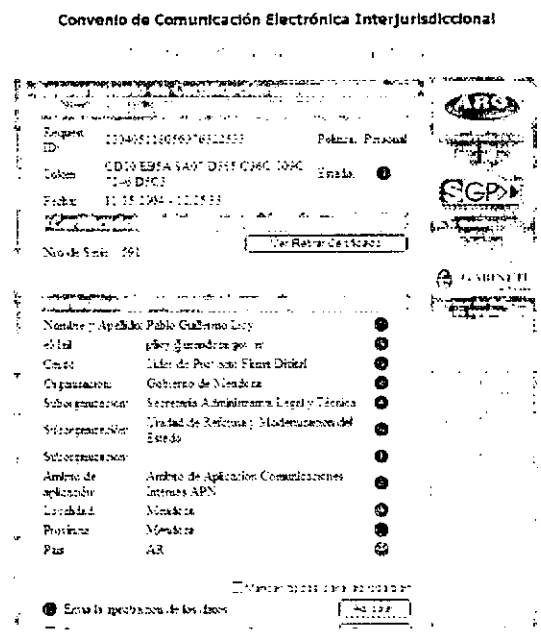
- Recepción de requerimientos de certificados
- Verificación de datos de solicitudes
- Aprobación o rechazo de la solicitud
- Revocación de certificados emitidos
- Renovación de certificados



PKI Firma
DIGITAL

Convenio de Comunicación Electrónica Interjurisdiccional





VI. PARTICIPAR Y PROMOVER LA CREACIÓN Y REFORMULACIÓN DE NORMATIVAS RELACIONADAS:

A. Tareas de seguimiento y allanamiento del proceso de aprobación del proyecto de Ley de Adhesión a la Ley Nacional de Firma Digital

El hecho de que la tecnología de firma digital sea de reciente data, determinada la necesidad de acompañar los cambios legales que propone de una adecuada información sobre sus alcances y utilidades. El equipo de Firma Digital ha desarrollado las siguientes tareas en este sentido:

- **Reuniones con los miembros de la Asesoría General de la Gobernación:** se mantuvieron tres reuniones con la citada dependencia, en donde se explicaron detalladamente los contenidos del proyecto de adhesión y se describieron los alcances y utilidades del proyecto de firma digital. Dichas reuniones desencadenaron la última aprobación necesaria desde el poder

ejecutivo para que el proyecto desembarcara en el poder legislativo.

- **Cámara de Diputados:** se realizaron reuniones con la Comisión de Desarrollo Social en las que se sensibilizó sobre los alcances, utilidades y beneficios de la aplicación de tecnologías de firma digital en la administración pública. A partir de allí el proyecto fue tratado en sesiones de la Cámara de Diputados y se le otorgó la correspondiente media sanción (N° expediente diputados 35936)

- **Cámara de Senadores:** el proyecto fue derivado a la L.A.C Cámara de Asuntos Legislativos, en dónde ya fue aprobado y actualmente ha tomado estado parlamentario a la espera de ser tratado en tablas a instancias de la preferencia otorgada por el cuerpo legislativo (N° de expedientes de senadores 47591)

B. Promoción de decretos desarrollados y propuestos en el proyecto antecedente de Firma Digital

Si bien es condición necesaria la aprobación definitiva, por parte de la Legislatura, del Proyecto de Ley de Adhesión a la Ley Nacional 25.506 para la posterior promulgación de la normativa reglamentaria de la Ley en el ámbito provincial, hemos esbozado aquí un modelo de decreto reglamentario que intentaremos proponer una vez que tal acontecimiento suceda.

VISTO el Decreto N° 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. 5º 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. 2º 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 1º 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 del 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) DÍAS 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 ju-

risdicciones. 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.

C. Promoción y participación en la reformulación de normativas existentes en función de reingenierías de trabajo administrativo provocadas por la aplicación de la nueva tecnología de Firma Digital

Las normativas existentes preparadas para regir en el mundo del papel quedan inevitablemente obsoletas con la aplicación de las nuevas tecnologías de firma digital, éstas contribuyen a la despapelización del Estado y obligan en último término a que las normas afectadas deban reformularse o replantearse desde el punto de vista de un nuevo enfoque. Es por ello que la Unidad de Reforma ha empezado por redefinir su rol en el Estado Provincial a través de un decreto que le otorgue nuevas funciones y represente el marco adecuado para las competencias en materia de firma digital otorgadas por el decreto reglamentario propuesto en el apartado anterior. Transcribimos a continuación los principales artículos del decreto que se encuentra en estado de elaboración:

Artículo 1°: Sustitúyase el nombre de "Unidad de Reforma del Estado", empleado por el Decreto 1778 del 6 de setiembre de 2001, por el de "Unidad de Modernización del Estado".

Artículo 2°: Dispóngase que además de las funciones enumeradas en el art. 3° del decreto 167 del 14 de febrero de 1996, y que fueran transferidas por el

art. 2º del Decreto 1778 del 6 de setiembre de 2001 a la Unidad de Reforma del Estado, ahora Unidad de Modernización del Estado, ésta tendrá las siguiente: Proyectar y promover la Modernización administrativa del Estado Provincial a través de la incorporación de las nuevas Tecnologías de la Información y Comunicación, priorizando la eficiencia, calidad y transparencia de los servicios que presta el Estado a los ciudadanos.

VII. IDENTIFICACIÓN NUEVOS ÁMBITOS DE APLICACIÓN DE LA TECNOLOGÍA DE FIRMA DIGITAL:

A. Aplicación y enriquecimiento de la estrategia de Identificación de Procedimientos aptos

A partir de la aplicación de nuestra estrategia de identificación de procedimientos, con el objeto de elegir y priorizar los circuitos administrativos adecuados para implementaciones piloto, no sólo hemos logrado identificar nuevas propuestas de implementación (presentadas al final del informe) sino que también hemos enriquecido y mejorado los criterios que conforman la estrategia. A continuación presentamos dichos avances conceptuales:

Estrategia para la Identificación de Procedimientos Aptos

Casi cualquier tipo 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

Guías de aplicación

- Transacciones electrónicas: la administración pública provincial puede expandir la prestación de sus servicios y acercarse al

ciudadano a través de transacciones electrónicas seguras. Cuando dichas transacciones revisten características particulares de importancia se puede estimular la aplicación de las tecnologías de firma digital para evitar sobrecostos o generar ahorros fomentando la transparencia en el accionar público.

- Privacidad, integridad y autenticación de la información: la administración pública quiere utilizar Internet como un canal de comunicaciones entre sus ministerios o dependencias, o entre ella y sus administrados en la prestación de los servicios públicos. Tales comunicaciones pueden estar en variedad de formas tales como correo electrónico, normativa interna, documentos, trámites, declaraciones juradas y, es muy frecuente que contengan información confidencial y con propiedad intelectual. Lograr que tales comunicaciones no se encuentren expuestas a falsificaciones o adulteraciones es una cuestión de alta prioridad.
- Ahorros y reducción de tiempos en el trabajo de oficina: la administración pública debe procesar documentos firmados y luego archivarlos por un período de tiempo extendido para satisfacer las disposiciones legales. Con la finalidad de reducir los costos de almacenamiento, soporte, procesamiento y archivo del trabajo de oficina resulta deseable reemplazar los documentos firmados en forma hológrafa con documentos firmados digitalmente.

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 sensible
- Circuitos que requieran de técnicas de firma única o reducida, es decir, aquellos que manejen gran cantidad de contraseñas a cambio de autenticar individualmente cada aplicación, se autentica un almacén de credenciales y se suministran las credenciales correctas para cada aplicación.

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 encriptadas

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

Tales pautas son 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, para fijar estos criterios, 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.

B. Creación de espacios de documentación y respuesta a las necesidades de aplicación de la tecnología desde la propia demanda local

Con el desarrollo del sitio web del proyecto de Firma Digital, disponible para consulta e interacción en www.firmadigital.mendoza.gov.ar, se da a los navegantes la posibilidad de contar con toda la información acerca del **Proyecto**, la **Legislación** sobre la materia, las **Alianzas estratégicas** desarrolladas y los contenidos explicativos de las **pruebas pilotos**.

Complementando dicha información nos gustaría destacar el apartado de **preguntas frecuentes** y conceptos básicos, un repositorio con **descargas de interés** y por último la posibilidad de pedir asesoramiento especializado y apoyo en la **zona de soporte.**

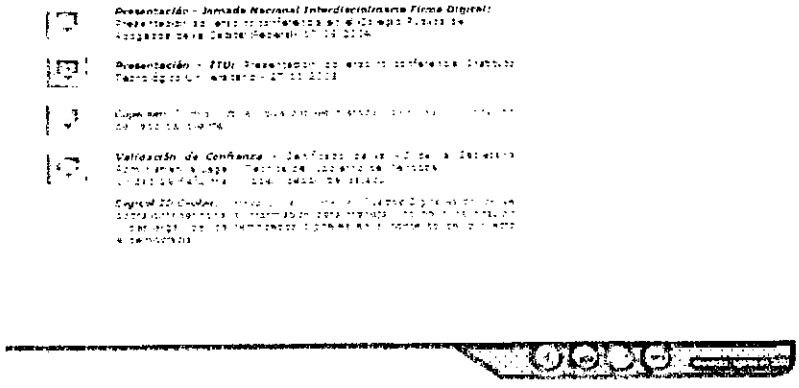
Preguntas frecuentes

PREGUNTAS FRECUENTES

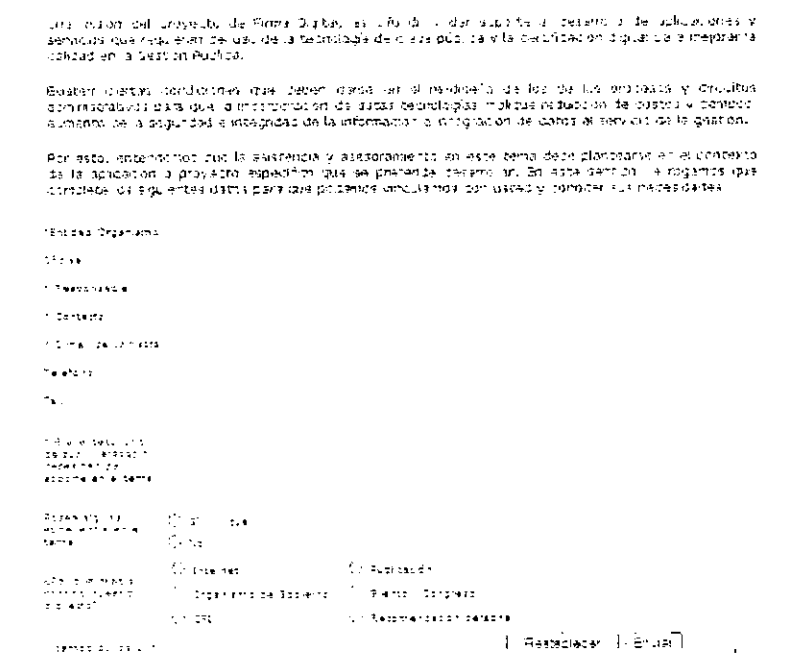
- ¿Qué es una firma digital?
- ¿En qué casos la FD puede reemplazar a la firma manuscrita?
- ¿Hay firmas digitales en la Argentina?
- ¿Es lo mismo firma digital y firma electrónica?
- ¿La firma electrónica reemplaza la firma manuscrita igual que la firma digital?
- ¿Podré hacer un contrato de alquiler de inmueble con firma digital?
- ¿Comete delito quien falsifica un documento digital?
- ¿Como firmo un correo electrónico?
- ¿La firma digital es una password?
- ¿Dónde residen la clave pública y la privada?
- ¿Cómo se ve una firma digital?
- ¿Firmar digitalmente un archivo es encriptarlo?
- ¿Como encripto la información que va en un correo electrónico?
- ¿Qué es un Certificado Digital?
- ¿Donde se almacenan los certificados digitales?
- ¿Qué es una Autoridad de Certificación?
- ¿Qué es una Autoridad de Certificación raíz?
- ¿Qué es una Autoridad de Registro?
- ¿Cómo puedo conseguir el certificado digital de otra persona?
- ¿Qué es una Lista de Certificados Revocados (CRL)?
- ¿Que es una Infraestructura de Clave Pública (PKI)?
- ¿Qué es la criptografía?
- ¿Que es una clave?
- ¿Qué es una Firma Electrónica?
- ¿Qué tipo de claves se emplean para realizar firmas electrónicas?
- ¿Como puedo ver una firma?
- ¿Puedo enviar mi firma sin peligro de que la copien para suplantarme?
- ¿Donde se guarda mi clave privada?
- ¿Como se protege mi clave privada?
- ¿Que garantías técnicas proporciona la firma electrónica?
- ¿Como puedo garantizar la confidencialidad?

Descargas de interés

DESCARGAS



Soporte especializado



C. Formulación de nuevas propuestas de implementación de experiencias piloto

Propuesta de implementación de sitio seguro

Gracias a la experiencia realizada en la guía de trámites, a través de nuestro plan de difusión y del espacio creado para brindar soporte a las dependencias de la Administración Pública Provincial que requieran la aplicación de tecnologías de firma digital, actualmente, estudiamos la posibilidad de aplicar Sitio seguro con autenticación de clientes en el sistema de mesa de entrada de la intranet de la Penitenciaría Provincial de Mendoza.

Sometimos el proyecto a consideración de nuestra estrategia para la identificación de procedimientos aptos y arrojó los siguientes resultados:

Guías de Aplicación

- Privacidad, integridad y autenticación de la información: la implementación de Sitio Seguro en la Penitenciaría sigue la línea de esta guía de aplicación ya que vendrá a proveer de seguridad en las comunicaciones internas y a otorgar garantías de integridad y confidencialidad a la información que viaja por la red.

Criterios de selección de circuitos administrativos

- Circuitos que requieren autenticación de las partes involucradas: en efecto la aplicación desitio seguro prevé la autenticación de usuarios como condición necesaria para permitir el acceso a información sensible sólo a aquellas personas autorizadas

Criterios de selección de transacciones aptas para ser encriptadas

- Aquellas que contengan información estrictamente confidencial: este es el caso de gran parte de la información web que circula por la Intranet de la Penitenciaría, la consulta y actualización de la información contenida en documentos tales como

los prontuarios de los reclusos exige la encriptación de los canales de comunicación que la transporten para evitar cualquier tipo de alteraciones o falsificaciones.

Propuesta de implementación de Correo Seguro

Otro de los proyectos que surgieron del Plan de Difusión implementado y de los espacios creados para el soporte especializado es el de la implementación de Correo Electrónico Seguro en el ámbito de los procesos de comunicación interna y transferencia de datos del sistema de planta funcional de recursos humanos de la DGE (Dirección General de Escuelas)

Nuevamente sometimos el proyecto de implementación a nuestra estrategia y obtuvimos los siguientes resultados:

Guías de aplicación

- Privacidad, integridad y autenticación de la información: la comunicación de información es parte del alcance de esta guía de aplicación toda vez que resulte necesario proveer de garantías tales como integridad y autoría de los datos que alimentan el sistema de planta funcional de recursos humanos de la DGE.
- Ahorros y reducción de tiempos en el trabajo de oficina: esta guía es aplicable a la aplicación en particular ya que creemos que una adecuada implementación del sistema de Correo Seguro sobre el circuito ahorraría tiempos y costos de traslado de información que actualmente se realizan en forma manual

Criterios de selección de circuitos administrativos

- Trámites con alta frecuencia de repetición a cargo de la misma oficina: es el caso de sistema de planta funcional de recursos humanos de la DGE que se encuentra centralizado en Casa de

Gobierno y que recibe información del personal desde sus delegaciones con periodicidad

- Circuitos que requieren autenticación de las partes involucradas: resulta altamente deseable conocer fehacientemente el origen de los datos que se reciben por exigencias en la calidad de la información a procesar.
- Circuitos administrativos que enlazan importantes distancias geográficas: esta característica viene dada en este caso por la importante dispersión geográfica de las delegaciones que proveen entradas de información al sistema.
- Circuitos administrativos de transferencia de información sensible: datos como las altas y bajas, presentismo, asistencias y licencias del personal revisten la característica de información sensible y deben ser tratados con las garantías que provee la tecnología de firma digital.

Criterios de transacciones aptas para ser firmadas digitalmente

- Aquellas que requieren efectiva autenticación de personas o entes involucrados en la transacción: nuevamente aquí debemos destacar que las exigencias de autenticidad y origen de la información transferida desde las delegaciones al sistema central de planta funcional de recursos humanos de la DGE debe hacerse mediante correos firmados digitalmente.

Criterio de selección de transacciones aptas para ser encriptadas

- Aquellas que contengan información estrictamente confidencial: como se vio anteriormente el tipo de datos que se transfieren desde las delegaciones y su característica de información sensible implica la necesidad de utilizar técnicas de encripción de correo que nos permitan asegurar su integridad al momento de la recepción.

Las propuestas anteriormente plasmadas se presentan como serias candidatas a la futura realización de implementaciones piloto de firma digital, cabe señalar que, de concretarse, las precisiones y los alcances particulares de las mismas serán oportunamente definidos cuando se defina la continuidad de nuestro proyecto.