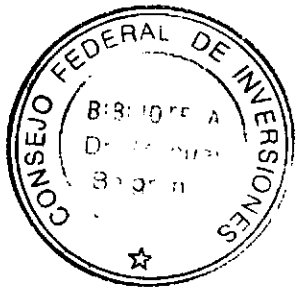
GOBIERNO DE MENDOZA

SECRETARÍA ADMINISTRATIVA LEGAL Y TÉCNICA

UNIDAD DE REFORMA DEL ESTADO

SEGUNDO INFORME PARCIAL



CONSEJO FEDERAL DE INVERSIONES

CONSULTOR: LIC. PABLO GUILLERMO LIOY

Fecha de impresión 28/04/2004 12:29

ÍNDICE

I. INTRODUCCIÓN

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

Actividad	Estado
2. Implementación de un prototipo de PKI	Concluido
Tareas	
• 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 pre-establecidas en el Estudio de Factibilidad para una PKI de pequeña escala.	Concluido
• Documentación del diseño prototipado.	Concluido
• 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.	Concluido
• Diseño de un Plan de Pruebas y ejecución	Concluido
• Evaluación de resultados.	Concluido
• Desarrollo de políticas de certificación específicas en función de las experiencias piloto implementadas	Concluido
• Desarrollo de manual de funciones y procedimientos para la gestión del CVS de los Certificados y la administración de las experien-	Concluido

cias piloto implementadas	
• Análisis de normas técnicas y estándares internacionales de licenciamiento de Autoridades Certificantes	Concluido
Actividad	**Estado**
3. Implementación de experiencia piloto en el Circuito de Resoluciones	Avance
Tareas	
• Desarrollo: desarrollo de aplicaciones informáticas que sustenten el archivo y gestión digital de resoluciones y la firma digital de las mismas	Concluido
Actividad	**Estado**
4. Diseño e implementación de un Plan de Difusión:	Avance
• Identificación de Agentes y Organismos relacionados	Concluido
• Análisis de Alternativas y medios de difusión	Concluido
• Diseño de iniciativas de difusión	Concluido
Actividad	**Estado**
5. Diseño e implementación de un Plan de Difusión:	Avance
• Identificación de experiencia piloto en la que se usarán los certificados de la ONTI	Concluido
• Determinación de Funciones de la RA	Concluido
• Designación de Oficiales de Registro	Concluido
• Determinación de Responsabilidades	Concluido

SEGUNDO INFORME DE PARCIAL: la culminación de la actividad 2 y el avance de la actividad 3,4 y 5 se presentará a los seis meses de iniciadas las tareas.

II. IMPLEMENTACIÓN DE UN PROTOTIPO PKI

A. Desarrollo del Prototipo AC-URME

En el informe precedente documentamos el avance realizado en el desarrollo del prototipo AC-URME en relación a los objetivos planteados para el mismo. En particular, se expusieron las tareas vinculadas a la:

- definición de un contexto para incorporar los desarrollos AC-URME
- construcción de los Profiles de Certificados.

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. Las siguientes fichas documentan la información mantenida sobre suscriptores.

Entidad Final

Username	tramite
End Entity Profile	Certificado de Servidor
Subject DN Fields	
CN, Common Name	www.tramite.mendoza.gov.ar
OU, Organization Unit	Unidad de Reforma y Modernizacion del Estado
OU, Organization Unit	Secretaria Administrativa Legal y Tecnica
OU, Organization Unit	
O, Organization	Gobierno de Mendoza
L, City	Capital
ST, State or Province:	Mendoza
DC, Domain Component	www.tramite.mendoza.gov.ar
C, Country	AR
Email	unidadreforma@mendoza.gov.ar
Certificate Profile	SERVIDOR
Token	PEM file
Created	10/24/03 11:22 AM
Modified	10/28/03 2:16 PM
Status	Generated

Entidad Final

Username prueba1
End Entity Profile Personal
Subject DN Fields
E, EmailAddress in DN prueba@mendoza.gov.ar
CN, Common Name Prueba de CRL
T, Title Ing.
OU, Organization Unit Gobierno de Mendoza
OU, Organization Unit Unidad de Mod. del Estado
OU, Organization Unit Firma Digital
O, Organization Gobierno
L, City Ciudad
ST, State or Province: Mendoza
DC, Domain Component www.reforma.mendoza.gov.ar
C, Country AR

Email prueba@mendoza.gov.ar
Certificate Profile prueba
Token Browser Generated

Created 3/1/04 5:12 PM
Modified 3/1/04 5:22 PM
Status Revoked

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.

La imagen que sigue ilustra los elementos básicos de un Certificado de Usuario Final emitido por el prototipo AC-URME.

Certificado de Usuario Final

Username	marianab
Certificate nr	1 of 1
Certificate Version	X509 V.3
Certificate Serial Number	18927CF68FD2F012
Issuer DN	CN=AC-URME Autoridad Certificante Unidad de Modernizacion del Estado Gobierno de Mendoza,OU=Unidad de Reforma y Modernizaci Estado,OU=Secretaria Administrativa Legal y Te Gobierno de Mendoza,O=Gobierno de Mendoza,
Valid from	9/9/03
Valid to	9/8/05
Subject DN	CN=Mariana Brachetta,OU=Direccion General de Escuelas,OU=Portal Educativo,O=Gobierno de Mendoza,L=Ciudad,C=AR
Public key	RSA (1024Bits)
Basic constraints	End Entity
Key usage	Digital Signature, Key encipherment
Signature Algorithm	SHA1WithRSAEncryption
Fingerprint SHA1	C782C39BD28EBE181A20401C034B13E9BE33
Fingerprint MD5	EBA68A516E20C8C5CB3BF4A34A3E95C3
Revoked	No

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

Revocación de Certificados

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.

Lo siguiente constituye una imagen de una CRL de prueba emitida por el prototipo AC-URME.

General Lista de revocaciones

Información de la lista de revocación de certificados

Campo	Valor
Versión	V2
Emisor	AR, Gobierno de Mendoza, Secret...
Fecha efectiva	Miércoles, 21 de Abril de 2004 02:...
Próxima actualización	Jueves, 22 de Abril de 2004 02:16...
Algoritmo de firma	sha1RSA
Identificador de cla...	Id. de clave=96 36 53 fb 6c e9 59...
Número CRL	7

Valor:

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 Modernizacion del Estado Gobierno de Mendoza

General Lista de revocaciones

Certificados revocados:

Número de serie	Fecha de revocación
01 63 89 60 99 35 22 05	Viernes, 24 de Octubre ...
0c 4b a2 84 7a 31 d7 3e	Martes, 28 de Octubre ...
26 d6 1b 1a 3c 94 95 da	Viernes, 24 de Octubre ...
40 e3 e4 73 a0 9f 63 d2	Viernes, 24 de Octubre ...
31 be 8f ca 01 be bf 36	Viernes, 24 de Octubre ...

Entrada de revocación

Campo	Valor
Número de serie	40 e3 e4 73 a0 9f 63 d2
Fecha de revocación	Viernes, 24 de Octubre de 2003 10:...
Código de razón de l...	La afiliación ha cambiado (3)

Valor:

B. Documentación del diseño prototipado

Se estableció previamente que la documentación de diseño de una Autoridad Certificante debe contemplar los siguientes aspectos fundamentales:

1. Diseño de la Política de Certificación – que regulará la emisión y gestión de Certificados
2. Diseño detallado del contenido de los Certificados – de acuerdo a criterios establecidos en la Política
3. Diseño del la CRL
4. Diseño de Procedimientos para gestionar el CVS de los Certificados emitidos

La Política de Certificación y el Diseño de Procedimientos para el prototipo AC-URME, han sido tratados en apartados específicos dentro del proyecto. En el informe anterior se documentó el diseño detallado del contenido de los certificados.

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.

ESPECIFICACIONES DE DISEÑO DE la Lista de Certificados Revocados - CRL

Se incluirán en la CRL del prototipo AC-URME los siguientes campos:

Formato Básico

CAMPO	DESCRIPCION	CONTENIDO CRL AC-URME
version	Describe la versión de la CRL. DEBE tener el valor 1 (correspondiente a la versión 2 del estándar X509).	1
signatureAlgorithm	DEBE contener el identificador de objeto (OID) del algoritmo usado para firmar la CRL. Este identificador define el tipo de función hash y el algoritmo de firma utilizado y DEBE ser alguno de los definidos en el RFC3279.	Sha1RSA -- OID for RSA signature generated with SHA-1 hash sha1WithRSAEncryption OBJECT IDENTIFIER ::={pkcs-1 5}
issuer	El campo "issuer" identifica a la entidad que firma y emite la CRL. El emisor se especifica utilizando un subconjunto de los siguientes atributos: DC domainComponent C countryName S stateOrProvinceName O organizationName L localityName	DC = www.firmadigital.mendoza.gov.ar C = AR (Según ISO3166-1 es Argentina) S = AR-M (Según ISO3166-2 es Mendoza en Argentina) L = Capital 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

CAMPO	DESCRIPCION	CONTENIDO CRL AC-URME
	SN SerialNumber	Modernizacion del Estado Gobierno de Mendoza SN = Número de Serie
thisUpdate	Indica la fecha de emisión de la CRL. Cualquier certificado revocado incluido en la lista debe tener una fecha de revocación anterior a este valor.	Cualquier fecha válida emitida por el sistema en formato UTC-Time o GeneralizadTime Ej: Miércoles, 21 de Abril de 2004 02:16:46 p.m.
nextUpdate	Indica la fecha límite de emisión de la próxima CRL. Este campo DEBE estar presente en todas las CRL emitidas.	Cualquier fecha válida emitida por el sistema en formato UTC-Time o GeneralizadTime, que corresponda a 24 hs. posteriores a la fecha consignada en el campo thisupdate Ej.:Jueves, 22 de Abril de 2004 02:16:46 p.m.
revokedCertificates	Contiene la lista de certificados revocados indicados por su número de serie, incluyendo extensiones específicas para cada entrada de esta lista.	

Extensiones de una CRL

EXTENSION	DESCRIPCION	CONTENIDO CRL AC-URME
Authority Key Identifier	Proporciona un mecanismo para identificar unívocamente la clave pública correspondiente a la clave privada utilizada para firmar la CRL. 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. 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	Para todos las CRLs emitidas por la AC-URME 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.

EXTENSION	DESCRIPCION	CONTENIDO CRL AC-URME
	este mecanismo en la AC-URME.	
IssuerAlternativeName	Permite asociar identidades estilo Internet al emisor de la CRL. Las opciones definidas incluyen una dirección del correo electrónico, un nombre DNS, una dirección IP, y un identificador uniforme de recurso (URI).	Se completará con datos alternativos cuando sea necesario en el contexto de una aplicación particular. Ej.: www.firmadigital.mendoza.gov.ar
CRLNumber	Contiene un número de secuencia creciente para una CRL y emisor dado. Esta extensión permite que los usuarios determinen fácilmente cuando una CRL particular reemplaza otra anterior. Esta extensión DEBE estar incluida en todos los certificados.	Entero Positivo. Ej.: 1, 2, 3, 4, 5, 6, 7
IssuingDistributionPoint	Identifica el punto de distribución y el alcance de una CRL particular. Indica, por ejemplo, si la CRL cubre la revocación de certificados de entidad final solamente, certificados del Certificador solamente, etc. De existir esta extensión DEBE ser crítica.	El uso de esta extensión no se implementará en el prototipo AC-URME

EXTENSION	DESCRIPCION	CONTENIDO CRL AC-URME
FreshestCRL	Freshest CRL (Delta CRL Distribution Point) indica dónde puede obtenerse la información de la "delta CRL" de una CRL completa.Esta extensión NO DEBE ser crítica.	El uso de esta extensión no se implementará en el prototipo AC-URME

Extensiones de una entrada de la lista "Revoked Certificates"

EXTENSION	DESCRIPCION
Reason Code	Indica la razón de revocación de una entrada de la CRL. Los motivos que se pueden consignar son: • Pérdida del soporte del certificado y claves • Posible compromiso de la clave • Abandono del puesto de trabajo • Errores graves en información del certificado • Cambio de datos fundamentales • Otros.
Hold Instruction Code	Indica la acción a seguir al encontrar un certificado suspendido (estado "*hold*"). Las aplicaciones que encuentren un código "*id-holdinstruction-callissuer*" DEBEN llamar al emisor del certificado o rechazarlo. Las aplicaciones que encuentren un código "*id-holdinstruction-reject*" DEBEN rechazar el certificado.
Invalidity Date	Indica la fecha en la cual se sabe o se sospecha que la clave privada fue comprometida o que el certificado pasó a ser inválido.

Certificate Issuer	Identifica al emisor del certificado asociado con una entrada en una CRL indirecta, es decir una CRL que tenga el indicador "indirectCRL" en su extensión "IssuingDistributionPoint" Esta extensión DEBE ser crítica.

C. Diseño 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:

1. Instalación del Certificado raíz de la jerarquía, certificado de la AC-URME.
2. Aceptación del acuerdo del suscriptor.
3. Llenado y envío del formulario de Solicitud de Certificado.
4. Recepción de la confirmación de "Recepción de Solicitud"
5. Recepción del "Mail de Verificación" de solicitud.
6. Confirmación por respuesta del "Mail de verificación".
7. Acreditación de identidad
8. Recepción del Mail de Notificación de emisión de certificado
9. 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.

D. Diseño y ejecución de un Plan de Pruebas

Documentamos a continuación el ***Conjunto de Pruebas*** al que fue sometido el protitpo 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	Evaluar flexibilidad del software PKI para trabajar con distintos repositorios	▪ Se configuró el software PKI para operar con MySQL, Hypersonic y PostgreSQL. ▪ Bajo cada una de estas con-	El software operó correctamente con los tres motores de base de datos. Se decidió la implementación final sobre

Descripción de la Prueba	Objetivo de la Prueba	Ejecución de la Prueba	Resultados/Conclusiones
emitidios y CRLs.	de Certificados	figuraciones se corrió un 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.	PostreSQL por sus características de seguridad y administración de grandes volúmenes de datos.
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

Descripción de la Prueba	Objetivo de la Prueba	Ejecución de la Prueba	Resultados/Conclusiones
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 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.	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.
Testear formatos de exportación de certificados soportados (PKCS12 , PEM, JKS)	Evaluar características de interoperabilidad del prototipo	Se emitieron 6 certificados de prueba, con datos ficticios: • 3 Certificados SSL, en for-	Todas las pruebas de uso y conversión entre formatos de representación de Certificados tuvieron resultados satisfactorios. No obstante se recomienda siempre que

Descripción de la Prueba	Objetivo de la Prueba	Ejecución de la Prueba	Resultados/Conclusiones
		matos 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 entre formatos de certificados con funciones de php-openssl y con librerías java.	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
		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	Los certificados fueron en su totalidad, correctamente emitidos. Las transacciones asociadas fueron debi-

Descripción de la Prueba	Objetivo de la Prueba	Ejecución de la Prueba	Resultados/Conclusiones
		proceso batch, haciendo uso del script provisto a tal efecto.	damente registradas en la base de datos y en los logs 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	Medir ajuste del prototipo	Se intentó la configura-	El prototipo soporta la emisión directa de

Descripción de la Prueba	Objetivo de la Prueba	Ejecución de la Prueba	Resultados/Conclusiones
Certificados con distintos algoritmos de firma md5withRSAEncryption, Sha1RSA y otros contemplados en la RFC3279.	a las especificaciones de diseño planteadas para el perfil de Certificados y la Política de Certificación. Evaluar características de interoperabilidad del prototipo.	ción de profiles para la emisión de certificados con distintos algoritmos de firma: • Sha1 with RSA Encryption • Md5withRSAEncrytpion	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 Certificados emitidos.	Evaluar seguridad en el comportamiento de los Certificados emitidos de acuerdo a la Política de Certificación.	Se realizaron pruebas de: 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.	Ambos intentos emitieron el mensaje de advertencia y error esperado.

Segundo [illegible]

Descripción de la Prueba	Objetivo de la Prueba	Ejecución de la Prueba	Resultados/Conclusiones

E. 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

.....

F. 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 INTRODUCCION

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

auditoría 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 auditoría 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 presta-

dores 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 IDENTIFICACION Y AUTENTICACION

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 polí-

ticas 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 articulo 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 periodo 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 TECNICA

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 ≥ 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"

G. 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:

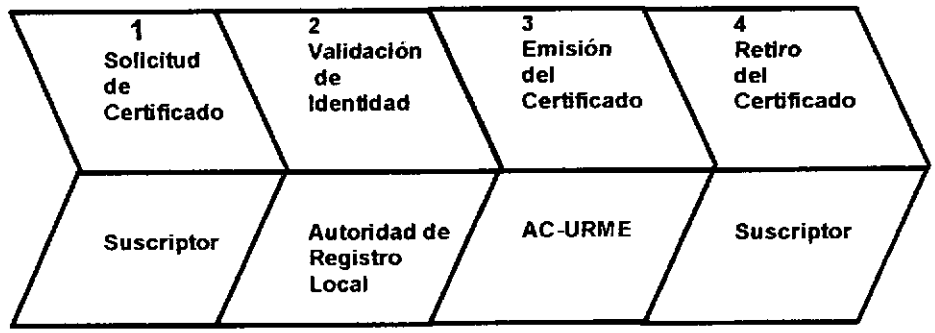
Los siguientes procedimientos describen el conjunto de pasos realizados por la Autoridad Certificante de la Administración Pública de la Provincia de Mendoza cuyas funciones son ejercidas por la Unidad de Reforma y Modernización del Estado de la Secretaría Administrativa Legal y Técnica de la Gobernación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

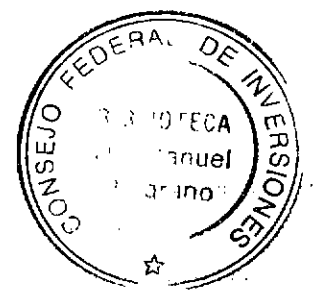
3. ***Suscriptor:*** recibe el mail y lo responde confirmando su efectiva recepción

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 identi-

ficatorios *(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 No-

ta 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 so-

licitud 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.)"

H. 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 do-

cumentos 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 los siguientes aportes:

Comentarios y aportes ONTI

Documento:	Requisitos Mínimos para Políticas de Certificación Borrador v1.1
Artículo:	1.3.- Participantes y aplicabilidad
Comentario de:	Adición
Redacción propuesta:	Se incluirán las distintas entidades que cumplen roles con relación al certificado y cuya integración se encuentre prevista para el cumplimiento de la actividad de certificación. Se incluirán las distintas entidades que cumplen roles con relación al certificado y cuya integración se encuentre prevista para el cumplimiento de la actividad de certificación. Como mínimo deberán figurar la Autoridad Certificante, Autoridad de Registro local y los suscriptores.
Justificación	Estimamos conveniente aclarar a qué tipo de entidades se refiere el artículo definiendo cuáles son las que deben estar como mínimo
Documento:	Requisitos Mínimos para Políticas de Certificación Borrador v1.1
Artículo:	1.3.2.- Autoridad de Registro
Comentario de:	Modificación
Redacción propuesta:	En caso de existir, se identificarán las Autoridades de Registro utilizadas por el Certificador en el pro-

	ceso de recepción de solicitudes de emisión de certificados, identificación y autenticación de los solicitantes de certificados y recepción y validación de solicitudes de revocación. Se identificarán las Autoridades de Registro locales (Establecida en el mismo lugar físico que la Autoridad de Certificación) o remotas (Establecida fuera del lugar físico de la Autoridad de Certificación); 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.
Justificación	No resulta claro si se hace referencia a Autoridades de Registro locales o remotas, se estima conveniente aclarar la distinción. La autoridad de Registro existe aunque forme parte de la Autoridad de Certificación.
Documento:	Perfil Mínimo de Certificados y Listas de Certificados Revocados Borrador v1.1
Artículo:	Apartado 2.2.4 Issuer
Comentario de:	Modificación
Redacción propuesta:	2.2.4 – Issuer El campo "issuer" DEBE identificar a la organización responsable de la emisión del certificado. La identidad del emisor se DEBE especificar utilizando los siguientes atributos: domainComponent countryName stateOrProvinceName

	organizationName localityName serialNumber Otros atributos pueden estar presentes, pero los mismos NO DEBEN ser necesarios para identificar a la organización emisora. Los contenidos y tipos de los atributos deben respetar las pautas establecidas para el campo "subject". El atributo "serialNumber" DEBE permitir identificar unívocamente a la organización responsable de la emisión del certificado y consiste un código cuyo formato y valor será definido por el Ente Licenciante al otorgar la Licencia habilitante. El contenido del atributo "countryName" DEBE estar codificado según el estándar ISO3166-1. El contenido del atributo "localityName" DEBE estar codificado según el estándar ISO3166-2.
Justificación:	•En primer lugar se recomienda eliminar la posibilidad de que el campo *issuer* este compuesto por un *"subconjunto"* de los atributos propuestos; ya que entendemos que es conveniente que todos los atributos consignados estén presentes y que es deseable que todos los certificadores licenciados provean los mismos datos acerca de su identidad en los Certificados que emitan. •Se propone una pauta para el formato y obtención del *serialNumber* a modo de ejemplificar alguna forma posible de organizar el contenido que los certificadores deberán dar a este atributo, ya que entendemos en la redacción actual este tema no queda claro.

Documento:	Perfil Mínimo de Certificados y Listas de Certificados Revocados Borrador v1.1
Artículo:	Apartado 2.2.5 Validity (notBefore, notAfter)
Comentario de:	Modificación y Adición
Redacción propuesta:	2.2.5 - Validity (notBefore, notAfter) El período de validez del certificado es el intervalo de tiempo durante el cual el Certificador garantiza que mantendrá información sobre el estado del certificado. El campo se representa como una secuencia de dos fechas: - *"notBefore"*: fecha en que el período de validez del certificado comienza. - *"notAfter"*: fecha en que el período de validez del certificado termina. El período de validez de un certificado es el período de tiempo de *"notBefore"* a *"notAfter"* inclusive. Se RECOMIENDAN los siguientes periodos de validez para certificados digitales, los cuales DEBEN ser especificados en la Política de Certificación : - Certificados de Certificador : 10 (DIEZ) años. - Certificados de proveedores de servicios de firma digital : 10 (DIEZ) años. - Certificados de Servidor: a lo sumo 2 (DOS) años. - Certificados de Personas Físicas o Jurídicas: a lo sumo 1 (UN) años. Un Certificador NO DEBE emitir un certificado digital con vencimiento posterior al de su certificado raíz.
Justificación:	Consideramos que un período de validez de un año para los Certificados de personas físicas y

	jurídicas, con posibilidades de renovación, es un período aceptable desde el punto de vista operativo; y reduce el riesgo de que el Certificador deba mantener por mucho tiempo información sobre Certificados que posiblemente hayan quedado en desuso por parte de sus suscriptores. Por otra parte, proponemos consignar explícitamente un período máximo de dos años para Certificados SSL que es lo que habitualmente manejan las Autoridades Certificantes más reconocidas.

Documento:	Perfil Mínimo de Certificados y Listas de Certificados Revocados Borrador v1.1
Artículo:	Apartado 2.2.6 Subject
Comentario de:	Adición
Redacción propuesta:	Para los certificados de 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 - En caso de ser necesario para identificar unívocamente el organismo, podrá utilizarse repetidamente el campo *organizationalUnitName*. (ej. CN=Dpto. de Mesa de Entradas, O=Gobierno de Mendoza, OU=Ministerio de Hacienda, OU=Dirección General de Rentas). El uso de más de un campo *organizationalUnitName* y la interpretación que debe darse a cada campo debe quedar consignado en la Política de Certificación.

Justificación:	Usar más de un campo *organizacionalUnit-Name* para completar datos que permiten identificar inequívocamente al suscriptor es una práctica observada en muchos certificadores comerciales, que consideramos de gran utilidad en el caso de la Aministración Pública, ya que en general las unidades operativas tienen más de un nivel de profundidad en la estructura jerárquica de la Organización. Aún más, en los certificados emitidos a personas físicas que ocupan un cargo en la Administración Pública, debería preverse un mecanismo de poder consignar el nombre del cargo o función del suscriptor.

Documento:	Perfil Mínimo de Certificados y Listas de Certificados Revocados Borrador v1.1
Artículo:	Apartado 2.3.3 Key Usage
Comentario de:	Adición
Redacción propuesta:	La extensión *"keyUsage"* define ... Para certificados de servidor: - El bit *"nonRepudiation"* DEBE tener valor 1 - El bit *"digitalSignature"* PUEDE tener valor 1 para propósitos de autenticación. - El bit *dataEncipherment* PUEDE tener valor 1 para propósitos de cifrado. - El bit *keyAgreement* DEBE tener valor 1 para negociar la clave a utilizar en la sesión segura. - El resto de bits DEBEN tener valor 0
Justificación:	En particular hemos observado que no se trata particularmente en el documento a los certificados SSL. Entendemos que dada la

	cados SSL. Entendemos que dada la importancia y difusión de las aplicaciones de sitio seguro sería conveniente mejorar este aspecto. Este apartado es un ejemplo de algunos aspectos en los que este tipo de certificados merece un tratamiento diferencial.

Documento:	Perfil Mínimo de Certificados y Listas de Certificados Revocados Borrador v1.1
Artículo:	Apartado 2.3.9 Extended Key Usage
Comentario de:	Adición
Redacción propuesta:	Esta extensión DEBE ser utilizada al menos en los siguientes casos: - Certificados para firma de respuestas OCSP DEBEN incluir el valor *"id-kp-OCSPSigning"* (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) - Autenticación de servidor (1.3.6.1.5.5.7.3.1) - Autenticación de cliente (1.3.6.1.5.5.7.3.2) - Correo seguro (1.3.6.1.5.5.7.3.4)
Justificación:	Consideramos importante detallar también los propósitos que se agregan.

III. IMPLEMENTACIÓN DE EXPERIENCIA EN EL CIRCUITO DE RESOLUCIONES

A. 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 Capacitacion 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 docu-

mentos 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 menúes.
- 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, periodos 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.

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 Técnológico 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 tra-

bajo 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

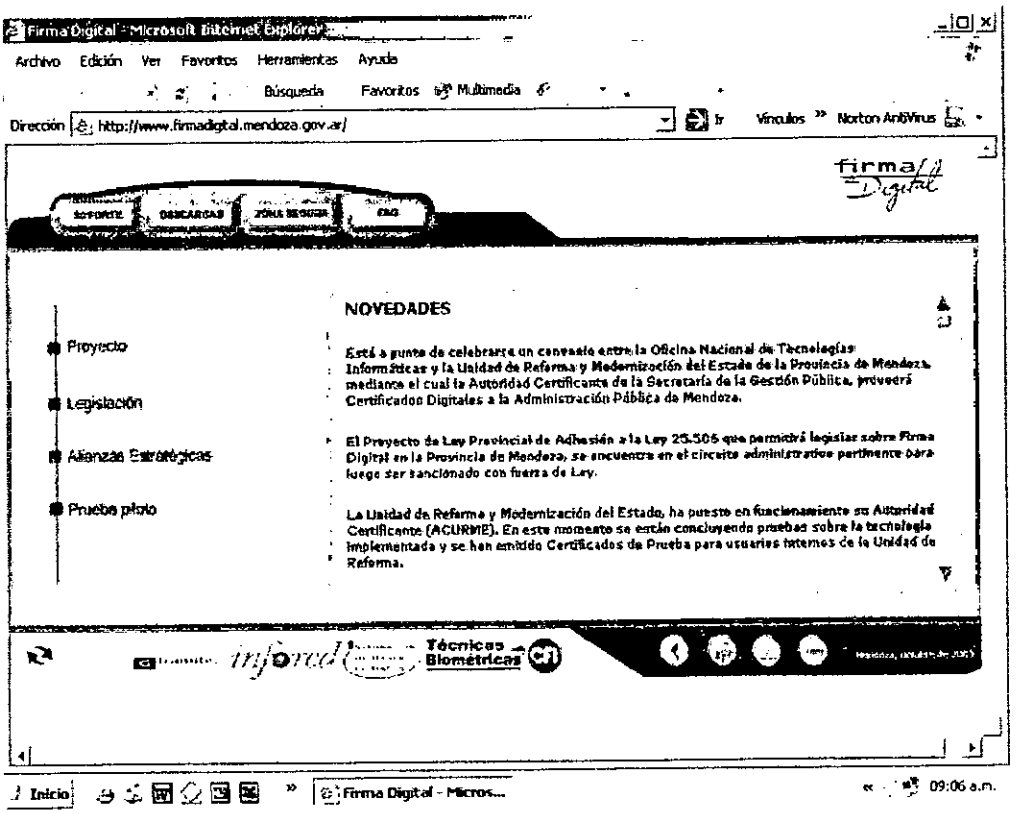
Firma Digital (www.firmadigital.mendoza.gov.ar)

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.

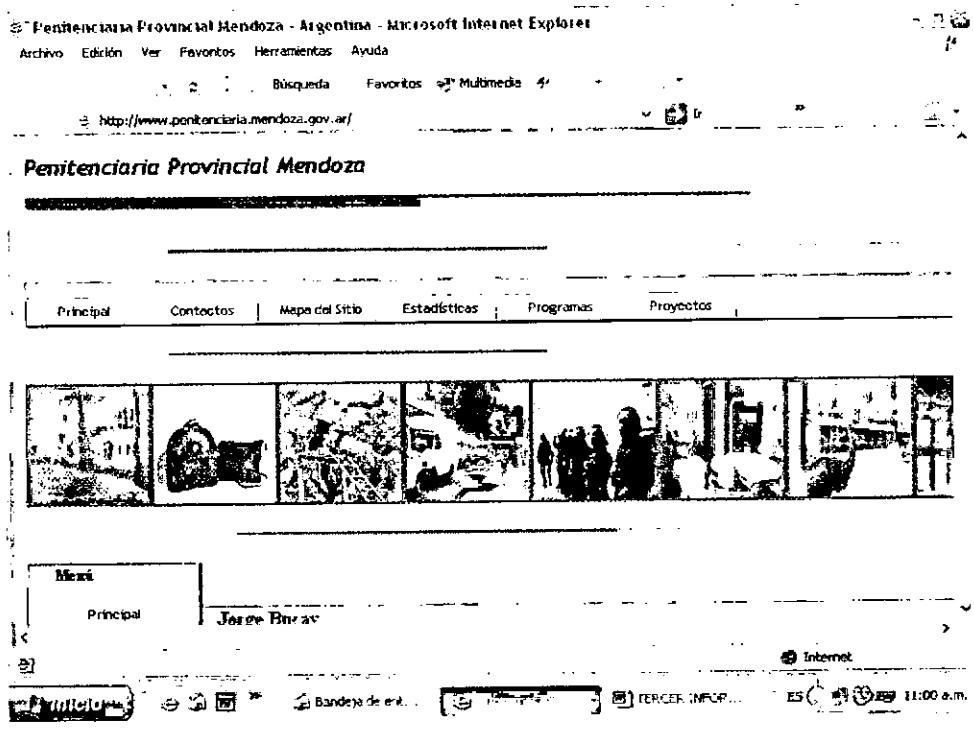
Convencidos de su impacto en los procesos de **despapelización** del Estado, de **reducción de gastos y tiempos** y por ser condición necesaria para asegurar **transparencia y confiabilidad** de cualquier iniciativa de Gobierno Digital lo invitamos a visitar nuestra **página web** www.firmadigital.mendoza.gov.ar, 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.



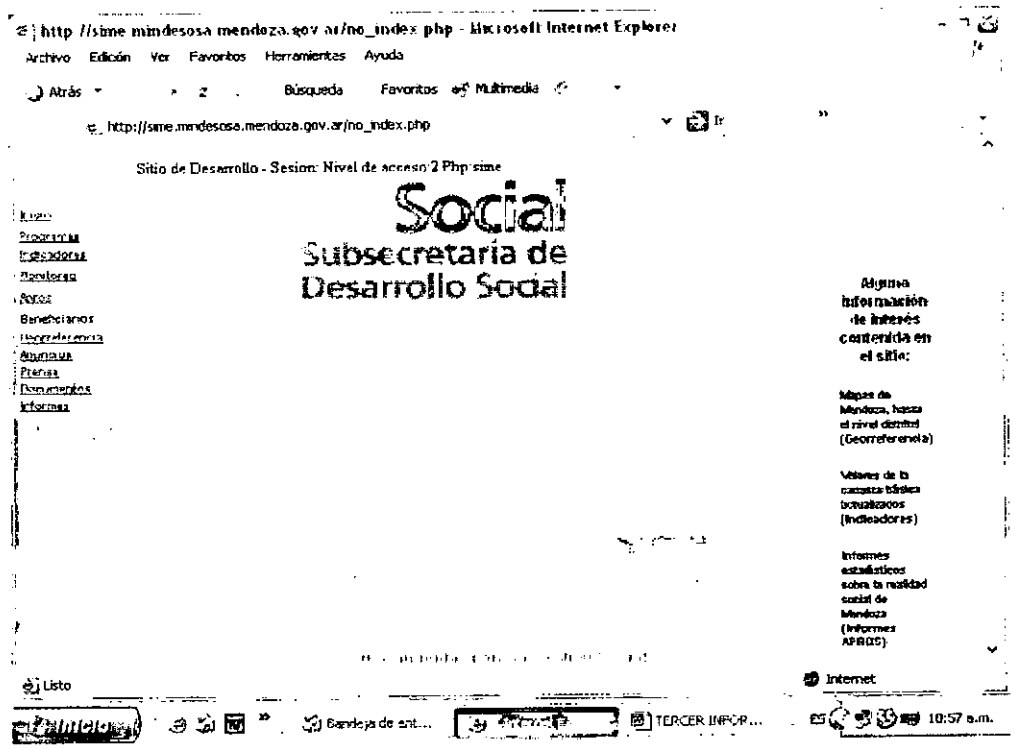
Reuniones Informativas: Se planea la realización de charlas informativas sobre distintos temas con los principales exponentes de las dependencias objetivos señaladas en apartados anteriores, a saber:

- (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 Lega 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)

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 encuentra en proceso de constitución 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

En el informe anterior 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 ex-

periencia 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

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.