ANEXO IV - RESOLUCIÓN N° 17 - MJGGC/09 (continuación)

ANEXO IV

POLÍTICA DE CERTIFICACIÓN

1 INTRODUCCIÓN

1.1 GENERALIDADES

La presente Política de Certificación establece las características y condiciones a las que se sujetan la solicitud, emisión, aceptación, renovación, revocación y uso de los certificados digitales definidos en este documento.

La Política de Certificación referida aquí es aplicable a la emisión de los certificados digitales personales para todos los agentes del Poder Ejecutivo de la Ciudad Autónoma de Buenos Aires, el que comprende la administración centralizada y los organismos descentralizados, entidades autárquicas, las empresas y sociedades del Estado, sociedades anónimas con participación estatal mayoritaria, sociedades de economía mixta y todas aquellas otras organizaciones empresariales donde el Gobierno de la Ciudad tenga participación mayoritaria en el capital o en la formación de las decisiones societarias.

Esta Política de Certificación ha sido redactada en conformidad con lo dispuesto por el Decreto N° 1.181/GCBA/08, por la Agencia de Sistemas de Información (ASI) del Gobierno de la Ciudad Autónoma de Buenos Aires, en su carácter de Autoridad Certificante (AC).

Esta Política de Certificación asume que el lector conoce los conceptos básicos de PKI (Public Key Infraestructure), certificado digital y firmas digital y electrónica, en caso contrario se recomienda al lector que se forme en el conocimiento de los anteriores conceptos antes de continuar con la lectura del presente documento. En la dirección https://ac.buenosaires.gov.ar se pueden encontrar los conceptos generales y usos referidos a las firmas digital y electrónica.

1.2 COMUNIDAD

1.2.1 AUTORIDAD DE CERTIFICACIÓN

La Autoridad de Certificación (AC) que puede emitir certificados acordes con esta política es la Agencia de Sistemas de Información perteneciente al Gobierno de la Ciudad Autónoma de Buenos Aires.

1.2.2 AUTORIDAD DE APLICACIÓN

La Jefatura de Gabinete de Ministros del Gobierno de la Ciudad Autónoma de Buenos Aires es la Autoridad de Aplicación conforme el Artículo 3° de la Ley N° 2.751.

1.2.3 AUTORIDAD DE REGISTRO

ANEXO IV - RESOLUCIÓN N° 17 - MJGGC/09 (continuación)

La Dirección General de Escribanía General del Gobierno de la Ciudad Autónoma de Buenos Aires es la Autoridad de Registro.

1.2.4 SUSCRIPTOR

Se entiende por suscriptor de un certificado digital a la persona física, que solicita y obtiene un certificado digital emitido por la Autoridad Certificante prevista en la presente reglamentación. El grupo de Suscriptores estará compuesto por los funcionarios y agentes del Gobierno de la Ciudad Autónoma de Buenos Aires.

1.3 ÁMBITO DE APLICACIÓN

Los certificados emitidos bajo esta Política de Certificación, pueden utilizarse para la firma electrónica, cifrado de cualquier información o documento y como mecanismo de identificación ante servicios y/o aplicaciones informáticas imple mentados por el Gobierno de la Ciudad Autónoma de Buenos Aires.

1.4 DATOS DE CONTACTO

Esta Política de Certificación pertenece a la Agencia de Sistemas de Información, en su carácter de Autoridad Certificante (AC) del Gobierno de la Ciudad Autónoma de Buenos Aires.

Nombre: Agencia de Sistemas de Información (ASI)

Dirección: Avda. Independencia 635, Ciudad Autónoma de Buenos Aires, República Argentina

Teléfono: (54) (11) 4323-9300

E-mail: ac@buenosaires.gov.ar

2 CLÁUSULAS GENERALES

2.1 OBLIGACIONES

2.1.1 OBLIGACIONES DE LA AC

- Informar a quien solicita un certificado con carácter previo a su emisión las condiciones precisas de utilización del certificado digital, sus características y efectos de la revocación de su propio certificado digital. Esta información deberá estar libremente accesible en redacción fácilmente comprensible e idioma nacional. La parte pertinente de dicha información también estará disponible para terceros;
- Mantener el control exclusivo de los datos utilizados para generar su propia firma digital y electrónica e impedir su divulgación y/o acceso a terceros no autorizados;
- Mantener la confidencialidad de toda información que no figure en el

ANEXO IV - RESOLUCIÓN N° 17 - MJGGC/09 (continuación)

certificado digital y a la que tenga acceso en ejercicio de las funciones definidas en el artículo precedente;

- 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 válidos y los 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 dete rmine la Autoridad de Aplicación;
- Revocar los certificados digitales emitidos en caso de verificar que los procedimientos de emisión y/o certificación han dejado de ser seguros;
- Comunicar a la Autoridad de Registro cualquier irregularidad detectada respecto de la información suministrada por el titular del certificado;
- Responder por la validez de los certificados digitales emitidos;

2.1.2 OBLIGACIONES DE LOS SUSCRIPTORES

- Proveer de modo completo y preciso toda la información necesaria para la emisión del certificado;
- Mantener el control exclusivo de los datos de creación de firma digital o electrónica, no compartirlos e impedir su divulgación.
- Informar a la Autoridad de Registro, el cambio de alguno de los datos contenidos en el certificado digital.
- Solicitar la revocación de su certificado ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma.

2.1.3 OBLIGACIONES COMUNES DE LAS PARTES

Es obligación de las partes que utilicen en los certificados emitidos por la Autoridad de Certificación:

- Limitar la fiabilidad de los certificados a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones del certificado y la Política de Certificación pertinente.
- Verificar la validez de los certificados en el momento de realizar o verificar cualquier operación basada en los mismos.
- Asumir su responsabilidad en la correcta verificación de las firmas digital y electrónica.
- Asumir su responsabilidad en la comprobación de la validez, revocación o suspensión de los certificados digitales que utiliza.
- Tener pleno conocimiento de las garantías y responsabilidades aplicables en la aceptación y uso de los certificados digitales que

ANEXO IV - RESOLUCIÓN N° 17 - MJGGC/09 (continuación)

utiliza, y aceptar sujetarse a las mismas.

2.2 PUBLICACIÓN DE REPOSITORIOS

2.2.1 FRECUENCIA DE PUBLICACIÓN

La Política y las Prácticas de Certificación se publicarán al crearse y al aprobarse cualquier modificación.

Los certificados emitidos se publica rán inmediatamente después de su emisión.

La publicación se realizará en la página https://ac.buenosaires.gov.ar

Las listas de certificados revocados serán publicadas como mínimo cada siete días o cada vez que se produzca una revocación.

2.2.2 ACCESIBILIDAD

El acceso a lectura de la información del repositorio es libre y estará disponible durante las veinticuatro horas de los siete días de la semana.

2.3 CONFIDENCIALIDAD

Se conside rará información confidencial y, por lo tanto no será divulgada a terceros excepto que sea exigida judicialmente:

- La clave privada de la Autoridad de Certificación.
- Toda la información relativa a las operaciones que lleve a cabo la AC.
- Toda la información relativa a seguridad, control y procedimientos de auditoría.
- Los datos de carácter personal proporcionados por los suscriptores durante el proceso de registro, con la salvedad de la información que se incluye en el certificado (apellido y nombres y dirección de correo electrónico).

Se considerará información pública:

- La información contenida en las Políticas y Prácticas de Certificación
- Los certificados emitidos
- Las lista de certificados revocados (CRL)

2.4 DERECHOS DE PROPIEDAD INTELECTUAL

Todos los derechos de propiedad intelectual incluyendo los referidos a certificados y CRL's emitidos, las Políticas y Prácticas de Certificación, así como cualquier otro documento, electrónico o de cualquier otro tipo, pertenecen al Gobierno de la Ciudad Autónoma de Buenos Aires.

3 REQUERIMIENTOS OPERATIVOS

ANEXO IV - RESOLUCIÓN N° 17 - MJGGC/09 (continuación)

3.1 SOLICITUD DE CERTIFICADOS

Un certificado digital puede ser generado y luego almacenado utilizando Hardware Criptográfico (Token) diseñado para tal fin que b rinda un alto nivel de seguridad, o directamente puede hacerse mediante el navegador web del suscriptor. Los procedimientos de solicitud dependen de cual de las dos opciones se requiera. Para tal efecto, se deberá remitir al manual de procedimientos del suscriptor vigente.

3.2 EMISIÓN DE CERTIFICADOS

La emisión del certificado tendrá lugar una vez que la Autoridad de Certificación lo firme.

La Autoridad de registro comunicará la emisión y disponibilidad del certificado al solicitante mediante correo electrónico.

La emisión del certificado al suscriptor implica su autorización para utilizarlo según los alcances definidos en la presente Política de Certificación.

3.3 ACEPTACIÓN DE CERTIFICADOS

El suscriptor demuestra su aceptación del certificado al retirarlo e instalarlo.

La aceptación del certificado implica el conocimiento y aceptación de la Política de Certificación por parte del suscriptor.

3.3.1 QUIÉN PUEDE SOLICITAR LA REVOCACIÓN

La revocación de un certificado podrá ser solicitada por el suscriptor del mismo, por la Autoridad de Registro, por la Autoridad de Aplicación, por la Autoridad Certificante, autoridades judiciales y/o por la autoridad máxima de la jurisdicción en la que se desempeñe el suscriptor del certificado digital.

3.3.2 PROCEDIMIENTO DE SOLICITUD DE REVOCACIÓN

La Autoridad de Certificación acepta solicitudes de revocación según los métodos que se indican en los manuales de procedimientos vigentes de la RA y del suscriptor, aprobados por la presente Resolución.

3.3.3 PUBLICACIÓN DE CRLS Y ACTUALIZACIÓN DEL REPOSITORIO

La revocación se realizará de forma inmediata al procesamiento de cada solicitud verificada como válida, actualizándose el repositorio en forma inmediata y emitiendo una nueva CRL dentro de las veinticuatro horas siguientes.

ANEXO IV - RESOLUCIÓN N° 17 - MJGGC/09 (continuación)

De no haber revocaciones, la AC emitirá las CRLs, como mínimo una vez por semana.

3.3.4 REQUISITOS DE COMPROBACIÓN DE CRLS

La verificación de la CRL es obligatoria para cada uso de los certificados de entidades finales.

Las partes deberán comprobar la validez de la CRL previamente a cada uno de sus usos y descargarse la nueva CRL del repositorio al finalizar el período de validez de la que posean.

3.4 PROCEDIMIENTOS DE SEGURIDAD

La AC registra todos los eventos que relacionados con la seguridad, en archivos de transacciones de auditoría, conservándolos por un período mínimo de diez años.

Tanto las normas para los controles de seguridad física e informática, como para la realización de las auditorías están regulados en el Manual de Seguridad de la AC.

3.5 POLÍTICAS PARA EL ARCHIVO DE REGISTROS

Toda la información recopilada en el proceso de certificación, será almacenada en un lugar seguro y de acceso restringido sólo a personal autorizado, según se establece en el Manual de Seguridad de la AC.

3.6 PLANES DE CONTINGENCIA Y RECUPERACIÓN

En presencia de alguna contingencia que obligue a la suspensión del servicio, se seguirán las pautas establecidas en los procedimientos definidos en las Prácticas de Certificación y en el Manual de Seguridad.

Estos procedimientos aseguran:

- la restauración inmediata de la operatoria mínima, esto incluye registración de solicitudes de revocación y publicación y consulta de listas de certificados revocados (CRLs)
- el restablecimiento del servicio completo dentro de las 24 horas.

En el caso de compromiso de la clave privada de la Autoridad Certificante se revocarán todos los certificados emitidos vigentes, informándole debidamente a las entidades involucradas (suscriptores). Estos procedimientos se efectuarán de acuerdo a lo establecido en el Manual de Seguridad de la AC.

3.7 CESE DE OPERACIONES DE LA AUTORIDAD CERTIFICANTE

En el caso que la Autoridad Certificante vaya a discontinuar sus operaciones, procederá a notificar fehacientemente y con una antelación mayor a 60 días a todos los suscriptores.

El procedimiento a seguir para el término de actividades, así como las medidas a tomar para el archivo de los registros y documentación necesaria, estará en conformidad con la ley y normas en vigencia.

ANEXO IV - RESOLUCIÓN N° 17 - MJGGC/09 (continuación)

4 CONTROLES DE SEGURIDAD FÍSICA, PROCEDURALES Y DE PERSONAL

A fin de resguardar en todo momento la seguridad de operación así como de las instalaciones y el personal que opera y administra la Autoridad de Certificación existen diversos procedimientos, políticas y controles de seguridad. Estas prácticas y procedimientos de seguridad deberán ser regularmente revisados y modificados.

4.1 CONTROLES DE SEGURIDAD FÍSICA

Todas las instalaciones que forman parte de la Autoridad de Certificación se encuentran debidamente protegidas mediante dispositivos y personal de vigilancia durante las 24 horas los 7 días de la semana, que restringen el acceso a los equipos, programas y datos sólo a aquellas personas autorizadas.

4.2 CONTROLES PROCEDURALES

Mediante normas de seguridad establecidas en el Manual de Seguridad de la AC, se limita el acceso a los recintos restringidos al personal habilitado, obligando a hacerlo en compañía del personal requerido para cada caso.

Sobre las actividades realizadas por cada empleado que ingresa a la AC se realizan auditorias periódicas.

El personal que interviene, es capacitado en forma permanente en la implementación de políticas y procedimientos de seguridad.

Los roles identificados para el control y la gestión del sistema son:

- **Responsable de la AC :** encargado de garantizar el correcto funcionamiento de la AC, seleccionar y designar a los funcionarios para cada uno de los roles
- **Responsable de Seguridad Informática:** encargado de definir las herramientas de seguridad informática de acuerdo a la Política y Manual de Procedimientos de Seguridad, verificar y controlar el cumplimiento de las disposiciones de la Política de Seguridad y del Manual de Procedimientos de Seguridad en cuanto a informática se refiere, revisar log´s de transacciones y del sistema e informar al Responsable de la AC y al Auditor Interno, y de autorizar las solicitudes de altas, bajas o modificaciones de accesos a la aplicación
- **Responsable de las Aplicaciones :** tiene a su cargo diseñar, desarrollar, implementar y mantener los sistemas aplicativos requeridos para el funcionamiento de AC, de acuerdo a las disposiciones establecidas en el Manual de Prácticas de Certificación
- **Auditor Interno:** debe verificar y controlar el cumplimiento de todas las disposiciones de la AC (Política de Seguridad, Procedimientos de Seguridad, Prácticas de Certificación), verificar y controlar la preparación de los procesos de emergencia (Plan de Contingencia),

ANEXO IV - RESOLUCIÓN N° 17 - MJGGC/09 (continuación)

verificar y controlar la preparación de los procesos de finalización (Plan Cese de Actividades) e informar al Responsable de la AC respecto de las desviaciones, incumplimientos o situaciones de riesgo que se detecten.

- **Oficial Certificador:** es el depositario de la clave privada de la AC, firma digitalmente los certificados de los suscriptores y las listas de certificados revocados (CRLs).

Todos los usuarios autorizados de la AC se identifican mediante certificados digitales emitidos por la propia PKI y se autentifican por medio de dispositivos criptográficos portátiles.

4.3 Controles de personal

La AC cuenta con una política de administración de empleados en la que se incluye la revisión de sus antecedentes personales y comerciales, tanto antes de ser contratados como periódicamente mientras trabajan en la AC, a fin de asegurar la confiabilidad y competencia del personal para el adecuado cumplimiento de sus funciones.

5 CONTROLES DE SEGURIDAD TÉCNICA

5.1 GENERACIÓN E INSTALACIÓN DE CLAVES

5.1.1 GENERACIÓN E INSTALACIÓN DE CLAVES

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.

La clave pública del suscriptor del certificado debe ser transferida a la AC de manera tal que se asegure que no pueda ser cambiada durante la transferencia.

5.1.2 INSTALACIÓN DE LA CLAVE PÚBLICA DE LA AC

La clave pública de la AC se puede descargar de https://ac.buenosaires.gov.ar.

5.1.3 TA MAÑO DE LAS CLAVES

Las claves usadas en el ámbito de esta PKI son como mínimo de 1024 bits.

5.1.4 HARDWARE / SOFTWARE PARA GENERACIÓN DE CLAVES

Para la generación de las claves de AC se utilizan módulos criptográficos, acorde a las recomendaciones del estándar FIPS140-2.

La generación de las claves de los usuarios o suscriptores es realizada por programas de software criptográficos, tales como los módulos

ANEXO IV - RESOLUCIÓN N° 17 - MJGGC/09 (continuación)

embebidos en los navegadores (browsers) de Internet (Mozilla Firefox, Microsoft Internet Explorer, Opera, etc.).

5.1.5 FINES DE USO DE LA CLAVE

Todos los certificados emitidos por la AC contienen las extensiones KEY USAGE y EXTENDED KEY USAGE definidas por el estándar X.509 v3 para la definición del propósito de uso y de las limitaciones de los certificados y las claves asociadas.

5.1.6 CARACTERÍSTICAS CRIPTOGRÁFICAS

El algoritmo de firma utilizado por la AC es SHA-1 con RSA.

5.2 PROTECCIÓN DE LA CLAVE PRIVADA

5.2.1 ESTÁNDARES PARA EL MÓDULO CRIPTOGRÁFICO

Se requiere que el módulo utilizado para la creación de claves utilizadas por la AC cumpla con la certificación FIPS140-1 de nivel 2.

5.2.2 CONTROL MÚLTIPLE DE LA CLAVE PRIVADA

La clave privada de la AC está sujeta a un control multi-personal.

Cuando se genera la clave privada por primera vez, se divide en múltiples fragmentos que son distribuidos cifrados con una clave de activación.

Los módulos criptográficos que manejan las claves privadas, tanto para su generación como eventual recuperación posterior, son activados usando claves de activación, las cuales son administradas sólo por personal autorizado.

5.2.3 CUSTODIA DE LA CLAVE PRIVADA

No se custodian claves privadas de firma de los suscriptores.

La clave privada de la Autoridad de Certificación se encuentra alojada en dispositivos de hardware criptográfico con certificación FIPS 140-1 de nivel 2.

5.2.4 COPIA DE SEGURIDAD DE LA CLAVE PRIVADA

Las copias de backup de las claves privadas de la AC se almacenan en dispositivos de hardware criptográfico con certificación FIPS 140-1 de nivel 2.

5.2.5 DESTRUCCIÓN DE LA CLAVE PRIVADA

Si por cualquier motivo deja de utilizarse la clave privada de la AC para crear firmas digitales y electrónicas, la misma será destruida.

5.3 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

5.3.1 ARCHIVO DE CLAVE PÚBLICA

La AC mantiene un archivo de todos los certificados emitidos por un período de diez años.

ANEXO IV - RESOLUCIÓN N° 17 - MJGGC/09 (continuación)

5.3.2 PERÍODO DE USO DE CLAVES PÚBLICAS Y PRIVADAS

El certificado de la AC tiene una validez de diez años.

5.3.3 DATOS DE ACTIVACIÓN

Los datos de activación de la Autoridad de Certificación se almacenan en dispositivos criptog ráficos portátiles en posesión de personal autorizado.

Solo el personal auto rizado conoce los PINs y contraseñas para acceder a los datos de activación.

5.4 CONTROLES DE SEGURIDAD INFORMÁTICA

La Autoridad Certificante efectúa los controles de Seguridad Informática de acuerdo a las normas especificadas en el Manual de Seguridad, que cumplen los requerimientos establecidos en la legislación y estándares vigentes.

5.5 CONTROLES DE SEGURIDAD DE LA RED

La Autoridad Certificante efectúa por medio de Seguridad Informática los controles de acuerdo a las normas especificadas en el Manual de Seguridad, que cumplen los requerimientos establecidos en la legislación y estándares vigentes.

6 PERFILES DE CERTIFICADO Y CRL

6.1 PERFIL DE CERTIFICADO

6.1.1 NÚMERO DE VERSIÓN

La presente política se implementa sobre certificados X.509 versión 3 (X.509 v3).

6.1.2 FORMATO DE NOMBRES

Los certificados emitidos contienen el distinguished name X.500 del emisor y el suscriptor del certificado en los campos issuer name y subject name respectivamente.

6.1.3 RESTRICCIONES DE NOMBRES

Los nombres contenidos en los certificados están restringidos a distinguished names X.500, únicos y no ambiguos.

6.2 PERFIL DE CRL

6.2.1 NÚMERO DE VERSIÓN

El formato de las CRLs utilizadas en la presente política es el especificado en la versión 2 (v2).

6.2.2 CRL Y EXTENSIÓNES

La presente Política de Certificación soporta y utiliza CRLs conformes al

estándar X.509.

7 ADMINISTRACIÓN DE ESTA POLÍTICA

7.1 CAMBIOS A LA POLÍTICA

La Autoridad Certificante informará a los suscriptores de certificados acerca de todos aquellos cambios significativos que se efectúen a esta Política.

ANEXO IV - RESOLUCIÓN N° 17 - MJGGC/09 (continuación)

GLOSARIO

- **Browser**: Navegador. Programa utilizado para visualizar las páginas web. Los más utilizados son Internet Explorer y Mozilla Firefox.
- **CA**: Autoridad certificante (AC o CA por sus siglas en inglés Certification Authority) es una entidad de confianza, responsable de emitir y revocar los certificados digitales, utilizados en la firma electrónica o digital.
- **Certificado digital**: es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto y su clave pública.
- **Clave pública y privada**: es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. El remitente usa la clave pública del destinatario para cifrar el mensaje, y una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje. De forma análoga el remitente usa su clave privada para asegurar la integridad e identidad del firmante del documento o mensaje, corroborando la misma con su clave privada.
- **Criptografía**: La criptografía (del griego κρύπτω krypto, «oculto», y γράφω graphos, «escribir», literalmente «escritura oculta») es el arte o ciencia de cifrar y descifrar información utilizando técnicas que hagan posible el intercambio de mensajes de manera segura que sólo puedan ser leídos por las personas a quienes van dirigidos.
- **CRL**: lista de revocación de certificados (o, en inglés, CRL, Certificate Revocation List)
- **Drivers**: pequeño programa cuya función es controlar el funcionamiento de un dispositivo de la PC.
- **Firma digital o Firma electrónica**: es un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma, puede, además, asegurar la integridad del documento o mensaje.

  La diferencia entre ambas firmas radica en que, en el caso del documento firmado digitalmente, si es verificado correctamente, se presume, salvo prueba en contrario, que proviene del suscriptor del certificado digital y que el mismo no fue modificado, situación ésta que no ocurre en caso de que el documento se encuentre firmado electrónicamente, ya que se invierte la carga probatoria, y de ser desconocida esta firma, corresponde a quien invoca su autenticidad acreditar su validez.
- **FIPS 140**: La Federal Information Processing Standard 140 son una serie de publicaciones que especifican los requerimientos para los

ANEXO IV - RESOLUCIÓN N° 17 - MJGGC/09 (continuación)

módulos criptográficos.

- **HSM**: Módulo de seguridad por hardware.
- **LOG's**: es un registro oficial de eventos durante un periodo de tiempo en particular.
- **PIN**: (Personal Identification Number o Número de Identificación Personal en castellano) es un valor numérico (generalmente) usado para identificarse y poder tener acceso a ciertos sistemas o artefactos, como un teléfono móvil o un cajero automático.
- **PKI**: (Public Key Infraestructure por sus siglas en inglés): En criptografía, una infraestructura de clave pública es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptog ráficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas. Una PKI debe proporcionar:
    - **Autenticidad**: la firma digital tendrá la misma validez que la manuscrita.
    - **Confidencialidad**: de la información transmitida entre las partes.
    - **Integridad**: debe asegurarse la capacidad de detectar si un documento firmado ha sido manipulado.
    - **No repudio**: de un documento firmado digitalmente.
- **RA**: La Autoridad de Registro controla la generación de certificados para los miembros de una entidad. Previa identificación, la Autoridad de Registro se encarga de realizar la petición del certificado y de guardar los datos pertinentes.
- **RSA**: El sistema criptográfico con clave pública RSA es un algoritmo asimétrico cifrador de bloques, que utiliza una clave pública, la cual se distribuye, y otra privada, la cual es guardada en secreto por su propietario.
- **SHA**: (Secure Hash Algorithm, Algoritmo de Hash Seguro), es un sistema de funciones hash criptográficas relacionadas de la Agencia de Seguridad Nacional de los Estados Unidos y publicadas por el National Institute of Standards and Technology (NIST).
- **Token**: Dispositivo criptográfico que permite la generación del par de claves necesarias para la generación de un certificado digital, y el posterior almacenamiento seguro de dicho certificado.
- **X.500**: es un conjunto de estándares de redes de computadoras de la ITU-T sobre servicios de directorio, entendidos estos como bases de datos de direcciones electrónicas (o de otros tipos). Los protocolos definidos por X.500 incluyen, protocolo de acceso al directo rio (DAP), el protocolo de sistema de directorio, el protocolo de ocultación de información de directorio, y el protocolo de gestión de enlaces operativos de directorio. Dentro de la serie X.500, la especificación que ha resultado ser la más difundida no trata de protocolos de directorio,

ANEXO IV - RESOLUCIÓN N° 17 - MJGGC/09 (continuación)

sino de certificados de clave pública X.509.

- **X.509**: es un estándar UIT-T para infraestructuras de claves públicas (en inglés, Public Key Infrastructure o PKI). X.509 especifica, entre otras cosas, formatos estándar para certificados de claves públicas y un algoritmo de validación de la ruta de certificación.

Volver a la Norma