Declaración de Prácticas de Certificación (CPS) Autoridad Certificadora UNAMgrid

Versión 2.0

OID 1.2.840.113612.5.4.2.5.2.2.1.2.0

Fecha de Revisión	Versión	Elaborado por	Número de páginas
Febrero de 2016	2.0 Vigente	Universidad Nacional Autónoma de México	64

1. Introducción

1.1 Presentación

El presente documento está estructurado conforme al RFC 3647, sin embargo no todas las secciones serán usadas. Este documento describe el grupo de reglas y procedimientos establecidos por la UNAMgrid CA para la operación de estos servicios.
Este documento contiene las políticas de certificación y las prácticas de Certificación para UNAMgrid CA. La autoridad certificadora es autofirmada.

La UNAMgrid AC se constituye como autoridad certificadora de la UNAM, proporcionando el servicio a los distintos miembros de la comunidad académica adheridos a la grid en México.

Información general

UNAMgrid CA es la infraestructura para apoyar las actividades del portal E- sciece proporcionadas por la UNAM y la investigación académica en México.

Este documento describe el conjunto de reglas y prácticas operativas que deben ser observadas por los usuarios de la UNAMgrid CA, la autoridad certificadora y los emisores de certificados.

Este documento estará disponible en el website

https://ca.unamgrid.unam.mx/

1.2 Nombre del documento e identificación

Título: Declaración de Políticas de Certificación UNAMgrid CA (PC) y Prácticas de Certificación (CPS)
Estructura de OID del documento:
Asignado por IGTF: 1.2.840.113612.5.4.2.5.2.2.1.2.0
Tipo de documento (CP/CPS): 1
Versión: 2.0, febrero 2016
Vencimiento: Válido a partir de la fecha de su publicación.
Localización: http://ca.unamgrid.unam.mx

1.3 Participantes PKI, comunidad de usuarios certificados

La UNAMgrid CA emite certificados principalmente para la comunidad académica y entidades (institutos, universidaes, centros de investigacion, entre otros) en México, que hace uso de recursos digitales Grid.

El presente documento establece las reglas de operación de esta comunidad de usuarios.

1.3.1 Autoridades de certificación

La UNAMgrid CA funge como el prestador de servicios de certificación para la UNAM e instituciones integradas a la grid. Esta constituida como CA raíz y no emite certificados a entidades emisoras subordinadas.

1.3.2 Autoridades de Registro

La RA es responsable de validar los antecedentes de identidad de los solicitantes y la pertenencia a proyectos en nombre de la CA UNAMgrid. Durante el proceso de solicitud de certificados, se encargará de garantizar la veracidad de la información y el cumplimiento de las politicas y reglas de operación de la CA.

Como responsables de la RA, asumen la obligación de seguir los procedimientos establecidos por la autoridad competente para su funcionamiento.

Entre sus principales funciones se encuentran:

- Comprobar la identidad de los solicitantes y la veracidad de la información proporcionada.
- Informar al solicitante vía correo electrónico de los requisitos para que su certificado sea emitido, asi como las limitaciones de uso.
- Verificar que la información contenida en el certificado digital es exacta y corresponde al solicitante, asi como que este cumple con los parámetros establecidos.
- Asegurar que el titular (suscriptor) del certificado está en posición de los datos de creación de su firma.

Las Autoridades de Registro (RA) se crearán por necesidad para apoyar las actividades de investigación académica en el país.

En el caso de la UNAMgrid CA la Autoridad Registradora principal que valida es:

Institución	RA Managers	Nombre de la RA	Contacto RA	Ubicación
DGTIC UNAM	-Jhonatan Rafael Pontaza López -Alejandro Gerbacio Gerbacio -Lizbeth Angélica Barreto Zúñiga	UNAMgrid	camanager@unam.mx	Ciudad de México

Asimismo podrán crearse más RA´s si por la naturaleza del proyecto, dispersión geográfica de los miembros o necesidades propias de la operación, se requiera de la integración de mas RA´s. Estas deberán apegarse en todo momento a la normatividad y reglas de operación establecidas en el presente documento.

Deberá requerirse a las RA que declaren su entendimiento de y adherencia a este CP/CPS, y que cumplan sus funciones de acuerdo con este CP/CPS y las mejores prácticas actuales definidas en el sitio de UNAMgrid.

1.3.3 Titulares (suscriptores), Usuarios finales

La UNAMgrid CA emite certificados a usuarios en entidades académicas y de investigación autorizados, vinculados a proyectos que hagan uso de recursos grid pertenecientes a UNAM y su red, tales como instituciones académicas, centros de investigación y otras organizaciones dedicadas a la investigación en México.

Asimismo emitirá certificados de servidor asociados a un titular (suscriptores) para la autorización de servidores a servicios pertenecientes a la grid.

1.3.4 Las partes que confían

Todos aquellos miembros y usuarios involucrados en procesos de autenticación, validación, envío de trabajos, uso de servicios y recursos de la grid. Estos pueden ser:

- Las personas físicas que accesan a los servidores y servicios.
- El host o servidor que permite a los usuarios autenticarse o enviar procesos y/o trabajos realizados (jobs).
- Los servicios llamados por los titulares de un certificado digital válido.

1.3.5 Otros participantes

No aplica.

1.4 Uso de los certificados

1.4.1 Usos autorizados de los certificados

El propósito principal de los certificados emitidos para la UNAMgrid es permitir mediante la autenticación, validar la identidad del titular y por ende su derecho a ingresar a recursos grid.

El certificado raíz de la CA sólo podrá ser utilizado para emitir y validar certificados que dicen ser emitidos por la UNAMgrid CA, generar Listas de Revocación de Certificados, asi como llevar el control y administración de los mismos.

LA UNAMgrid CA asimismo, emite certificados de entidad final, X.509 versión 3, de dos tipos:

1) personales
2) servidor

El certificado de entidad final, se utilizará principalmente para:
Autenticación de usuarios, hosts y acceso a servicios.

Otros posibles usos de este certificado serán:

- Autenticación de correos electrónicos firmados.

1.4.2 Usos no autorizados de los certificados

Los certificados emitidos por UNAMgrid CA no deben ser compartidos, transferidos o utilizados para usos distintos a los autorizados.

No se deben utilizar para transacciones financieras de ninguna índole.

No deben ser utilizados en actos que contravengan las leyes mexicanas o la ley del país destino en el uso del certificado.

1.5 Administración de las políticas

1.5.1 Organización responsable del CPS

La UNAM a traves de la DGTIC - Departamento de Identidad y Firma Electrónica Avanzada es responsable del registro, mantenimiento, e interpretación de este CP/CPS.

El documento estará disponible en su versión impresa en:

Universidad Nacional Autónoma de México
Dirección General de Cómputo y de Tecnologías de Información y Comunicación
Departamento de Identidad y Firma Electrónica Avanzada
Edificio Anexo de la DGB 1er piso
Circuito Exterior, Ciudad Universitaria.
C. P. 04510, Ciudad de México, México
Teléfono: + 52 (55) 56223975
Correo electrónico: camanager at unam.mx

Asimismo la versión digital se podrá consultar en:

http:// ca.unamgrid.unam.mx/

1.5.2 Persona de contacto para el CPS

Responsable del documento y su custodia:

Mtra. Lizbeth Angélica Barreto Zuñiga
Jefa del Departamento de Identidad y Firma Electrónica Avanzada,
DGTIC, UNAM.
Departamento de Identidad y Firma Electrónica Avanzada
Edificio Anexo de la DGB, 1er piso
Circuito Exterior, Ciudad Universitaria.
C. P. 04510, Ciudad de México, México
Teléfono:+ 52 (55) 56 22 39 75

Correo electrónico: bazuli at unam.mx

1.5.3 **Competencia para determinar adecuación de políticas de CPS con las diferentes políticas de certificación**

El responsable de la UNAMgrid CA es responsable de determinar la idoneidad o adecuaciones a las políticas del CPS.

1.5.4 CPS y procedimientos de aprobación

Este documento CP / CPS requiere la aprobación por parte de The Americans Grid Policy Managment Authority (http://www.tagpma.org)

Asimismo será revisado y avalado por la Oficina del Abogado General (OAG) representante legal de sus derechos e intereses institucionales, así como de la difusión de la normatividad de la UNAM, teniendo como marco la Constitución General de la República, la Ley Orgánica y el Estatuto General.

1.6 Definiciones y acrónimos

1.6.1 Definiciones

Autenticación
El proceso en el que se establece que los individuos, organizaciones o cosas son quien o lo que dicen ser. En el contexto de una PKI, autenticación puede ser el proceso de establecer que un individuo u organización que solicite o que pretenda ingresar a algo bajo un cierto nombre es, de hecho, el individuo u organización identificada.

Autenticación también puede referirse a un servicio de seguridad que proporciona garantías de que las personas, organizaciones o cosas son quien o lo que dicen ser, o que un mensaje u otros datos se originaron a partir de un individuo, organización o dispositivo específico.

Certificado personal
Un certificado utilizado para la autenticación, que permite establecer una identidad como persona en la grid. Siempre representará a un individuo.

Certificado de Servicio
Un certificado para un servicio particular que se ejecuta en un host. Representará un sólo servicio en un sólo host.

Certificado Host
Un certificado para la certificación del servidor y el cifrado de las comunicaciones (SSL / TSL). Cada certificado representa a una sola máquina. Los certificados de host se utilizan internamente por el servicio PKI y no se emiten a otros sitios.

Cliente OCSP

Aplicación (cliente) que permite la verificación del servicio OCSP, su implementación y operación es responsabilidad del tercero (parte confiada) y deberá cumplir el RFC 2560.

Emisión de la Autoridad de Certificadora (CA emisora)
En el contexto de un certificado particular, la entidad emisora es la CA que emitió el certificado.

Identificación
El proceso de establecer la identidad de un individuo u organización, es decir, para demostrar que es un individuo u organización específico. En el contexto de una PKI, la identificación se refiere a dos procesos: (1) establecer que un nombre dado de un individuo u organización corresponde a una identidad real de un individuo u organización, y (2) determinar que un individuo u organización que solicite o la búsqueda de acceso a algo bajo ese nombre es, de hecho, el nombre individuo u organización.

Una persona que busca la identificación puede ser un solicitante de certificado, o una persona que busca el acceso a una aplicación de red o software, como un administrador de CA que solicite el acceso a los sistemas de CA.

Operador de Registro (RAg)
Es la entidad que interactúa con la RA con el fin de hacer que la CA emita certificados.

Organización Virtual (VO)
Una organización que se ha creado para representar un esfuerzo de investigación o desarrollo en particular independiente de los sitios físicos en que el científico o ingenieros trabajan (por ejemplo PPDG, FNC, EDG, etc).

Punto de contacto
El miembro de un sitio (organización virtual) que se ha elegido para gestionar todas las comunicaciones sobre asuntos de políticas y gestión con el responsable de UNAMgrid CA.

Parte Confiada (tercero)
El beneficiario de un certificado que actúa en dependencia de ese certificado y / o firmas digitales verificado mediante ese certificado.

Repositorio
Un área de almacenamiento, por lo general en línea, que contiene listas de certificados emitidos, CRL, documentos de política, etcétera.

RFC 3280
Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, April 2002.

RFC 1778
The String Representation of Standard Attribute Syntaxes.

Servicio Consulta de Certificados en Línea (OSCP Responder)
Servicio que permite conocer el estado de vigencia de los certificados en línea en tiempo real.

Solicitante
Entidad final, organización o persona que realiza solicitud de emisión del certificado (CSR).

Suscriptor (Titular)
A veces llamado entidad final, es una persona o servidor a quien se expide un certificado digital.

X.509 versión 3
Estándar desarrollado por la Unión Internacional de Telecomunicaciones (organización internacional de las Naciones Unidas para coordinación de servicios de redes de telecomunicaciones entre Gobiernos y empresas) para las Infraestructuras de Llave Pública y los Certificados digitales.

1.6.2 Acrónimos

CA (Autoridad de Certificación)
Una autoridad de confianza para uno o más usuarios (suscriptores) que crea y asigna certificados de llave pública y es responsable de ellos durante toda su vida útil. Certificados de identidad X.509 que emite la entidad / sistema (coloca un nombre de objeto y la llave pública en un documento y luego firma digitalmente el documento utilizando la llave privada de la CA).

CENAM (Centro Nacional de Metrología)
Laboratorio nacional de referencia en materia de mediciones. Es responsable de establecer y mantener los patrones nacionales, ofrecer servicios metrológicos como calibración de instrumentos y patrones. Proporciona servicios de sincronía y calibración de sistemas informáticos con la hora oficial de los Estados Unidos Mexicanos.

CPS (Certificate Practice Statement)
Una declaración de las prácticas, que una autoridad de certificación emplea en la emisión de certificados.

CRL (Certificate Revocation List)
Listado de los certificados revocados o suspendidos que es firmada con la llave privada de la CA.

CSR (solicitud de firma de certificado)
Un mensaje enviado a una CA con el fin de solicitar un certificado digital. Contiene información de identificación del solicitante y la llave pública elegida por el solicitante. Si se aprueba la solicitud, el CA devolverá un certificado que ha sido firmado digitalmente con la llave privada de la CA.

DRP (Disaster Recovery Plan)

Plan de recuperación ante desastres, proceso que permite mantener la continuidad de los servicios mediante el establecimiento de medidas para recuperar los datos, hardware y software crítico de la aplicación o sistema en caso de un desastre natural, evento inesperado o error humano.

HSM (Hardware Security Module)
Dispositivo criptográfico basado en hardware que genera, almacena y protege llaves criptográficas, garantizando la unicidad e integridad de la llave raíz.

IETF (Internet Task Force)
Entidad que regula las propuestas y los estándares de Internet, se compone de técnicos y profesionales en el área de redes, tales como investigadores, integradores, diseñadores de red, administradores, vendedores, entre otros.

IGTF (International Grid Trust Federation)
Comunidad científica internacional de Grids computacionales cuyo principal objetivo es el avance de la ciencia y la ingeniería. La promesa de Grids computacionales globales requiere de políticas y procedimientos que identifiquen de forma fiable a los titulares (suscritores) y los recursos Grid. Se han establecido Policy Management Authorities (PMA), cada una es responsable de la gestión y autenticación en sus grids.

NTP (Network Time Protocol)
Protocolo de internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable.

OCSP (Online Certificate Status Protocol)
Protocolo para verificación de estatus de certificados en línea.

RA (Autoridad de Registro)
Entidad responsable de la identificación y autenticación de los titulares del certificado, pero no firma o emite certificados.

Registration Manager (RM)
Es un servidor web que proporciona una interfaz de usuario Web para titulares (suscriptores) y agentes de CA, para la emisión de certificados x509.

RFC (Request for comments)
Publicación que recopila las mejores prácticas, procesos, procedimientos avalados por la IETF y que son convención a nivel internacional.

TAGPMA (The Americas Grid PMA)
Federación de entidades de certificación de grid y anexos que operan en la región conocida como las Américas. Se regirá por una Policy Management Authority (PMA), que está formada por miembros con responsabilidades en grid en las Américas. El objetivo de la federación es facilitar las relaciones de confianza necesarias entre dominios para desplegar las redes en las Américas y en el mundo.

UNAM

Universidad Nacional Autónoma de México.

2. Publicación y responsabilidades del repositorio

2.1 Repositorios

El repositorio en línea de información de la UNAMgrid CA es público y se encuentra accesible en formato PDF, en la dirección http://ca.unamgrid.unam.mx/

Estará disponible 24x7x365, excepto cuando se realicen procesos de mantenimiento o migración del sistema, en cuyo caso la restricción de acceso al servicio no podrá superar las 8 horas.

2.2 Las publicaciones de información de CA

El UNAMgrid CA operará un repositorio en línea que contiene:

- Certificado del UNAMgrid CA (disponible en PEM, CRT, CER), y todos los necesarios para comprobar la validez de los certificados,
- El listado de los certificados emitidos por la PKI, y sus diversos estatus
- Una lista de revocación de certificados (CRL) (disponible en DER, PEM y TXT),
- Una copia de la versión más reciente de esta política y todas las versiones anteriores,
- Otra información que se considere relevante para el servicio UNAMgrid CA.

Asimismo se contará con el servicio de publicación en línea del estatus de los certificados mediante el protocolo OCSP*.

*Para hacer uso de este servicio, es responsabilidad del verificador contar con un cliente OCSP que cumpla con el RFC 2560.

2.3 Tiempo de la frecuencia de publicación

Toda la información publicada será hasta la fecha actual, manteniendo una constante actualización de los contenidos.

El listado de los certificados será publicado en el repositorio UNAMgrid CA tan pronto como sean emitidos.

La lista de revocación de certificados (CRL) tendrá una vida útil de un máximo de 30 días. La UNAMgrid CA debe emitir una nueva CRL al menos 7 días antes del vencimiento o inmediatamente después de haber procesado una revocación, lo que ocurra primero. Una nueva CRL debe ser publicada inmediatamente después de su emisión.

El CP/ CPS se publicará cada vez que se actualicen las políticas y/o el sistema y una vez que se haya recibido la aprobación por parte de las autoridades universitarias correspondientes (Oficina del Abogado General) y TAGPMA.

2.4 Controles de Acceso en los repositorios de certificados

El repositorio en línea se mantiene en una base de datos disponible 7x24x365, con ventanas de mantenimiento programables.

La UNAMgrid CA no tendrá ninguna restricción y/o control de acceso a su CP/ CPS, información de certificados emitidos, OCSP o CRL.

Sólo los responsables de la AC UNAMgrid están autorizados para modificar, sustituir o eliminar información, siempre en apego a lo establecido por TAGPMA.

3. Identificación y autenticación de los titulares de certificados

3.1 Denominación (registro de nombres)

3.1.1 Tipos de nombres

El campo Subject DN (Distinguished Name) contiene toda la información de identificación de la entidad para la que se emite el certificado, ya sea persona jurídica, física, o cualquier otro tipo. Dicha información debe identificar unívocamente a un certificado emitido por una misma CA.

Los siguientes atributos deberán formar parte de los certificados digitales emitidos por la UNAMgrid CA:

CN	Nombre y apellidos
OU	Departamento, área, organización a la que pertenece
O	Instituto, universidad
C	País (código ISO)

Asimismo los nombres deberán cumplir con los siguientes requisitos:

- El nombre de sujeto es del tipo X.500 v3
- El componente CN tiene una de las siguientes formas:

Certificado personal

- Nombre y apellido como aparece en el documento de autenticación, separado por un punto (.) o un texto directamente derivado de su nombre (alias). El nombre no aceptará caracteres especiales ni espacios.

CN = Jorge.hernandez.perez (solicitante)
CN= jorhep

En caso de existir homonimia entre usuarios, estos deberán conservar su nombre completo seguido de un número.

- El conjunto de caracteres permitidos para CommonName (CN), en los certificados personales es:

'a' - 'z', 'A' - 'Z', '0' - '9' se aceptan punto.
No se aceptan espacios, no se aceptan caracteres no imprimibles.

- Nombres comunes (CNs) deben ser codificados como cadenas imprimibles (printableStrings) conforme al RFC 1778. La longitud máxima del CN es de 128 caracteres.

Certificado de servidor (host)

- Para el certificado de servidor, el nombre del servidor y el de dominio completo (FQDN). El nombre debe estar en minúsculas. No se aceptan direcciones IP

CN = serv1.unam.mx

- El dominio deberá ser resoluble por DNS al momento de la solicitud.

- Nombres comunes (CNs) deben ser codificados como cadenas imprimibles (printableStrings) conforme al RFC 1778. La longitud máxima del CN es de 128 caracteres.

- El conjunto de caracteres permitidos para CommonName (CN), en los certificados de servidor es:

'a' - 'z', '0' - '9' se aceptan punto y guión medio.

No se aceptan espacios, mayúsculas ni caracteres no imprimibles.

3.1.2 Necesidad de nombres sean significativos

El Nombre Distintivo de un sujeto (DN) en un certificado debe tener una asociación razonable con la identidad del usuario; debe ser lo más completo posible con el fin de evitar colisiones de nombres entre diferentes usuarios e identificar plenamente al usuario. Los solicitantes deben elegir una representación de sus nombres acordes a los caracteres permitidos (véase 3.1.1). El nombre no debe referirse a un rol. Los solicitantes no pueden ser anónimos ni utilizar seudónimos.

3.1.3 Del anonimato o seudónimos de los solicitantes

No se expedirán certificados de persona física a los roles o funciones, sólo se realizará para personas nombradas e identificadas.

3.1.4 Unicidad de los nombres

Los nombres distintivos (DN) deben ser únicos para cada sujeto y no deben producir ambiguedad.

Asimismo, no deben existir dos certificados activos emitidos por una misma CA cuyo subject DN sea idéntico, excepto cuando se encuentren en proceso de transición por renovación, cuyo periodo no excederá los 30 días.

En caso de controversia será la UNAMgrid CA, la responsable de establecer criterios de resolución apegada a las políticas de certificación.

3.1.5. Resolución de conflictos relativos a nombres

Para garantizar la unicidad en los nombres, el sistema en el momento de la solicitud rechazara cualquier tipo de homonimia, para resolverlo el usuario deberá agregar un número al final o modificar el nombre.

1) CN=jose.luis.valle
2) CN=jose.luis.valle2

La AC UNAMgrid no resolverá disputas relativas a la titularidad o preferencias de nombres, entidades o personas, nombres de dominio o marcas personales.

Los certificados deben aplicarse a personas o recursos únicos.

3.2 Validación de identidad inicial

3.2.1 Método para probar la posesión de la llave privada

Se verifica la posesión de la llave privada mediante la validación de la firma electrónica de la solicitud de emisión del certificado (CSR).

3.2.2 Autenticación de la identidad de una organización

Se verificará que el solicitante, la organización o la unidad de una organización tiene derecho (ver 1.3.3) a obtener un certificado de la UNAMgrid CA para que se apruebe la emisión.

La primera vez que un solicitante quiera obtener un certificado para persona física, servidor o servicio, tiene que acudir al punto de registro y notificar a la UNAMgrid CA.

Debe demostrar que existe la organización (VO) o unidad organizativa y que se tiene derecho a solicitar un certificado UNAMgrid.

Para este fin se solicitará un oficio en hoja membretada, por parte de la institución, que permita validar la pertenencia a una organización, o proyecto, la autorización y su vigencia,

esta deberá estar firmada en original por el responsable del proyecto y el solicitante. Esta información será validada por parte de la UNAMgrid CA con el punto de registro de la grid.

En caso de que se solicite la adhesión de varios usuarios de un mismo proyecto, estos se podrán integrar en un solo oficio.

Esta documentación se renovará al término de vigencia de los certificados con la finalidad de mantener actualizado el archivo de identidad de la organización.

3.2.3 Autenticación de la identidad individual

Con el fin de permitir autenticar la identidad del solicitante éste debe reunirse de manera presencial con el punto de registro autorizado por la CA UNAMgrid y entregar la siguiente documentación:

- Carta de intención del usuario (solicitante) esta deberá ser individual y firmada en autógrafa en original.
- Copia simple por ambos lados de la identificación oficial (como INE, pasaporte, cédula profesional, credencial de estudiante o académico de la institución).
- Carta compromiso del titular, documento de reconocimiento de derechos y obligaciones en el uso del certificado digital.

Asimismo, el responsable de la verificación de identidad, solicitará mostrar la identificación original para cotejo.

3.2.4 Información del usuario (solicitante) no verificada

En caso de que la información del usuario no pueda ser verificada no se podrá emitir certificado digital a nombre del solicitante.

3.2.5 Validación de la autoridad

Para la validación de las personas autorizadas a solicitar certificados en la autoridad de servidor (host) o de servicio, se deberá entregar en el punto de registro, un documento físico, firmado por una persona autorizada por la institución donde se especifique al administrador del sistema responsable.

Esto deberá ser suficiente para los futuros intercambios de información o peticiones provenientes de esa organización/entidad.

La organización/entidad deberá informar a la UNAMgrid CA en caso de rescindir la autorización del individuo por escrito.

3.3 Identificación y autenticación de las solicitudes de renovación de llave

3.3.1 Identificación y autenticación de la solicitud de renovación

La renovación de certificados digitales podrá hacerse vía remota a través de la interfaz web del sitio de la UNAMgrid AC:

https://ca.unamgrid.unam.mx/

Si se cuenta con certificado aún vigente, este se deberá presentar como mecanismo de acceso para utilizar la interfaz web. En el menú, *Renovar certificado*, se podrá solicitar la renovación, el proceso de generación del nuevo par de llaves está amparado por la llave privada almacenada en el equipo de cómputo de la solicitante, misma que lo autentica.
El periodo para realizar la solicitud de un certificado será 30 días antes del vencimiento del mismo. Una vez que el certificado haya perdido vigencia no podrá ser renovado.

3.3.2 Identificación y autenticación de las solicitudes de renovación de llave después de una revocación

Después de la revocación de un certificado, la renovación no es posible, debe realizarse nueva solicitud de registro.

Para ello deberá ingresar al sitio web de la UNAMgrid AC https://ca.unamgrid.unam.mx/, en el menú, Solicitud de certificado y llenar el formulario correspondiente.

Debido a que ya no se cuenta con elementos que garanticen de forma fiable e inequívoca la identidad del solicitante y la autenticidad de la solicitud, para que la aprobación de la renovación proceda esta deberá incluir la entrega de un documento membretado por parte de la institución donde se valide su permanencia en el proyecto y su autorización (ver 3.2.2 y 3.2.3.).

3.4 Identificación y autenticación para solicitud de revocación

A menos que la solicitud de revocación se origine en la UNAMgrid CA porque se ha identificado que se ha comprometido la llave en forma alguna, la solicitud de revocación deberá ser verificada y la parte solicitante deberá autenticarse.

Para la solicitud de revocación correspondiente el usuario deberá ingresar desde el equipo donde tenga su certificado digital al sitio web de la UNAMgrid CA https://ca.unamgrid.unam.mx/ en el menú, Revocación.

Una vez que solicite su revocación el titular (suscriptor) recibirá un correo por parte de la UNAMgrid CA, notificando la solicitud.

Si la solicitud no es confirmada por parte del titular (suscriptor), no se llevará a cabo.

En caso de no contar con el certificado, la revocación puede iniciarse a través de la comunicación directa vía correo electrónico (camanager at unam.mx) con la UNAMgrid CA.

El titular deberá indicar los motivos por los que solicita la revocación y confirmar vía sistema su solicitud.

La UNAMgrid CA determinará los medios para validar la identidad del usuario y proceder a la revocación.

4. Ciclo de vida de certificados

4.1 Solicitud de certificados

La UNAMgrid CA determinará previamente los requisitos y reglas para la aprobación y/o rechazo de las solicitudes de certificados digitales, observando en todo momento las estipulaciones previstas en este documento.

Asimismo será responsable de aprobar los tipos de certificado digital en función de los perfiles de los solicitantes y las autorizaciones para tal efecto.

4.1.1 De los autorizados a presentar solicitud de certificado digital

La UNAMgrid CA emite certificados para las siguientes entidades:

- Entidades académicas principalmente en México integradas a proyectos grid (universidades, institutos, entre otros).
- Centros de investigación académica principalmente en México integrados a proyectos grid (ya sea los sin fines de lucro, públicos o privados)
- Otras organizaciones con las afiliaciones de investigación y desarrollo
- Individuos autorizados pertenecientes a cualquiera de las entidades mencionadas anteriormente.

Las entidades sujetas de certificación pueden ser:

- Persona natural, para la autenticación de un individuo solamente;
- Hosts, administrados por la organización solicitante,

Asimismo estas solicitudes deberán cumplir con ciertos requisitos:

- Para el certificado personal:
  Que el solicitante este en posesión de la llave privada correspondiente y sea responsable de la gestión de la llave privada.

- Para los certificados de host:
  Que el solicitante es el administrador responsable del sistema y/o servidor para el que se solicita el certificado;

4.1.2 Proceso y responsabilidades de enrolamiento

El solicitante deberá ingresar al sitio web https://ca.unamgrid.unam.mx/ en el apartado Solicitud de certificados y proporcionar la información solicitada en el formulario.

La información capturada, deberá ser verificable y fidedigna, cualquier error deliberado u omisión de la misma podrá resultar en la negativa a continuar con el proceso de solicitud de certificado por parte de la CA.

Después de que el formulario se ha completado, la llave privada cifrada será almacenada en el navegador, al que únicamente tendrá acceso el solicitante.

Se generarán un par de llaves con un tamaño de llave de 2048 bits.

Adicionalmente los solicitantes deberán:

• Leer y apegarse a los procedimientos publicados en este documento.
• Utilizar el certificado exclusivamente para los propósitos autorizados.
• Autorizar el procesamiento y conservación de los datos personales por parte de la CA (conforme a la norma en materia de protección de datos).
• Tomar todas las precauciones para evitar la pérdida, divulgación o acceso no autorizado o el uso de la llave privada asociada al certificado, incluyendo:

- Uso de una contraseña robusta;
- Protección de la frase de seguridad y resguardo de su secrecía;
- Notificación inmediata al CA UNAMgrid y demás involucrados si la llave privada se encuentra comprometida;
- Solicitud de revocación, si la información en el certificado es incorrecta, se ha comprometido la llave o si ha prescrito el derecho a poseer uno.

4.2 Tramitación de solicitudes de certificados

4.2.1 Realizando funciones de identificación y autenticación

A través de la RA se realizará la comprobación de la identidad del solicitante y la veracidad de su información antes de procesar una solicitud pendiente, la AC UNAMgrid la aprobará en función de la información que retroalimente la RA.

En el caso de una solicitud para servidor/servicio deberá también verificar que el usuario es responsable del host dentro de la organización o unidad propietaria del host.

4.2.2 Aprobación o rechazo de solicitudes de certificado

La aprobación de la solicitud de un certificado digital dependerá de:

- Que el solicitante esté autorizado conforme a lo establecido en el apartado 4.1.1 de este documento.
- Que demuestre su participación en un proyecto grid.
- Que se pueda comprobar la validez y veracidad de la información de identidad.
- Que la RA otorgue su aprobación y visto bueno.
- Que cumpla con las reglas de operación establecidas en el presente documento.

Si la información de autenticación es inexacta o si una parte solicitante no cumple con los requisitos de autenticación mencionados anteriormente, dentro de los 10 días hábiles, luego de que la solicitud haya sido recibida por la RA, la solicitud será rechazada. Si la parte solicitante insiste en conseguir un certificado deberá iniciar una nueva solicitud.

Toda la documentación referente a la identificación y autenticación del titular de un

certificado digital, será clasificada y archivada de manera física en el departamento responsable de la administración de la UNAMgrid AC.

Asimismo estará disponible de manera digital en un repositorio de datos público pero con acceso restringido únicamente a los miembros de la grid, esto en apego a la legislación en materia de protección de datos personales de la UNAM.

4.2.3 Tiempo para procesar solicitudes de certificado

El tiempo que se requiere en el lapso comprendido desde la solicitud hasta la emisión depende mayormente del proceso de entrega de documentación, validación y autenticación, pero el certificado debe emitirse dentro de los tres días siguientes a la recepción de la documentación.

4.3 Emisión de Certificados

4.3.1 Acciones de la CA durante la emisión de certificados

Una vez creado el CSR y validada su pertinencia, el sistema creará y firmará el certificado. El certificado firmado podrá ser entonces transferido y entregado a su titular.

La UNAMgrid CA:

- Utiliza un procedimiento de emisión de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la llave pública certificada.
- Protege la confidencialidad e integridad de los datos de registro.
- Toma medidas contra la falsificación de certificados.
- Emite basado en las normas establecidas por el último CP/CPS aprobado por TAGPMA.

4.3.2 Notificación al titular (suscriptor) por la CA acerca de la emisión del certificado

El sistema de la UNAMgrid CA notificará al solicitante vía correo electrónico de la aprobación de su solicitud, asimismo enviará una URL de la página de descarga del certificado y un reconocimiento de la emisión a la RA correspondiente.

Un certificado (personal o de host) será válido por 13 meses a partir de la fecha de emisión o menos en casos específicos (por ej., si se prevé que la afiliación del solicitante con la organización / unidad terminará en menos de un año).

4.4 Aceptación de certificados

4.4.1 Conducta de aceptación de un certificado

El solicitante deberá en primer lugar, una vez recibido el correo electrónico que indica la URL para la descarga de su certificado, verificar las características del certificado y el uso apropiado del mismo, si el resultado es correcto y no hay ninguna objeción, el titular deberá notificar a la UNAMgrid CA y a la RA de su aceptación del certificado.

Si el certificado es rechazado, deberá notificar a la CA sobre el rechazo, explicando a la CA y la RA las razones de ese rechazo. Los certificados cuyo rechazo no hayan sido recibidos por la CA dentro de una semana serán considerados aceptados.

4.4.2 Publicación del certificado por la CA

La UNAMgrid CA publicará los certificados tan pronto como sean emitidos, en su sitio web.

http://ca.unamgrid.unam.mx/

4.4.3 Notificación de emisión de certificado por la CA a otras entidades

No estipulado.

4.5 Par de llaves y uso del certificado

4.5.1 Llave privada del titular (suscriptor) y uso del certificado

Los certificados emitidos por la UNAMgrid CA y sus llaves privadas asociadas deben ser usados exclusivamente para los fines autorizados, establecidos en la sección 1.4.

Deben ser usados sólo de acuerdo a los campos de uso de llave del certificado. Asimismo cuando un certificado es revocado o ha expirado, la llave privada asociada no deberá ser usada nunca más.

Los titulares (suscriptores), no deben compartir certificados. La UNAMgrid CA se reserva el derecho de revocarlos por uso indebido de los mismos.

4.5.2 Llave pública y uso del certificado del tercero aceptante

Una entidad que confía (tercero aceptante) debe, luego de obtener un certificado emitido por la UNAMgrid CA, comprobar su validez:

- Verificando que el certificado procede la UNAMgrid CA
- Consultando el OCSP o la CRL de la UNAMgrid CA en vigor en el momento de su uso
- Verificando su uso adecuado conforme a los campos de uso incluidos en el certificado

4.6 Renovación del certificado

La renovación del certificado es el proceso por el cual se genera un nuevo certificado, con un nuevo período de validez extendido. Los usuarios pueden renovar su certificado mientras no haya sido revocado o expirado el anterior. La renovación del certificado debe estar respaldada por la RA correspondiente, que deberá constatar que no hay riesgos en la reutilización.

4.6.1 Circunstancias de renovación del certificado

Un certificado puede ser renovado si no ha llegado al término de su periodo de validez, si no ha sido revocado y si el nombre del titular (suscriptor) y atributos aún son correctos.

Únicamente cuando la RA verifica que el certificado no ha sido revocado, la CA acepta y procesa la solicitud de renovación. La UNAMgrid CA puede decidir rechazar esa renovación por motivos de seguridad, para evitar riesgos derivados de largas exposiciones de llaves privadas. La RA deberá validar que el solicitante todavía esté trabajando en el proyecto original. El solicitante de la renovación debe preguntar al líder de proyecto que originariamente confirmó la necesidad del usuario de un certificado, para informar a la RA que el usuario todavía tiene derecho a un certificado.

El periodo para realizar la solicitud de renovación de un certificado será 30 días antes del vencimiento del mismo.

4.6.2 Quién puede pedir renovación

El titular del certificado puede pedir la renovación de su certificado digital, antes de que este expire a través de la interfaz web, utilizando su certificado digital vigente como método de autenticación, el cual deberá de tener el mismo DN.

Para los certificados de servidor (host), estos pueden ser solicitados por los responsables del servidor o servicio y deben presentar el certificado que se solicita renovar como medio de autenticación.

4.6.3 Procesamiento de solicitudes de renovación de certificados

Una vez recibida la solicitud correspondiente, respaldada por la RA, la UNAMgrid CA procesa la renovación como una petición de certificado nuevo.

Los usuarios pueden hacer nuevas solicitudes de certificados, pero deben probar su identidad usando su certificado actual. La solicitud debe tener el mismo DN que el certificado usado para probar la identidad.

Luego de la recepción de la solicitud constatada por la RA correspondiente, la UNAMgrid CA deberá procesar la renovación como una solicitud de certificación nueva.

4.6.4 Notificación de nueva emisión de certificado a titular (suscriptor)

La UNAMgrid CA deberá notificar al titular de la emisión, tal como se describe en la sección 4.3.2.

4.6.5 Conducta de aceptación de un certificado de renovación

Véase 4.4.1

4.6.6 Publicación del certificado de renovación por parte de la CA

Véase 4.4.2

4.6.7 Notificación de emisión de certificado por la CA a otra entidad

No estipulado.

4.7 Renovación de llaves

4.7.1 Circunstancias para el cambio de llaves de certificados

La renovación de llaves, implica la generación de un nuevo certificado conservando el mismo DN.

Las razones para solicitar la renovación pueden ser debido a llave comprometida, daño del certificado o pérdida del mismo.

4.7.2 Quién puede solicitar una nueva llave

El titular de un certificado válido puede solicitar la certificación de una nueva llave pública en un CSR firmado con su llave privada vigente y válida.

Si el certificado ya ha expirado, debe realizarse el procedimiento de solicitud de certificado nuevo.

4.7.3 Procesamiento de solicitudes de cambio de contraseña de certificados

Debido a que no existe la modalidad de cambio de contraseña de un certificado activo vigente. Para realizar el cambio se deberá generar una solicitud de certificación nueva.

4.7.4 Notificación de emisión de nuevos certificados a titulares (suscriptores)

La UNAMgrid CA notificará a los titulares sobre la emisión como se describe en 4.3.2. para la emisión de certificado nuevo.

4.7.5 Conducta de aceptación de un certificado con contraseña nueva

Mismo procedimiento descrito en 4.4.1

4.7.6 Publicación del certificado con nueva contraseña por la CA

Véase 4.4.2.

4.7.7 Notificación de emisión de certificado de CA a otras entidades

No estipulado.

4.8 Modificación de certificado

4.8.1 Circunstancias de modificación de certificado

Los certificados no pueden ser modificados. Deberán ser revocados, y un nuevo par de llaves deberán ser generadas así como también una nueva solicitud para los contenidos del certificado modificado. La revocación puede ser condicional a la emisión y aceptación del nuevo certificado, y así el certificado anterior será revocado sólo luego de que el nuevo sea aceptado.

4.8.2 Quién puede solicitar modificación de un certificado

El titular (suscriptor) de un certificado digital podrá solicitar la modificación de los datos contenidos en el certificado, cuando estos sean inexactos o hayan cambiado, sólo si se refieren a datos personales.

El responsable de un certificado de host podrá solicitar la modificación de los datos contenidos en el certificado, cuando estos sean inexactos o hayan cambiado.

En todos los casos la modificación implicará la revocación del certificado actual.

4.8.3 Procesamiento de solicitudes de modificación de un certificado

Para la solicitud de modificación de datos, el titular (suscriptor) deberá enviar un correo a la RA indicando las razones de la solicitud, así como los documentos probatorios correspondientes del motivo del cambio.

4.8.4 Notificación de emisión de un nuevo certificado al titular (suscriptor)

La UNAMgrid CA deberá notificar al titular de la emisión, tal como se describe en la sección 4.3.2.

4.8.5 Conducta de aceptación del certificado modificado

Mismo procedimiento descrito en 4.4.1

4.8.6 Publicación del certificado modificado por la CA

Véase 4.4.2.

4.8.7 Notificación de emisión del certificado de la CA a otras entidades

No estipulado.

4.9 Revocación y suspensión de un certificado

La revocación de un certificado digital implica la baja permanente del par de llaves y la pérdida de sus privilegios de acceso y uso en los sistemas grid. Esta baja no libera la responsabilidad sobre el uso de este, mientras estuvo vigente.

4.9.1 Circunstancias de revocación

Las principales razones para solicitar una revocación serán:

- Debido a que el titular (suscriptor) ha dejado de ser un miembro o asociado de un programa o actividad de UNAMgrid CA.
- La llave privada del titular (suscriptor) se extravía o se sospecha está comprometida.
- No se necesita más.
- La información en el certificado del titular (suscriptor) es incorrecta o imprecisa.
- El titular (suscriptor) no cumplió con la reglas del presente documento,
- El sistema (host o servicio) para el cual fue emitido el certificado, fue dado de baja.
- La llave privada de la CA se ha extraviado o se encuentra comprometida.
- A solicitud del titular (suscriptor).

4.9.2 Quién puede solicitar revocación

Una revocación puede ser solicitada por:

- El propietario de la llave certificada.
- La UNAMgrid CA o la RA que tenga prueba de llave comprometida.
- La organización o entidad que desea revocar su consentimiento a estar incluida en un certificado.
- La RA que autenticó al propietario del certificado.
- El titular (suscriptor) del certificado.
- Cualquier persona que presente prueba de conocimiento de que la contraseña del titular (suscriptor) está comprometida o que los datos del titular (suscriptor) han cambiado.

4.9.3 Procedimiento para solicitud de revocación

A menos que la UNAMgrid CA realice directamente la revocación, la solicitud de revocación debe ser efectuada por:

- El titular (suscriptor) del certificado, debidamente autenticado, usando las opciones de revocación dispuestas en la página web. En caso de emergencia o no contar con pérdida de la llave privada del certificado, deberá informar a la RA tan pronto como sea posible y solicitarle realice la revocación.

- El administrador de la CA usando una interfaz web segura, solamente en el caso de pérdida de la llave privada del certificado por parte del usuario.

Antes realizar la revocación, la UNAMgrid CA deberá verificar la fuente de la solicitud de acuerdo con los procedimientos para el registro inicial.

Asimismo el titular (suscriptor) deberá confirmar un correo de solicitud de revocación para que esta se lleve a cabo.

4.9.4 Período de gracia para solicitudes de revocación

Se tendrán máximo 7 días hábiles para confirmar la solicitud de revocación. En caso contrario el certificado permanecerá activo y se notificará nuevamente al titular.

En caso de recibir confirmación por parte del titular, la UNAMgrid CA tramitará la solicitud con prioridad y publicará la revocación inmediatamente.

4.9.5 Tiempo dentro del cual la CA deberá procesar la solicitud de revocación

La UNAMgrid CA debe procesar las solicitudes de revocación con la más alta prioridad, estas no podrán exceder 2 días hábiles a partir de la solicitud confirmada.

4.9.6 Requerimientos de verificación de revocaciones en partes dependientes

Se recomienda que las entidades que confían y las partes dependientes, verifiquen un certificado contra la CRL más actualizada publicada por la CA para validar el uso del certificado o a través del servicio OCSP proporcionado.

4.9.7 Frecuencia de emisión de CRL (si fuera aplicable)

Las CRLs se actualizan y vuelven a emitirse luego de cada revocación o por lo menos 7 días antes de la expiración de la CRL anterior.

4.9.8 Latencia máxima de CRL (si fuera aplicable)

No aplica.

4.9.9 Disponibilidad de verificación en línea de revocaciones/estatus

La última CRL está siempre disponible en el sitio Web de la UNAMgrid. La UNAMgrid CA publicará la CRL en efecto en su repositorio (véase 2.1). El servicio en línea de OCSP estará disponible en todo momento.

Para consultarla se puede acceder y descargar el archivo en la URL

http://ca.unamgrid.unam.mx/pub/crl/unamgrid-crl.crl

4.9.10 Verificación en línea de requisitos de las revocaciones

Una entidad que confía debe comprobar a través la CRL, antes de utilizar y confiar en un certificado. La única CRL válida para los certificados emitidos por la UNAMgridCA será la publicada en su sitio web, esta se genera y firma con la llave de la CA. El servicio en línea de OCSP estará disponible en todo momento.

4.9.11 Otras formas de publicación de las revocaciones disponibles

Se encontrará disponible el servicio en línea de OCSP para la consulta del estatus de los certificados incluyendo los revocados.

En todos los casos se informará a los titulares (suscriptores) de los cambios de estatus de sus certificados a través de un correo electrónico.

4.9.12 Requisitos especiales de renovación de llaves comprometidas

No aplican requisitos especiales, véase 4.6

4.9.13 Circunstancias para suspensión

No está estipulado.

4.9.14 Quién puede solicitar suspensión

No está estipulado.

4.9.15 Procedimiento para solicitud de suspensión

No está estipulado.

4.9.16 Límites del período de suspensión

No está estipulado.

4.10 Servicios de comprobación de estatus del certificado

4.10.1 Características operativas

La UNAMgrid CA deberá guardar en su repositorio público y hacer disponibles a través de su web site:

- El certificado de raíz de la CA
- Todos los certificados emitidos y sus estatus
- La CRL más actualizada
- La URL del servicio en línea de OCSP

4.10.2 Disponibilidad del servicio

La UNAMgrid CA deberá mantener disponible los servicios de forma continua, 24x7x365, salvo casos de fuerza mayor, no obstante en ningún caso la disponibilidad, podrá ser inferior a un 99,5% al mes.

Para este fin, la UNAMgrid CA contará con redundancia en sus sistemas, garantizando la continuidad de los mismos. Asimismo contará con un DRP de aplicación inmediata en caso de contingencia.

Las ventanas de mantenimiento serán notificadas a todos los involucrados en el sistema, vía correo electrónico, con un mínimo de 48 horas de antelación y serán realizadas preferentemente en horas y días no hábiles.

El horario de atención a usuarios por parte del personal a cargo, es de lunes a viernes de 9:00 horas a 19:15 horas en periodo de actividades regulares de la UNAM. Este horario se extenderá si las solicitudes se realizan vía correo electrónico.

4.10.3 Características opcionales

No estipuladas.

4.11 Finalización de la suscripción

La suscripción finaliza con la expiración del certificado si no es renovado o cambiadas sus llaves (re-key) antes de esa fecha. Una suscripción puede finalizar si el titular (suscriptor) solicita la revocación de su certificado.

4.12 Preservación de llave y recuperación

4.12.1 Políticas y prácticas de preservación y recuperación de contraseñas

No se proveen políticas al respecto. El dueño de la llave deberá tomar sus propias precauciones para prevenir la pérdida de su contraseña.

4.12.2 Políticas y prácticas de encapsulamiento y recuperación contraseñas de acceso

Véase 4.12.1

5 INSTALACIÓN, ADMINISTRACIÓN Y CONTROLES DE SEGURIDAD FÍSICA Y OPERACIÓN

5.1 Controles de seguridad física y lógica

La UNAMgrid CA se encuentra alojada en la Ciudad de México, en un centro de datos TIER IV, el cual cumple con los más altos estándares de seguridad física y perimetral así como con disponibilidad de los servicios del 99.9% e infraestructura redundante necesaria.

Los servidores se encuentran alojados en edificio inteligente con construcción antisismica y muros perímetrales de concreto armado, asimismo el acceso a los gabinetes es a través de chapas de combinación electrónica.

Para la protección de la llave raíz de la autoridad, está se encuentra resguarda en un dispositivo criptográfico HSM (Hardware Security Module) FIPS 140-2 nivel 3, que imposibilita que está sea extraída o replicada, garantizando la confiabilidad e integridad de la llave.

Se requiere de la intervención de 3 responsables de la custodia de los tokens para realizar cualquier modificación o intervención en la configuración del HSM y la llave raíz.

5.1.1 Ubicación y construcción

La UNAMgrid CA se encuentra alojada en un centro de datos en la Ciudad de México, administrado fuera de las instalaciones de la UNAM.

Para mayor información al respecto contatar al Departamento de Identidad y Firma Electrónica Avanzada de la UNAM.

5.1.2 Acceso físico

El ingreso al sitio de alojamiento de la UNAMgrid CA es mediante acceso controlado con vigilante, para poder acceder es necesario contar con una autorización previa por parte de la UNAM y presentar credenciales de identificación ante los responsables en sitio. Todos los asistentes son registrados a traves del uso de dispositivos biométricos y se lleva el control, en bitácora.

En ningún caso se permite el acceso sin la presencia de al menos un responsable registrado por parte de la UNAM.

El centro de datos, cuenta con una bitácora de responsables autorizados para ingresar o permitir el acceso a terceros.

Se monitorea permanente a los visitantes durante su estancia, vía circuito cerrado 7x24.

5.1.3 Suministro eléctrico y aire acondicionado

Entre los principales servicios proporcionados por el sitio de alojamiento estan:

- Doble acometida eléctrica.
- Generación de energía eléctrica en caso de contingencia (planta de emergencia)
- Sistema de enfriamiento de precisión redundante, que permiten mantener las condiciones ideales para el óptimo funcionamiento de los servidores y dispositivos

de la UNAMgrid CA.

5.1.4 Exposición al agua

El sitio cuenta con detectores de presencia de agua, no obstante que el diseño y ubicación del edificio garantiza la inexistencia de peligro por inundación.

5.1.5 Prevención y protección del fuego

Se cuenta con sistemas de prevención, detección y supresión de incendios VESDA y de extinción automática.

5.1.6 Medios de Almacenamiento

Los medios removibles (tokens) que protegen al HSM y a la llave raíz se encuentran almacenados en lugar seguro (caja de seguridad de la dependencia) y con acceso restringido.

5.1.7 Eliminación de residuos

Los medios de almacenamiento o soportes que contengan datos que requieran protección (datos criptográficamente relevantes como contraseñas o llaves privadas, o datos personales) serán desechados de manera que se garantice que la información no pueda volver a utilizarse.

5.1.8 Respaldo fuera del sitio

Un respaldo mensual es almacenado de manera remota en un sitio alterno alojado en la UNAM.

Este respaldo permitirá activar el plan de emergencia para la alta disponibilidad del servicio en caso de incidente grave o caída del sitio principal.

5.2 Controles de Procedimiento

5.2.1 Roles de confianza

No está estipulado

5.2.2 Número de personas requeridas por tarea

Se requieren al menos tres personas para la generación, almacenamiento y activación de llave raíz en los HSM´s. Cualquier modificación a los parámetros requiere de la autenticación de los tres autorizados con privilegios suficientes.

El administrador de la UNAMgrid no tiene acceso a esta información, ni a los dispositivos (tokens) de acceso.

5.2.3 Identificación y autenticación para cada rol

No está estipulado

5.2.4 Roles que requieren separación de tareas

Excepto por la administración, ningún tipo de rol en la UNAMgrid CA requiere separación de tareas.

La información sobre un titular (suscriptor) almacenada en el sitio físico de la UNAMgrid CA que se considere privada (véase 9.4.2) debe ser sólo accesible a los operadores de la RA.

Toda la información proporcionada estará protegida por el "Reglamento de Transparencia, Acceso a la Información Pública y Protección de Datos Personales para la Universidad Nacional Autónoma de México", publicado el 12 de septiembre de 2011, en Gaceta UNAM.

5.3 Controles de seguridad de personal

5.3.1 Aptitudes, experiencia y requerimientos de acreditación

El equipo de la UNAMgrid CA se encuentra conformado por diversos perfiles enfocados a la administración y gestión de la CA.

Estos perfiles estan divididos en administrador de base de datos, administrador de sistema, administrador de proyectos, oficial de seguridad y desarrolladores en Java.

El personal de la UNAMgrid CA tiene más de 10 años de experiencia en tecnologías de PKI y habilidades de administración de sistemas.

Todo el personal de la UNAMgrid CA es de absoluta integridad y confianza.

5.3.2 Procedimientos de comprobación de antecedentes

Todo el personal responsable de la gestión y operación de la UNAMgrid CA es personal contratado por la UNAM, por lo tanto se apega a las validaciones y verificaciones de probidad y honradez que la UNAM sigue para sus empleados.

5.3.3 Requerimientos de capacitación

Todo miembro del equipo de UNAMgrid CA recibirá capacitación por parte del equipo de UNAMgrid que desarrolló la interfaz de la CA.

Asimismo recibirán capacitación en temas de:

- Infraestructura de Llave Pública (PKI)
- Autoridades Certificadoras
- Aspectos legales de certificación
- Aspectos operativos de certificación
- Conocimiento de CPS

- DRP y planes de contingencia

5.3.4 Requerimientos y frecuencia de repetición de capacitación

La capacitación y su frecuencia estará determinada por:

- Cambios o modificaciones al software actual.
- Implementación de nueva plataforma de software.
- Modificación en reglas de operación y/o procedimientos organizacionales.
- Necesidades específicas del departamento.
- Incorporación de nuevos integrantes al equipo de trabajo.
- Redefinición de responsabilidades o roles.
- Actualización y reforzamiento de conocimientos por cambios tecnológicos.

5.3.5 Frecuencia y secuencia de rotación de tareas

No existe rotación en los perfiles y roles asignados al personal que administra la UNAMgrid CA.

5.3.6 Sanciones por acciones no autorizadas

En el caso de que ocurra una acción no autorizada, abuso de autoridad o uso no autorizado de sistemas de entidades de parte de los operadores de CA y RA, el administrador de CA puede revocar todos los privilegios implicados.

Adicionalmente, en función de la gravedad de la falta, se podrán aplicar diversas acciones previstas en la normatividad UNAM.

5.3.7 Requerimientos de contratante independiente

No está estipulado.

5.3.8 Documentación proporcionada al personal

Toda documentación necesaria para cumplir las tareas correspondientes deberá ser facilitada al personal de la UNAMgrid CA.

- Es responsabilidad del administrador de la CA suministrar a los operadores de la CA una copia de los “Procedimientos del Operador UNAMgrid CA”.
- Es responsabilidad del administrador de CA suministrar al administrador de la RA una copia de los “Procedimientos del Administrador UNAMgrid CA”.
- Es responsabilidad del administrador de la RA suministrar a los operadores de la RA una copia de los “Procedimientos del Operador UNAMgrid CA”.

5.4 Procedimientos de historial (log) para auditoría

5.4.1 Tipos de eventos registrados

Los siguientes eventos deberán ser registrados:

UNAMgrid CA host

- login / logout / reinicio
- Solicitud de certificados
- Creación y firma de certificados
- Cambio de estatus de certificados
- Validación de solicitud de certificado de la RA

5.4.2 Frecuencia de procesamiento de historial (log)

Los archivos de historial (log) deberán ser analizados una vez al mes o luego de que se sospeche o conozca una potencial brecha de seguridad; lo que ocurra primero.

5.4.3 Período de retención de los registros de auditoría

El período mínimo de retención de los registros de auditoría es de 3 años para los archivos de registro.

El período de retención mínimo de los historiaes (log´s) es de 3 años para archivos de historial (log).

5.4.4 Protección de los registros de auditoría

Los historiales (logs) para auditoría deberán ser accesibles sólo para los administradores UNAMgrid CA y personal de auditoría autorizado. La CA deberá seguir las buenas prácticas en la materia e instrumentar estrategias para proteger los logs.

5.4.5 Procedimientos de respaldo del historial para auditoría

Los registros de auditoría deberán respaldarse en un medio removible diaria excepto días festivos y cuando no hay actividad en el servidor y se deberá tener sólo acceso de lectura a los repositorios en línea cuando el servidor esté en línea.

El medio de backup deberá ser almacenado en un lugar seguro con acceso restringido.

5.4.6 Sistema de recopilación de auditoría (interno vs. externo)

No está definido.

5.4.7 Notificación al sujeto causa del evento

No está definido.

5.4.8 Análisis de vulnerabilidades

En lo que respecta a las posibles vulnerabilidades por intrusiones o accesos, lógicos o físicos se solicitará al sitio que aloja a la infraestructura, que entregue reportes mensuales.

Asimismo el personal de la UNAMgrid CA solicitará a la Coordinación de Seguridad de la Información de la DGTIC UNAM, realice auditorias de seguridad a sus sistemas. Una vez detectadas se realizarán las correcciones pertinentes.

5.5 Archivo de Registros

5.5.1 Tipos de registros archivados

Véase 5.4.1

5.5.2 Período de retención del archivo

El período mínimo de retención es de 5 años.

5.5.3 Protección del archivo

El archivo deberá ser accesible sólo para el personal autorizado de la UNAMgrid CA y se encontrará cifrado para su protección y confidencialidad.

5.5.4 Procedimiento de respaldo del archivo

Deberá hacerse un respaldo del registro en un medio removible, que deberá ser almacenado en un sitio con acceso restringido.

5.5.5 Requerimientos para estampado de tiempo de los registros

Todos los registros de eventos deberán soportar estampillado de tiempo, y estar sincronizados, basandose en el protocolo NTP, utilizando de referencia el reloj atómico del Centro Nacional de Metrología en México (CENAM).

5.5.6 Sistema de recolección de información (interno o externo)

El sistema de recolección de información es interno.

5.5.7 Procedimientos para obtener y verificar información del archivo

Sólo personal autorizado tiene acceso a los archivos físico de soportes y archivos digitales, para llevar a cabo verificaciones de integridad u otras.

Periodicamente se realizarán comprobaciones de la integridad de los archivos electrónicos de respaldo (backups).

5.6 Cambio de llave de la CA

El cambio de llave es el proceso por el cual se asigna una nueva llave pública a los usuarios de una CA. Cuando los datos criptográficos de la CA necesiten ser cambiados, la transición será hecha; desde el momento de distribución de los nuevos datos criptográficos, solo la nueva llave será usada para propósitos de firma. La superposición de la llave vieja y nueva debe ser de un año. El certificado viejo pero aún vigente debe estar disponible para verificar firmas viejas – y la llave privada para firmar CRLs – hasta que todos los certificados firmados usando la llave privada asociada, hayan expirado.

La CA generará un nuevo par de llaves raíz por lo menos un año antes de que expire el certificado de la CA. En el último año el certificado viejo de la CA estará disponible para propósitos de validación solamente, mientras que los nuevos certificados y CRLs serán firmados con la nueva llave de la CA.

El procedimiento para proporcionar la nueva llave de la CA a los titulares (suscriptores) y terceros aceptantes, es el mismo que para proporcionar la llave pública vigente.

La nueva llave pública estará disponible en el sitio web de UNAMgrid CA:

http://ca.unamgrid.unam.mx/

5.7 Recuperación en caso de compromiso de una llave o de desastre

5.7.1 Procedimientos de manejo de incidentes y compromiso de la llave

- Si la llave privada de la RA está comprometida o se sospecha esté comprometida, el operador o administrador de RA deberá informar a la CA y solicitar la revocación del certificado del operador de RA.

- Si la llave privada de la CA se encuentra o se sospecha comprometida, la CA deberá:

    - Informar a las Autoridades Registradoras, subscriptores, partes dependientes y CAs de certificación cruzada de los cuales la CA esté conciente.
    - Detener los servicios de certificación y distribución de CRL para certificados que usen la llave comprometida.
    - Revocar el certificado comprometido.
    - Generar un nuevo par de llaves y certificado de CA y publicar el nuevo certificado en el repositorio,
    - Revocar todos los certificados firmados usando la llave comprometida, y
    - Publicar la nueva CRL en el repositorio.

5.7.2 Recursos de cómputo, software y/o datos corruptos

La CA tomará precauciones en base al mejor esfuerzo para lograr la recuperación.

Para poder retomar la operación lo más pronto posible luego de que la infraestructura de cómputo de la CA está corrupta los siguientes pasos deberán ser tomados:

- Deberá hacerse un respaldo de todo el software de la CA en medios removibles luego de que una nueva versión de cualquiera de sus componentes es instalada.

- Deberá hacerse un respaldo de todos los archivos de datos de la CA fuera de línea en un medio removible después de cada cambio, antes de que se cierre la sesión.

En caso de corrupción de alguna parte del sistema mientras esta en operación, un hardware funcional deberá ser cargado con un respaldo del último estado del software y datos en un medio de sólo lectura y deberán considerarse como no corruptos. Si existiesen copias cifradas de las llaves privadas de la UNAMgrid AC que no han sido destruidas o perdidas, y no se hallan comprometidas, la operación deberá ser restaurada cuanto antes posible sin necesidad de revocar todos los certificados emitidos.

5.7.3 Procedimientos de compromiso de llave privada de entidad

En caso de que la llave de una entidad final se extravíe o comprometa, la entidad final debe informar a su RA para la solicitud de su certificado.

En el caso de que la llave de una entidad final o de una RA esté comprometida, el certificado correspondiente debe ser revocado. Está información será publicada por la CRL. Las partes de confianza conocerán esta información al consultar la CRL o hacer uso del servicio OCSP.

5.7.4 Capacidad de continuidad luego de un desastre

En caso de indisponibilidad en el acceso a hardware o software de la CA, por un periodo superior a 6 horas, se procederá a activar el DRP correspondiente.

Este plan garantizará la recuperación de los servicios y la disponibilidad con recursos alternos en menos de 12 horas a partir de su puesta en marcha.

5.8 Terminación o cese de operativa de CA

Las principales causas para la terminación de la CA serán:

- Compromiso de la llave privada de la CA.
- Decisión a voluntad de las partes (RA, titulares (suscriptores) y partes dependientes de la CA).
- Causas fortuitas o de fuerza mayor.

Antes de que la UNAMGrid CA termine sus servicios, deberá:

- Informar a TAGPMA.
- Informar a las RA, suscriptores y partes dependientes que la CA conozca.
- Proporcionar la información disponible.
- Dejar de emitir certificados.
- Revocar todos los certificados.

- Emitir y publicar una CRL.
- Destruir sus llaves privadas y copias de éstas.

En el caso de una terminación normal (programada), el tiempo de notificación mínimo debe ser de 60 días. El administrador de la CA será responsable del archivo posterior de todos los registros al momento de terminación como requerido en la sección 5.5.2.

El administrador de la CA puede decidir permitir que la CA emita CRLs solo durante el último año (por ejemplo, el tiempo de validez máximo del certificado de un titular (suscriptor) antes de la terminación definitiva; esto permitirá que los certificados de los titulares (suscriptores) puedan usarse hasta que expiren. En este caso la notificación de terminación se dará a no menos de un año y a 60 días previos a la terminación, por ejemplo, no menos de 60 días antes de que la CA deje de emitir nuevos certificados.

6 CONTROLES DE SEGURIDAD TÉCNICA

6.1 Generación e instalación del par de llaves

6.1.1 Generación del par de llaves

La llave privada de la CA se encuentra bajo control de multipersona, esta se activa mediante la inicialización y creación de la llave en el HSM por medio de una combinación de al menos 3 miembros de la comunidad universitaria relacionados con la administración, operación y uso de la UNAMgrid CA.

El par de llaves para la UNAMgrid CA es generado en un HSM mediante una ceremonia de creación de llaves diseñada para tal fin. En esta ceremonia connotados miembros de la comunidad universitaria de manera presencial testifican la creación en el HSM de la llave raíz.

Los pares de llaves para certificados personales, hosts o servicios son generados en la interfaz web, por las partes solicitantes en su equipo personal bajo su control total.

6.1.2 Entrega de llaves privadas a un titular (suscriptor)

Cada titular (suscriptor) debe generar su propio par de llaves usando la interfaz web de UNAMgrid.

La CA no entrega llaves privadas para sus titulares (suscriptores) de manera presencial.

6.1.3 Entrega de llave pública a un emisor de certificados

Las llaves públicas de los titulares (suscriptores) son entregadas a la CA emisora por el protocolo HTTP vía interfaz web de UNAMgrid CA.

6.1.4 Entrega de llaves públicas de CA a partes dependientes

El certificado de la CA (conteniendo su llave pública) es entregado a los titulares (suscriptores) en línea desde el servidor web de la UNAMgrid CA. Asimismo este puede ser descargado desde el repositorio (Véase 2.1).

6.1.5 Tamaño de llaves

Llaves de longitud menor a 2048 bits no serán aceptadas. La llave de la UNAMgrid CA es de 4096 bits de longitud.

6.1.6 Parámetros de generación de llaves públicas y control de calidad

No está definido.

6.1.7 Propósitos de uso del campo llave (X.509 v3)

Las llaves deberán ser usadas de acuerdo al tipo de certificado:

- Con un certificado de entidad final para:
  - Autenticación.
  - No-repudio.
  - Cifrado de datos y llaves.
  - Integridad del mensaje.
  - Establecimiento de sesión.
  - Creación de proxy y firmado.

- Con un certificado de RA para:
  - Algunas de las actividades necesarias para el trabajo de un agente de la RA.

- Con el certificado auto firmado por la CA
  - Firma de certificados.
  - Firma de CRL.
  - Firma de OCSP.

La llave privada de la CA es la única llave que puede ser usada para firmar certificados, OCSP y CRLs.

6.2 Protección de Llave Privada y Controles de Ingeniería de Modelo Criptográfico

6.2.1 Estándares y controles de módulos criptográficos

La llave privada de la UNAMgrid CA es generada directamente a través del software del módulo criptográfico HSM (FIPS 140-2 nivel 3), bajo estrictas medidas de seguridad y con un protocolo de generación definido. Esta es resguardada desde su creación hasta el tiempo de vida de su vigencia en el módulo.

Una instancia extra de la llave privada cifrada con una contraseña generada al aleatoriamente de por lo menos 15 caracteres es almacenada en un módulo criptográfico alterno, la frase de seguridad deberá ser almacenada en un medio removible o escrito, y el medio o papel deberá ser colocado en un sobre sellado y almacenado en un lugar seguro.

La llave privada de la CA residirá exclusivamente en dispositivos criptográficos (HSM) sin acceso a externos en línea.

Las entidades finales generan a través del sitio web disponible de la UNAMgrid CA para generación de llaves y CSR.

6.2.2 Control multipersona de llave privada (n de m)

La llave privada de la CA se encuentra bajo control de multipersona, esta se activa mediante la inicialización y creación de la llave en el HSM por medio de una combinación de al menos 3 miembros de la comunidad universitaria relacionados con la administración, operación y uso de la UNAMgrid CA.

6.2.3 Custodia de llave privada

Las llaves privadas no son recuperadas, el personal de la UNAMgrid CA no tiene acceso a estas ni las recupera por ningún medio.

6.2.4 Respaldo de la llave privada

El respaldo de la llave privada de la CA se encuentra alojado en un dispositivo HSM alterno, bajo estrictas medidas de seguridad físicas y lógicas. El sitio donde se resguarda cuenta con protección ante siniestros, y con control de acceso y monitoreo constante.

6.2.5 Archivo de llaves privada

No está estipulado.

6.2.6 Transferencia de llave privada desde o hacia un módulo criptográfico

La llave privada se resguarda en el módulo criptográfico desde su creación y permanece hasta el término de su vigencia.

6.2.7 Almacenamiento de llave privada en un módulo criptográfico

Ver 6.2.1

6.2.8 Método de activación de la llave privada

La llave privada de la CA es activada en un esquema multipersona con el uso de dispositivos criptográficos portátiles (tokens) en el HSM.

6.2.9 Método de desactivación de la llave privada

La desactivación de la llave privada se realizará en un esquema multipersona con el uso de dispositivos criptográficos portátiles (tokens) en el HSM.

6.2.10 Método de destrucción de llave privada

Debido a que la llave privada se encuentra resguardada en el HSM desde su creación, esta se autodestruirá en caso de intento de intrusión, extracción o robo.

En caso de que la destrucción de la llave sea un proceso programado, se procederá a la reinicialización del HSM, ya que durante este proceso se produce el borrado seguro de las llaves contenidas en el.

La destrucción siempre deberá ser precedida de la revocación del certificado asociado a la llave siempre y cuando aún este vigente.

6.2.11 Clasificación del Módulo Criptográfico

Los módulos criptográficos utilizados son FIPS 140-2 nivel 3 y cumplen con las recomendaciones en materia de perfil de protección de dispositivos seguros de firma electrónica de autoridades certificadoras.

6.3 Otros aspectos de la administración del par de llaves

6.3.1 Archivo de llave pública

La CA archivará todos los certificados emitidos en un medio removible que será almacenado *off line* en una bóveda de seguridad.

6.3.2 Períodos de uso llaves públicas y privadas de certificados.

No hay estipulación en cuanto a la validez del par de llaves generadas. Sólo la validez del certificado emitido por la UNAMgrid CA es definida por este documento CP/CPS.

Los certificados de los titulares (suscriptores) tienen un período de validez de 13 meses o menos si la afiliación de la parte solicitante al grupo participante en la UNAMGrid es menor a un año.

El certificado de CA tiene un período de validez de 10 años.

6.4 Datos de activación

6.4.1 Generación de los datos de activación e instalación

La llave privada de la UNAMgrid CA es protegida por una frase de seguridad sólida que consiste al menos de 15 caracteres.

6.4.2 Protección de datos de activación

Los administrdores de la UNAMgrid CA conocen los datos de activación para la llave privada de la CA y tienen acceso a la copia cifrada. Ninguna otra persona conoce los datos de activación. Sin embargo, los datos de activación para la CA también son conservados en un sobre sellado en un lugar seguro separado de los sitios seguros que contienen la llave privada y las copias de su respaldo.

6.4.3 Otros aspectos de datos de activación

No está estipulado.

6.5 Controles de seguridad de cómputo

6.5.1 Requerimientos técnicos específicos de seguridad informática

La UNAMgrid CA garantiza la administración efectiva y controlada de acceso a los sistemas en sus diferentes roles, manteniendo una vigilancia constante sobre accesos, modificaciones, gestión de cuentas y otros eventos.

No hay otros servicios o software cargados u operados en el servidor de la CA. El servidor recibe actualizaciones y otros ajustes ocasionales si el riesgo de seguridad lo justifica, o si es indicado a juicio del personal de la UNAMgrid CA.

El servidor que aloje el producto CA es ejecutado en el sistema operativo Linux.

6.5.2 Evaluación del nivel de seguridad informática

No está estipulado

6.6 Controles de seguridad del ciclo de vida

6.6.1 Controles de desarrollo de sistemas

Durante los procesos de diseño, desarrollo e implementación se realiza un análisis exhaustivo de requisitos de seguridad en todos los componentes y aplicaciones asociados a la Autoridad.

Asimismo existen procedimientos de control de cambios para las nuevas versiones, actualizaciones y parches de emergencias a los componentes.

6.6.2 Controles de administración de seguridad

No está estipulado.

6.6.3 Controles de seguridad de vida útil

No está estipulado.

6.7 Controles de seguridad en redes

La UNAMgrid CA se encuentra alojada en un sitio con seguridad perimetral y servicios de firewall administrado, algunas de las características son:

- Firewall tipo full application inspection.
- Bloqueo de puertos y direcciones.
- Protección con traducción de las direcciones de red (NAT/PAT).
- Configuraciones de seguridad de acuerdo con las políticas UNAM.
- Prevención de ataques de DDoS.
- Bloqueo y análisis de protocolos UDP/TCP/ICMP entre otros.
- Alta disponibilidad.
- Creación de túneles (IPSEC/SSL).
- VPN administrada.
- Nivel de soporte y monitoreo de 7x24x365.

6.8 Estampillado de tiempo

Ver 5.5.5

7 Perfiles de Certificado, CRL y OCSP

7.1 Perfil de certificado

Todos los certificados emitidos por la UNAMgrid CA cumplen con la recomendación del IGTF para certificados X.509 como está definido por RFC 3280.

7.1.1 Número(s) de Versión

La UNAMgrid CA emite exclusivamente certificados X.509 versión 3.

7.1.2 Extensiones del certificado

Las extensiones al certificado X.509 v3, que deben estar presentes en los certificados de la UNAMgrid CA son:

Certificados personales:

Basic Constraints	critical, ca: false
Subject Key Identifier	hash
Authority Key Identifier	Keyid
Subject Alternative Name	Email
Key Usage	critical, Firma digital, Sin repudio, Cifrado de llave, Cifrado de datos (f0)
Extended Key Usage	Autenticación del servidor (1.3.6.1.5.5.7.3.1) Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4)
X509v3 CRL Distribution Points	URI (CRL) http://ca.unamgrid.unam.mx/pub/crl/unamgrid-crl.crl
X509v3 OCSP	URI

Certificados para servidores/servicios:

Basic Constraints	critical, ca: false
Subject Key Identifier	Hash
Authority Key Identifier	Keyid
Subject Alternative Name	Email
Key Usage	critical, Firma digital, Cifrado de llave, Cifrado de datos (f0)
Extended Key Usage	Autenticación del servidor (1.3.6.1.5.5.7.3.1) Autenticación del cliente (1.3.6.1.5.5.7.3.2)
X509v3 CRL Distribution Points	URI (CRL) http://ca.unamgrid.unam.mx/pub/crl/unamgrid-crl.crl
X509v3 OCSP	URI

Certificados para la CA:

Basic Constraints	critical, ca true
Subject Key Identifier	hash
Authority Key Identifier	keyid
Key Usage	Firma digital, Firma de certificados, Firma CRL sin conexión, Firma de lista de revocación de certificados (CRL) (86)

7.1.3 Algoritmos identificadores de objetos (OID)

Los OID para algoritmos usados para firma de certificados emitidos por la UNAMgrid CA son:

Función hash	id- sha256	2.16.840.1.101.3.4.2.1
Cifrado	rsaEncryption	1.2.840.113612.1.1.1
Firma	sha256RSAEncryption	1.2.840.113549.1.1.11

7.1.4 Formatos de nombres

Cada entidad tiene, Distinguushed Name (DN) único e inequívoco en todos los certificados emitidos a la misma entidad por la UNAMgrid CA. El DN está estructurado como es definido en ITUT Standards Recommendation X.501.

Issuer:

C=MX, O=UNAMgrid, OU=UNAM, CN=CA
C=MX O=UNAM OU=UNAMgrid CN=PKIUNAMgrid

Subject:

C=MX, O=UNAM, OU=UNAMgrid, CN=nombre y apellido del titular (suscriptor)
C=MX, O=UNAM, OU=UNAMgrid, CN=FQDN

El campo subject contiene el DN de la entidad con los siguientes atributos:

Top-level domain (México)	Mx
Organization	UNAM
Unit Organization	UNAMgrid
CommonName	Name [“.” surname] [service “/”] FQDN

7.1.5 Restricciones de los nombres

No hay ninguna restricción de nombre salvo las derivadas de lo estipulado en 7.1.4, 3.1.2 y 3.1.1.

7.1.6 Identificador de objeto (OID) de la Política de Certificación

Cada política de certificados UNAMgrid tiene un identificador de objeto asociado único (OID). El OID para esta política es definido en la Sección 1.2

El OID de este documento es: 1.2.840.113612.5.4.2.5.2.2.1.2.0

7.1.7 Uso de la extensión de Restricciones de Política

No está estipulado.

7.1.8 Sintaxis y semántica de calificadores de política

No está estipulado.

7.1.9 Procesamiento de semántica para la extensión de Políticas de Certificado críticas

No está estipulado.

7.2 Perfil CRL

7.2 1 Número(s) de Versión

La UNAMgrid CA crea y publica CRLs X.509 v2.

7.2.2 CRL y extensiones de entrada de CRL

La UNAMgrid CA deberá emitir CRLs completas para todos los certificados emitidos por ella independientemente de la razón de la revocación. La razón de la revocación no deberá estar incluida en la CRL.

La CRL deberá incluir la fecha para la cual la próxima CRL deberá ser emitida. Una nueva CRL deberá ser emitida antes de esa fecha si nuevas revocaciones son emitidas.

Las extensiones de CRL que deberán estar incluidas son:

- El Identificador de Llave de Autoridad.
- El número de CRL.

Las extensiones de entrada de la CRL que pueden estar incluidas son:

- Fecha inválida.

7.3 Perfil OCSP

Los certificados OCSP responder serán emitidos por la AC de la UNAMgrid y serán conforme a las normas del RFC3280, así como al IETF RFC 2560 Online Certificate Status Protocol.

7.3.1 Número(s) de version

Los certificados de OCSP Responder utilizarán el estándar X.509 versión 3 (X.509 v3).

7.3.2 Extensiones OCSP

No está estipulado.

7.3.3 Restricciones de nombre

No hay ninguna restricción de nombre salvo las derivadas de las estipulaciones en 7.1.4, 3.1.2 y 3.1.1.

7.3.4 Identificador de objeto de Política de Certificado

El OID de este CP/CPS es 1.2.840.113612.5.4.2.5.2.2.1.2.0 (versión en español)

7.3.5 Uso de la extensión de Restricciones de Política

No está estipulado.

7.3.6 Sintáctica y semántica de calificadores de política

No está estipulado.

7.3.7 Procesamiento de semántica para la extensión de Políticas de Certificado críticas

No está estipulado.

8 Auditoría de cumplimiento y otras evaluaciones

8.1 Frecuencia o circunstancias de evaluación

La UNAMgrid CA deberá hacer por lo menos una vez al año una autoevaluación para comprobar el cumplimiento de la operación con el documento CP/CPS vigente.

La CA debe al menos una vez al año evaluar el cumplimiento de los procedimientos de cada RA con el documento CP/CPS vigente.

Las auditorías operacionales internas serán realizadas por la Coordinación de Seguridad de la Información de la UNAM. Las auditorías internas deben realizarse por lo menos una vez al año.

8.2 Identidad/calificación del evaluador

No está definido.

8.3 Relación entre el auditor y la entidad auditada

Las inspecciones serán hechas por personal de la UNAMgrid CA o miembros de la comunidad UNAMgrid.

Una auditoría externa puede ser realizada por organismo del Gobierno Mexicano o por una institución académica de México.

En el caso de que otras CAs de confianza o partes dependientes pidieran una inspección externa, el costo de la inspección será cubierto por la parte demandante, exceptuando el costo del personal e infraestructura de la UNAMgrid CA.

8.4 Temas incluidos por la evaluación

La auditoría verificará que los servicios provistos por la CA se rijan por la última versión aprobada del CP/CPS.

8.5 Acciones a tomar como resultado de una deficiencia

En caso de una deficiencia, el administrador de la UNAMgrid CA anunciará los pasos que deberán seguirse para remediar esta deficiencia. Este anuncio deberá incluir un horario programado.

Si una deficiencia descubierta tuviera consecuencias directas en la confiabilidad del proceso de certificación, los certificados (sospechados de haber sido) emitidos bajo la influencia de este problema deberán ser revocados cuanto antes.

8.6 Comunicación de resultados

El resultado de la auditoría estará disponible de manera pública en el sitio web de la CA.

9 Otros asuntos legales y comerciales

9.1 Tarifas

No se cobra por el servicio de certificación por la circunscripción de la UNAM y, por tanto, no hay gravámenes financieros.

9.1.1 Tarifas de emisión o renovación de certificados

Véase 9.1.

9.1.2 Tarifas de acceso al certificado

Véase 9.1.

9.1.3 Tarifas de acceso a información de estado o revocación

Véase 9.1.

9.1.4 Tarifas por otros servicios

No se cobrarán tarifas por acceder a la CP y CPS u otra información de estado de CA.

9.1.5 Política de reembolso

Véase 9.1.

9.2 Responsabilidad financiera

No se aceptará responsabilidad financiera alguna por certificados emitidos bajo esta política.

9.2.1 Cobertura de seguro

No está estipulado.

9.2.2 Otros activos

No está estipulado.

9.2.3 Cobertura de garantía o seguro para entidades finales

No está estipulado.

9.3 Confidencialidad de información comercial

9.3.1 Alcance de la información confidencial

No está estipulado.

9.3.2 Información fuera del alcance de la información confidencial

No está estipulado.

9.3.3 Responsabilidad de protección de información confidencial

No está estipulado.

9.4 Información privada o personal

El servicio de la UNAMgrid CA recolecta información sobre sus titulares (suscriptores). La información incluida en certificados y CRLs emitidos no es considerada confidencial.

La UNAMgrid CA recolecta el nombre del titular (suscriptor), los números telefónicos del lugar de trabajo, copia electrónica de identificación oficial y dirección de correo electrónico.

La información incluida en los certificados y CRLs emitidas es pública (esta información no es considerada confidencial). Cualquier otra información que no esté incluida en los certificados y CRL debe ser considerada confidencial y no deberá ser liberada fuera de la UNAMgrid CA y de la RA que realiza el registro. Adicionalmente, para administradores y operadores RA, la información personal de contacto será guardada por la CA (número telefónico y dirección del lugar de trabajo).

9.4.1 Plan de protección de datos personales

Toda la información proporcionada estará protegida por el "Reglamento de Transparencia, Acceso a la Información Pública y Protección de Datos Personales para la Universidad Nacional Autónoma de México", vigente en la UNAM.

9.4.2 Información considerada privada

La información provista por el titular (suscriptor) para verificar su identidad será tomada como confidencial, exceptuando la incluida en el certificado.

9.4.3 Información considerada no privada

La información incluida en certificados y CRLs emitidos no es considerada confidencial. La información de contacto de una RA no es considerada confidencial ya que es información que generalmente está disponible en las páginas Web de los empleadores de la RA.

Las estadísticas referidas a emisión y revocación de certificados contienen información no personal y no es considerada confidencial.

9.4.4 Responsabilidad de protección de información privada

La responsabilidad de proteger la información privada recae en la UNAMgrid CA y en todas sus RAs acreditadas.

9.4.5 Aviso y consentimiento del uso de información privada

En caso de que la UNAMgrid CA o cualquiera de sus RAs acreditadas deba usar información privada deberá pedir al titular (suscriptor) que exprese su consentimiento escrito de manera libre y consensuada.

9.4.6 Divulgación en virtud de un proceso judicial o administrativo

La UNAMgrid CA no deberá revelar información confidencial a ninguna tercera persona o parte excepto por expresa autorización del titular (suscriptor) o cuando se requiera por oficiales de seguridad pública que exhiban la apropiada documentación legal.

9.4.7 Otras circunstancias de divulgación de información

Divulgación a petición del propietario se hará de acuerdo con al Reglamento de Transparencia, Acceso a la Información Pública y Protección de Datos Personales para la Universidad Nacional Autónoma de México" vigente. Específicamente, la información será revelada al titular (suscriptor) si la CA ha recibido un e-mail firmado del titular (suscriptor) pidiendo la información. La CA no pedirá remuneración monetaria por este servicio.

La CA reconocerá solicitudes escritas para la revelación de información personal de un titular (suscriptor) sólo si el titular (suscriptor) puede ser autenticado apropiadamente.

9.5 Derechos de propiedad intelectual

La UNAMgrid CA no reclamará ningún Derecho de Propiedad Intelectual (DPI) sobre certificados que haya emitido.

Este documento está basado principalmente en la traducción al español del documento Certification Authority UNAMgrid CA version 1.0, así como en las adecuaciones y modificaciones propias de las reglas de uso y operación de la UNAMgrid CA en su nueva plataforma.

Cualquier persona podrá copiar cualquier versión de la CP/CPS de la UNAMgrid CA, siempre y cuando incluyan un reconocimiento de la fuente.

Como miembro de TAGPMA e IGTF se otorga el derecho de redistribución ilimitada de su información.

9.6 Declaraciones y garantías

9.6.1 Declaraciones y garantías de la CA

La UNAMgrid CA garantiza la emisión de certificados sólo a titulares (suscriptores) identificados por solicitudes recibidas de RAs por vías seguras. La UNAMgrid CA revocará un certificado sólo en respuesta a una solicitud autenticada del titular (suscriptor) o la RA, el cual aprobó la solicitud del titular (suscriptor), o si lleva consigo prueba razonable de que las circunstancias de revocación están presentes.

La UNAMgrid CA no garantiza sus procedimientos ni se responsabiliza de problemas que surjan de su operación o el uso de los certificados que provee, y no da garantías de la seguridad o idoneidad del servicio.

La CA sólo garantiza verificar las identidades de los titulares (suscriptores) de acuerdo a los procedimientos descritos en este documento.

La CA no acepta responsabilidades por pérdidas financieras o de otra índole originadas por daños o impedimentos accidentales resultantes de su operación. Ninguna otra responsabilidad, implícita o explícita, es aceptada.

9.6.2 Declaraciones y garantías de la RA

Todas las RAs acreditadas deberán realizar las tareas de identificación de las partes solicitantes como está descrito en 3.2.3. y 3.2.2. con base al mejor esfuerzo. No se aceptan otras garantías.

Una RA puede concluir, a su propio riesgo estrictamente, un acuerdo más estricto con sus titulares (suscriptores), pero esto nunca deberá comprometer a la UNAMgrid CA ni a ninguna otra RA acreditada.

Es responsabilidad de la RA solicitar la revocación de un certificado si la RA considera que las circunstancias de revocación están presentes.

9.6.3 Obligaciones y garantías de los titulares (suscriptores)

Al solicitar un certificado a la UNAMgrid CA se compromete a usar y proteger el certificado y las llaves asociadas de acuerdo a las estipulaciones del documento CP/CPS en efecto a la fecha de emisión de dicho certificado. El titular (suscriptor) podrá, sin embargo, aplicar observaciones más estrictas.

Los titulares (suscriptores) deben:

- Leer y adherirse a los procedimientos publicados en este documento.
- Usar el certificado para los propósitos permitidos solamente.
- Autorizar el procesamiento y la conservación de datos personales (como requerido bajo la ley de Protección de Datos).
- Tomar toda precaución posible para prevenir la pérdida, publicación o acceso no autorizado a las llaves privadas asociadas al certificado, incluyendo:

    - Seleccionando una Contraseña fuerte de al menos 8 caracteres.
    - Protegiendo la contraseña de otros.
    - Notificando inmediatamente a la UNAMgrid CA y otras partes dependientes si la llave privada se pierde o está comprometida.
    - Solicitar revocación si el titular (suscriptor) ya no se encuentra en derecho de un certificado, o si la información en el certificado se vuelve incorrecta o imprecisa.

En caso de un incumplimiento de las estipulaciones en el documento CP/CPS al cual el titular (suscriptor) se ha adherido al solicitar un certificado de la UNAMgrid CA, el certificado deberá ser revocado inmediatamente. No se requieren mayores garantías del titular (suscriptor).

9.6.4 Obligaciones y garantías de las partes dependientes

Una parte dependiente deberá aceptar el certificado del titular (suscriptor) para propósitos de autenticación si:

- La parte dependiente verificó el estado del certificado.
- La parte dependiente conoce las CP y CPS de la CA que generaron el certificado antes de llegar a conclusiones sobre si confiar en el certificado del titular (suscriptor); y
- La dependencia es razonable y de buena fe en vista de todas las circunstancias conocidas por la parte dependiente en el momento de dependencia; y
- El certificado es usado para propósitos permitidos solamente; y
- La parte dependiente ha verificado el estado del certificado para su propia satisfacción antes de la dependencia.

La CRL debe estar convalidada por la parte dependiente y el certificado del titular (suscriptor) debe estar verificado contra la CRL.

9.6.5 Obligaciones y garantías de otros participantes

No está estipulado.

9.7 Renuncia de garantías

La UNAMgrid CA utiliza software y procedimientos para la autenticación de entidades que, para su mejor conocimiento, se ejecutan de acuerdo a este documento CP/CPS. Sin embargo, declina cualquier garantía de su completa exactitud.

Además, la UNAMgrid CA no puede hacerse responsable de cualquier uso incorrecto de su certificado por un titular (suscriptor) o cualquier otra parte que deba encontrarse en posesión de la llave privada correspondiente, y de cualquier aceptación sin previo estudio de cualquiera de sus certificados por una parte dependiente.

Cualquier parte dependiente que acepte un certificado para cualquier uso para el cual este no haya sido emitido lo hace bajo su propio riesgo y responsabilidad.

9.8 Limitaciones de responsabilidad

Excepto que se exprese lo contrario por la ley mexicana, la UNAMgrid CA declina cualquier responsabilidad por daños sufridos por una parte dependiente que haya aceptado uno de sus certificados, o un titular (suscriptor) cuyo certificado válido sea rechazado o cuyo certificado revocado sea aceptado sin problemas por una parte dependiente.

También declina cualquier responsabilidad por daños causados por la no-emisión de un certificado solicitado, o por la revocación de un certificado iniciado por la CA o la RA apropiada en conformidad con este documento CP/CPS.

9.9 Indemnizaciones

La UNAMgrid CA declina cualquier pago de indemnizaciones por daños ocasionados por el uso o rechazo de certificados que emite.

Las entidades finales deberán indemnizar y eximir de responsabilidad a la UNAMgrid CA y todas las RAs operando bajo este CP/CPS de todas los reclamos y acuerdos resultantes de información fraudulenta proporcionada con el formulario de certificación, y el uso y aceptación de un certificado que viole las provisiones de este documento CP/CPS.

9.10 Vigencia y terminación

9.10.1 Período

Este documento es efectivo luego de su publicación en el sitio electrónico de la UNAMgrid CA con la fecha de comienzo especificada en el sitio.

No se estipula un período para su expiración.

9.10.2 Finalización

Este CP/CPS permanece efectivo hasta ser sustituido por una nueva versión.

9.10.3 Efecto de terminación y supervivencia

Su texto deberá permanecer disponible por lo menos 5 años luego de que el último certificado emitido bajo este CP/CPS expire o sea revocado.

9.10.4 Avisos individuales y comunicación con participantes

Todas las comunicaciones por e-mail entre la CA y sus RAs acreditadas deben ser firmadas con una llave certificada.

Todas las comunicaciones por e-mail entre la CA o una RA y un titular (suscriptor) deben ser firmadas con una llave certificada para poder tener validez de prueba. Todas las peticiones para cualquier acción deben ser firmadas.

9.11 Enmiendas

9.11.1 Procedimiento de enmienda

Las enmiendas (correcciones o adecuaciones) a este CP/CPS deben pasar el mismo procedimiento que la aprobación inicial (véase 1.5.4). La reformulación de provisiones para mejorar su entendimiento y correcciones puramente gramáticales no son consideradas enmiendas.

9.11.2 Período y mecanismo de notificación

El documento CP/CPS enmendado será publicado en las páginas web de la UNAMgrid CA por lo menos dos semanas antes de hacerse efectivo.

La UNAMgrid CA informará de esto a sus titulares (suscriptores) y todas las partes dependientes que conozca por medio de un correo electrónico.

9.11.3 Circunstancias bajo las cuales el OID deberá ser cambiado

El OID que hay que añadir, también debe reflejar el número de versión del CP.
En cada nueva versión del CP/CPS DEBE cambiar el OID. Cambios sustanciales pueden causar el cambio de OID. Esta decisión es tomada por el administrador de la UNAMgrid CA y enviada a TAGPMA para su aprobación.

9.12 Disposiciones de solución de controversias

Las controversias originadas por el CP/CPS deberán ser resueltas por el administrador de la UNAMgrid AC.

9.13 Ley gobernante

La UNAMgrid AC y su operación están sujetas a las Leyes Mexicanas. Todas las controversias legales que surjan del contenido de este documento CP/CPS, la operación de la UNAMgrid AC y sus RAs acreditadas, el uso de sus servicios, la aceptación y uso de cualquier certificado emitido por la UNAMgrid AC deberán ser tratadas de acuerdo con las leyes mexicanas.

9.14 Cumplimiento de la ley aplicable

Todas las actividades relacionadas a la solicitud, emisión, uso o acepto de un certificado de la UNAMgrid AC debe cumplir con la ley mexicana.

Todas las actividades iniciadas en o destinadas a otro país diferente a México también deberán cumplir la ley de aquel país.

9.15 Provisiones misceláneas

9.15.1 Acuerdo entero

Este documento CP/CPS suplanta a cualquier acuerdo, escrito u oral, entre las partes cubiertas por el presente documento.

9.15.2 Asignación

No está estipulado.

9.15.3 Divisibilidad

Si una cláusula del presente documento CP/CPS se volviera nula porque ha sido declarada no válida o no ejecutable por una corte u otra entidad del cumplimiento de la ley, esta cláusula se tornará nula (y debería ser reemplazada lo más pronto posible por una cláusula pertinente), pero el resto del documento seguirá siendo aplicable.

9.15.4 Cumplimiento (tarifas de abogados y dispensa de derechos)

No está estipulado.

9.15.5 Fuerza mayor

Todos los eventos que comprometan a los servicios de la UNAMgrid AC serán tratados en principio por la UNAM a traves de sus responsables y conforme a la norma y procesos

establecidos para tal fin, en caso de que estos eventos no sean resueltos o exista controversia alguna, serán atendidos por TAGPMA.

9.16 Otras provisiones

No está estipulado.

10 Referencias

- Certification Authority AustrianGrid CA Certificate Policy (CP) and Certification Practices Statement (CPS), Version 1.0.0, Marzo 2005 https://ca.austriangridca.at/CP_CPS/AustrianGridCA_CP_CPS_1_0_0.pdf.
- SWITCH (the Swiss Education & Research Network) Certificate Policy and Certification Practice Statement (CP/CPS) ver:1.1.6 http://www.switch.ch/pki/SWITCH_CP-CPS.pdf
- DOEGrids Certificate Policy And Certification Practice Statement. Version 2.6. http://www.doegrids.org/Docs/CP-CPS.pdf
- Esnet Root CA Certificate Policy And Certification Practice Statement, Version 1.3, September 2003 http://www.ar.net/CA/d1b603c3/Certificate%20Policy.pdf
- Eugridpma. European Policy Management Authority for Grid Authentication http://www.eugridpma.org/
- Grid Canada Certification Authority Certificate Policy and Certification Practices Statement. http://www.gridcanada.ca/ca/gc-ca-cp-cps-1.1.htm
- IGTF. International Grid Trust Federation. http://www.gridpma.org/
- R. Housley, W. Ford, W. Polk and D. Solo, " Internet X.509 Public Key Infrastructure
- Certificate and CRL Profile" , RFC 2459, Enero 1999
- http://www.ietf.org/rfc/rfc2459.txt
- R. Housley, W. Polk, W. Ford and D. Solo, " Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" , RFC 3280, Abril 2002 http://www.ietf.org/rfc/rfc3280.txt
- RedIris Certification Authority Certificate Policy and Certification Practices Statement http://www.irisgrid.es/pki/policy/1.3.6.1.4.1.7547.2.2.4.1.0.0/
- S. Chokani and W. Ford, " Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework" , RFC 2527, Marzo 1999 http://www.ietf.org/rfc/rfc2527.txt
- S. Chokani, W. Ford, R. Sabett, C. Merrill and S. Wu, " Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" , RFC 3647, Noviembre 2003 [reemplaza a RFC 2527] http://www.ietf.org/rfc/rfc3647.txt
- TAGPMA. The Americas Grid Policy Management Authority. http://www.tagpma.org/
- The Americas Grid. Policy Management AuthorityCharter. Septiembre 20, 2005 UK eScience Certification Authority Certificate Policy and Certification Practices Statement, Version 1.1, Marzo 2005 http://www.grid-support.ac.uk/files/cps/cps-1.1.pdf

11 Control de versiones anteriores

Versión actual:

UNAMgrid CA Certificate Policy (CP) and Certification Practice Statement (CPS)
Last Version: 1.0, November 22, 2007

2007 Nov 22 - 560 KB - UNAMgridCPSv1.0
2007 Oct 11 - 560 KB - UNAMgridCPSv0.9
2007 Jun 12 - 560 KB - UNAMgridCPSv0.8
2007 Jun 12 - 560 KB - UNAMgridCPSv0.7
2007 Mar 21 - 556 KB - UNAMgridCPSv0.6
2007 Feb 21 - 554 KB - UNAMgridCPSv0.5
2006 Dec 15 - 551 KB - UNAMgridCPSv0.4
2006 Nov 16 - 534 KB - UNAMgridCPSv0.2c
2006 Sept 08 - 548 KB - UNAMgridCPSv0.2b
2006 Sept 08 - 545 KB - UNAMgridCPSv0.2a
2006 Sept 08 - 524 KB - UNAMgridCPSv0.1.1a
2006 Sept 08 - 524 KB - UNAMgridCPSv0.1a