Universidad Nacional

de La Plata

UNLP PKIGrid CA

Buenas Prácticas –

Operadores de CA & RA

Staff:

- Javier Díaz, CA Manager
- Maria del Carmen Lago, RA Manager
- Lía Molinari & Viviana Ambrosi, Responsables de Políticas y Procedimientos internos y externos
- Miguel Luengo, Responsable de Networking
- Nicolás Macia, Responsable de Políticas de Seguridad del Firewall y Sensores
- Paula Venosa, Responsable de Modificación y Testing de OpenCA
- Juan Pablo Giecco, Responsable de Mantenimiento del Sitio https://www.pkigrid.unlp.edu.ar
- Aldana Gómez Ríos, Responsable de Traducción Ingles-Español.

Documento OID 1.2.840.113612.5.4.2.3.4.0.1.0S
Noviembre 16, 2006

1 Nombre del documento e identificación

Título del documento	UNLP PKIGrid CA Buenas Prácticas – Operadores CA & RA
Versión del Documento	Versión 1.0
Fecha del Documento	Noviembre 16, 2006
Estructura OID del Documento	
Asignado por IGTF	1.2.840.113612.5.4.2.3
Tipo de Documento (Información General)	4
Sub -Tipo de Documento	0
Versión	1
Sub -Versión	0S

2 Recomendaciones generales sobre la operación

A continuación se enumeran un conjunto de buenas prácticas para los operadores tanto de la RA como de la CA.

- Conocer el procedimiento de backup y el plan de contingencia
- Haber leído y comprendido, y **tener una copia accesible** de los documentos de obligaciones del operador, manual de procedimientos del operador, CP/CPS.
- Mantener actualizado el libro de Novedades.
- Al final de la jornada, guardar en lugar seguro el dispositivo criptográfico, el libro de novedades, y la documentación que requiere confidencialidad.
- En caso de dudas sobre la operación dirigirse al manager (RA o CA, según corresponde).
- Tener en lugar seguro y accesible los números de teléfono y formas alternativas de comunicación con el RA manager, CA operador y CA manager, y de los diferentes directores de proyectos.
- Periódicamente realizar un informe estadístico que indique, en un determinado período de tiempo, las actividades realizadas en el ámbito de la CA como cantidad de presentaciones a la RA para completar la solicitud de certificados, inconvenientes observados, cantidad de certificados emitidos, etc.
- No dejar el dispositivo criptográfico conectado, ni sesiones abiertas.
- Ninguna password ni passphrase pueden ser accedidas por terceras personas.
- Ante cualquier sospecha de compromiso de clave o dispositivo criptográfico se debe comunicar inmediatamente con el CA manager.

3 Recomendaciones específicas para el operador de la RA

- Redireccionar automáticamente los mails dirigidos al operador de la RA provenientes del responsable de la organización solicitante a una carpeta del correo (Solicitudes entrantes).

- Ante la llegada la notificación de certificado emitido, redireccionar el mail a la carpeta de Certificados Emitidos.

- Determinar un horario de atención al público: en ese horario se atenderán a los solicitantes que realizan la presentación personal ante la RA.

- Cuando lo que se requiere es un certificado de administrador/host o de servicio, verificar que quien lo solicita es el administrador responsable.

- Cumplir con lo especificado en el CP/CPS.

4 Recomendaciones específicas para el operador de la CA

- En ninguna situación conectar la CA off line a la red.

- Establecer y comunicar la jornada laboral/semanal para respetar los tiempos definidos en la CP/CPS.

- Cumplir con lo especificado en el CP/CPS.

5 Sobre la dependencia

El lugar físico donde funciona la RA debe contar con una ventanilla de atención al público, y las condiciones de seguridad física necesarias para resguardar la documentación y elementos relacionados con su tarea.

El lugar físico donde funcionan tanto la RA como la CA off line, debe contar con una caja fuerte o armario con llave para el resguardo de los dispositivos criptográficos y documentación que se considere confidencial.