CARACTERÍSTICAS MÍNIMAS DE SEGURIDAD PARA LAS AUTORIDADES DE REGISTRO DE LA PKI-Paraguay

LIZ ROSANNA CRAMER CAMPOS

Firmado digitalmente por LIZ ROSANNA CRAMER CAMPOS
Fecha: 2020.09.30 16:52:07 -04'00'

DOC-PKI-05

Versión 2.0

CONTROL DOCUMENTAL

Documento	
Título: Características Mínimas de Seguridad para las Autoridades de Registro de la Infraestructura de Claves Públicas del Paraguay.	**Nombre Archivo:** DOC-PKI-05 V2.0
Código: DOC-PKI-05	**Soporte Lógico:** https://www.acraiz.gov.py/
Fecha: 30/09/2020	**Ubicación Física:** DGFDyCE
Versión: 2.0	

Registro de Cambios		
Versión	**Fecha**	**Motivo de Cambio**
1.0	28/10/2016	Versión inicial
2.0	30/09/2020	1. Disposiciones Generales
		2. Seguridad personal
		3. Seguridad Física
		4. Seguridad Lógica
		5. Seguridad de redes
		6. Seguridad de la información
		7. Ciclo de vida del certificado
		8. Acuerdos de funcionamiento
		9. Prohibiciones - ítem incorporado

		10. Documentos de referencia - item incorporado

Distribución del documento	
Nombre	**Área**
Ministerio de Industria y Comercio (MIC)	Dirección General de Firma Digital y Comercio Electrónico (DGFDyCE)
Autoridad Certificadora (CA)	Prestadores de Servicios de Certificación (PSC)
Documento Público	https://www.acraiz.gov.py/

Control del Documento		
Elaborado por:	**Verificado por:**	**Aprobado por:**
JENNY ELIZABETH RUIZ DIAZ LEZCANO Digitally signed by JENNY ELIZABETH RUIZ DIAZ LEZCANO Date: 2020.09.30 14:14:52 -04'00'	MARIA LUJAN OJEDA CHAMORRO Firmado digitalmente por MARIA LUJAN OJEDA CHAMORRO Fecha: 2020.09.30 15:17:22 -04'00'	LUCAS ATILIO SOTOMAYOR LLANO Firmado digitalmente por LUCAS ATILIO SOTOMAYOR LLANO Fecha: 2020.09.30 15:35:05 -04'00'
JENNY RUÍZ DÍAZ	***LUJAN OJEDA***	***LUCAS SOTOMAYOR***

Contenido

1. DISPOSICIONES GENERALES

Este documento tiene por objeto regular los procedimientos mínimos que deben ser adoptados por las Autoridades de Registro (RA) que operan en el marco de la Infraestructura de Claves Públicas del Paraguay (PKI-Paraguay). Complementa, para estas entidades, la normativa contenida en el documento DOC-PKI-04 [2].

Estas normas se establecen para todas las RAs.

Para este documento, se aplican los siguientes conceptos:

1. **Acuerdo de Suscriptores:** es un acuerdo entre la CA Raíz-Py y el PSC, y entre el PSC y el usuario final, que establece los derechos, obligaciones y responsabilidades de las partes con respecto a la emisión y gestión de los certificados. Este acuerdo, requiere la aceptación explícita de las partes intervinientes.
2. **Autoridad de Aplicación:** Ministerio de Industria y Comercio a través de la Dirección General de Firma Digital y Comercio Electrónico, dependiente del Viceministerio de Comercio y Servicios.
3. Autoridad de Certificación: entidad que presta servicios de emisión, gestión, revocación u otros servicios inherentes a la certificación digital. En el marco de la PKI-Paraguay, son Autoridades de Certificación, la CA Raíz-Py y el PSC.
4. **Autoridad de Certificación Raíz del Paraguay:** órgano técnico, cuya función principal es coordinar el funcionamiento de la PKI-Paraguay. La CA Raíz-Py tiene los certificados de más alto nivel, posee un certificado autofirmado y es a partir de allí, donde comienza la cadena de confianza. Las funciones de la CA Raíz-Py son ejercidas por la AA.
5. **Agente de Registro:** persona responsable de la realización de las actividades inherentes a la RA. Es la persona que realiza la identificación de los solicitantes en la solicitud de emisión/revocación de certificado.
6. **Autoridad de Registro:** entidad responsable de la interfaz entre el usuario y el Prestador de Servicios de Certificación (PSC). Siempre está vinculado a un PSC y su objetivo es recibir solicitudes de emisión o revocación de certificados digitales del solicitante, identificar de forma presencial al mismo y remitir la solicitud al PSC. La RA puede ser propia del PSC o delegada a un tercero.
7. **Confirmación de la identidad de una persona física:** es la comprobación de que la persona física que se presenta como el titular o responsable del certificado o como

el representante de una persona jurídica, es realmente aquella cuyos datos están contenidos en la documentación presentada.

8. **Confirmación de la identidad de una persona jurídica:** es la comprobación de que los documentos presentados se refieren efectivamente a la persona jurídica titular del certificado y que la persona física que se presenta como el representante de la persona jurídica realmente tiene tal atribución.
9. **Documento de identidad:** documento válido y vigente que permite acreditar la identidad de la persona, a los efectos del proceso de emisión/revocación del certificado digital será considerada la cédula de identidad o el pasaporte del solicitante.
10. **Desvinculación de un Agente de Registro:** se produce en los siguientes casos:
    I. Cuando un empleado o funcionario que cumple el rol de AGR es desvinculado de la organización;
    II. Cuando un empleado o funcionario que cumple el rol de AGR deja de ejercer de forma permanente el mencionado rol, incluso aunque continúe trabajando en la organización, en la instalación técnica o puesto provisorio de la RA.
11. **Dossier de Agente de Registro:** conjunto de documentos relativos al AGR: comprobante de profesión, comprobante de residencia, comprobantes de entrenamientos realizados, comprobante de verificación de antecedentes penales, y otros mencionados en el ítem 2 de este documento.
12. **Dossier de titular del certificado:** conjunto formado por la verificación de los documentos de identificación utilizados para la emisión del certificado y solicitud de certificado y acuerdo de suscriptores, y por la solicitud de revocación, cuando sea el caso. Este dossier deberá estar en formato de archivo digital, en el cual se escanean los documentos en formato papel, si los hubiere y se firma la solicitud de certificado y acuerdo de suscriptores con la clave privada del titular, después de la autorización del AGR por medio de la firma de dichos documentos, siempre y cuando sea informado y aceptado su contenido por parte de su solicitante y firmada digitalmente después de la generación de las claves y anterior a la instalación del certificado correspondiente.
13. **Emisión de certificado:** es la autorización de la emisión del certificado en el sistema del PSC previa comprobación de la concordancia de los datos de solicitud del certificado con los contenidos en los documentos presentados.

14. **Firma Digital:** es una firma electrónica certificada por un prestador habilitado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincula únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría.
15. **Firma digital de la Solicitud y Acuerdo de Suscriptores:** documento electrónico firmado digitalmente, utilizando exclusivamente una de las suites de firmas definidas en el documento DOC-PKI-06 [3], como se define en RFC 8017 (PKCS # 1), con el hash, SHA-256 o superior, de la clave pública insertada en el documento.
16. **Identificación de solicitud de certificado:** comprende la etapa de la confirmación de la identidad de una persona física o jurídica, realizado a través de la presencia física del interesado, con base en los documentos de identificación, y la etapa de emisión del certificado, conforme al documento DOC-PKI-03 [1].
17. **Infraestructura de Claves Públicas del Paraguay:** conjunto de personas, normas, leyes, políticas, procedimientos y sistemas informáticos necesarios para proporcionar una plataforma criptográfica de confianza que garantiza la presunción de validez legal para actos electrónicos firmados o cifrados con certificados digitales y claves criptográficas emitidas por esta infraestructura.
18. **Punto centralizado del PSC:** único local en el territorio nacional, donde el PSC almacena copias de los dossieres de todos los AGRs de las RAs vinculadas a él. Se almacenan también el dossier de los titulares de certificados de la PKI-Paraguay.
19. **Prestador de Servicios de Certificación:** entidad habilitada por la AA, encargada de operar una CA en el marco de la PKI-Paraguay. El PSC debe contar con un certificado digital emitido por la CA Raíz-Py y solo podrá emitir certificados a usuarios finales.
20. **Solicitud de certificado:** documento que se instrumenta mediante un formato autorizado de solicitud de certificado suscripto por el solicitante en nombre propio en el caso de certificados para persona física, o bien en nombre del titular en el caso de certificados de persona jurídica ya sea en un documento específico de la solicitud o como parte del Acuerdo de Suscriptores.
21. **Suspensión del Agente de Registro:** se produce cuando un empleado o funcionario quien ha recibido el rol de AGR deja de ejercer de manera temporal. La suspensión sólo implica un cambio en los permisos del AGR en el sistema del PSC,

y no es necesario realizar una entrevista de terminación o firmar los términos de terminación.

Para este documento, se aplican las siguientes siglas y acrónimos

Tabla Nº 1 - Siglas y Acrónimos

Sigla/Acrónimo	Descripción
AA	Autoridad de Aplicación (AA por sus siglas en inglés Application Authority)
AGR	Agente de Registro
CA	Autoridad de Certificación (CA por sus siglas en inglés Certificate Authority)
CA Raíz-Py	Autoridad Certificadora Raíz del Paraguay
DGFDyCE	Dirección General de Firma Digital y Comercio Electrónico dependiente del Viceministerio de Comercio y Servicios.
MIC	Ministerio de Industria y Comercio
PKI	Infraestructura de Clave Pública (PKI por sus siglas en inglés, Public Key Infrastructure).
PKI-Paraguay	Infraestructura de Claves Públicas del Paraguay
PSC	Prestador de Servicios de Certificación
RA	Autoridad de Registro (RA por sus siglas en inglés, Registration Authority).
RAR	Registro de Agentes de Registro
SO	Sistema Operativo

Sólo podrán expedir certificados en el marco de la PKI-Paraguay, las RA que se encuentran debidamente habilitadas por el MIC según el procedimiento establecido por el mismo.

El cumplimiento de las normas en este documento será verificado por auditorías e inspecciones llevadas a cabo por la CA Raíz-Py o entidad autorizada por este.

En caso de cambio de dirección de la RA, el hecho debe ser previamente reportado al PSC responsable. Este enviará una solicitud de habilitación con los datos actualizados, solicitando una nueva autorización de funcionamiento a la CA Raíz-Py.

2. SEGURIDAD PERSONAL

2.1. DISPOSICIONES GENERALES

Las regulaciones que se refieren a la seguridad de las personas, están descritas en el documento DOC-PKI-03 [1].

No se admiten pasantes ni funcionarios tercerizados en el ejercicio de actividades como AGR. Los AGR deben ser empleados o funcionarios de la propia organización habilitada como RA por la CA Raíz-Py.

La RA debe enviar al PSC la lista actualizada de los AGR en actividad, sus perfiles cualificados y sus necesidades de acceso a informaciones de gestión del ciclo de vida de los certificados. El PSC debe mantener esas informaciones actualizadas, organizadas y consolidadas en su instalación técnica, inclusive con un histórico de los cambios realizados, a disposición de la CA Raíz-Py para los procedimientos de auditoría e inspección.

2.2. DOCUMENTACIÓN DEL AGENTE DE REGISTRO

Cada AGR que está actuando o que ha servido en la RA debe tener un dossier que incluya:

a) contrato de trabajo, donde consten los términos de la contratación y la función que cumple en la organización;
b) certificado original de antecedentes policiales;
c) certificado original de antecedentes judiciales;
d) curriculum vitae que incluya histórico de empleos anteriores y formación educativa con respaldo documental;

e) certificado original de vida y residencia;
f) comprobante de capacitación/entrenamiento recibido;
g) resultado de la entrevista inicial con la firma del entrevistador;
h) declaración en la que afirma conocer sus atribuciones y que asume el deber de cumplir con la Política de Seguridad del PSC responsable, las políticas y reglas establecidas por la CA Raíz-Py y la normativa que rige la materia. En tal declaración asume también el deber de mantener la confidencialidad y exclusividad de la información proporcionada por el PSC a la RA y mantenerlo en secreto, incluso cuando se desvincula de la RA, respecto a todas las informaciones y los procesos ejecutados en la RA;
i) resultado de la revisión periódica prevista en la Política de Seguridad del PSC;
j) confirmación por parte del PSC sobre la inclusión de un AGR en su sistema de certificación.

Si el AGR ha sido desvinculado de sus actividades en la RA, el expediente adicionalmente debe contener:

a) la confirmación por parte del PSC sobre la inhabilitación del AGR en el sistema de certificación y en el RAR que se mantiene en el sitio web de la CA Raíz-Py;
b) una declaración firmada por el AGR, donde manifieste que no tiene asuntos pendientes, como los previstos en la Política de Seguridad del PSC referentes a seguridad del personal; y
c) resultado de la entrevista de desvinculación del personal con la firma del entrevistador.

Los documentos mencionados en el primer párrafo de este ítem, del literal “a” al “h”, que componen el dossier, deben ser examinados por una de las siguientes personas, que declaran, bajo pena de la normativa, la existencia de tales documentos y que estos documentos comprueban efectivamente que el AGR cumple con todos los requisitos relevantes de la PKI-Paraguay:

a) auditor Interno de la RA, inscripto ante la CA Raíz-Py;
b) auditor externo independiente inscripto ante la CA Raíz-Py;
c) auditor o funcionario designado por el PSC a la que está vinculada la RA inscripto ante la CA Raíz-Py; y

d) representante legal propio de la RA.

Sólo después de la solicitud de vinculación del AGR y la declaración prevista en el párrafo anterior, el PSC puede incluirlo en la base de datos y concederle los permisos de acceso en el sistema de certificación, siendo necesario para ello, la previa autorización documentada del Gerente del PSC o del responsable por él designado.

Los dossiers de todos los AGR de una RA, deben permanecer en un mismo Punto Centralizado del PSC, que será informado a la CA Raíz-Py.

2.3. ENTRENAMIENTO DEL AGENTE DE REGISTRO

Todo AGR, en el momento de la admisión, debe recibir capacitación o entrenamiento documentado, con una carga horaria mínima de 16 horas, sobre los siguientes temas:

a) principios y mecanismos de seguridad de la RA;
b) sistema de certificación en uso del PSC;
c) procedimientos de recuperación de desastres y de continuidad del negocio;
d) reconocimiento de firmas y validez de los documentos presentados; y
e) otros asuntos relacionados con las actividades bajo su responsabilidad.

En la formación sobre principios y mecanismos de seguridad deben ser presentadas la Política de Seguridad del PSC, sus normas y procedimientos relativos al tratamiento de informaciones y/o los datos sensibles, con el fin de desarrollar y mantener una efectiva concienciación sobre la seguridad, así como instruir a su fiel cumplimiento.

El entrenamiento en el reconocimiento de firmas y la validez de los documentos deberá ser suministrado (o preparado, cuando se trata de entrenamientos tipo e-learning) por la empresa o profesional especializado en grafotecnia.

2.4. ACOMPAÑAMIENTO PERIÓDICO

La RA debe acompañar el desempeño de las funciones de sus AGR y evaluarlos anualmente con el propósito de detectar las necesidades de actualización técnica y de seguridad. Este proceso debe ser documentado.

La RA deberá exigir y verificar la renovación de los antecedentes judiciales y policiales de todos sus AGR con una frecuencia de 2 años.

Para los casos en que el acompañamiento anual advierta la necesidad de suspender o desvincular a un AGR, dicha situación deberá ser inmediatamente solicitada al PSC.

La RA debe archivar los comprobantes relativos a los procedimientos anteriores en el dossier de los AGR que obran en su poder.

2.5. SUSPENSIÓN Y DESVINCULACIÓN

Cuando el AGR fuere suspendido o desvinculado de sus actividades, la RA inmediatamente providenciará la revocación de sus permisos de acceso al sistema de certificación del PSC y permisos de acceso físico y lógico a los equipamientos y mecanismos inherentes a la actividad del referido AGR. Estos procesos serán documentados y archivados en el dossier del AGR, los cuales deberán ser mantenidos en poder del PSC.

3. SEGURIDAD FÍSICA

Las actividades de la RA relacionadas con la identificación de la solicitud de certificado deben realizarse observando lo establecido en los ítems que tratan de “Identificación y Autenticación” en el documento DOC-PKI-03 [1].

El mantenimiento preventivo/correctivo de las estaciones de trabajo de la RA debe ser realizado únicamente por agentes autorizados (por el fabricante, asistencia técnica autorizada o por una persona designada por el PSC), dentro del período de mantenimiento recomendado. Los eventos de mantenimiento deben ser documentados.

4. SEGURIDAD LÓGICA

4.1. ESTACIONES DE TRABAJO

Las estaciones de trabajo de la RA, incluidos los equipamientos portátiles deben ser protegidos frente a amenazas y acciones no autorizadas, así como contra el acceso no autorizado, y del uso o la exposición indebida y, además:

a) las particiones de los discos duros de las estaciones de trabajo de la RA que contienen componentes de la aplicación del PSC/RA o que almacenen datos de solicitantes de certificados digitales deben ser encriptados; o políticas de seguridad

deben ser aplicadas a las estaciones de trabajo de la RA de forma a no permitir la grabación de archivos locales en estos equipamientos.

b) las estaciones de trabajo de la RA deben implementar una aplicación que controle la integridad de la configuración de la aplicación de la RA, así como los archivos de configuración o la información crítica que se guarda en la estación de trabajo.

c) las estaciones de trabajo de la RA deberán contener solo aplicaciones y servicios que sean suficientes y necesarios para las actividades corporativas.

Las estaciones de trabajo de la RA, incluidos los equipamientos portátiles, deben recibir, por lo menos, las siguientes configuraciones de seguridad:

a) control de acceso lógico al SO;

b) la exigencia de utilizar contraseñas fuertes y seguras;

c) políticas de contraseñas y bloqueo de cuentas;

d) logs de auditoría del SO activo que registre:

I. inicio y apagado del sistema;

II. intentos de crear, eliminar, establecer contraseñas o cambiar los privilegios de los sistemas de operaciones de la RA;

III. cambios en la configuración de la estación;

IV. intentos de acceso (login) y de salida del sistema (logoff) ;

V. intentos no autorizados de acceso a los archivos del sistema; y

VI. intentos de iniciar, eliminar, habilitar y deshabilitar a los usuarios y de actualizar y recuperar sus claves.

e) poseer antivirus, antispyware y antitrojan, instalados, actualizados y habilitados;

f) firewall personal activado, con permisos de acceso mínimo necesarios para las actividades. Este requerimiento puede ser sustituido por firewall corporativo, para los equipos instalados en redes que tienen tal dispositivo;

g) protector de pantalla accionado como tiempo máximo de 2 (dos) minutos de inactividad y exigiendo para su desbloqueo la contraseña del usuario;

h) SO actualizado, con la aplicación de las correcciones necesarias (patches, hotfix, etc) ;

i) utilizar solamente software con licencias y solamente aquellos necesarios para llevar a cabo las actividades del AGR;

j) impedimento de acceso remoto, a través de otro equipo conectado a la red utilizado por la RA, excepto para las actividades de soporte remoto;

k) equipo que requieran la identificación de forma segura del AGR durante la identificación del solicitante del certificado; y
l) sincronizar fecha y hora utilizando una fuente confiable de tiempo ajustados a la fecha y hora oficial paraguaya.

Los registros de auditoría del SO deben registrar el acceso al equipo y deben almacenarse localmente para su evaluación por parte del equipo de auditoría o seguridad operativa.

El análisis de estos logs deberá realizarse en caso de sospechas de accesos no autorizados o para resolver otro tipo de dudas que puedan surgir sobre el uso del equipo.

El AGR no debe tener perfil de administrador ni contraseña de root del equipo ni con privilegios especiales del sistema, delegando esta tarea a otros empleados o funcionarios de la propia organización, para permitir la segregación de funciones. El AGR sólo debe tener acceso a servicios y aplicaciones que hayan sido específicamente autorizados para su uso.

4.2. APLICATIVO DE LA RA

El aplicativo que hace de interfaz entre la RA y el sistema de certificación de del PSC debe poseer por los menos las siguientes características de seguridad:

a) acceso permitido solamente mediante autenticación por medio de certificado de tipo F2 o F3 del AGR, autorizado formalmente por la autoridad competente para registrarse en el sistema del PSC;
b) acceso permitido únicamente a dispositivos autenticados en el sistema (por ejemplo: ¡usando registro previo de la dirección IP, certificado digital del equipo u otra solución que permita al sistema identificar de forma inequívoca al equipo);
c) timeout de sesión de acuerdo con el análisis de riesgo de la CA;
d) registro en logs de auditorías de los eventos citados en el ítem “Tipos de eventos registrados” del documento DOC-PKI-03 [1];
e) histórico de inclusión y exclusión de los AGR en el sistema y de los permisos concedidos o revocados; y
f) mecanismo de revocación automática de certificados digitales.

Para el cumplimiento de lo dispuesto en el ítem “Generación e instalación del par de claves” del documento DOC-PKI-03 [1] la aplicación debe:

a) haber sido desarrollado con documentación formal;
b) contar con mecanismos de control de versiones;
c) tener la documentación de pruebas realizadas a cada versión;
d) poseer documentación que evidencie la homologación de cada versión en un ambiente con las mismas características al que se presentará cuando sea utilizado en producción, siendo estos ambientes obligatoriamente separados unos de otros;
e) tener la aprobación documentada del gerente o el responsable designado del PSC al cual está vinculada la RA, para instalar cada versión a un ambiente de producción; y
f) reportar cualquier incidente al PSC.

Los logs generados por este aplicativo deben ser almacenados en el PSC al cual está vinculada la RA, por un período de diez años.

5. SEGURIDAD DE REDES

La RA remitirá las solicitudes de emisión o revocación de certificados al PSC utilizando un VPN (Virtual Private Network -- red privada virtual), SSL (Secure Socket Layer - protocolo/capa de conexión/comunicación seguro/a) u otra tecnología de igual o mayor nivel de seguridad y privacidad.

6. SEGURIDAD DE LA INFORMACIÓN

6.1. DIRECTRICES GENERALES

El PSC debe tener un dossier que contenga lo siguiente:

a) contrato de los AGR que están trabajando o que han trabajado en la RA con sus respectivos números de cédula de identidad policial o número de pasaporte;
b) topología de red de comunicación entre la RA y el PSC;
c) manual de operaciones del AGR;
d) inventario de activos;
e) plan de continuidad del negocio; y
f) análisis de riesgos.

El Análisis de Riesgo y Plan de Continuidad del Negocio deben elaborarse de acuerdo con lo dispuesto en la Política de Seguridad del PSC.

La RA también debe tener una copia del Plan de Continuidad del Negocio.

El Inventario de Activos debe estar siempre actualizado, manteniendo un historial de cambios y debe estar firmado por el responsable de RA.

El inventario de los bienes debe indicar al menos:

a) los equipos de la RA, con sus respectivas especificaciones, actualizados mensualmente; y
b) los softwares instalados en los equipos, actualizados mensualmente;

En el Inventario de Activos, solo podrán constar los equipamientos de propiedad o de posesión de la RA. La prueba de propiedad o posesión del equipo referido deberá realizarse siempre que lo solicite CA Raíz-Py, mediante la presentación por parte de la RA de la respectiva factura. Para casos de préstamo, arrendamiento, donación, contrato de alquiler del equipo u otro, documentación de respaldo equivalente.

6.2. ALMACENAMIENTO, MANIPULACIÓN, ARCHIVADO Y DESTRUCCIÓN DE DOCUMENTOS.

Los documentos que componen el dossier de los titulares de certificados y de los AGR deben ser enviados al PSC vinculado, incluidas las antiguas, y guardados, preferiblemente, en un entorno informático protegido, con acceso permitido solo a los AGR vinculados o responsables designados formalmente para trabajar con los documentos.

El PSC puede sustituir la custodia física de los documentos que componen el dossier del AGR y el dossier del Titular del Certificado mediante la reproducción digital de los mismos, observando que:

a) los documentos cuyas copias deben constar en el dossier (por ejemplo: documentos de identidad presentada por el titular, curriculum del AGR, etc.) deben ser escaneados y firmados digitalmente con un certificado de firma digital de la PKI-Paraguay;
b) los documentos cuyos originales deban constar en el dossier (por ejemplo: solicitud de certificados y acuerdos de suscriptores, contrato de AGR, etc.) pueden ser

digitalizados para su inclusión en el dossier respectivo, debiendo permanecer los documentos originales archivados en el Punto centralizado del PSC por el período estipulado en las resoluciones de la CA Raíz-Py;

c) todos los archivos que componen un dossier deben ser organizados de forma a permitir su recuperación conjunta, con fines de inspección y auditoría;

d) el directorio del sistema donde son almacenados esos archivos deben tener protección contra lectura y escritura, dando permiso de acceso sólo a los AGR vinculados o a los responsables designados formalmente para trabajar con esos documentos; y

e) deben ser especificados procedimientos de copias y recuperación en el caso de un siniestro.

Los originales referenciados en el literal “b”, del párrafo anterior, podrán ser destruidos desde que el proceso de digitalización haya sido realizado con la aplicación de un certificado digital del responsable autorizado por el PSC o de la RA, quién verificó la integridad del documento digitalizado.

En caso de que la digitalización sea realizada por la RA, considerar lo establecido en el párrafo anterior, adicionalmente, la referida RA deberá emitir un recibo conteniendo la identificación de todos los dossiers digitalizados remitidos al PSC. Después de comprobar los dossiers digitalizados, el PSC deberá firmar el recibo.

El almacenamiento definitivo de los dossiers de titulares de certificado, digitalizados o electrónicos será en el Punto Centralizado del PSC a la cual la RA está vinculada.

El envío o transmisión del dossier para el almacenamiento definitivo debe ser realizado por un medio seguro (por ejemplo: entrega con acuse de recibo de los documentos en papel y la transmisión vía VPN para los documentos digitalizados), dentro de los 7 (siete) días corridos, a partir de la generación del dossier.

El PSC debe utilizar un sistema en el que se pueda determinar, fácilmente y en cualquier momento, la ubicación en el cual se encuentra cada dossier del titular del certificado que está bajo su cuidado.

El Punto Centralizado del PSC debe ser informado al MIC, así como cualquier alteración que se realizare posteriormente.

Todos los documentos en papel que contienen informaciones clasificadas como sensibles deben ser destruidos, de forma que sea irrecuperable la información contenida, antes de ser desechadas. Se incluyen en esta categoría las copias no utilizadas de los documentos de los titulares de certificados, solicitud de certificados y acuerdos de suscriptores, diagramas de red, etc.

Al eliminar archivos que contienen copias de documentos de los dossiers de los titulares del certificado, se debe realizar un borrado completo, incluida la limpieza de la basura, para evitar su recuperación y uso indebido.

7. CICLO DE VIDA DEL CERTIFICADO

Los procesos relativos al ciclo de vida del certificado (solicitud, identificación de la solicitud, emisión y revocación) se describen en el documento DOC-PKI-03 [1].

8. ACUERDOS DE FUNCIONAMIENTO

Según lo previsto en el ítem 1.3.2 del documento DOC-PKI-03 [1], el PSC habilitado por el MIC podrá celebrar un contrato de acuerdo operacional, de modo a que las actividades asignadas a una RA corran por cuenta de un tercero.

Estos contratos deben tener al menos las siguientes cláusulas:

a) identificación de la RA y PSC;
b) identificación de las atribuciones que le tocará a cada uno de los intervinientes del contrato;
c) La identificación del sitio y responsable de la custodia de los dossiers de los titulares de certificados;
d) El compromiso de que los celebrantes del mismo, se ajusten a cumplir con la Leyes y las Normas que rigen para la PKI-Paraguay, en todos los procedimientos realizados;
e) El período para el que se suscriba el contrato que no debe exceder al máximo previsto en el Código Civil Paraguayo, salvo que la actividad pueda enmarcarse dentro de las excepciones establecidas en el mismo cuerpo normativo señalado; y
f) Obligación del PSC contratista, de verificar el cumplimiento de los procesos ejecutados por la RA contratada.

9. PROHIBICIONES

Está prohibido, por el PSC y RA habilitadas por la CA Raíz-Py, la divulgación, anuncio o cualquier otra forma de publicidad de actividades, servicios o productos relacionados con la comercialización del certificado digital de la PKI-Paraguay que no estén estandarizados y autorizados en el marco de la PKI-Paraguay.

Se prohíbe cualquier otra forma de emisión de certificados, fuera de las circunstancias no previstas expresamente en la legislación y en la normativa que rige en la PKI-Paraguay.

Se prohíbe delegar o transferir a terceros, no habilitados, las actividades privativas de entidades habilitadas o autorizadas por la CA Raíz-Py, a cualquier título.

En caso de incumplimiento de las reglas de emisión de certificados, el MIC podrá determinar la revocación inmediata del certificado digital emitido en incumplimiento de las reglas que rigen en el marco de la PKI-Paraguay, las cuales no han cumplido con los requisitos establecidos en la normativa, con el debido respeto al derecho de terceros. de buena fe.

10. DOCUMENTOS DE REFERENCIA

10.1 REFERENCIAS

- Ley N° 4017/2010 "De validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico".
- Ley N° 4610/2012 "Que modifica y amplía la Ley Nº 4017/10 "de validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico".
- Decreto N° 7369/2011 "Por el cual se aprueba el reglamento general de la Ley Nº 4017/2010 "de validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico".

10.2. REFERENCIAS A DOCUMENTOS QUE COMPONEN LA PKI-Paraguay

Tabla - Documentos Referenciados

REF.	NOMBRE DEL DOCUMENTO	CÓDIGO
[1]	Directivas obligatorias para la formulación y elaboración de la declaración de prácticas de certificación de los prestadores de servicios de certificación de la PKI-Paraguay.	DOC-PKI-03
[2]	Directivas obligatorias para la formulación y elaboración de la política de certificación de los prestadores de servicios de certificación de la PKI-Paraguay.	DOC-PKI-04
[3]	Normas de algoritmos criptográficos de la PKI-Paraguay.	DOC-PKI-06