DIRECTIVAS OBLIGATORIAS PARA LA FORMULACIÓN Y ELABORACIÓN DE LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LOS PRESTADORES DE SERVICIO DE ALMACENAMIENTO DE LA PKI-Paraguay

LIZ ROSANNA CRAMER CAMPOS

Firmado digitalmente por LIZ ROSANNA CRAMER CAMPOS
Fecha: 2020.09.30 16:53:38 -04'00'

DOC-PKI-07

Versión 1.0

CONTROL DOCUMENTAL

Documento	
Título: REQUISITOS MÍNIMOS PARA LA DECLARACIONES DE PRÁCTICAS CERTIFICACIÓN DE PRESTADORES DE SERVICIO DE ALMACENAMIENTO DE LA PKI-Paraguay	**Nombre Fichero:** DOC-PKI-07 V1.0
Código: DOC-PKI-07	**Soporte Lógico:** https://www.acraiz.gov.py
Fecha: 30/09/2020	**Ubicación Física:** DGFDyCE
Versión: 1.0	

Registro de Cambios		
Versión	**Fecha**	**Motivo de Cambio**
1.0	30/09/2020	Versión Inicial

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 Servicio 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 14:20:40 -04'00'	MARIA LUJAN OJEDA CHAMORRO Firmado digitalmente por MARIA LUJAN OJEDA CHAMORRO Fecha: 2020.09.30 15:19:18 -04'00'	LUCAS ATILIO SOTOMAYOR LLANO Firmado digitalmente por LUCAS ATILIO SOTOMAYOR LLANO Fecha: 2020.09.30 15:36:25 -04'00'
JENNY RUÍZ DÍAZ	***LUJAN OJEDA***	***LUCAS SOTOMAYOR***

Contenido

1. INTRODUCCIÓN

1.1 DESCRIPCIÓN GENERAL

Este documento es parte de un conjunto de normativas creadas para regular a los Prestadores de Servicios de Almacenamiento (PSA) dentro del alcance de la Infraestructura de Claves Públicas de Paraguay (PKI-Paraguay). Dicho conjunto consta de los siguientes documentos:

a) DOC-PKI-07 (este documento); y
b) DOC-PKI-08 [3].

El PSA es una entidad habilitada y supervisada por el Ministerio de Industria y Comercio (MIC) que deberá estar vinculada a un Prestador de Servicios de Certificación (PSC) y se encuentra autorizada a prestar servicios de almacenamiento de claves privadas para usuarios finales o servicios de firma digital y de verificación de firmas digitales en documentos y transacciones electrónicas o ambos en los términos establecidos en el documento DOC-PKI-04 [1]. La suscripción a los servicios prestados por un PSA es de carácter opcional.

Las claves privadas de los usuarios finales almacenadas en dispositivos estandarizados conforme lo establecido en el documento DOC-PKI-04 [1], y las firmas digitales hechas por la clave privada del usuario en otros sistemas son válidas de conformidad a la Ley N° 4017/2010.

Un Prestador de Servicios de Certificación habilitado, conforme a las disposiciones de la normativa vigente, tiene prohibido almacenar y copiar claves privadas de sus suscriptores, por lo cual no puede constituirse en un Prestador de Servicios de Almacenamiento.

Este documento establece los requisitos mínimos que obligatoriamente deberán ser observados por los PSA integrantes de la PKI-Paraguay, para la formulación y la elaboración de su Declaración de Prácticas como Prestador de Servicios de Almacenamiento (CPS-PSA). La CPS-PSA es el documento que describe las prácticas, procedimientos operativos y técnicos empleados por el PSA para la prestación de sus servicios. No obstante, el PSC al cual está vinculado un PSA deberá adecuar su respectiva Declaración de Prácticas de Certificación (CPS) y Política de Certificación (CP) para el almacenamiento de claves de sus usuarios finales.

El PSA debe utilizar sistemas y productos fiables, incluidos canales de comunicación electrónicos seguros, aplicar procedimientos y mecanismos técnicos y organizativos adecuados,

para garantizar que el entorno sea confiable y que los datos de creación de firma se utilicen bajo el control exclusivo del titular del certificado. Además, deben custodiar y proteger los datos de creación de firma frente a cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad.

Este documento se basa en los estándares de la PKI-Paraguay, RFC 4210, 4211, 1305, 2030, 3447, 3647 de IETF y Reglamento (UE) 910/2014.

Toda CPS-PSA elaborada en el ámbito de la PKI-Paraguay debe obligatoriamente adoptar la misma estructura empleada en este documento.

Las regulaciones previstas en los otros documentos de la PKI-Paraguay también se aplican a los PSA como integrantes de la referida PKI, según corresponda:

a) Sistema de auditoría al cual se someterán los Prestadores de Servicios de Certificación habilitados (resolución MIC N° 1430/2017 y resolución MIC N° 1105/2015).

b) NORMA ISO/IEC 27002:2013. Tecnologías de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información.

c) DOC-PKI-04 [1].

d) DOC-PKI-06 [2].

Esta CPS-PSA cumple con el RFC 3647 de Internet *Engineering Task Force* (IETF) y puede someterse a actualizaciones periódicas.

1.2 NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

En este ítem debe ser identificada la CPS-PSA.

1.3 PARTICIPANTES Y APLICABILIDAD

1.3.1. PRESTADOR DE SERVICIOS DE ALMACENAMIENTO

En este ítem, debe ser identificado el PSA integrante de la PKI-Paraguay al que se refiere esta CPS-PSA e igualmente, debe ser identificada la dirección de la página web (URL) donde se publican los servicios prestados por el PSA. El PSA deberá mantener actualizadas las informaciones requeridas.

El PSA es una entidad vinculada indefectiblemente a un PSC mediante un acuerdo operacional que deberá ser autorizada por la CA Raíz-Py con la habilitación correspondiente para prestar servicios de almacenamiento de claves privadas para usuarios finales o servicios de firma digital y de verificación de firmas digitales en documentos y transacciones electrónicas o ambos.

Entiéndase el servicio de firma digital indicado en el párrafo anterior, al proceso de firma digital realizado por medio de la clave privada del titular de un certificado digital emitido por un PSC cuya clave privada se encuentra almacenada en un dispositivo HSM en custodia de un PSA.

1.3.2. SUSCRIPTORES

En este ítem, deben ser caracterizadas las personas físicas o jurídicas que podrán solicitar los servicios descriptos en esta CPS-PSA.

Los suscriptores deberán manifestar plenamente la aprobación de los servicios del PSA, así como el nivel de monitoreo que el PSA deberá informar, para fines exclusivos de protección de la clave privada del titular, ya sea en la prestación de servicio de almacenamiento de claves privadas o servicios de firma digital y de verificación de firmas digitales.

Los suscriptores deberán tener acceso, al usar el servicio de firma digital de un PSA, por medio de un entorno de usuario, como mínimo, a las 10 (diez) últimas firmas digitales realizadas.

Los suscriptores podrán revocar la autorización otorgada al PSA para la prestación de los servicios, para lo cual deberá solicitar la revocación de su certificado al PSC que lo emitió. Formalizada la revocación, el PSC ordenará de manera inmediata al PSA, la eliminación de la clave privada del usuario almacenada en el dispositivo criptográfico por éste custodiado.

1.3.3. APLICABILIDAD

En este ítem, la CPS-PSA debe enumerar e identificar los servicios prestados por el PSA que se definen cómo cada uno de los servicios autorizados y que deberán ser utilizados por los participantes. Las descripciones estarán relacionadas a las aplicaciones para las cuales los participantes utilizarán los servicios.

1.4. DATOS DE CONTACTO

En este ítem deben ser incluidos el nombre, la dirección y otras informaciones del PSA responsable de la CPS-PSA. También deben ser informados el nombre, los números de teléfonos y la dirección de correo electrónico de una persona para contacto.

1.5. PROCEDIMIENTOS DE CAMBIO DE ESPECIFICACIÓN

En este ítem deben ser descritos la política y los procedimientos utilizados para realizar cambios en la CPS-PSA. Cualquier cambio en la CPS-PSA deberá ser sometido a la aprobación de la Autoridad Certificadora Raíz del Paraguay (CA Raíz-Py).

La CPS-PSA deberá ser actualizada siempre que el PSA responsable implemente un nuevo servicio o cuando la autoridad competente lo determine.

1.5.1. POLÍTICAS DE PUBLICACIÓN Y NOTIFICACIÓN.

En este ítem, deben ser descritos los mecanismos utilizados para la distribución de la CPS-PSA a los participantes involucrados.

1.5.2. PROCEDIMIENTOS DE APROBACIÓN

Toda CPS-PSA deberá presentarse para su aprobación, durante el proceso de habilitación del PSA responsable, según lo determinado por la normativa vigente.

1.6. DEFINICIONES, SIGLAS Y ACRÓNIMOS

1.6.1 DEFINICIONES

1) **Autenticación:** proceso técnico que permite determinar la identidad de la persona que firma electrónicamente, en función del mensaje firmado por ésta, y al cual se le vincula. Este proceso no otorga certificación notarial ni fe pública.
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) **Certificado Digital:** es un documento electrónico, generado y firmado por una CA legalmente habilitada para el efecto, el cual vincula un par de claves con una persona física o jurídica confirmando su identidad.
6) **Cifrado:** es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido de manera que sólo pueda leerlo la persona que disponga de la clave del cifrado adecuada para decodificarla.
7) **Claves criptográficas:** valor o código numérico que se utiliza con un algoritmo criptográfico para transformar, validar, autenticar, cifrar y descifrar datos.
8) **Compromiso:** violación de la seguridad de un sistema a raíz de una posible divulgación no autorizada de información sensible.
9) **Data Center (Centro de Datos):** infraestructura compuesta por el espacio físico para la instalación de equipos informáticos y de comunicación con adecuados sistemas de energía, aire acondicionado y seguridad. Es parte de una CA, constituye un recinto seguro que alberga, entre otras cosas, los módulos criptográficos de hardware, protege la infraestructura tecnológica y es el lugar donde se ejecutan servicios del ciclo de vida del certificado. La importancia del data center radica en la protección que brinda a la clave privada y asegura la confianza en los certificados digitales emitidos por la CA.
10) **Datos de activación:** valores de los datos, distintos al par de claves, que son requeridos para operar los módulos criptográficos y que necesitan estar protegidos.
11) **Declaración de Prácticas de Certificación:** declaración de las prácticas que emplea una CA al emitir certificados y que define la infraestructura, políticas y procedimientos que utiliza la CA para satisfacer los requisitos especificados en la CP vigente.
12) **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.
13) **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 lo 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.

14) **Generador:** máquina encargada de generar electricidad a partir de un motor de gasolina o diésel. La instalación de este equipo deberá ser de tal forma que, al interrumpirse el suministro de energía eléctrica del proveedor externo, el mismo debe arrancar automáticamente tomando la carga de las instalaciones del Data center de la CA, incluyendo los circuitos de iluminación, de los equipos informáticos, equipos de refrigeración, circuitos de monitoreo, prevención de incendios; en fin, de todos los circuitos eléctricos críticos para el funcionamiento de las instalaciones tecnológicas.
15) **Habilitación:** autorización que otorga el MIC, una vez cumplidos los requisitos y condiciones establecidos en la norma.
16) **Identificación del Titular de certificado:** comprende la etapa de la confirmación de la identidad de una persona física o jurídica, realizada a través de la presencia física del interesado, con base en los documentos de identificación, y la etapa de emisión del certificado, conforme a la presente CPS.
17) **Infraestructura de Clave Pública del Paraguay:** es un conjunto de personas, 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) **Integridad:** característica que indica que un mensaje de datos o un documento electrónico no ha sido alterado desde la transmisión por el iniciador hasta su recepción por el destinatario.
19) **Lista de Certificados Revocados:** lista emitida por una CA, publicada periódicamente y que contiene los certificados que han sido revocados antes de sus respectivas fechas de vencimiento.
20) **Módulo criptográfico:** software o hardware criptográfico que genera y almacena claves criptográficas.
21) **Módulo de Seguridad de Hardware**: dispositivo basado en un módulo criptográfico tipo hardware que genera, almacena y protege claves criptográficas.
22) **Normas Internacionales:** requisitos de orden técnico y de uso internacional que deben observarse en la emisión de firmas electrónicas y en las prácticas de certificación.
23) **Parte que confía:** (relying parties): es toda persona física o jurídica diferente del titular, que decide aceptar y confiar en un certificado emitido en el marco de la PKI-Paraguay.
24) **Perfil del certificado:** especificación del formato requerido para un tipo particular de certificado (incluyendo requisitos para el uso de los campos estándar y extensiones).

25) **Política de Certificación:** documento en el cual la CA, define el conjunto de reglas que indican la aplicabilidad de un certificado a una comunidad particular y/o una clase de aplicaciones con requisitos comunes de seguridad.
26) **Prestador de Servicios de Almacenamiento:** es una entidad vinculada indefectiblemente a un PSC mediante un acuerdo operacional que deberá ser autorizada por la CA Raíz-Py con la habilitación correspondiente para prestar servicios de almacenamiento de claves privadas para usuarios finales o servicios de firma digital y de verificación de firmas digitales en documentos y transacciones electrónicas o ambos.
27) **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.
28) **Registro de Auditoría:** registro cronológico de las actividades del sistema, el cual es suficiente para permitir la reconstrucción, revisión e inspección de la secuencia de los ambientes y de las actividades que rodean o que conducen a cada acontecimiento en la ruta de una transacción desde su inicio hasta la salida de los resultados finales.
29) **Repositorio:** sitio principal de Internet confiable y accesible, mantenido por la CA con el fin de difundir su información pública.
30) **Suscriptor:** persona física o jurídica titular de un certificado digital emitido por una CA. En el contexto de esta CPS son las personas físicas o jurídicas titulares de un certificado que podrán solicitar los servicios prestados por un PSA.
31) **Usuario final:** persona física o jurídica titular de un certificado digital emitido por un PSC.
32) **Verificación de firma:** determinación y validación de que la firma digital fue creada durante el periodo operacional de un certificado válido por la clave privada correspondiente a la clave pública que se encuentra en el certificado y que el mensaje no ha sido alterado desde que su firma digital fue creada.

1.6.2 SIGLAS Y ACRÓNIMOS

Tabla Nº 1 - Siglas y Acrónimos

Sigla / Acrónimo	Descripción
AA	Autoridad de Aplicación
CA	Autoridad de Certificación (CA por sus siglas en inglés Certificate Authority)
CA Raíz-Py	Autoridad Certificadora Raíz del Paraguay
CP	Políticas de Certificación (CP por sus siglas en inglés, Certificate Policy)
CPS	Declaración de Prácticas de Certificación (CPS por sus siglas en inglés, Certification Practice Statement)
CRL	Lista de Certificados Revocados (CRL por sus siglas en inglés, Certificate Revocation List)
DGFDyCE	Dirección General de Firma Digital y Comercio Electrónico dependiente del Viceministerio de Comercio y Servicios.
HSM	Módulo de seguridad criptográfico basado en Hardware (HSM por sus siglas en inglés, Hardware Security Module)
ISO	Organización Internacional para la Estandarización (ISO por sus siglas en inglés, International Organization for Standardization).
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
PSA	Prestador de Servicios de Almacenamiento
PSC	Prestador de Servicios de Certificación
PY	Paraguay

RFC	Petición de Comentarios (RFC por sus siglas en inglés, Request For Comments)
UPS	Sistemas de alimentación ininterrumpida (UPS por sus siglas en inglés, Uninterruptible Power Supply)
URL	Localizador uniforme de recursos (URL por sus siglas en inglés, Uniform Resource Locator).
IEC	por sus siglas en inglés International Electrotechnical Commission
ISO	por sus siglas en inglés International Organization for Standardization
PCN	Plan de Continuidad de Negocio

2) RESPONSABILIDAD DEL REPOSITORIO Y PUBLICACIÓN

2.1. PUBLICACIÓN

2.1.1 PUBLICACIÓN DE INFORMACIÓN DE PSA

En este ítem, deben ser definidas las informaciones que serán publicadas por el PSA responsable de la CPS-PSA, el modo por el cual serán disponibilizadas y su disponibilidad.

Las siguientes informaciones, como mínimo, deberán ser publicadas por el PSA en su sitio web:

a) capacidad de almacenamiento de las claves privadas de los suscriptores que opera;
b) su CPS-PSA;
c) los servicios que implementan;
d) las condiciones generales mediante la cual son prestados los servicios de almacenamiento de claves privadas o servicio de firma digital y verificación de firma digital;

2.1.2. FRECUENCIA DE PUBLICACIÓN

En este ítem, debe ser informada la frecuencia de publicación de las informaciones referidas en el ítem anterior, de modo a asegurar la disponibilidad actualizada de sus contenidos.

2.1.3. CONTROLES DE ACCESO

En este ítem, deben ser descriptos los controles y cualquier restricción para el acceso, lectura y escritura de la información publicada por el PSA, de acuerdo con lo establecido en las normas, criterios, prácticas y procedimientos de la PKI-Paraguay.

3) IDENTIFICACIÓN Y AUTORIZACIÓN

En este ítem, el PSA responsable debe describir la forma utilizada para identificar y autorizar a los suscriptores, en el caso de ser necesario tales procedimientos.

4) REQUERIMIENTOS OPERACIONALES

4.1. ALMACENAMIENTO Y ACCESO A LAS CLAVES PRIVADAS DEL SUSCRIPTOR

En este ítem de la CPS-PSA, además de lo descripto en el documento DOC-PKI-08 [3], el PSA debe informar cómo los componentes de software se comunicarán entre la aplicación del suscriptor y el acceso al certificado y sus claves, describiendo:

a) el lenguaje de programación utilizado para la construcción de la plataforma de acceso;

b) los medios de acceso puestos a disposición del suscriptor (aplicaciones para dispositivos móviles, para PC, páginas web, entre otros);

c) el canal de seguridad en el que viajan las autenticaciones;

d) la arquitectura de red de la aplicación de acceso.

4.2. SERVICIO DE CREACIÓN Y VERIFICACIÓN DE FIRMA DIGITAL.

En este ítem de la CPS-PSA, además de lo descrito en el documento DOC-PKI-08 [3]**,** el PSA debe informar sobre el funcionamiento de las plataformas de firma digital y verificación de firma digital.

4.3. PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

En los siguientes ítems de la CPS-PSA, deben ser descriptos los aspectos relacionados a los sistemas de auditoría y de registro de eventos implementados por el PSA responsable con el objetivo de mantener un ambiente seguro.

4.3.1. TIPOS DE EVENTOS REGISTRADOS

El PSA responsable de la CPS-PSA deberá registrar en archivos de auditoría todos los eventos relacionados con la seguridad de su sistema. Entre otros, los siguientes eventos deberán obligatoriamente estar incluidos en los archivos de auditoría:

a) arranque y apagado de los sistemas del PSA;
b) tentativas de crear, eliminar, establecer contraseñas o cambiar los privilegios de los Sistemas Operativos del PSA;
c) cambios en la configuración de los sistemas del PSA;
d) tentativas de acceso (login) y de salida del sistema (logoff);
e) tentativas de acceso no autorizados a los archivos del sistema;
f) registros de almacenamiento de claves privadas y/o certificados digitales;
g) tentativas de iniciar, eliminar, habilitar y deshabilitar a usuarios de sistemas;
h) operaciones fallidas de escritura o lectura, cuando sea aplicable;
i) todos los eventos relacionados sincronizados con una fuente confiable de tiempo ajustados a la fecha y hora oficial paraguaya;
j) registros de las firmas digitales creadas y verificaciones realizadas;
k) registros de acceso a los documentos de los suscriptores;
l) registros de acceso o tentativas de acceso a la clave privada del suscriptor.

El PSA responsable de la CPS-PSA deberá también registrar, electrónica o manualmente, informaciones de seguridad no generada directamente por sus sistemas, tales como:

a) registros de accesos físicos;
b) mantenimiento y cambios en la configuración de sus sistemas;
c) cambios en el personal y de perfiles cualificados;
d) informes de discrepancia y compromiso; y
e) registros de destrucción de medios de almacenamiento que contienen claves criptográficas, datos de activación de certificados o información personal de los suscriptores.

Este ítem de la CPS-PSA debe especificar todas las informaciones que deberán ser registradas por el PSA responsable.

La CPS-PSA debe prever que todos los registros de auditoría deberán contener la identidad del agente que los causó, así como la fecha y hora del evento. Los registros de

auditoría electrónicos deberán contener la hora *Universal Time Coordinated* (UTC). Los registros manuales en papel podrán contener la hora local siempre que se especifique la ubicación.

Para facilitar los procesos de auditoría, toda la documentación relacionada con los servicios del PSA deberá ser almacenada, ya sea de forma electrónica o manual, en una única ubicación, conforme a lo establecido en el ítem 12 “seguridad en la operativa” de la norma ISO 27002/2013.

4.3.2. FRECUENCIA DE AUDITORÍA DE REGISTRO (LOGS)

La CPS-PSA debe establecer la periodicidad, que no exceda de una semana, con la cual los registros de auditoría del PSA responsable serán analizados por su personal operacional. Todos los eventos significativos deberán ser explicados en un informe de auditoría de registros. Tales análisis deberán involucrar una breve inspección de todos los registros, con la verificación de que no hayan sido alterados, seguida de una investigación más detallada de cualquier alerta o irregularidad en esos registros. Todas las acciones tomadas como resultado de este análisis deberán ser documentadas.

4.3.3. PERIODO DE CONSERVACIÓN DE REGISTROS (LOGS) DE AUDITORÍA

En este ítem la CPS-PSA debe establecer que el PSA responsable mantendrá localmente sus registros de auditoría durante al menos 2 (dos) meses y que posteriormente deberá almacenarlos de la manera descripta en el ítem 4.5.

4.3.4. PROTECCIÓN DEL REGISTRO (LOG) DE AUDITORÍA.

En este ítem, la CPS-PSA debe describir los mecanismos obligatorios incluidos en el sistema de registro de eventos del PSA responsable para proteger sus registros de auditoría contra la lectura no autorizada, modificación y eliminación.

También deben ser descriptos los mecanismos obligatorios para proteger las informaciones manuales de auditoría contra la lectura no autorizada, modificación y eliminación.

Los mecanismos de protección descriptos en este ítem deben obedecer a lo dispuesto en el ítem 12 “seguridad en la operativa” de la norma ISO 27002/2013.

4.3.5. PROCEDIMIENTOS PARA COPIA DE SEGURIDAD (BACKUP) DE REGISTRO (LOG) DE AUDITORÍA

En este ítem de la CPS-PSA deben ser descriptos los procedimientos adoptados por el PSA responsable para generar copias de seguridad *(backup*) de sus registros de auditoría y su periodicidad, que no debe ser superior a una semana.

4.3.6. SISTEMA DE RECOPILACIÓN DE DATOS DE AUDITORÍA

En este ítem de la CPS-PSA, deben ser descriptos y localizados los recursos utilizados por el PSA responsable para la recopilación de datos de auditoría.

4.3.7. NOTIFICACIÓN DE AGENTES CAUSANTES DE EVENTOS.

La CPS-PSA debe indicar que cuando un evento es registrado por el conjunto de sistemas de auditoría del PSA responsable, ninguna notificación deberá ser enviada a la persona, organización, dispositivo o aplicación que causó el evento.

4.3.8. EVALUACIONES DE VULNERABILIDAD

La CPS-PSA debe garantizar que los eventos que indiquen posibles vulnerabilidades, detectados en el análisis periódico de los registros de auditoría del PSA responsable, serán analizados detalladamente y, dependiendo de su gravedad, registrados por separado. Las acciones correctivas resultantes deberán ser implementadas por el PSA y registradas para fines de auditoría.

4.4. ARCHIVO DE REGISTROS

En los ítems siguientes de la CPS-PSA debe ser descripta la política general de archivo de registros, para uso futuro, implementada por el PSA responsable.

4.4.1. TIPOS DE REGISTROS ARCHIVADOS

En este ítem de la CPS-PSA deben ser especificados los tipos de registros archivados, que deberán incluir, entre otros:

a) notificaciones de compromiso de las claves privadas de los suscriptores por cualquier motivo;
b) notificaciones de compromiso de los archivos almacenados de los suscriptores por cualquier motivo;
c) informaciones de auditoría previstas en este ítem.

Este ítem, de la CPS-PSA, debe establecer los períodos de retención para cada registro archivado, señalando que los registros de almacenamiento de claves privadas y/o certificados digitales, de firmas digitales creadas, de verificaciones de firmas digitales y, tal vez, de los documentos almacenados, incluidos los archivos de auditoría, deberán conservarse durante al menos 5 (cinco) años.

4.4.2. PROTECCIÓN DE ARCHIVOS

La CPS-PSA debe establecer que todos los registros archivados deben ser clasificados y almacenados con los requisitos de seguridad consistentes con esa clasificación, conforme a lo establecido en el ítem 12 “seguridad en la operativa” de la norma ISO 27002/2013.

4.4.3. PROCEDIMIENTOS PARA LA COPIA DE SEGURIDAD (BACKUP) DE ARCHIVO

La CPS-PSA debe establecer que una segunda copia de todo el material archivado deberá ser almacenada en un ambiente diferente a las instalaciones principales del PSA responsable, recibiendo el mismo tipo de protección utilizada por él, en el archivo principal.

Las copias de respaldo deberán seguir los períodos de retención definidos para los registros de los cuales son copias.

El PSA responsable de la CPS-PSA deberá verificar la integridad de esas copias de seguridad, al menos, cada 6 (seis) meses.

4.4.4. REQUISITOS PARA FECHADO DE REGISTROS

Este ítem, de la CPS-PSA debe establecer los formatos y estándares de fecha y hora contenidos en cada tipo de registro.

4.4.5. SISTEMA DE RECOPILACIÓN DE DATOS DE ARCHIVOS

En este ítem de la CPS-PSA, deben ser descriptos y localizados los recursos utilizados por el PSA responsable para la recopilación de datos de archivo.

4.4.6. PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN DE ARCHIVO

En este ítem de la CPS-PSA, deben ser detalladamente descriptos los procedimientos definidos por el PSA responsable para la obtención o verificación de sus informaciones de archivo.

4.5. LIBERACIÓN DE ESPACIO DEL SUSCRIPTOR

En este ítem, la CPS-PSA debe describir los procedimientos técnicos y operacionales implementados por el PSA responsable para la liberación de un espacio (*slot*) destinado a un suscriptor donde estaba almacenada la clave privada del mismo, en caso de expiración o revocación del certificado.

4.6. COMPROMISO Y RECUPERACIÓN ANTE DESASTRES

4.6.1. DISPOSICIONES GENERALES

En los ítems siguientes de la CPS-PSA deben ser descriptos los requisitos relacionados con los procedimientos de notificación y de recuperación de desastres, previstas en el PCN del PSA responsable, conforme a lo establecido en el ítem 16 “gestión de incidentes en la seguridad de la información” de la norma ISO 27002/2013, para garantizar la continuidad de sus servicios críticos.

El PSA debe garantizar, en caso de que su operación se vea comprometida por cualquiera de los motivos enumerados en los ítems situados más abajo, que las informaciones relevantes serán disponibilizadas a los suscriptores y a las terceras partes. El PSA debe disponibilizar a todos los suscriptores y terceras partes una descripción del compromiso que se ha producido.

En caso de compromiso de una operación de almacenamiento y acceso a las claves de uno o más suscriptores, el PSA ya no deberá más proveer ese servicio, hasta que la CA Raíz-Py tome las medidas administrativas correspondientes, informando a los suscriptores sobre el problema y las derivaciones a tomar como consecuencia del suceso.

En el caso de compromiso de una operación de servicio de firma digital o verificación de la firma digital de los documentos firmados, siempre que sea posible, el PSA debe disponibilizar a todos los suscriptores y las terceras partes las informaciones que puedan ser

utilizadas para identificar cuáles documentos pudieron haber sido afectados, a menos que viole la privacidad de los suscriptores o comprometa la seguridad de los servicios del PSA.

4.6.2. RECURSOS COMPUTACIONALES, SOFTWARE Y DATOS CORROMPIDOS.

En este ítem de la CPS-PSA, deben ser descriptos los procedimientos de recuperación utilizados por el PSA responsable cuando los recursos computacionales, el software o los datos estuvieren corrompidos o se sospecha que están dañados.

4.6.3. SINCRONISMO DEL PSA

En este ítem, la CPS-PSA debe describir los procedimientos de recuperación previstos por el PSA para su utilización en caso de sincronismo con una fuente confiable de tiempo, el cual debe estar ajustado a la hora a la fecha y hora paraguaya, o, si corresponde, con el grupo HSM para la operación.

4.6.4. SEGURIDAD DE LOS RECURSOS DESPUÉS DE UN DESASTRE NATURAL O DE OTRA NATURALEZA

En este ítem de la CPS-PSA deben ser descriptos los procedimientos de recuperación utilizados por el PSA responsable después de la ocurrencia de un desastre natural o de otra naturaleza, antes de la restauración de un ambiente seguro.

4.7. EXTINCIÓN DE SERVICIOS DE UN PSA

Este ítem de la CPS-PSA debe describir los requisitos y los procedimientos que deberán ser adoptados en caso de extinción de los servicios del PSA responsable.

El PSA debe garantizar que las posibles interrupciones con los suscriptores y terceras partes, como resultado del cese de los servicios de almacenamiento de claves privadas o del servicio de firmas digitales y de verificación de las firmas digitales, serán mínimos y, en particular, asegurar el mantenimiento continuo de la información necesaria para que no haya perjuicio para sus suscriptores y terceras partes.

Antes del cese de sus servicios, el PSA deberá ejecutar, como mínimo los siguientes procedimientos:

a) disponibilizará a todos los suscriptores y terceras partes informaciones respecto a su extinción;

b) transferirá a otro PSA, después de la aprobación de CA Raíz-Py, las obligaciones relativas con el mantenimiento del almacenamiento de las claves, de certificados y documentos firmados, si fuera el caso, y de auditoría necesarios para demostrar el correcto funcionamiento del PSA, por un periodo razonable;

c) mantendrá o transferirá a otro PSA, después de la aprobación de CA Raíz-Py, sus obligaciones relativas con la disponibilidad de sus sistemas y hardware, por un período razonable;

d) notificará a todas las entidades afectadas.

El PSA proporcionará los medios para cubrir los costos de cumplimiento de estos requisitos mínimos en caso de quiebra o por otras razones que impidan cubrirlos.

5) CONTROLES DE SEGURIDAD FÍSICA, DE PROCEDIMIENTO Y PERSONAL

En los ítems siguientes deben ser descriptos los controles de seguridad implementados por el PSA responsable de la CPS-PSA para ejecutar de modo seguro sus funciones, de conformidad con el DOC-PKI-08 [3].

5.1. SEGURIDAD FÍSICA

En los ítems siguientes de la CPS-PSA, deben ser descriptos los controles físicos referentes a las instalaciones que albergan los sistemas del PSA responsable.

5.1.1 CONSTRUCCIÓN Y LOCALIZACIÓN DE LAS INSTALACIONES DEL PSA.

En este ítem, la CPS-PSA, debe describir los aspectos de la construcción de las instalaciones del PSA responsable, relevantes para los controles de seguridad física, incluyendo, entre otros:

a) instalaciones para equipamientos de apoyo, tales como: equipos de aire acondicionado, grupos de generadores, *UPS*, baterías, tableros de distribución de energía y telefonía;

b) instalaciones para sistemas de telecomunicaciones;

c) sistemas de puesta a tierra y de protección contra rayos; e

d) iluminación de emergencia.

5.1.2. ACCESO FÍSICO EN LAS INSTALACIONES DE PSA.

Todo PSA integrante de la PKI-Paraguay deberá implementar un sistema de control de acceso físico que garantice la seguridad de sus instalaciones, conforme con lo establecido en el ítem 9 “control de accesos”, ítem 11 “seguridad física y ambiental” de la norma ISO 27002/2013, y los requisitos que siguen.

5.1.2.1. NIVELES DE ACCESO

El PSA debe describir detalladamente cada nivel de acceso y su conjunto de sistemas, *software* y *hardware* implementados, de acuerdo con las descripciones de los niveles de acceso dispuestos en el documento DOC-PKI-08 [3].

5.1.2.2. SISTEMAS FÍSICOS DE DETECCIÓN

La seguridad de todos los ambientes del PSA deberá llevarse a cabo bajo un régimen de vigilancia 24 x 7 (veinticuatro horas al día, siete días a la semana).

La seguridad se puede lograr mediante:

a) guardia armado, uniformado, debidamente entrenado y apto para la tarea de vigilancia; o
b) circuito interno de TV, sensores de intrusión instalados en todas las puertas y ventanas, y sensores de movimiento, monitoreados local o remotamente por una compañía de seguridad especializada.

El ambiente de nivel 3 deberá ser dotado, adicionalmente, de un circuito interno de TV conectado a un sistema local de grabación 24x7. El posicionamiento y la capacidad de estas cámaras no deberían permitir la captura de contraseñas ingresadas en los sistemas.

Los medios resultantes de esta grabación deben almacenarse durante al menos 1 (un) año, en un ambiente de nivel 2.

El PSA debe contar con mecanismos que permitan, en caso de falta de energía:

a) iluminación de emergencia en todos los ambientes, activada automáticamente;
b) continuidad y funcionamiento de los sistemas de alarma y del circuito interno de TV.

5.1.2.3. SISTEMA DE CONTROL DE ACCESO

El sistema de control de acceso deberá estar instalado en un ambiente de nivel 3.

5.1.3. ENERGÍA Y AIRE ACONDICIONADO DE NIVEL 3 DEL PSA

La infraestructura del ambiente de nivel 3 del PSA deberá ser diseñada con sistemas y dispositivos que garanticen el suministro ininterrumpido de electricidad a las instalaciones. Las condiciones de la fuente de alimentación deben ser mantenidas para atender los requisitos de disponibilidad de los sistemas del PSA y sus respectivos servicios. Se deberá implementar un sistema de puesta a tierra.

Todos los cables eléctricos deberán estar protegidos por tuberías o conductos apropiados.

Deberán ser utilizados tuberías, conductos, canaletas, marcos y cajas de pasaje, distribución y terminación diseñadas y construidas de forma a facilitar las inspecciones y la detección de tentativas de violación. Deberán ser utilizados conductos separados para los cables de energía, de teléfono y de datos.

Todos los cables deberán ser catalogados, identificados e inspeccionados periódicamente, al menos cada 6 (seis) meses, en busca de evidencias de violación u otras anormalidades.

Deberán ser mantenidos actualizados los registros sobre la topología de la red de cableado, sujeto a los requisitos de confidencialidad establecidos en el ítem 13 “Seguridad de las Telecomunicaciones” de la norma ISO 27002/2013. Cualquier modificación en esta red deberá ser documentada y autorizada previamente.

No deberán ser admitidos instalaciones temporales, cableado expuesto o directamente conectado a tomas eléctricas sin la utilización de conectores adecuados.

El sistema de aire acondicionado deberá cumplir con los requisitos de temperatura y humedad exigidos por los equipamientos utilizados en el ambiente.

La temperatura de los ambientes atendidos por el sistema de aire acondicionado deberá ser monitoreada permanentemente.

La capacidad de redundancia de toda la estructura de energía y aire acondicionado del ambiente de nivel 3 del PSA debe ser garantizada por medio de UPS y generadores de tamaño compatible.

5.1.4. EXPOSICIÓN AL AGUA EN LAS INSTALACIONES DEL PSA

El ambiente de nivel 3 del PSA debe estar instalado en un lugar protegido contra la exposición al agua, filtraciones e inundaciones.

5.1.5. PREVENCIÓN Y PROTECCIÓN CONTRA INCENDIO EN LAS INSTALACIONES DEL PSA

En las instalaciones del PSA no será permitido fumar ni portar objetos que produzcan fuego o chispas, desde el nivel 2 en adelante.

Deberá haber extintores de clase B y C en el interior del ambiente de nivel 3, para extinguir incendios en combustibles y equipamientos eléctricos, dispuestos en el ambiente de forma a facilitar su acceso y manejo. En caso de existencia de un sistema de rociadores en el edificio, el ambiente de nivel 3 del PSA no deberá poseer salidas de agua, para evitar daños a los equipamientos.

El ambiente de nivel 3 debe poseer un sistema de prevención de incendios, que accione las alarmas preventivas una vez que se detecta humo en el ambiente.

En los otros ambientes del PSA, deberán existir extintores de incendio para todas las clases de fuegos, dispuestos en lugares que faciliten su acceso y manejo.

El PSA deberá implementar mecanismos específicos para garantizar la seguridad de su personal y de sus equipamientos en situaciones de emergencia. Estos mecanismos deberán permitir que las puertas se desbloqueen mediante accionamiento mecánico, para la salida de emergencia de todos los ambientes con control de acceso. La salida efectuada a través de estos mecanismos debe accionar inmediatamente las alarmas de apertura de las puertas.

5.1.6. ALMACENAMIENTO DE MEDIOS EN LAS INSTALACIONES DEL PSA

El PSA deberá asegurar el adecuado manejo y protección de los medios de almacenamiento de información, que contengan datos críticos o sensibles del sistema, contra daños accidentales (agua, fuego, electromagnetismo) y deberá impedir, detectar y prevenir su uso no autorizado, acceso o su divulgación.

La información relacionada a la infraestructura del PSA debe almacenarse de forma segura en armarios ignífugos y cofres de seguridad, según la clasificación de la información en ellos contenida.

5.1.7. ELIMINACIÓN DE RESIDUOS EN LAS INSTALACIONES DEL PSA

Todos los documentos en papel que contengan información clasificada como sensible, deberán ser triturados antes de ir como residuo.

Todos los dispositivos electrónicos que ya no se pueden usar y que se han utilizado previamente para almacenar informaciones sensibles, deberán ser físicamente destruidos.

5.1.8. ARCHIVO EXTERNO (OFF-SITE) DEL PSA

Una sala de almacenamiento externo a la instalación técnica principal del PSA debe ser usada para el almacenamiento y la retención de la copia de seguridad de datos. Esta sala deberá estar disponible para el personal autorizado las 24 (veinticuatro) horas del día, los 7 (siete) días de la semana y deberá cumplir con los requisitos mínimos establecidos por este documento para un ambiente de nivel 2.

5.2. CONTROLES PROCEDIMENTALES

En los ítems siguientes de la CPS-PSA deben ser descriptos los requisitos para la caracterización y el reconocimiento de perfiles cualificados en el PSA responsable, con las responsabilidades definidas para cada perfil. Para cada tarea asociada con los perfiles definidos, deben también ser establecidos el número de personas requeridas para su ejecución.

5.2.1. PERFILES CUALIFICADOS

El PSA responsable de la CPS-PSA deberá garantizar la segregación de tareas para las funciones críticas, a fin de evitar que un empleado o funcionario utilice indebidamente los servicios del ambiente sin ser detectado. Las acciones de cada empleado o funcionario deberán estar limitadas de acuerdo con su perfil.

El PSA deberá establecer un mínimo de 3 (tres) perfiles distintos para su operación:

a) Administrador del sistema: autorizado para instalar, configurar y mantener los sistemas de confianza, así como para administrar la implementación de las prácticas de seguridad de PSA;
b) Operador del sistema: responsable del funcionamiento diario de los sistemas de confianza del PSA. Autorizado para realizar copias de seguridad y recuperación del sistema.
c) Auditor del sistema: autorizado para ver archivos y auditar los registros de los sistemas de confianza del PSA.

Todos los empleados o funcionarios del PSA deberán recibir capacitación específica antes de obtener cualquier tipo de acceso. El tipo y nivel de acceso serán determinados, en un documento formal, en función de las necesidades de cada perfil.

Cuando un empleado o funcionario deja de pertenecer al plantel del PSA, sus derechos de acceso deberán ser revocados de inmediato. Cuando hay un cambio en la posición o función que el empleado o funcionario ocupa dentro del PSA, deberán ser revisados sus permisos de acceso. Deberá existir una lista de revocación, con todos los recursos, antes disponibilizados, que el empleado o funcionario deberá devolver al PSA al momento de su desvinculación.

5.2.2. NÚMEROS DE PERSONAS REQUERIDAS POR TAREA

Todas las tareas realizadas en el cofre o gabinete donde se localizan los servicios del PSA deberán requerir la presencia de al menos 2 (dos) empleados o funcionarios con perfiles cualificados. Para los casos de copias de las claves de los usuarios, se requerirán al menos 3 (tres) empleados o funcionarios con perfiles distintos y cualificados. Las otras tareas del PSA pueden ser realizadas por un solo empleado o funcionario.

5.2.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA PERFIL.

La CPS-PSA debe garantizar que todo empleado o funcionario del PSA responsable tendrá su identidad y perfil verificados antes de:

a) ser incluido en una lista de acceso físico a las instalaciones del PSA;
b) ser incluido en una lista de acceso lógico a los sistemas de confianza del PSA;
c) ser incluido en una lista para el acceso lógico a los demás sistemas del PSA.

Los certificados, cuentas y contraseñas utilizados para identificar y autenticar a los empleados o funcionarios deberán:

a) ser asignados directamente a un solo empleado o funcionario;
b) no ser compartidos; y
c) estar restringidos a acciones asociadas con el perfil para el que fueron creadas.

El PSA debe implementar un estándar para el uso de "contraseñas seguras", definido en su Política de Seguridad y de acuerdo con el ítem 9 “Control de Acceso” de la norma ISO 27002/2013, con procedimientos para validar esas contraseñas.

5.3. CONTROLES DE PERSONAL

En los ítems siguientes de la CPS-PSA deben ser descriptos los requisitos y procedimientos, implementados por el PSA responsable en relación a todo su personal, con respecto a aspectos tales como: verificación de antecedentes e idoneidad, capacitación profesional, rotación de cargo, sanciones por acciones no autorizadas, controles de contratación y documentación a proporcionar. La CPS-PSA debe garantizar que todos los empleados del PSA responsable, a cargo de las tareas operativas, hayan registrado en un documento formal los siguientes términos de responsabilidad:

a) los términos y condiciones del perfil que ocuparán;
b) el compromiso de observar las reglas, políticas y reglas aplicables en el marco de la PKI-Paraguay; y
c) el compromiso de no divulgar información confidencial a la que tengan acceso.

5.3.1. ANTECEDENTES, CUALIFICACIÓN, EXPERIENCIA Y REQUISITOS DE IDONEIDAD

Todo el personal del PSA responsable involucrado en actividades directamente relacionadas con los procesos de gerenciamiento de los sistemas de almacenamiento de claves privadas, firmas digitales y verificaciones de firmas digitales deberán ser admitidos de acuerdo con el ítem 7 “seguridad ligada a los recursos humanos” de la norma ISO 27002/2013. El PSA responsable podrá definir requisitos adicionales para la admisión.

5.3.2. PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES

Con el propósito de resguardar la seguridad y la credibilidad de las entidades, todo el personal del PSA responsable involucrado en actividades directamente relacionadas con los procesos de gerenciamiento de los sistemas de almacenamiento de claves privadas, firmas digitales y verificaciones de firmas digitales deberá ser sometido a:

a) verificación de antecedentes policiales y judiciales;
b) verificación del certificado de vida y residencia; y
c) comprobación de educación y del historial de trabajos anteriores.

El PSA responsable puede definir requisitos adicionales para la verificación de antecedentes.

5.3.3. REQUISITOS DE ENTRENAMIENTO

Todo el personal del PSA responsable involucrado en actividades directamente relacionadas con los procesos de gerenciamiento de los sistemas de almacenamiento de claves privadas, firmas digitales y verificaciones de firmas digitales deberán recibir capacitación documentada, suficiente para gestionar los siguientes temas:

a) principios y tecnologías de sistemas y hardware de almacenamiento de claves privadas, firmas digitales y verificación de firmas digitales en uso en el PSA;
b) PKI-Paraguay;
c) principios y tecnologías para la certificación digital y las firmas digitales;
d) principios y mecanismos de seguridad de redes y seguridad del PSA;
e) procedimientos de recuperación ante desastres y continuidad del negocio;
f) familiaridad con los procedimientos de seguridad, para las personas con responsabilidad de Oficial de Seguridad;
g) familiaridad con los procedimientos de auditoría en sistemas informáticos, para personas con la responsabilidad de Auditor de Sistemas;
h) otros asuntos relacionados con actividades bajo su responsabilidad.

5.3.4. FRECUENCIA Y REQUISITOS PARA CAPACITACIÓN TÉCNICA

Todo el personal del PSA responsable que participe en actividades directamente relacionadas con los procesos de gerenciamiento de sistemas de almacenamiento de claves privadas, firmas digitales y verificaciones de firmas digitales deberá mantenerse actualizado ante eventuales cambios tecnológicos en los sistemas del PSA. Como mínimo deberán recibir capacitación técnica al menos 1 (una) vez al año.

5.3.5. FRECUENCIA Y SECUENCIA DE ROTACIÓN DE CARGOS

En este ítem, la CPS-PSA puede definir una política a ser adoptada por los PSA responsables para la rotación del personal entre los diferentes cargos y perfiles por ellos establecidos. Esa política no deberá contradecir los propósitos establecidos en el ítem 5.2.1 para la definición de los perfiles cualificados. La rotación del personal debe darse al menos cada 3 (tres) años.

5.3.6. SANCIONES POR ACCIONES NO AUTORIZADAS.

La CPS-PSA debe estipular, así como en su política de RRHH que, en caso de que una persona a cargo de un proceso operativo lleve a cabo una acción no autorizada, real o

sospechosa, el PSA deberá suspender inmediatamente el acceso de esa persona a los sistemas, instruir procedimientos administrativos para investigar los hechos y, si corresponde, adoptar las medidas legales apropiadas.

El proceso administrativo mencionado anteriormente deberá contener al menos con:

a) informe de la ocurrencia con el modo de operación;
b) identificación de los involucrados;
c) posibles daños causados;
d) sanciones aplicadas, si fuera el caso; y
e) conclusiones.

Una vez concluido el proceso administrativo, el PSA responsable deberá enviar sus conclusiones a la CA Raíz-Py.

Las sanciones previstas de aplicación como resultado de un procedimiento administrativo son:

a) advertencia;
b) suspensión para un período determinado; o
c) cese de sus funciones.

5.3.7. REQUISITOS PARA CONTRATAR PERSONAL

Todo el personal responsable del PSA involucrado en actividades directamente relacionadas con los procesos de gerenciamiento de los sistemas de almacenamiento de claves privadas, firmas digitales y verificación de firmas digitales deberá ser contratado según lo establecido en el ítem 7 “seguridad ligada a los recursos humanos” de la norma ISO 27002/2013. El PSA responsable puede definir requisitos adicionales para la contratación.

5.3.8. DOCUMENTACIÓN PROPORCIONADA AL PERSONAL

La CPS-PSA debe garantizar que el PSA responsable pondrá a disposición de todo su personal al menos:

a) su CPS-PSA;
b) la norma ISO 27002/2013;
c) documentación operacional relacionada con sus actividades; y
d) contratos, normas y políticas relevantes para sus actividades.

Toda la documentación proporcionada al personal deberá estar clasificada de acuerdo con la política de clasificación de información definida por el PSA y debe mantenerse actualizada.

6) CONTROLES TÉCNICOS DE SEGURIDAD

En este ítem, la CPS-PSA, debe definir las medidas de seguridad implementadas por el PSA responsable para proteger las claves privadas de los suscriptores, mantener los servicios relacionados con las firmas digitales, así como el sincronismo de sus sistemas con la fuente de tiempo confiable. También deben ser definidos otros controles técnicos de seguridad utilizados por el PSA en el desempeño de sus funciones operacionales.

6.1. CONTROLES DE SEGURIDAD COMPUTACIONAL

6.1.1. DISPOSICIONES GENERALES

En este ítem, la CPS-PSA debe indicar los mecanismos utilizados para proporcionar seguridad a sus estaciones de trabajo, servidores y otros sistemas y equipamientos, de conformidad con las disposiciones establecidas en el ítem 9 “control de acceso”, 10 “cifrado”, 11 “seguridad física y ambiental” de la norma ISO 27002/2013.

6.1.2. REQUISITOS TÉCNICOS ESPECÍFICOS PARA LA SEGURIDAD COMPUTACIONAL

La CPS-PSA debe prever que los sistemas y los equipamientos del PSA responsable, utilizados en los procesos de gerenciamiento de los sistemas de almacenamiento de claves privadas, firmas digitales y verificaciones de firmas digitales, deberán implementar, entre otras, las siguientes características:

a) control de acceso a los servicios y perfiles del PSA;
b) separación clara de tareas y atribuciones relacionadas con cada perfil cualificado del PSA;
c) uso de cifrado para la seguridad de la base de datos, cuando así lo requiera la clasificación de sus informaciones;
d) generación y almacenamiento de registros de auditoría del PSA;
e) mecanismos internos de seguridad para garantizar la integridad de los datos y procesos críticos; y
f) los mecanismos de copia de seguridad (*backup).*

Estas características deberán ser implementadas por los sistemas operacionales del PSA y con los mecanismos de seguridad física.

Cualquier equipamiento, o parte de él, cuando sea enviado para mantenimiento deberá tener la información sensible contenida en el mismo borrado y deberá ser controlado su número de serie y las fechas de envío y recepción del mismo. Al regresar a las instalaciones del PSA, el equipamiento que pasó por mantenimiento deberá ser inspeccionado. En todo equipamiento que dejará de ser utilizado permanentemente, sujeto a las disposiciones del acto de eliminación, deberán ser destruidas de manera definitiva toda las informaciones sensibles almacenadas relacionada con la actividad del PSA. Todos estos eventos deberán ser registrados para fines de auditoría.

Cualquier equipamiento incorporado en el PSA deberá ser preparado y configurado según lo dispuesto en la Política de Seguridad implementada o en otro documento aplicable, a fin de preservar el nivel de seguridad necesario para su propósito.

6.1.3. CLASIFICACIÓN DE SEGURIDAD COMPUTACIONAL

En este ítem de la CPS-PSA se deberá informar, cuando esté disponible, la calificación asignada a la seguridad computacional del PSA responsable, de acuerdo a criterios tales como: *Trusted System Evaluation Criteria (TCSEC), Canadian Trusted Products Evaluation Criteria, European Information Technology Security Evaluation Criteria (ITSEC), Common Criteria e eIDAS.*

6.2. CONTROLES TÉCNICOS DEL CICLO DE VIDA

En los siguientes ítems de la CPS-PSA deben ser descriptos, cuando corresponda, los controles implementados por el PSA responsable en el desarrollo de los sistemas y del gerenciamiento de la seguridad.

6.2.1. CONTROLES DE DESARROLLO DEL SISTEMA

En este ítem de la CPS-PSA deben ser abordados aspectos tales como: seguridad del ambiente y del personal de desarrollo, prácticas de ingeniería de *software* adoptadas, metodología de desarrollo de *software*, entre otras, aplicadas al *software* del sistema del PSA o a cualquier otro *software* desarrollado o utilizado por el PSA responsable.

Los procesos de diseño y desarrollo realizados por el PSA deberán proporcionar documentación suficiente para respaldar las evaluaciones externas de seguridad de los componentes del PSA.

6.2.2. CONTROLES DE GESTIÓN DE LA SEGURIDAD

En este ítem de la CPS-PSA deben ser descriptas las herramientas y procedimientos empleados por el PSA responsable para garantizar que sus sistemas y redes operativas implementen los niveles de seguridad configurados.

Se deberá utilizar una metodología formal de gerenciamiento de configuración para la instalación y el mantenimiento continuo del sistema del PSA.

6.2.3. CICLO CLASIFICACIONES DE SEGURIDAD VIDA

En este ítem de la CPS-PSA debe ser informado el nivel de madurez atribuido al ciclo de vida de cada sistema, cuando esté disponible, con base en criterios tales como: *Trusted Software Development Methodology* (TSDM), *Capability Maturity Model do Software Engineering Institute* (CMM-SEI).

6.3. CONTROLES DE SEGURIDAD DE REDES

6.3.1. DISPOSICIONES GENERALES

En este ítem de la CPS-PSA deben ser descriptos los controles relacionados con la seguridad de la red, incluyendo el firewall y recursos similares, observando las disposiciones establecidas en el ítem 13. “seguridad en las telecomunicaciones” de la norma ISO 27002/2013.

Todos los servidores y elementos de la infraestructura y protección de red, tales como: enrutadores, hubs, switches, firewalls y sistemas de detección de intrusos (IDS), localizados en el segmento de red que aloja los sistemas del PSA, deberán estar ubicados y en funcionamiento al menos en el nivel 3.

Las versiones más recientes de los sistemas operacionales y las aplicaciones de los servidores, así como las correcciones (*parches*) disponibilizadas por los respectivos fabricantes deberán ser implementadas inmediatamente después de las pruebas en un ambiente de desarrollo o homologación.

El acceso lógico a los elementos de la infraestructura y protección de red deberá ser restringido a través de un sistema de autenticación y autorización de acceso. Los enrutadores

conectados a redes externas deberán implementar filtros de paquetes de datos, que permitan solamente conexiones a los servicios y servidores previamente definidos como sujeto a acceso externo.

El acceso a Internet deberá ser proporcionado por al menos dos líneas de comunicación desde diferentes sistemas autónomos.

El acceso vía red a los sistemas del PSA deberá ser permitido para los siguientes servicios:

a) por el PSA, para la administración de los sistemas de gestión desde equipos conectados por una red interna o por VPN establecida por medio de una dirección IP fija previamente registrada.

b) por el suscriptor, para el almacenamiento y acceso a la clave privada y servicios de firma digital y verificación de la firma digital.

6.3.2. FIREWALL

Los mecanismos de *firewall* deberán ser implementados en equipos para usos específicos, configurados exclusivamente para esa función. Los *firewalls* deberán estar dispuestos y configurados de forma a promover el aislamiento, en sub-redes específicas, los equipos servidores con acceso externo (denominada "zona desmilitarizada" (DMZ)) en relación a los equipos con acceso exclusivamente interno al PSA.

El *software* de firewall, entre otras características, deberá implementar registros de auditoría.

El oficial de seguridad deberá verificar periódicamente las reglas del *firewall,* para garantizar que solo se permita el acceso a los servicios realmente necesarios y permitidos, y que se bloquee el acceso a puertos innecesarios o no utilizadas.

6.3.3. SISTEMA DE DETECCIÓN DE INTRUSOS (IDS)

El sistema de detección de intrusos deberá tener la capacidad de ser configurado para reconocer ataques en tiempo real y responder automáticamente, con medidas tales como: enviar trampas SNMP, ejecutar programas definidos por la administración de la red, enviar correos electrónicos a los administradores, enviar mensajes de alerta al *firewall* o terminal de administración, para desconectar automáticamente conexiones sospechosas o para reconfigurar el *firewall.*

El sistema de detección de intrusos deberá ser capaz de reconocer diferentes patrones de ataque, inclusive contra el propio sistema, presentando la posibilidad de la actualización de su base de reconocimiento.

El sistema de detección de intrusos debe proporcionar el registro de eventos en *logs*, recuperables en archivos de tipo texto, además de implementar la gestión de la configuración.

6.3.4. REGISTRO DE ACCESO NO AUTORIZADO A LA RED.

Los intentos de acceso no autorizados en enrutadores, *firewall* o IDS deberán ser registrados en archivos para su posterior análisis, que podrán ser automatizadas. La frecuencia del examen de los archivos de registro deberá ser al menos semanal y todas las acciones tomadas como resultado de este examen deberán ser documentadas.

6.3.5. OTROS CONTROLES DE SEGURIDAD DE RED

El PSA debe implementar un servicio *proxy*, restringiendo el acceso, desde todas sus estaciones de trabajo, a servicios que puedan comprometer la seguridad del ambiente del PSA.

Las estaciones de trabajo y servidores deberán estar equipados con antivirus, *antispyware* y otras herramientas de protección contra las amenazas que emanan de la red a la que están vinculados.

6.4. CONTROLES DE INGENIERÍA DEL MÓDULO CRIPTOGRÁFICO

En este ítem la CPS-PSA debe describir los requisitos aplicables al módulo criptográfico utilizado para el almacenamiento de la clave privada de los suscriptores del PSA responsable. Podrán ser indicados estándares de referencia, como los definidos en el documento**, DOC PKI-06[3].**

7) POLÍTICAS DE FIRMA

En este ítem de la CPS-PSA, el PSA en el caso que ofrezca el servicio de Firma Digital debe informar las Políticas de Firma Digital que practica.

8) AUDITORÍAS Y EVALUACIONES DE CONFORMIDAD

8.1. INSPECCIÓN DE CUMPLIMIENTO Y AUDITORÍA

Las inspecciones y procesos de auditoría realizadas a los PSA que forman parte de la PKI-Paraguay tienen como objetivo verificar que sus procesos, procedimientos y actividades estén acordes con sus respectivas CPS-PSA, Procedimiento Operativo y Política de Seguridad, y demás normas y procedimientos establecidos por el MIC.

Las inspecciones a los PSA que integran la PKI-Paraguay serán realizadas por la CA Raíz-Py administrada por la DGFDyCE, cada 12 meses, salvo casos de denuncias motivadas sobre la prestación del servicio o causas justificadas donde serán realizadas de oficio.

El proceso de auditoría al PSA que integra la PKI-Paraguay será realizado aplicando en forma análoga lo dispuesto en el reglamento que establece el **SISTEMA DE AUDITORÍA AL CUAL SE SOMETERÁN LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN HABILITADOS (RESOLUCIÓN MIC N°1430/2017 Y RESOLUCIÓN MIC Nº 1105/2015)**.

En este punto de la CPS-PSA, el PSA debe informar al PSC al cual está vinculado que ha recibido auditoría e inspección previa de CA Raíz-Py para efectos de habilitación en el ámbito PKI-Paraguay y que se audita anualmente, con el objeto de mantener la habilitación aplicando análogamente lo dispuesto en el **SISTEMA DE AUDITORÍA AL CUAL SE SOMETERÁN LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN HABILITADOS (RESOLUCIÓN MIC N° 1430/2017 Y RESOLUCIÓN MIC Nº 1105/2015)**

En este ítem de la CPS-PSA, el PSA responsable deberá informar que el PSC a la cual está vinculada, también ha recibido una auditoría previa, con fines habilitación, y que el PSC es responsable de llevar a cabo auditorías anuales, con el propósito de mantener la habilitación.

9) OTROS ASUNTOS COMERCIALES Y LEGALES

9.1. OBLIGACIONES Y DERECHOS

En los siguientes ítems deben ser incluidas las obligaciones generales de las entidades involucradas. Si se implementan obligaciones específicas, las mismas deben ser descritas.

9.1.1. OBLIGACIONES DEL PSA

En este Ítem deben ser incluidas las obligaciones del PSA responsable de la CPS-PSA, contendiendo, al menos, las que se enumeran a continuación:

a) operar de acuerdo con su CPS-PSA y la descripción de los servicios que realiza;

b) gestionar y garantizar la protección de las claves privadas de los suscriptores;

c) mantener el PSA sincronizado con una fuente confiable de tiempo ajustado con la fecha y hora oficial paraguaya;

d) tomar las medidas apropiadas para garantizar que los suscriptores y demás entidades involucradas conozcan sus respectivos derechos y obligaciones;

e) supervisar y controlar el funcionamiento de los servicios prestados;

f) notificar al suscriptor titular de la clave y el certificado, cuando su clave privada se ve comprometida y solicitar la revocación inmediata del certificado correspondiente o la finalización de sus actividades;

g) publicar en su sitio web su CPS-PSA y las Políticas de Seguridad (PS) aprobadas que implementa;

h) publicar, en su sitio web, la información definida en el punto 2.1.1 de este documento;

i) identificar y registrar todas las acciones realizadas, de acuerdo con las normas, prácticas y reglas establecidas en el marco de la PKI-Paraguay por la CA Raíz-Py;

j) adoptar las medidas de seguridad y control previstas en la CPS-PSA, en el Procedimiento Operativo y Política de Seguridad que implementa, involucrando sus procesos, procedimientos y actividades, observando los estándares, criterios, prácticas y procedimientos de la PKI-Paraguay;

k) mantener la conformidad de sus procesos, procedimientos y actividades con las normas, prácticas y reglas de la PKI-Paraguay y con la legislación vigente;

l) mantener y garantizar la integridad, confidencialidad y seguridad de la información tratada por ella;

m) mantener y probar anualmente su PCN;

n) mantener un seguro que cubra la responsabilidad civil derivada de la actividad y el almacenamiento de claves privadas para usuarios finales, con cobertura suficiente y compatible con el riesgo de estas actividades;

o) informar a los suscriptores que contratan sus servicios sobre la cobertura, las condiciones y las limitaciones estipuladas por la póliza de seguro de responsabilidad civil contratada en los términos anteriores; y

p) informar a CA Raíz-Py, mensualmente, el número de claves privadas o los certificados digitales correspondientes almacenados y las firmas realizadas y verificadas.

9.1.2. OBLIGACIONES DEL SUSCRIPTOR

El suscriptor debe asegurarse, a través de las aplicaciones disponibles al aceptar el servicio de un PSA, que su par de claves y/o certificados digitales se hayan almacenado correctamente y que la clave privada utilizada para firmar esta funcional.

9.1.3 DERECHOS DEL TERCERO (RELYING PARTY)

Se considera que el tercero es la parte que confía en el contenido, la validez y la aplicabilidad del servicio de firma digital, y de la verificación de la firma digital.

Constituyen derechos de tercera parte:

a) rehusarse a utilizar el servicio de firma digital y de verificación de la firma digital de documentos electrónicos prestados por el PSA para fines distintos de su propósito de uso en el marco de la PKI-Paraguay.
b) verificar, en cualquier tiempo, la validez de firma digital. Una firma digital en el marco de la PKI-Paraguay se considera válida cuando:

i. el certificado digital no aparece en la CRL del PSC emisor;

ii. la clave privada utilizada para firmar digitalmente no ha sido comprometida en el momento de la verificación;

iii. puede ser verificada utilizando la cadena de certificados que lo generó;

iv. el propósito del uso está de acuerdo con lo definido en la política del certificado digital de los firmantes.

El incumplimiento de estos derechos no elimina la responsabilidad del PSA responsable y del titular del certificado.

9.2. RESPONSABILIDADES

9.2.1 RESPONSABILIDADES DEL PSA

El PSA responsable debe responder por cualquier daño causado.

En este ítem debe indicarse la responsabilidad del PSA ante eventuales situaciones relacionadas al alcance de la prestación de servicios, uso indebido del servicio, exención de responsabilidad en caso de fuerza mayor, caso fortuito, entre otros.

9.3. RESPONSABILIDAD FINANCIERA

9.3.1. INDEMNIZACIONES A TERCEROS (RELYING PARTY)

En este ítem debe ser establecida la inexistencia de responsabilidad del tercero (*relying party*) ante el PSA, excepto en el caso de un acto ilegal.

En este ítem debe indicarse el alcance de responsabilidad a terceros que confían.

9.3.2. RELACIONES FIDUCIARIAS

En este ítem deben ser indicadas las condiciones del PSA responsable, de corresponder.

9.3.3. PROCEDIMIENTOS ADMINISTRATIVOS

En este ítem, se deben enumerar los procesos administrativos aplicables relacionados con las operaciones del PSA responsable de la CPS-PSA.

9.4. INTERPRETACIÓN Y EJECUCIÓN

9.4.1. LEGISLACIÓN

En este ítem, se debe indicar la legislación que acompaña la CPS-PSA.

9.4.2. FORMA DE INTERPRETACIÓN Y NOTIFICACIÓN.

En este ítem, deben ser enumeradas las medidas a tomar en el caso de que una o más de las disposiciones de la CPS-PSA. se consideren, por cualquier motivo, inválidas, ilegales o no aplicables.

También se definirá la forma en que serán realizadas las notificaciones, las solicitudes o cualquier otra comunicación necesaria, relativas a las prácticas descritas en la CPS-PSA.

9.4.3. PROCEDIMIENTOS DE RESOLUCIÓN DE DISPUTAS

En este ítem, deben ser definidos los procedimientos a ser adoptados en caso de conflicto entre la CPS-PSA y otras declaraciones, políticas, planes, acuerdos, contratos o documentos que adopte el PSA.

También debe ser establecido que la CPS-PSA del PSA responsable no prevalece sobre las reglas, criterios, prácticas y procedimientos establecidos por el MIC.

Los casos omitidos deberán ser remitidos para su consideración a la CA Raíz-Py.

9.5. LAS TASAS DE SERVICIO

En los siguientes ítems, deben ser especificados por el PSA responsable de la CPS-PSA la política tarifaria y de reembolso aplicable, si fuera el caso, así como los costos asociados al servicio de:

a) almacenamiento de claves privadas para los usuarios finales;
b) de firma digital y de verificación de firma digital;
c) otras tarifas.

9.6. CONFIDENCIALIDAD

9.6.1. DISPOSICIONES GENERALES

La clave privada de los suscriptores será mantenida por el PSA, que será responsable de su confidencialidad, manteniendo registros de auditoría con la hora y fecha de acceso disponibles para el suscriptor.

Tanto las firmas digitales como las verificaciones de firmas digitales podrán ser realizadas por el PSA, quien será responsable de su confidencialidad, manteniendo los registros de auditoría sincronizados con la hora y fecha una fuente UTC confiable ajustados a la fecha y hora paraguaya, inclusive pudiendo identificar cuál documento, IP o URL, entre otros, que deben ser previamente autorizados por el suscriptor, fueron firmados con la clave privada del suscriptor.

Los documentos firmados digitalmente por los suscriptores podrán ser conservados por el PSA, siempre que se acuerde expresamente con el suscriptor y de conformidad con la legislación vigente.

9.6.2. TIPOS DE INFORMACIONES CONFIDENCIALES

En este ítem, deben ser identificados los tipos de informaciones consideradas confidenciales por el PSA responsable de la CPS-PSA, de acuerdo con los estándares, criterios, prácticas y procedimientos de la PKI-Paraguay.

La CPS-PSA, debe establecer, como principio general, que no se deben divulgar documentos, información o registros proporcionados por el suscriptor al PSA, excepto cuando se haga un acuerdo con el suscriptor.

9.6.3. TIPOS DE INFORMACIÓN NO CONFIDENCIALES

En este ítem, deben ser indicados los tipos de informaciones consideradas no confidenciales por el PSA responsable de la CPS-PSA, las cuales deberán comprender, entre otros:

a) los certificados del suscriptor;
b) la CPS-PSA del PSA;
c) versiones públicas de su Política de Seguridad; y
d) la conclusión de los informes de auditoría.

9.6.4. INCUMPLIMIENTO DE LA CONFIDENCIALIDAD POR RAZONES LEGALES.

Este ítem de la CPS-PSA debe establecer el deber del PSA responsable de la CPS-PSA de proporcionar documentos, información o registros bajo su custodia, por orden judicial.

9.6.5. INFORMACIÓN A TERCEROS.

Este ítem de la CPS-PSA, deberá establecer como una guía general que ningún documento, información o registro bajo la custodia del PSA responsable de la CPS-PSA se proporcionará a ninguna persona, excepto cuando la persona que lo solicite, por medio de un instrumento debidamente constituido, esté autorizado para hacerlo y esté correctamente identificado.

9.6.6. OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN.

En este ítem de la CPS-PSA, deben ser descriptas, cuando corresponda, cualquier otra circunstancia en la que se pueda divulgar información confidencial.

9.7 DERECHOS DE PROPIEDAD INTELECTUAL.

En este ítem de la CPS-PSA, deben abordarse los problemas relacionados con los derechos de propiedad intelectual de los certificados, políticas, especificaciones de prácticas y procedimientos, nombres y claves criptográficas y documentos firmados digitalmente de acuerdo con la legislación vigente.

10) REFERENCIAS

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".
- RFC 4210: Internet X.509 Public Key Infrastructure. Certificate Management Protocol (CMP).
- RFC 4211: Internet X.509 Public Key Infrastructure. Certificate Request Message Format (CRMF).
- RFC 1305: Network Time Protocol (Version 3). Specification, Implementation and Analysis.
- RFC 2030: Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI.
- RFC 3447: Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography. Specifications Version 2.1.
- RFC 3647: Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework.
- Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo del 23 de julio de 2014 - relativo a la identificación electrónica y los servicios de confianza para transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

10.2 REFERENCIAS A DOCUMENTOS QUE COMPONEN LA PKI-Paraguay

Tabla Nº2 – Documentos Referenciados

REF.	NOMBRE DEL DOCUMENTO	CÓDIGO
[1]	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
[2]	Normas de algoritmos criptográficos de la PKI-Paraguay.	DOC-PKI-06
[3]	Procedimientos operacionales mínimos para los prestadores de servicios de almacenamiento de la PKI-Paraguay.	DOC-PKI-08