PROCEDIMIENTOS OPERACIONALES MÍNIMOS PARA LOS PRESTADORES DE SERVICIOS DE ALMACENAMIENTO DE LA PKI - Paraguay

LIZ ROSANNA CRAMER CAMPOS

Firmado digitalmente por LIZ ROSANNA CRAMER CAMPOS
Fecha: 2020.09.30 16:54:26 -04'00'

DOC-PKI-08

Versión 1.0

Control de Cambio

Documento	
Título: PROCEDIMIENTOS OPERACIONALES MÍNIMOS PARA LOS PRESTADORES DE SERVICIOS DE ALMACENAMIENTO DE LA PKI Paraguay	**Nombre Fichero:** DOC-PKI-08 V1.0
Código: DOC-PKI-08	**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 14:23:18 -04'00'	MARIA LUJAN OJEDA CHAMORRO Firmado digitalmente por MARIA LUJAN OJEDA CHAMORRO Fecha: 2020.09.30 15:21:45 -04'00'	LUCAS ATILIO SOTOMAYOR LLANO Firmado digitalmente por LUCAS ATILIO SOTOMAYOR LLANO Fecha: 2020.09.30 15:36:57 -04'00'
JENNY RUÍZ DÍAZ	***LUJAN OJEDA***	***LUCAS SOTOMAYOR***

Contenido

1 - DESCRIPCIÓN GENERAL

El objetivo de este documento es regular los requisitos mínimos de seguridad y los procedimientos operacionales que deben adoptar los Prestadores de Servicios de Almacenamiento (PSA) de la Infraestructura de Claves Públicas del Paraguay (PKI-Paraguay).

Complementa, para los PSA, los reglamentos contenidos en los documentos DOC-PKI-03 [1], DOC-PKI-04 [2], DOC-PKI-06 [3] y DOC-PKI-07 [4].

Los requisitos contenidos en este documento deberán ser acreditados por el PSA en el proceso de habilitación para ser autorizados a prestar servicios de almacenamiento de claves privadas de usuarios finales o servicios de firma digital y verificación de firmas digitales, o ambos si fuere el caso, los cuales deben mantenerse actualizados durante su operación y mientras la entidad se encuentre habilitada e integre la PKI-Paraguay.

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.

El dispositivo HSM debe estar homologado por el MIC y para el efecto deberán considerarse las disposiciones aplicables de este documento y la norma DOC-PKI-06 [3], sea el caso para almacenamiento de claves privadas de usuarios finales, para creación de firma o ambos.

El PSA debe contar con una Política de Seguridad de la Información compuesta por directrices, normas y procedimientos que describen los controles de seguridad que deben seguirse en sus dependencias y actividades, en consonancia con la norma ISO 27002/2013.

Deberá existir un ejemplar de la Política de Seguridad de la Información, en formato impreso, disponible para consulta en el Nivel 1 de seguridad del PSA (ver la reglamentación en el ítem 3).

La Política de Seguridad de la información deberá ser aplicada por todo el personal involucrado en las actividades realizadas por el PSA, incluido al personal contratado.

Este documento define los estándares operacionales y de seguridad que deberán aplicarse en las áreas internas del PSA, así como en el tránsito de informaciones, en el almacenamiento de claves privadas, en los servicios de firma digital y verificación de firma digital y en materiales con entidades externas.

A continuación, serán informados los requisitos que deben ser observados en términos de seguridad del personal, seguridad física, seguridad lógica, seguridad de la red, requisitos mínimos para el almacenamiento de claves privadas, servicios de firma digital y verificación de firma digital, clasificación de información, protección activos de la información, gerenciamiento de riesgos, plan de continuidad del negocio, análisis de registro de eventos y plan de capacidad operacional.

1.1. DEFINICIONES, SIGLAS Y ACRÓNIMOS

1.1.1 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) **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.

9) **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.

10) **Datos de creación de la firma:** los datos únicos que utiliza el firmante para crear una firma digital.

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 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.

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) **Infraestructura de Clave Pública:** es un conjunto de personas, políticas, procedimientos y sistemas informáticos necesarios para proporcionar servicios de autenticación, integridad y no repudio, mediante el uso de criptografía de claves públicas y privadas y de certificados digitales, así como la publicación de información, consultas de vigencia y validez de los mismos.

17) **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.

18) **Módulo criptográfico**: software o hardware criptográfico que genera y almacena claves criptográficas.

19) **Módulo de Seguridad de Hardware:** dispositivo basado en un módulo criptográfico tipo hardware que genera, almacena y protege claves criptográficas.

20) **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.

21) **No Repudio:** refiere que la posesión de un documento electrónico y la firma digital asociada al mismo será prueba efectiva del contenido y del autor del documento.

22) **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.

23) **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.

24) **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.

25) **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.

26) **Repositorio:** sitio principal de Internet confiable y accesible, mantenido por la CA con el fin de difundir su información pública.

27) **Solicitante de Certificado:** persona física o jurídica que solicita la emisión de un certificado a una CA.

28) **Solicitud de Firma de Certificado:** petición de certificado digital que se envía a la CA. Mediante la información contenida en el CSR, la CA, puede emitir el certificado digital una vez realizadas las comprobaciones que correspondan.

29) **Suscriptor:** persona física o jurídica titular de un certificado digital emitido por una CA. Un suscriptor puede ser un PSC o un usuario final.

30) **Usuario final:** persona física o jurídica que adquiere un certificado digital de un PSC.

31) **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.

1.1.2 SIGLAS Y ACRÓNIMOS

Tabla Nº 1 – Siglas y Acrónimos

Sigla / Acrónimo	Descripción
CA	Autoridad de Certificación (CA por sus siglas en inglés Certificate Authority)
CadES	CMS Advanced Electronic Signature
CA Raíz-Py	Autoridad Certificadora Raíz del Paraguay
CPS-PSA	Declaración de Prácticas de Certificación del (CPS por sus siglas en inglés, Certification Practice Statement) de un Prestador de Servicio de Almacenamiento (PSA).
CI	Cédula de Identidad
CSR	Solicitud de firma de Certificado (CSR por sus siglas en inglés, Certificate Signing Request)
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
LPSA	Lista de Prestadores de Servicios de Almacenamiento
PadES	PDF Advanced Electronic Signatures
PAS	Pasaporte
PCO	Planificación de Capacidad Operativa
PCN	Plan de Continuidad del Negocio
PIN	Número de Identificación Personal, (por sus siglas en inglés, Personal Identification Number)

PUK	Clave Personal de Desbloqueo (PUK por sus siglas en inglés, Personal Unlocking Key)
PKCS	Norma de criptografía de clave pública (PKCS por sus siglas en inglés, Public Key Cryptography Standard)
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)
RUC	Registro Único del Contribuyente
SSL	Secure Sockets Layer
TLS	Capa de conexión segura (TLS por sus siglas en inglés, Transport Layer Security)
TOTP	Por sus siglas en inglés, Time-based One-Time Password algorithm
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)
XadES	XML Advanced Electronic Signatures
XML	eXtensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

2 - SEGURIDAD PERSONAL

El PSA deberá tener una Política de Gestión de Talento Humano que disponga sobre los procesos de contratación, despido, descripción del cargo, evaluación del desempeño y capacitación.

La comprobación de la capacidad técnica del personal involucrado en los servicios prestados por el PSA, deberá estar disponible para eventuales auditorías e inspecciones.

Todo el personal involucrado en las actividades realizadas por el PSA, personal propio o contratado, debe firmar un acuerdo que garantice la confidencialidad de la información interna y de terceros, incluso después de su desvinculación por despido o la terminación del contrato.

El acuerdo de confidencialidad de la información deberá contener una cláusula explícita de responsabilidad en caso de incumplimiento de las normas o regulaciones que rigen en el marco de la PKI-Paraguay.

El acuerdo de confidencialidad de la información se aplicará a cualquier otra entidad que pueda tener acceso a información interna y de terceros proveniente de los proyectos coordinados por el PSA.

El PSA deberá tener procedimientos formales para la verificación y la rendición de cuentas en caso de incumplimiento de las normas establecidas por sus políticas o por las normas que rigen en el marco de la PKI-Paraguay.

Todo el personal del PSA deberá contar con un dossier que contenga los siguientes documentos:

i. contrato de trabajo o instrumento formal de vinculación;
ii. curriculum vitae donde consten antecedentes de contratación;
iii. certificado original de antecedentes policiales;
iv. certificado original de antecedentes judiciales;
v. curriculum vitae que incluya histórico de empleos anteriores y formación educativa con respaldo documental;
vi. certificado original de vida y residencia;
vii. comprobante de capacidad técnica;
viii. resultado de la entrevista inicial, con la firma del entrevistador;

ix. declaración en la que afirma conocer sus atribuciones y en la que asume el deber de cumplir con las normas aplicables en el marco de la PKI-Paraguay;
x. acuerdo de confidencialidad; y
xi. documento formal de asignación de rol y asignación de mecanismos de control de acceso.

No serán admitidos pasantes en el ejercicio de las actividades de PSA.

A su desvinculación, dicho dossier debe contener los siguientes documentos:

i. evidencia de exclusión de acceso físico y lógico en entornos del PSA; y
ii. declaración firmada por el personal desvinculado de que no posee pendientes, conforme lo dispuesto en el punto ítem 7 “seguridad ligada a los recursos humanos” de la norma ISO 27002/2013.

3 - SEGURIDAD FÍSICA

Serán definidos al menos 4 (cuatro) niveles de acceso físico a los diferentes ambientes del PSA.

El primer nivel, o nivel 1, deberá ubicarse después de la primera barrera de acceso a las instalaciones del PSA. El ambiente de nivel 1 del PSA en la PKI-Paraguay desempeña una función de interfaz con clientes o proveedores que necesitan asistir al PSA.

El segundo nivel, o nivel 2, será interno al primero y deberá requerir la identificación individual de las personas que ingresan. Este será el nivel mínimo de seguridad requerido para la ejecución de cualquier proceso operacional o administrativo del PSA. Para el paso del primer nivel al segundo nivel, se deberá exigir la identificación por medios electrónicos y el uso de un carnet o credencial identificatoria:

a) el ambiente del nivel 2 deberá estar separado del nivel 1 por paredes divisorias de oficinas, mampostería o placas premoldeadas de yeso acartonado. No debe haber ventanas ni ningún otro tipo de abertura al exterior, excepto la puerta de acceso;
b) el acceso a este nivel sólo deberá ser permitido a las personas que trabajan directamente con las actividades de servicios de almacenamiento de claves para usuarios finales y servicios de firma digital y de verificación de la firma digital o el personal responsable del mantenimiento de los sistemas y equipos del PSA, como administradores de red y técnicos de soporte de informática. Los demás empleados/funcionarios del PSA no deberán acceder a este nivel;

c) preferiblemente, UPS, generadores y otros componentes de la infraestructura física deben alojarse en este nivel, para evitar accesos al ambiente de nivel 3 por parte de los proveedores de servicios de mantenimiento;

d) excepto en los casos previstos por la ley, no se permitirá la posesión de armas en las instalaciones del PSA, comenzando en el nivel 2. A partir de ese nivel, equipos de grabación, fotografía, video, sonido o equipo similar, así como computadoras portátiles, tendrán ingreso controlado y solo se puede usar con autorización formal y bajo supervisión.

El tercer nivel, o nivel 3, deberá estar dentro del segundo nivel y será el primer nivel para albergar material y actividades sensibles de la operación del PSA. Cualquier actividad relacionada con el almacenamiento de las claves de los usuarios y servicios de firma digital y de verificación de la firma digital deberá llevarse a cabo a partir de este nivel. Solo las personas autorizadas podrán permanecer en este nivel:

a) en el tercer nivel, deberán ser controladas tanto las entradas como las salidas de cada persona autorizada. Se deben requerir dos tipos de mecanismos de control para ingresar a este nivel: algún tipo de identificación individual, como una credencial identificatoria, e identificación biométrica o ingreso de contraseña;

b) las paredes que delimitan el ambiente del nivel 3 deberán estar hechas de mampostería o material de resistencia equivalente o superior. No deberá haber ventanas ni otro tipo de abertura al exterior, excepto la puerta de acceso;

c) si el ambiente de Nivel 3 tiene un falso techo o piso falso, deberán ser adoptados recursos para evitar el acceso al entorno a través de estos, tales como rejillas de hierro que se extiendan desde las paredes hasta las losas de concreto superior e inferior; y

d) debe haber una única puerta de acceso al entorno de nivel 3, deberá abrirse solamente después de que el empleado o funcionario se haya autenticado electrónicamente en el sistema de control de acceso. La puerta deberá estar equipada con bisagras que permitan la apertura para el lado externo, para facilitar la salida y dificultar el ingreso al ambiente, así como un mecanismo de cierre automático, para evitar que permanezca abierto más tiempo del necesario.

El tercer nivel avanzado, o nivel 3.1, específicamente para los PSA, en el interior del ambiente de nivel 3, deberá comprender al menos un gabinete reforzado bloqueado, que albergará todo el *hardware* y *software* utilizado por el PSA, el cual, para garantizar la seguridad del material almacenado, debe cumplir con las siguientes especificaciones mínimas:

i. Estar hecho de acero o material de resistencia equivalente; y

ii. Poseer una cerradura con llave.

El cuarto nivel, o nivel 4, específicamente para los PSA que prestan servicios de almacenamiento de claves privadas, interior al tercero, es donde deberán ocurrir actividades especialmente sensibles de la operación. Todos los sistemas y equipamientos necesarios para estas actividades deberán ubicarse a partir de ese nivel. El nivel 4 deberá tener los mismos controles de acceso que el nivel 3 y, adicionalmente, debe exigir, en cada acceso a su ambiente, la identificación de al menos 2 (dos) personas autorizadas. En este nivel, se deberá exigir la permanencia de estas personas mientras el ambiente está ocupado.

En el cuarto nivel, todas las paredes, pisos y techos deben estar cubiertos con acero y concreto u otro material de resistencia equivalente. Las paredes, el piso y el techo deben ser sólidos, constituyendo una celda hermética contra las amenazas de acceso inadecuado, agua, vapor, gases y fuego. Los conductos de refrigeración y energía, así como los conductos de comunicación, no deberán permitir la invasión física de las áreas del cuarto nivel. Además, estos ambientes de nivel 4, que constituyen las llamadas salas cofre, deberán tener protección contra la interferencia electromagnética externa.

Las salas cofre deben construirse de acuerdo con las normas paraguayas aplicables. Cualquier omisión en estas normas debe ser subsanada por las normas internacionales pertinentes.

Podrán existir, en el PSA, varios ambientes de tercer nivel avanzado, en el caso de PSA que presta servicios de firma digital, o varios ambientes de cuarto nivel, en el caso del PSA que presta servicios de almacenamiento de claves privadas, para albergar y segregar, cuando sea el caso:

a) equipamientos de producción *on-line*; y
b) equipamientos de red e infraestructura (firewall, enrutadores, switches y servidores).

Todos los servidores y elementos de la infraestructura y protección del segmento de red, tales como ruteadores, hubs, switches y firewall deben:

a) operar en un ambiente con seguridad equivalente, al menos, en el tercer nivel avanzado, para el caso del PSA que presta servicios de firma digital, o en el cuarto nivel, en el caso del PSA que presta servicios de almacenamiento de clave privada citados en este documento; y

b) poseer acceso lógico restringido por medio de un sistema de autenticación y autorización de acceso.

Los PSA también deben cumplir los siguientes requisitos:

a) el ambiente físico del PSA deberá contener dispositivos que autentiquen y registren el acceso de personas informando la fecha y hora de esos accesos;
b) el PSA deberá contener imágenes que garanticen la identificación de las personas cuando acceden físicamente a cualquier parte de su ambiente;
c) la sincronización de la fecha y la hora entre los mecanismos de seguridad física es obligatoria, garantizando el seguimiento de auditoría entre los dispositivos de control de acceso físico y de imagen;
d) todos los que transitan en el ambiente físico del PSA deben llevar credenciales de identificación, incluidos los visitantes;
e) el tránsito de material de terceros a través de los ambientes físicos del PSA sólo se permitirá mediante el registro, garantizando el seguimiento de la auditoría con informaciones sobre dónde pasó el material, la fecha y la hora en que ocurrió el tránsito y quién fue responsable de manejarlo;
f) el PSA deberá contener dispositivos de prevención y control de incendios, temperatura, humedad, iluminación y fluctuaciones en la corriente eléctrica en todo su ambiente físico;
g) todo material crítico inutilizable, desechable o que ya no se pueda utilizar deberá tener un tratamiento de destrucción especial, garantizando la confidencialidad de la información contenida en el mismo. Los equipamientos enviados para mantenimiento deberán tener sus datos borrados, irreversiblemente, antes de ser retirados del ambiente físico del PSA;
h) las computadoras personales, servidores y dispositivos de redes, y sus respectivos softwares, deberán ser inventariados con información que permitan la identificación inequívoca;
i) en caso de inoperancia de los sistemas automáticos, el control de acceso físico debe realizarse provisionalmente por medio de un libro de registro donde conste quién accedió a él, la fecha, la hora y el motivo del acceso;
j) deberán ser proporcionados mecanismos para garantizar la continuidad del suministro de energía en áreas críticas, manteniendo los activos críticos de información en funcionamiento hasta que todos los procesos y datos estén asegurados en caso de que se agote el suministro de emergencia;

k) en el caso de almacenamiento de claves privadas para usuarios finales, debe tener al menos dos ambientes físicos, siendo uno obligatorio para la operación y otro para la contingencia; y

l) todo equipamiento y ambiente computacional que será utilizado en el PSA deberá tener fecha y hora sincronizadas con una fuente confiable de tiempo ajustado con la fecha y hora oficial paraguaya.

4 - SEGURIDAD LÓGICA

El acceso lógico al ambiente computacional del PSA será como mínimo mediante un usuario y contraseña, que deberá cambiarse periódicamente.

Todos los equipamientos del parque computacional deberán ser controlados de tal manera que permita solo el acceso lógico a las personas autorizadas.

Los equipamientos deberán tener mecanismos para bloquear sesiones inactivas.

El PSA deberá tener una política explícita para registrar, suspender y eliminar usuarios en su ambiente computacional. Los usuarios deberán estar registrados en los perfiles de acceso que permitan un privilegio mínimo para llevar a cabo sus actividades.

Los usuarios especiales (como por ejemplo del *root* y el administrador) de sistemas operacionales, hardware criptográfico, bases de datos y aplicaciones en general deben tener sus contraseñas segregadas para que, el acceso lógico a estos ambientes sea de por al menos 2 (dos) personas autorizadas.

Todo equipamiento del PSA deberá tener un *log* activo y su hora sincronizada con una fuente confiable de tiempo que guarde concordancia con la fecha y hora oficial paraguaya.

La información como *log*, pistas de auditoría (de almacenamiento de claves privadas y el servicio de firma), los registros de acceso (físico y lógico) y las imágenes deberán tener una copia de seguridad cuyo almacenamiento será durante 5 (cinco) años.

Los *softwares* de los sistemas operacionales, los antivirus y las aplicaciones de seguridad deben ser mantenidos actualizados.

Se prohíbe cualquier tipo de acceso remoto por parte de los operadores del PSA al entorno de nivel 3.

5 - SEGURIDAD RED

El tráfico de informaciones en el ambiente de red deberá ser protegido contra daños o pérdidas, así como contra el acceso, uso o exposición indebidos.

No se podrá permitir el acceso externo a la red interna del PSA. Los intentos de acceso externo deberán ser inhibidos y monitoreados a través de aplicaciones que crean barreras y filtros de acceso, así como mecanismos de detección de intrusos.

Las pruebas de seguridad deberán aplicarse en la red interna y externa con aplicativos especializados, al menos 1 (una) vez al mes. Los testeos en la red deberán documentarse y las vulnerabilidades detectadas deberán ser corregidas.

6 - REQUISITOS PARA ALMACENAMIENTO DE CLAVES PRIVADAS

6.1 ALMACENAMIENTO DE CLAVES PRIVADAS Y CERTIFICADOS DIGITALES.

Las claves privadas de los usuarios finales, para los certificados del Tipo F3 o C3 obligatoriamente deben ser generados y almacenados en hardware criptográficos tipo HSM. Las mismas deben estar almacenadas dentro de los espacios de la frontera criptográfica, o equivalente dentro del contexto de seguridad del HSM. Se exige que las claves sean activadas y utilizadas únicamente dentro del hardware físico de dicho HSM bajo control exclusivo del usuario titular del certificado.

Los HSM deben presentar esquema de gestión de claves apto para, además de proteger las mismas, asegurar el intercambio de información a través de un marco de seguridad.

Los HSM deberán cumplir los siguientes requisitos:

1) garantizar como mínimo, por medios técnicos y de procedimiento adecuados, que:
   a) esté garantizada razonablemente la confidencialidad de los datos de creación de firma utilizados para la creación de firmas digitales;
   b) los datos de creación de firma utilizados para la creación de firma digital sólo puedan aparecer una vez en la práctica;
   c) exista la seguridad razonable de que los datos de creación de firma utilizados para la creación de firma digital no pueden ser hallados por deducción y de que la firma está

protegida con seguridad contra la falsificación mediante la Tecnologías disponible en el momento; y

d) los datos de creación de la firma utilizados para la creación de firma digital puedan ser protegidos por el firmante legítimo de forma fiable frente a su utilización por otros.

2) No alterarán los datos que deben firmarse ni impedirán que dichos datos se muestren al firmante antes de firmar.

Los espacios para el almacenamiento de las claves privadas de los usuarios finales podrán ser liberados desde que no haya renovación por parte del usuario o revocación de las claves, sin embargo, el registro de almacenamiento de claves debe mantenerse de acuerdo con la Declaración de Prácticas del Prestador de Servicios de Almacenamiento de la PKI-Paraguay (CPS-PSA).

El PSA y el PSC deberán documentar cuales son los procedimientos concretos que ponen en práctica para garantizar que la clave privada del Solicitante fue generada y almacenada en el HSM en custodia del PSA, y que el titular tiene el control exclusivo del mecanismo de autenticación que protege el uso de su clave privada generada.

6.2 MECANISMO DE AUTENTICACIÓN PARA ACCESO A LA CLAVE PRIVADA

El acceso a las claves privadas de los usuarios debe ser de uso, conocimiento y control exclusivo del titular del certificado, sin la posibilidad de ingreso por parte de otros titulares en el mismo HSM, cualquier empleado/funcionario del PSA o dependiente de otras claves criptográficas.

El PSA debe proporcionar mecanismos de doble factor de autenticación al titular del certificado para el acceso a su clave privada, debiendo:

i. ser un factor dentro del límite de la frontera criptográfica del HSM y otro dentro del ambiente seguro y la primera interfaz de comunicación con el HSM, o
ii. ambos dentro del límite de la frontera criptográfica del HSM.

Se recomienda que cada factor sea de una clase diferente (conocimiento, posesión o biometría).

Los mecanismos de autenticación deben emplear un método o protocolo de validación que proteja los datos de transmisión y los datos de autenticación por medio de criptografía y los siguientes requisitos técnicos:

i) Usuario y contraseñas: de acuerdo con las reglas que establezca la CA Raíz-Py;
ii) PIN de firma (PIN/PUK): de acuerdo con las reglas que establezca la CA Raíz-Py;
iii) OTP: de acuerdo con las reglas de RFC 6238 (TOTP), RFC 6287, RFC 4226 (HOTP);
iv) Biometría: de acuerdo con las reglas que establezca la CA Raíz-Py;
v) Certificado digital: de acuerdo a la normas establecidas en el marco de la PKI-Paraguay;
vi) Notificación Push: de acuerdo con las reglas del protocolo de extensión XMPP o similar; o
vii) Otras autenticaciones semánticas de acuerdo con este documento y previamente aprobadas por CA Raíz-Py.

6.3 PROTOCOLOS

Los HSM homologados por el MIC deben soportar una interfaz PKCS#11 o similar, atendiendo las exigencias de especificación de la CA Raíz-Py y además de los informados en este documento, cumpliendo con los siguientes requisitos generales:

a) ejecutar los algoritmos que sean parte de las funciones *core* de una firma digital en forma interna al hardware del HSM;
b) generar y destruir claves simétricas y asimétricas en forma interna al hardware del HSM;
c) activar y desactivar claves en forma interna al hardware del HSM cuando su titular lo autorice;
d) proteger las claves privadas y sólo habilitar su activación y uso en forma interna del hardware del HSM; y
e) habilitar el uso de punteros, manejadores, alias o tokens de claves privadas a las aplicaciones que se conecten, evitando el uso directo de las mismas en claro desde el exterior en forma interna al hardware del HSM.

Los HSM homologados por el MIC podrán soportar el Protocolo KMIP (Key Management Interoperability Protocol), versión 1.3 o superior o otras de acuerdo con este documento y previamente aprobadas por CA Raíz-Py.

6.4 REDES y DISPONIBILIDAD

El PSA deberá disponibilizar mecanismos para asegurar a los usuarios finales la disponibilidad del sistema para uso de sus claves privadas y certificados.

Entre dichos mecanismos para asegurar la disponibilidad:

a) se deberá hacer una copia de las claves de los usuarios finales, en otro ambiente de contingencia física o disponer de mecanismos de recuperación de claves, observando los mismos requisitos de almacenamiento que el ambiente principal. El ambiente de contingencia debe estar listo para operar dentro de las 48 horas;
b) podrá ser diseñado un *pool* o cluster de HSM para operación, replicación y gerenciamiento de las claves de los usuarios finales, debiendo seguir, además de los descritos en este documento, los siguientes requisitos.
    i. especificación y establecimiento de comunicación segura (sesión SSL/TLS) o equivalente entre los HSM;
    ii. los HSM podrán estar en diferentes ambientes/entornos siempre que los mecanismos de acceso y seguridad se mantengan como se describe en este documento; y
    iii. el número de conjuntos de datos duplicados no podrá superar el mínimo necesario para garantizar la continuidad del servicio.

Los PSA dentro del ámbito de la PKI-Paraguay deberán contar, además de las exigencias relacionadas a sus instalaciones, sistemas, procedimientos y otros requerimientos indicados en este documento, con:

a) procedimientos e indicaciones de recuperación de claves y del esquema de disponibilidad de las mismas;
b) controles de seguridad para recuperación de claves y para el funcionamiento de esquema de disponibilidad de claves; y
c) pruebas de recuperación y funcionamiento de esquema de disponibilidad de claves.

Los PSA dentro del ámbito de la PKI-Paraguay deben cumplir con los criterios mínimos de 99.95% de "nivel de tiempo de actividad " (*uptime*) que se verificará por mes.

6.5. REQUISITOS PARA SERVICIOS DE USO DE CLAVES PRIVADAS

6.5.1. DEFINICIONES PARA LA INTERFAZ DE LOS SERVICIOS

Deberá ser utilizado el protocolo TLS, definido por RFC 5246 o su versión actualizada, para la comunicación con los servicios.

Deberá ser utilizado el framework OAuth 2.0 (RFC 6749 y RFC 7636) para la implementación de la interfaz con los servicios del PSA.

Adicionalmente, podrá ser implementada otra interfaz para servicios, siempre que el PSA proporcione el software necesario para permitir al titular utilizar sus claves privadas de forma segura.

6.5.2. DEFINICIONES PARA EL URI DE BASE PARA SERVICIOS.

El URI de base (URI-base) definirá el estilo y el formato de las direcciones HTTPS de servicios del PSA.

El URI-base deberá ser registrado ante la CA Raíz bajo la PKI-Paraguay.

Ejemplo de URI-base:

https://servicio.prestador_de_almacenamiento.com.py

Obs. La dirección *servicio.prestador_de_almacenamiento.com.py* representa en este ejemplo la porción de autoridad del URI en el dominio utilizado por el PSA.

Las porciones restantes del URI de los servicios registrados del PSA deben concatenarse con el URI-base.

6.5.3 LISTA DE SERVICIOS PROPORCIONADOS POR EL PSA

a) Servicios Obligatorios

1) Servicio de autorización:

I. Código de Autorización (Authorization Code Request): servicio para obtener del Titular del Certificado la autorización de uso de su clave privada o autorizar una autenticación sin uso la clave privada.

Si el titular tiene más de un certificado, el PSA debe presentarlos para que el titular pueda hacer la elección en el mismo contexto de aplicación en el que se trasladan los factores de autenticación.

Corresponderá al PSA habilitar los scopes (alcance) para las aplicaciones registradas. Corresponderá a la aplicación previamente registradas presentar los scopes durante el proceso de autorización/autenticación;

II. Token de Acceso: después de obtener el código de autorización, el Token de Acceso debe ser solicitado. Los tokens de acceso son credenciales que se utilizan para acceder o utilizar recursos protegidos por el Titular, como ser datos de información u otros atributos del titular, incluyendo sus datos de creación de firmas;

2) Firma: servicio de firma digital conforme al ítem 6, para el cual deberá tener un token de acceso válido; y
3) Registro de Aplicaciones: servicio de registro de una aplicación en el PSA a través de un servicio o una operación administrativa en la plataforma.

b) Servicios Opcionales
1) Recuperación de Certificado: servicio para recuperar un certificado almacenado en el PSA. La aplicación deberá tener un token de acceso válido;
2) Localización del Titular: servicio para encontrar a un titular a través del número CI, PAS o RUC; y
3) Autorización con credencial de titular: servicio para obtener autorización del titular del certificado para utilizar su clave privada, con solicitud de factores de autenticación.

6.5.4. AUTORIZACIÓN Y AUTENTICACIÓN PARA SOLICITUD DE SERVICIOS.

El PSA deberá disponibilizar los servicios web (o APIs web) de autorización y autenticación atendiendo a la finalidad de sus funciones.

Dichos servicios son consumidos por las aplicaciones cliente de firma.

6.5.4.1. Flujo básico para Uso de Servicios.

a) Seguido del flujo de autorización establecido por el RFC 6749, el uso de claves privadas en el PSA deberá ir precedido de una solicitud exitosa, por parte de las aplicaciones. Este requerimiento se aplica para los siguientes servicios:
i. Servicio de Autorización (Código de Autorización y Token de Acceso); y
ii. Firma.

En el modelo propuesto toda aplicación que quiera acceder a un recurso debe ser autorizada por el propietario del recurso (titular del certificado), y acreditar después esta autorización ante el proveedor del mismo. De este modo, cuando una aplicación quiere acceder a un recurso del recurso a través del servicio del PSA, debe presentar un token de acceso válido que acredite que efectivamente cuenta con la correspondiente autorización del propietario del recurso.

Las aplicaciones cliente o sistemas de los titulares de certificados que se conecten con los servicios del PSA deben utilizar las operaciones de flujos OAuth 2.0 y obtener un token de acceso.

b) Cuando fuera necesario utilizar un servicio destinado únicamente a la autenticación del titular, es decir, sin el uso de una clave privada, deberá ir precedido de una solicitud exitosa, por parte de las aplicaciones. Este requerimiento se aplica para los siguientes servicios:
   i. Servicios de Autorización (Código de Autorización y Token de Acceso); y
   ii. Recuperación de certificado.

6.5.4.2. Tránsito de los Factores de Autenticación.

Se deberán implementar los mecanismos de autenticación contemplando los requerimientos de acceso exclusivo a clave del titular del certificado según indicado en el presente documento.

Las aplicaciones no deberán recopilar factores de autenticación del titular del certificado. Para este fin, los PSA deberán comunicarse directamente con el equipo o sistema del titular, previamente identificado y registrado en el PSA de forma segura.

El Servicio de "*Autorización con Credencial*" *de* Titular se encuentra exento de esta regla.

6.5.4.3. Autenticación de aplicaciones de Firma.

Para que una aplicación pueda utilizar los servicios del PSA tiene que solicitar el registro en la plataforma de firma y obtener un mecanismo de acceso para su conexión. Por tanto, en cuanto a la autenticación de aplicaciones de firma: para obtener acceso a los servicios, los PSAs deberán implementar obligatoriamente un *Servicio de Registro de Aplicaciones*.

El *Servicio de Registro de Aplicaciones* podrá estar basado en certificados digitales o en mecanismos sin certificados pero que utilicen una API Key dentro del modelo OAuth. En este último caso, como resultado del registro, la aplicación obtendrá un identificador (identificador de cliente), un secreto compartido con la plataforma (secreto de cliente) y una API-Key. La aplicación

deberá utilizar la API Key como credencial de autenticación en todas las peticiones que dirija al servicio de autenticación y autorización para obtener un token de acceso a cualquiera de los recursos protegidos de la plataforma (datos de un usuario y de su proceso de autenticación, identidades de firma de un usuario, etc). Para ello, tal como establece OAuth 2.0, pondrá la API Key en la cabecera de autorización de dichas peticiones.

Los PSAs podrán implementar, para las aplicaciones, otros métodos de acceso a sus servicios, siempre que se evalúen los riesgos asociados y se permita la trazabilidad.

6.6 LISTA DE PRESTADORES DE SERVICIOS DE ALMACENAMIENTO (LPSA)

La LPSA estará integrada por las entidades habilitadas en virtud de la PKI-Paraguay como PSA. La LPSA será publicada por la CA Raíz-Py y actualizada dentro de un período máximo de 180 días.

La LPSA se publicará en el repositorio de la CA Raíz-Py en versión textual, para lectura humana, y en XML, para procesamiento para máquina.

La autenticidad e integridad de la versión procesable por máquina de la lista compilada se garantiza mediante una firma digital XMLDSig respaldada por un certificado digital.

Las versiones del LPSA y el certificado que firma el LPSA se publicarán en el repositorio raíz de la CA Raíz-Py, disponible en: https://www.acraiz.gov.py/**.**

La autenticidad e integridad de la lista compilada debe ser verificada por las partes confiables antes de cualquier uso.

7. SERVICIO DE FIRMA DIGITAL Y VERIFICACIÓN DE FIRMA DIGITAL.

7.1. INTRODUCCIÓN

Los siguientes requisitos se basaron en los estándares para crear y validar firmas definidas en las especificaciones del ETSI.

El PSA deberá disponer de documentación para desarrolladores para la integración a su servicio de firma estableciendo las condiciones para su uso y/o integración en concordancia con lo dispuesto en este documento. Independientemente de la implementación del servicio de firma,

en todo momento se deberá asegurar el exclusivo control del firmante sobre su clave privada de firma digital en custodia.

7.2. CREACIÓN DE FIRMAS

El propósito de crear firmas es generar una firma que cubra un documento electrónico (texto, sonido, imagen, entre otros) del firmante, el certificado de firma o una referencia a ese certificado, así como los atributos de firma que la respaldan.

Un modelo funcional básico de un ambiente para crear firmas está constituido por:

i. firmante que quiere crear una firma en un documento electrónico;
ii. una aplicación conductiva que representa un ambiente de usuario (por ejemplo, una aplicación comercial) que el suscriptor usa para acceder a la funcionalidad de firma; y
iii. un sistema de creación de firma, que implementa la funcionalidad de firma, ubicada en el PSA.

Antes de procesar la petición de firma, el PSA debe garantizar que el usuario titular del certificado sea autenticado y debe verificar la validez de dicho certificado.

La participación humana de un firmante no siempre es necesaria. La firma puede ser un proceso automatizado e implementado en la aplicación en el entorno del usuario.

7.3. DISPOSITIVOS PARA LA CREACIÓN DE FIRMAS

Son sistemas o equipos configurados para implementar códigos y/u otros mecanismos que permiten la activación de la clave privada del firmante para la creación de firmas digitales.

Los dispositivos para creación de firmas, además de poder verificar los datos de autenticación del firmante, deben contener:

i) la clave privada del firmante; y
ii) el correspondiente certificado digital relacionado a esa clave privada o tener una referencia inequívoca a él.

El PSA deberá utilizar un HSM y sistemas de software correspondiente autorizados por el MIC para brindar los servicios que expone, permitiendo que el titular del certificado tenga acceso, control y uso exclusivo de sus datos de creación de firmas. Dichos componentes están

delimitados dentro de la frontera criptográfica del HSM y dentro del ambiente seguro de la primera interfaz de comunicación con el HSM.

7.4. INTERFAZ DE APLICACIÓN CON EL DISPOSITIVO DE CREACIÓN DE FIRMA.

La interfaz entre la aplicación de firma y el dispositivo o equipo de creación deben garantizar que solo con la autenticación del titular del certificado, el cual debe tener el control exclusivo de la clave privada, sea posible requerir la creación de datos de una firma digital.

El uso del dispositivo de creación debe requerir que el usuario ingrese datos específicos de autenticación del firmante. Toda la información intercambiada entre la aplicación y el dispositivo debe viajar en forma cifrada.

Se debe usar más de un mecanismo de autenticación para proporcionar una garantía de autenticación suficiente.

El mecanismo de autenticación de un firmante debe evitar los ataques de suplantación.

La naturaleza de los mecanismos de autenticación y de los datos de autenticación del firmante son determinados por el dispositivo de creación de firmas. Existen estándares para diferentes interfaces, tipos de dispositivos o equipos y mecanismos de autenticación.

En algunos casos, el uso de datos de autenticación del firmante será obligatorio y se pueden imponer otros requisitos sobre la naturaleza de los mecanismos e interfaces de autenticación.

7.5. SUITES DE FIRMA

Todos los algoritmos y tamaños de clave involucrados en el cálculo de cualquier elemento de la firma digital se definen en el documento DOC-PKI-06 [3].

7.6. FORMATOS DE FIRMA

Las políticas de firmas podrán proporcionar firmas en los formatos CAdES, XAdES y PAdES.

Los PSA deben implementar firmas digitales basadas en políticas de firma estandarizadas conforme al DOC-PKI-06 [3] atendiendo como referencia las disposiciones establecidas en los siguientes documentos:

- ETSI. ASN.1 Format for Signature Policies. Number TR 102 272.

- ETSI. XML Format for Signature Policies. Number TR 102 038.
- ETSI. Electronic Signatures and Infrastructures; PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles. TS 102 778-3.
- ETSI. Electronic Signatures and Infrastructures; PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES-LTV Profile. TS 102 778-4.

7.7. LA FIRMA CON EL SELLO DE TIEMPO

Una firma digital con una marca de tiempo muestra que la firma digital ya existía en la fecha contenida en la marca de tiempo. Los Sellos de tiempo son emitidos por las Autoridades de Sello de Tiempo, proporcionan la fecha/hora como una propiedad añadida a una firma digital y su aplicación es de carácter opcional.

Los PSA podrán utilizar políticas de firma que requieran el uso de la marca de tiempo basadas en normas internacionales.

El modelo de sello de tiempo adoptado en su infraestructura debe seguir como referencia las recomendaciones estipuladas en los siguientes documentos:

- RFC 2030, IETF - Simple Network Time Protocol (SNTP) version 4.0.
- RFC 2527, IETF - Internet X-509 Public Key Infrastructure Certificate Policy and Certifications Practices Frame work, março de 1999.
- RFC 3161, IETF - Public Key Infrastructure Time Stamp Protocol (TSP), agosto de 2001.
- RFC 3628, IETF - Policy Requirements for Time Stamping Authorities, November 2003.
- ETSI TS 101.861 Technical Specification/Time Stamping Profile.
- ETSI TS 102.023 Technical Specification / Policy Requirements for Time Stamping Authorities.

7.8. VALIDACIÓN DE FIRMAS

Consiste en primer lugar, 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.

El proceso de validación de una firma digital debe ser realizado conforme una política de firma digital explícita, que consiste en un conjunto de restricciones de validación, denominada

Política de firma, y debe generar un informe que indique el estado de validación (Válido, Inválido o Indeterminado), que proporciona los detalles de la validación técnica de cada una de las restricciones aplicables, que pueden ser relevantes para la aplicación exigente en la interpretación de los resultados.

El firmante crea una firma digital de acuerdo con una política de firma. y el verificador evalúa la validez de una firma digital utilizando la misma política de firma utilizada en la creación de esa firma digital. El ítem 6.6 define los formatos y perfiles que podrán ser utilizados.

7.9. ACUERDO DE NIVEL DE SERVICIO

El acuerdo de nivel de servicio para todos los servicios acreditados por el PSA debe ser de al menos 99.95%.

8 - CLASIFICACIÓN DE LA INFORMACIÓN

Toda la información generada y custodiada por el PSA debe clasificarse de acuerdo con su contenido crítico y grado de confidencialidad, de acuerdo con su propia Política de Clasificación de Información.

La clasificación de la información en el PSA deberá ser realizada independientemente de los medios donde se almacena o los medios por el cual que se transporta.

La información se puede clasificar en:

i. pública: cualquier activo de información, propiedad del PSA o no, que pueda ponerse a disposición del público sin consecuencias perjudiciales para el funcionamiento normal del PSA. cualquier persona puede acceder a este, ya sea interno o externo al PSA. La integridad de la información no es vital.
ii. personal: Cualquier activo de información relacionado con información personal. Por ejemplo: mensaje de correo electrónico personal, archivo personal, datos personales, entre otros.
iii. interna: cualquier activo de información, propiedad del PSA o no, que no se considere público. La divulgación no autorizada del activo de la información podría afectar la imagen del PSA. Por ejemplo: código fuente del programa, cronograma de actividades, actas de reuniones, entre otros.
iv. confidencial: cualquier activo de información que sea crítico para las actividades del PSA en relación con la confidencialidad y la integridad.

Si el PSA es una entidad de la Administración Pública deberá considerar las disposiciones legales aplicables.

9 - SALVAGUARDA DE ACTIVOS DE INFORMACIÓN

El PSA, en su Política de Seguridad de la Información, definirá cómo se guardarán los activos de información en formato electrónico, también denominado backup.

La protección de los activos de información deberá describir las formas de ejecutar los siguientes procesos:

i. Procedimientos de backup;
ii. Indicaciones para usar los métodos de backup;
iii. Tabla de temporalidad;
iv. Ubicación y restricciones de almacenamiento y salvaguarda en función a la fase de uso;
v. Tipos de medios;
vi. Controles ambientales de almacenamiento;
vii. Controles de seguridad;
viii. Prueba de restauración de backup.

El PSA debe tener una política de recepción, manejo, depósito y descarte de materiales de terceros.

10 - GESTIÓN DE RIESGOS

El PSA deberá tener un proceso de gestión de riesgos actualizado para evitarlos, incluidos los derivados de las nuevas tecnologías, con el objetivo de elaborar planes de acción adecuados para proteger los componentes amenazados, actualizados al menos anualmente.

11 - PLAN DE CONTINUIDAD DE NEGOCIOS

Un plan de continuidad del negocio (PCN) deberá ser implementado y probado en el PSA, al menos una vez al año, para garantizar la continuidad de los servicios críticos para el negocio en caso de una inoperancia total o parcial de su ambiente.

12 - ANÁLISIS DE REGISTRO DE EVENTOS

Todos los registros de eventos (logs, registros de auditoría e imágenes) deberán analizarse al menos una vez al mes y se debe generar un informe con la firma de la persona responsable del PSA.

13 - PLAN DE CAPACIDAD OPERACIONAL (PCO)

Los PSA deben preparar y mantener un PCO anualmente para determinar la capacidad de producción actual y futura con niveles de rendimiento satisfactorios para responder a las nuevas demandas, proporcionando niveles satisfactorios de servicios a los usuarios, con el objetivo de escalar los sistemas para soportar el crecimiento orgánico, uso máximo y estacionalidad.

El PCO deberá, como mínimo:

i. Determinar los niveles de servicio requeridos por los usuarios;
ii. Analizar la capacidad de procesamiento de datos instalada; y
iii. Dimensiones de la infraestructura necesaria, el hardware, la comunicación de datos y la capacidad de enlace a Internet para cumplir con los niveles de servicio actuales y futuros.

14 - REFERENCIAS

14.1 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 6238: TOTP: Time-Based One-Time Password Algorithm
- RFC 6287: OCRA: OATH Challenge-Response Algorithm
- RFC 4226 HOTP: An HMAC-Based One-Time Password Algorithm
- ETSI TS 102 231 - Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information.

- RFC 2030: Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OS.
- RFC 2527: Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework.
- RFC 3161: Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP)
- RFC 3628: Policy Requirements for Time-Stamping Authorities (TSAs)
- RFC 5246: The Transport Layer Security (TLS) Protocol. Version 1.2
- RFC 6749: The OAuth 2.0 Authorization Framework.
- RFC 7636: Proof Key for Code Exchange by OAuth Public Clients
- ETSI TS 101.861 - Technical Specification/Time Stamping Profile.
- ETSI TS 102.023 - Technical Specification/Policy Requirements for Time Stamping Authorities.
- ETSI. ASN.1 Format for Signature Policies. Number TR 102 272.
- ETSI. XML Format for Signature Policies. Number TR 102 038.
- ETSI. Electronic Signatures and Infrastructures; PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles. TS 102 778-3. V1.2.1. 2010.
- ETSI. Electronic Signatures and Infrastructures; PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES-LTV Profile. TS 102 778-4. V1.1.1. 2009.

14.2 REFERENCIAS A DOCUMENTOS QUE COMPONEN LA PKI-Paraguay

Tabla Nº 2 – 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
[4]	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.	DOC-PKI-07