DIRECTIVAS OBLIGATORIAS PARA LA FORMULACIÓN Y ELABORACIÓN DE LA PRÁCTICA DE CERTIFICACIÓN DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN (PSC)

Abog. Yadys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Contenido

Abog. Rodolfo Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Abog. Rodyl Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Abog. Rocío Rolón A.
DIRECTORA GENERAL
Firma Digital y Comercio Electrónico

Abog. Rocys Alison A.
DIRECTOR GENERAL
Dirección General de Firma Digital y Comercio Electrónico

Abog. Rocys Rojas A.
DIRECTORA GENERAL
Firma Digital y Comercio Electrónico

Don. Rodrigo Rolón A.
Directora GENERAL
Firma Digital y Comercio Electrónico

Abog. Rocys Rojon A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Abog. Rody Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Abog. Rocio Zarza A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Abog. Rocío Zorrilla A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

CONTROL DOCUMENTAL

Documento	
Título:	Nombre Fichero:
Código:	Soporte Lógico
Fecha:	Ubicación Física:
Versión:	

Registro de Cambios		
Versión	Fecha	Motivo de Cambio

Distribución del documento	
Nombre	Área

Control del Documento		
Preparado por:	Revisado por:	Aceptado por:

Abog. Nadys Rolón A.
DIRECTORA GENERAL
Firma Digital y Comercio Electrónico

1. INTRODUCCIÓN

1.1 DESCRIPCIÓN GENERAL

Este documento establece los requisitos mínimos que deben ser obligatoriamente cumplidos por los prestadores de servicios de certificación (PSC) en su carácter de autoridad certificadora intermedia, integrantes de la Infraestructura de clave pública del Paraguay (PKI Paraguay) en la formulación y elaboración de su Declaración de Prácticas de Certificación (CPS). La CPS es un documento que describe los procedimientos empleados por una autoridad certificadora (CA) para la correcta ejecución de sus servicios.

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

1.2 NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

En este ítem debe ser identificado la CPS, indicando como mínimo el nombre, versión, fecha de aprobación, localización y el OID (Object Identifier) del documento.

1.3 PARTICIPANTES DE LA PKI

1.3.1. AUTORIDADES CERTIFICADORAS (CA)

En este ítem debe ser identificada las CA, integrantes de la PKI Paraguay a la que se refiere la CPS.

Abog. Rocys Rolón A.
DIRECTORA GENERAL
Firma Digital y Comercio Electrónico

1.3.2. AUTORIDADES DE REGISTRO (RA)

En este ítem debe identificarse la dirección de la página web (URL), donde se publican los datos referentes a las autoridades de registro (RA) habilitadas por el PSC para el proceso de recepción, validación y direccionamiento de solicitudes de emisión o de revocación de certificados digitales y de identificación de sus solicitantes. Las informaciones a ser publicadas en el sitio son:

a) La lista de todas las RA del PSC, con informaciones sobre las CP que implementan;

b) Para cada RA del PSC, las direcciones de todas las instalaciones técnicas, autorizadas por la CA Raíz del Paraguay para funcionar;
c) Acuerdo operacionales celebrados entre un PSC y una RA delegada.

EL PSC deberá mantener las informaciones siempre actualizadas.

Las RA delegadas son autoridades de registro vinculadas a un PSC mediante un contrato de prestación de servicios; el funcionamiento de las mismas deberá estar en conocimiento y autorizadas por la CA raíz.

1.3.3. PRESTADORES DE SERVICIOS DE SOPORTE (PSS)

Es este ítem se identifica la dirección de página web (URL), donde deberán estar publicados los datos referentes a los Prestadores de Servicio de Soporte (PSS) vinculados al PSC, sea directamente o sea por intermedio de sus RA.

PSS son entidades externas a las que recurre la CA o la RA para desempeñar actividades descritas en esta CPS o en una CP y se clasifican en tres categorías, conforme al tipo de actividades prestadas.

a) Disponibilización de infraestructura física y lógica;
b) Disponibilización de recursos humanos especializados;
c) Disponibilización de infraestructura física y lógica y de recursos humanos especializados.

El PSC deberá mantener las informaciones arriba citadas siempre actualizadas.

1.3.4. SUSCRIPTORES

En este ítem se especifican las personas físicas o jurídicas que podrán ser titulares de los certificados emitidos según esta CPS.

Abog. Gladys Rolón A.
DIRECTORA GENERAL
Firma Digital y Comercio Electrónico

1.3.5. PARTE QUE CONFÍA

Se entenderá por parte que confía, toda persona física o jurídica, diferente al titular del certificado que decide aceptar y confiar en un certificado digital emitido dentro de la jerarquía PKI Paraguay.

Una parte que confía puede o no ser un suscriptor.

1.3.6. OTROS PARTICIPANTES

Sin estipulaciones.

1.4 USO DEL CERTIFICADO

1.4.1 USOS APROPIADOS DEL CERTIFICADO

En este ítem, la CPS debe relacionar e identificar las CP implementadas por el PSC, que definen como deberán ser utilizados los certificados emitidos. En estas CP estarán especificadas las aplicaciones para las cuales sean adecuados, el uso de los certificados emitidos por un PSC.

1.4.2. USOS PROHIBIDOS DEL CERTIFICADO

Este ítem de la CPS debe relacionar e identificar las CP implementadas por el PSC, que definen las aplicaciones para las que esté prohibido el uso de los Certificados emitidos por el PSC.

1.5 ADMINISTRACIÓN DE LA POLÍTICA

1.5.1. ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

En este ítem deben ser incluidos, el nombre, la dirección y otras informaciones del PSC responsable de la elaboración de la CPS

1.5.2. PERSONA DE CONTACTO

En este ítem, deben ser incluidos, el nombre, los números de teléfonos, el correo electrónico, de la persona de contacto asignado por el PSC.

1.5.3. PERSONA QUE DETERMINA LA ADECUACIÓN DE LA CPS A LA POLÍTICA

En este ítem debe ser incluido el nombre de la persona que determina la adecuación de la CPS a la Política.

1.5.4 PROCEDIMIENTOS DE APROBACIÓN DE LA CPS

En este Ítem se especifica el procedimiento de aprobación de la CPS.

Abog. Rubys Rolón A.
DIRECTORA GENERAL
Firma Digital y Comercio Electrónico

1.6 DEFINICIONES Y ACRÓNIMOS

1.6.1 DEFINICIONES

Acuerdo de Suscriptores: es un acuerdo entre la CA Raíz y el PSC, y entre el PSC y el usuario final, que establece los derechos, obligaciones y responsabilidades de las partes con respecto a la emisión y gestión de los certificados. Éste acuerdo, requiere la aceptación explícita de las partes intervinientes.

Armario ignífugo: armario equipado con sistemas de protección contra el fuego para aislar los productos almacenados en su interior.

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.

Autoridad de Aplicación (AA): se designa al Ministerio de Industria y Comercio como órgano regulador competente por Ley, establecido por el artículo 38 de la Ley 4610/2012 que modifica y amplía la Ley N° 4017/2010 "De validez jurídica de la Firma Electrónica, Firma Digital, los Mensajes de Datos y el Expediente Electrónico". Ejerce funciones a través de su unidad administrativa, la Dirección General de Firma Digital y Comercio Electrónico, dependiente del Viceministerio de Comercio.

Autoridad de Certificación (CA): 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 del Paraguay y el PSC.

Autoridad Certificadora Raíz o **Autoridad de Certificación Raíz (CA Raíz):** es el órgano técnico dentro de la PKI, cuya función principal es intervenir en el proceso de habilitación habilitar al PSC y emitir a éste, el certificado digital correspondiente. Posee un certificado autofirmado y es a partir de allí, donde comienza la cadena de confianza.

Abog. Gladys Rolón A. DIRECTORA GENERAL Firma Digital y Comercio Electrónico

Autoridad de Certificación Intermedia (CAI): entidad cuyo certificado de clave pública ha sido firmado digitalmente por la autoridad de certificación raíz; es responsable de la emisión de certificados a usuarios finales.

Autoridad de Registro (RA): entidad responsable de la identificación y autenticación de titulares de certificados digitales; la misma no emite ni firma certificados. Una RA interviene en el proceso de solicitud del certificado, en el proceso de revocación

o en ambos. La RA, no necesita ser un organismo separado, sino que puede ser parte de la CA.

Autoridad de Validación (VA): entidad responsable de suministrar información sobre la vigencia de los certificados que a su vez hayan sido registrados por una autoridad de registro y certificados por la autoridad de certificación. La VA, no necesita ser un organismo separado sino que puede ser parte de la CA.

Cadena de certificación: lista ordenada de certificados que contiene un certificado de usuario final y certificados de CA, que termina en un certificado raíz. El emisor del certificado del usuario final es el titular del certificado de CA y a su vez, el emisor del certificado de CA es el titular del certificado de CA Raíz. El usuario final o la parte que confía, debe verificar la validez de los certificados en la cadena.

Ceremonia de claves: procedimiento mediante el cual es generado un par de claves de CA, su clave privada es generada y almacenada en un módulo criptográfico, y debe ser respaldada con el mismo nivel de seguridad que la clave original. Este procedimiento debe ser documentado.

Certificado Digital (CD): 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.

Abog. Rocys Rolón A. DIRECTORA GENERAL Firma Digital y Comercio Electrónico

Cifrado: es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido de manera que solo pueda leerlo la persona que disponga de la clave del cifrado adecuada para decodificarla.

Cifrado asimétrico: tipo de cifrado que utiliza un par de claves criptográficas diferentes (ejemplo: privado y público) y matemáticamente relacionadas.

Claves criptográficas: valor o código numérico que se utiliza con un algoritmo criptográfico para transformar, validar, autenticar, cifrar y descifrar datos.

Clave pública y privada: la criptografía en la que se basa la PKI Paraguay, es la criptografía asimétrica. En ella se emplea un par de claves: lo que se cifra con una de ellas, sólo se puede descifrar con la otra y viceversa. A una de esas claves se la denomina pública y está incorporada en el certificado digital, mientras que a la otra se le denomina privada y está bajo la custodia del titular del certificado.

Cofre de seguridad: compartimiento para almacenar materiales o documentos sensibles de la CA, debe ser resistente al fuego y ofrecer protección a aperturas forzadas.

Compromiso: violación de la seguridad de un sistema a raíz de una posible divulgación no autorizada de información sensible.

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.

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.

Declaración de Prácticas de Certificación (CPS): 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.

Abog. Rocys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Delta CRL: partición del CRL, dentro de una unidad de tiempo, que contiene los cambios realizados al CRL base desde su última actualización.

Emisión: comprende la generación del certificado, cuyo proceso es una función de la CA

Emisor del certificado: organización cuyo nombre aparece en el campo emisor de un certificado.

Estándares Técnicos Internacionales: requisitos de orden técnico y de uso internacional que deben observarse en la emisión de firmas electrónicas y en las prácticas de certificación.

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.

Grupo Electrógeno: 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.

Abog. Rodys Rolón A.
DIRECTOR
Firma Digital y Comercio Electrónico

Habilitación: autorización que otorga el MIC al PSC para emitir certificados digitales a usuarios finales, una vez cumplidos los requisitos y condiciones establecidos en la norma.

Huella digital (Código de verificación o resumen): secuencia de bits de longitud fija obtenida como resultado de procesar un mensaje de datos con un algoritmo, de tal manera que: (1) el mensaje de datos produzca siempre el mismo código de verificación cada vez que se le aplique dicho algoritmo (2) sea improbable, a través de medios técnicos, que el mensaje de datos pueda ser derivado o reconstruido a partir del código de verificación producido por el algoritmo (3) sea improbable, por medios técnicos, que se pueda encontrar dos mensajes de datos que produzcan el mismo código de verificación al usar el mismo algoritmo.

Identificación: procedimiento de reconocimiento de la identidad de un solicitante o titular de certificado dentro de la jerarquía PKI Paraguay.

Identificador de Objeto (OID): los identificadores de objeto son un sistema de identificación para entidades físicas o virtuales basado en una estructura arbórea de componentes de identificación. El árbol de OID se define plenamente en las Recomendaciones UIT-T y las normas internacionales ISO.

Infraestructura de Clave Pública (PKI): 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

Integridad: característica que indica que un mensaje de datos o un documentos electrónico no ha sido alterado desde la transmisión por el iniciador hasta su recepción por el destinatario.

Abog. Gladys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Jerarquía PKI: jerarquía de confianza que se conforma por un conjunto de autoridades de certificación que mantienen relaciones de confianza por las cuales una CA de nivel superior (CA Raíz) garantiza la confiabilidad de una o varias de nivel inferior (PSC) y a su vez, de los certificados emitidos por éstos a los suscriptores.

Lista de certificados revocados (CRL): lista emitida por una CA, publicada periódicamente y que contiene los certificados que han sido revocados antes de sus respectivas fechas de vencimiento.

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

Módulo de Seguridad de Hardware (HSM, Hardware Security Module): dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas.

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.

Par de claves: son las claves privada y pública de un criptosistema asimétrico. La clave privada y la clave pública están relacionadas matemáticamente y poseen ciertas propiedades, entre ellas que es imposible deducir la clave privada de la clave pública conocida.

PKCS#1: estándar de criptografía de clave pública #1, desarrollado por RSA Security Inc., que proporciona las definiciones básicas y recomendaciones para la implementación de algoritmo RSA para criptografía de clave pública.

PKCS#10 (Certification Request Syntax Standard): Estándar desarrollado por RSA que define la sintaxis de una petición de certificado.

Abog. Rodys Rolón A. DIRECTOR GENERAL Firma Digital y Comercio Electrónico

Parte que confía: es toda persona física o jurídica diferente del titular, que decide aceptar y confiar en un certificado emitido bajo la jerarquía de la PKI Paraguay.

Perfil del certificado: especificación del formato requerido para un tipo particular de certificado (incluyendo requisitos para el uso de los campos estándar y extensiones).

Período de operación: periodo de vigencia de un certificado, que comienza en la fecha y la hora en que es emitido por una CA, y termina en la fecha y la hora en que expira o se revoca el mismo.

Período de uso: rrefiere al tiempo establecido para los certificados emitidos dentro la jerarquía de la PKI para determinados usos.

Política: orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado.

Política de Certificación: (CP) 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.

Práctica: modo o método que particularmente observa alguien en sus operaciones.

Prestador de Servicios de Certificación (PSC): 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 del Paraguay y solo podrá emitir certificados a usuarios finales.

Abog. Rocío Rolón A. DIRECTORA GENERAL Firma Digital y Comercio Electrónico

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.

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

Rol de confianza: función crítica que desempeña personal de la CA, que si se realiza insatisfactoriamente puede tener un impacto adverso sobre el grado de confianza proporcionado por la CA.

Ruta del certificado: secuencia ordenada de certificados de entidades que, junto a la clave pública de la entidad inicial en la ruta, puede ser procesada para obtener la clave pública de la entidad final en la ruta.

Servicio OCSP: permite utilizar un protocolo estándar para realizar consultas en línea al servidor de la CA sobre el estado de un certificado.

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

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

Suscriptor: persona física o jurídica titular de un certificado digital emitido por una CA.

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

Validez de la firma: aplicabilidad (apto para el uso previsto) y estado (activo, revocado o expirado) de un certificado.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Verificación de la firma: determinación y validación de: a) 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; b) que el mensaje no ha sido alterado desde que su firma digital fue creada.

X. 500: estándar desarrollado por la ITU que define las recomendaciones del directorio. Da lugar a la serie de recomendaciones siguientes: X.501, X.509, X.511. X.518, X.519, X.520, X.521, X.525.

X. 509: estándar desarrollado por la ITU, que define el formato electrónico básico para certificados electrónicos.

1.6.2 ACRÓNIMOS

Tabla N° 1 - Acrónimos

Acrónimo	Descripción
C	País (C por sus siglas en inglés, Country)
CA	Autoridad de Certificación (CA por sus siglas en inglés Certificate Authority)
CAI	Autoridad de Certificación Intermedia (Certificate Authority Intermediate)
CA Raíz	Autoridad Certificadora Raíz del Paraguay
CI	Cédula de identidad
CN	Nombre común (CN por sus siglas en inglés, Common Name)

Abog. Rodys Rolón A. DIRECTORA GENERAL Firma Digital y Comercio Electrónico

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)
CSR	Solicitud de firma de Certificado (CSR por sus siglas en inglés, certificate Signing Request)
DGFDyCE	Dirección General de Firma Digital y Comercio Electrónico dependiente del Vice Ministerio de Comercio.
DNS	Servicio de nombre de dominio (DNS por sus siglas en inglés Domain Name server)
FIPS	Estándares Federales de Procesamiento de la Información (FIPS por sus siglas en inglés, Federal Information Processing Standards).
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).
ITU-T	Unión Internacional de Telecomunicaciones - Sector de normalización de las telecomunicaciones (ITU-T por sus siglas en inglés Internationa,l Telecomunication Union - Telecomunication Standardization Sector)
MIC	Ministerio de Industria y Comercio
O	Organización (por su sigla en inglés, Organization)
OCSP	Servicio de validación de certificados en línea (OCSP por sus siglas

Abog. Carlos Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

	en inglés, Online Certificate Status Protocol).
OID	Identificador de Objeto (OID por sus siglas en inglés, Object Identifier).
OU	Unidad Organizacional (OU por sus siglas en inglés, Organization Unit)
PIN	Número de Identificación Personal, (por sus siglas en inglés, Personal Identification Number)
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).
PSC	Prestador de Servicios de Certificación
PY	Paraguay
RA	Autoridad de Registro (RA por sus siglas en inglés, Registration Authority).
RFC	Petición de Comentarios (RFC por sus siglas en inglés, Request for Comments)
RSA	Sistema criptográfico de clave pública desarrollado por Rivers, Shamir y Adleman
RUC	Registro único del contribuyente
SN	Número de Serie (por sus siglas en inglés, Serial Number)
TLS	Capa de conexión segura (TLS por sus siglas en inglés, Transport Layer Security)
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).
VA	Autoridad de validación (VA por sus siglas en inglés, Validation Vutorithy)

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

2 RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO

2.1. REPOSITORIOS

En este ítem deben ser descriptos, los requisitos aplicables a los repositorios utilizados por el PSC responsable de la CPS, tales como:

a) Localización física y lógica
b) Disponibilidad
c) Protocolos de acceso y
d) Requisitos de seguridad

2.2 PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

En este ítem se debe definir la información que será publicado por el PSC responsable de la CPS. El servicio de publicación de información de un PSC debe estar disponible durante las veinticuatro horas, los siete días de la semana. En caso de interrupción por causa de fuerza mayor, el servicio se deberá restablecer en un plazo no mayor a veinticuatro horas, garantizando la disponibilidad del servicio con un mínimo de 99% anual, un tiempo programado de inactividad máximo de 0.5% anual

Las siguientes informaciones, como mínimo, deberán ser publicadas por el PSC en su servicio de repositorio:

- CP y CPS que implementan;
- El Certificado de la CA Raíz;
- Su propio Certificado;
- La Lista de Certificados Revocados ;
- Consulta de Certificados Emitidos;
- Proforma de contrato de Suscriptor;
- Las Resoluciones que Habilitan, Suspenden o Revocan al PSC:
- La información relevante del resultado de la última auditoría que hubiere sido objeto;
- Leyes, decretos, reglamentos y resoluciones que rigen la actividad de la PKI

Abog. Rocys Rolón A.
DIRECTORA GENERAL
Firma Digital y Comercio Electrónico

Paraguay;

- Identificación, domicilio y medios de contacto; y
- Una lista, actualizada periódicamente, que contiene las RA propias y delegadas con sus respectivas direcciones de las instalaciones técnicas de operación;
- Una lista, actualizada periódicamente de los PSS vinculados a un PSC.

2.3 TIEMPO O FRECUENCIA DE PUBLICACIÓN

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

2.4 CONTROLES DE ACESSO

En este ítem deben ser descriptos, los controles y las eventuales restricciones para el acceso, lectura y escritura de las informaciones publicadas por el PSC, de acuerdo a lo establecido en las normas, criterios, prácticas y procedimientos de la PKI Paraguay.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

En esta sección y en la siguiente, la CPS debe describir en detalle, los requisitos y procedimientos utilizados por las RA vinculadas al PSC responsable de llevar a cabo los siguientes procesos:

a) **Validación de solicitud de certificado:** realizada mediante presencia física del interesado presentando los documentos de identificación indicados en los ítems 3.2.2 ,3.2.3 y 3.2.4 comprendiendo las siguientes etapas:

   I. ***Confirmación de Identidad de la persona física:*** comprobar que la persona que se presenta como titular interesado en un certificado de persona física sea realmente aquella cuyos datos constan en la documentación presentada. Está prohibido cualquier especie de representación para este fin. En caso de persona jurídica, comprobar que la persona física que se presenta como su representante es realmente aquella cuyos datos constan en la documentación presentada. El responsable de uso del certificado digital para

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

persona jurídica debe comparecer presencialmente. Está prohibido cualquier especie de representación para este fin;

II. ***Confirmación de la identidad de una persona jurídica:*** comprobar que los documentos presentados refieren efectivamente a la persona jurídica, titular del certificado y de que la persona que se presenta como representante legal de la persona jurídica realmente posea tal atribución; y

III. ***Autorización de emisión del certificado:*** confirmar los datos de solicitud de certificado con el conjunto de los documentos presentados y autorizar la expedición del certificado en el sistema del PSC;

b) **Verificación de la solicitud de certificado:** confirmar la validación realizada, señalando que debe ser ejecutado, obligatoriamente:

I. por el agente de registro distinto al que ejecutó la tarea en la etapa de validación;

II. en una de las instalaciones técnicas de la RA debidamente autorizada a funcionar por el PSC al cual está vinculada;

III. únicamente después de la recepción, en la instalación técnica de la RA, de las copias de las documentaciones presentadas en la etapa de validación; y

IV. antes del inicio de la validez del certificado, debiendo ser revocado inmediatamente en el caso que la verificación no se haya realizado antes del inicio de su validez.

El proceso de validación de la identidad podrá ser realizado por el agente de registro fuera del ambiente físico de la RA, siempre que haya utilizado un ambiente computacional auditable y debidamente registrado en el inventario de hardware y software de la RA.

Todas las etapas de los procesos de validación y verificación de la solicitud de certificados deben ser registradas y firmadas por los ejecutantes, Estos registros se realizan a los efectos de permitir la reconstrucción completa de procesos ejecutados, con fines de auditoría.

Debe ser mantenido un archivo con las copias de todos los documentos utilizados para la confirmación de la identidad de una organización y/o individuo. Las copias podrán ser mantenidas en papel o en forma digitalizada, sujeto a las condiciones expuestas en este documento.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

3.1. NOMBRES

3.1.1. TIPOS DE NOMBRES

En esta sección, deben ser definidos los tipos de nombres admitidos para los titulares de los certificados emitidos por el PSC responsable de la CPS. Entre los tipos de nombres considerados podrán estar el "**distinguished name**" según lo establecido en la ITU X.500, la dirección de correo y la dirección de página web (URL).

3.1.2. NECESIDAD DE NOMBRES SIGNIFICATIVOS

En este apartado, la CPS debe definir la necesidad de usar nombres significativos, es decir, nombres que hacen que sea posible determinar la identidad de la persona física o jurídica, a los efectos de identificar a los titulares de los certificados emitidos por el PSC.

3.1.3. ANONIMATO O SEUDÓNIMOS DE LOS SUSCRIPTORES

No se admite el anonimato en los certificados emitidos por un PSC. Asimismo, el seudónimo no se considera un nombre significativo del solicitante y no se utilizará como parte del certificado.

3.1.4 REGLAS PARA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRES

En esta sección deben ser descriptas, cuando sea aplicable, las reglas para la interpretación de varias formas de nombres admitidas por la CPS.

Certificado de Persona Jurídica

La Cédula Tributaria – RUC es expedida por la Subsecretaría de Estado de Tributación y debe cumplir el siguiente formato

Ariadna Portillo Rolón A.
DIRECTORA GENERAL
Firma Digital y Comercio Electrónico

Tabla N° 2 - Certificado de Persona Jurídica

Cédula Tributaria – RUC	RUC	RUC99999999-9

Certificado de Persona Física

La Cédula de identidad es expedida por el Departamento de Identificaciones de la Policía Nacional, y deben cumplir el siguiente formato:

Tabla N° 3 - Certificado de Persona Física

Cédula de identidad	CI	CI999999

Certificado de máquina o aplicación

Tabla N° 4 - Certificado de máquina o aplicación

Cédula de identidad	MCI	CI999999
Cédula Tributaria – RUC	MRUC	RUC99999999-9

3.1.5. UNICIDAD DE NOMBRES

En este ítem, la CPS debe establecer, que identificadores del tipo "Distinguished Name" (DN), deberán ser únicos para cada titular del certificado, en el ámbito del PSC emitente. Números y letras adicionales podrán ser incluidos al nombre de cada entidad para asegurar la unicidad del campo.

3.1.6 RECONOCIMIENTO, AUTENTICACIÓN Y ROL DE LAS MARCAS REGISTRADAS

En este apartado, la CPS debe establecer que los procesos de tratamiento, reconocimiento, autenticación y rol de marcas registradas, serán ejecutados de acuerdo con la legislación vigente sobre la materia.

Además, la CPS debe reservar al PSC, el derecho de tomar todas las decisiones en el caso de que haya conflicto derivado de los nombres iguales entre varios solicitantes de certificados. También debe contemplar que, durante el proceso de verificación de identidad, corresponderá al solicitante del certificado demostrar su derecho a usar un nombre específico.

Abog. Rocío Rolón A.
DIRECTORA GENERAL
Firma Digital y Comercio Electrónico

3.2 VALIDACIÓN INICIAL DE IDENTIDAD

3.2.1 MÉTODO PARA PROBAR POSESIÓN DE LA CLAVE PRIVADA

La CPS debe indicar los procedimientos ejecutados por el PSC responsable y sus RA, a ella vinculadas para confirmar que la persona física o jurídica solicitante, posea la clave privada correspondiente a la clave pública para el cual está siendo solicitado el certificado digital, pudiendo utilizar las referencias contenidas en el RFC 2510, relativos a POP (Proof of Possession). En el caso que sean requeridos procedimientos específicos para las CP implementadas, los mismos deben ser descriptos en esa CP, en el ítem correspondiente.

3.2.2 AUTENTICACIÓN DE IDENTIDAD DE PERSONA JURÍDICA

En este ítem deben ser definidos los procedimientos empleados por las RA para la confirmación de la identidad de una persona jurídica.

El titular del certificado de persona jurídica, será la persona física, designada por la organización como responsable del certificado, que será el titular de la clave privada.

La confirmación de la identidad de la persona jurídica y de la persona física deberá realizarse en los siguientes términos:

a) La confirmación de la identidad de una persona jurídica se hará mediante la presentación, de por lo menos los siguientes documentos:
   I. Si la entidad es pública:
      - copia simple de la Ley o Carta Orgánica que crea o autoriza su creación;
      - documento que acredite la representación legal de la máxima autoridad; y
      - número de registro único del contribuyente (RUC), en caso de que la entidad pública sea sujeto tributario.
   II. si la entidad es privada:
      - copia autenticada del documento de constitución de la Sociedad;
      - copia autenticada de acta de la última asamblea ordinaria y extraordinaria;
      - copia autenticada del Acta de la última sesión;
      - prueba de la inscripción en el registro nacional de personas jurídicas;
      - certificado de cumplimiento tributario;
      - número de registro único del contribuyente (RUC); y

Abog. Aldys Rolón A.
Dirección General de Firma Digital y Comercio Electrónico

La confirmación de la identidad de él/los representante/s legal/es de la persona jurídica y del responsable del uso del certificado, se hará mediante la presentación de los documentos exigidos en el Ítem 3.2.3,con la presencia física de estos y la firma del documento de **solicitud de certificado** que trata el ítem 4.1.

La información obligatoria contenida en los campos del certificado expedido a una persona jurídica, debe coincidir exactamente con la información contenida en los siguientes documentos:

a) Nombre de la razón social según documento constitutivo, sin abreviaturas, en el campo *Subject*, como parte del *Common Name*, que compone parte del *Distinguished Name*;
b) Número de registro único del contribuyente (RUC) según la cédula tributaria en el campo *Subject*, como parte del *SerialNumber*, que compone parte del Distinguished Name;
c) Nombre completo de la persona física responsable del certificado según documento de identidad, sin abreviaturas, en el campo *Subject Alternative Name* OID=2.5.4.3
d) Número de cédula de Identidad Policial de la persona física responsable del certificado según documento de identidad, en el campo *Subject Alternative Name* OID=2.5.4.5.

La RA vinculada al PSC debe comprobar la información suministrada por el solicitante contra los datos oficiales correspondientes. Si hay diferencias en relación con los datos del documento de identidad de la persona física, la expedición del certificado digital debe ser suspendida y el solicitante debe regularizar su situación ante el organismo competente.

Cada CP puede definir como obligatoria llenar otros campos.

Además el titular del certificado, a su criterio y mediante una declaración explícita en el documento de **solicitud de certificado,** puede solicitar llenar los campos con las siguientes informaciones:

a) el correo del titular del certificado; y
b) El cargo que ocupa en la organización el responsable del certificado.

Para ello, el titular deberá presentar la documentación que respalde la información, caso por caso, en su versión original y una copia autenticada por notario público para dejar agregado al legajo. Debe tenerse un archivo con copias de todos los documentos utilizados.

Abog. Reinis Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

3.2.3 AUTENTICACIÓN DE IDENTIDAD DE PERSONA FÍSICA

En esta sección se deben definir los procedimientos empleados por la RA para confirmar la identidad de la persona física. Esta confirmación debe ser realizada mediante la presencia física de la persona, sobre la base de los documentos de identificación legalmente aceptados y cotejados con registros oficiales. Podrá implementarse un proceso de identificación biométrica.

Para la confirmación de la identidad de la persona física se deben presentar la siguiente documentación en su versión original:

a) Cédula de Identidad Policial Paraguaya;
b) Otro documento oficial, por ejemplo la licencia de conducir del solicitante.

La información obligatoria contenida en los campos del certificado expedido a una persona física, debe coincidir exactamente con la información contenida en los siguientes documentos:

a) Nombre completo de la persona física titular del certificado, según el documento de identidad, en el campo *Subject* , como parte del *Common Name*, que compone parte del *Distinguished Name*; y
b) Número de cédula de Identidad Policial de la persona física, según documento de identidad, en el campo *Subject*, como parte del *SerialNumber*, que compone parte del *Distinguished Name*.

La RA debe comprobar la información suministrada por el solicitante contra los datos oficiales correspondientes. Si hay diferencias en relación con los datos del documento de identidad, la expedición del certificado digital debe ser suspendida y el solicitante debe regularizar su situación ante el organismo competente.

Cada CP puede definir como obligatoria llenar otros campos.

Además el titular del certificado, a su criterio y mediante una declaración explícita en el documento de ***solicitud de certificado***, puede solicitar llenar los campos con las siguientes informaciones:

c) El correo del titular del certificado;
d) El nombre de la organización en el que presta servicio el titular del certificado;

Abog. Roque Rubín A.
DIRECTOR
Dirección General Firma Digital y Comercio Electrónico

e) El nombre de la unidad de la organización en el que presta servicio el titular del certificado;
f) El número de cédula tributaria correspondiente al titular del certificado; y
g) El cargo o título del titular del certificado.

Para ello, el titular deberá presentar la documentación que respalde la información, caso por caso, en su versión original y una copia autenticada por notario público para dejar agregado al legajo. Debe tenerse un archivo con copias de todos los documentos utilizados.

3.2.4 AUTENTICACIÓN DE IDENTIDAD DE UN MAQUINA O APLICACIÓN

En el caso de los certificados expedidos para una maquina o aplicación, el titular es la persona física o jurídica que solicita el certificado. En el caso de que el solicitante sea una persona jurídica, se deberá indicar al responsable del certificado, que será el titular de la clave privada.

Si el titular del certificado es una persona física, se deberá confirmar su identidad según lo estipulado en el Ítem 3.2.3 y la firma del documento de ***solicitud de certificado*** qué trata el Ítem 4.1.

Si el titular del certificado es una persona jurídica, se deberá confirmar su identidad según lo estipulado en el Ítem 3.2.2 y la firma del documento de ***solicitud de certificado*** qué trata el Ítem 4.1.

Procedimientos para la identificación de una maquina o aplicación:

a) Para emisión de certificados de máquinas que se utilizan como servidores, la solicitud deben contener el nombre del servidor y el número de serie del equipamiento.
b) Para certificados de maquina o aplicación que utilizan URL en el campo *Common Name*, se debe comprobar si el solicitante del certificado tiene el registro del nombre de dominio por el órgano competente, o tenga el permiso del propietario del dominio para utilizar ese nombre. En este caso, se debe presentar la documentación correspondiente (autorización o similar) firmado por el titular del dominio.

La información obligatoria contenida en los campos del certificado expedido a un dispositivo o aplicación, debe coincidir exactamente con la información contenida en los siguientes documentos:

a) URL o nombre de la aplicación, en el campo *Subject*, como parte del *Common Name*, que compone el *Distinguished Name*;

Abog. Pedro Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

b) En el caso que el titular sea una persona jurídica:
b1 número de registro único del contribuyente (RUC) de la persona jurídica según la cédula tributaria en el campo *Subject,* como parte del *SerialNumber*, que compone parte del Distinguished Name;

b.2 nombre de la razón social de la persona jurídica según documento constitutivo, en el campo *Subject Alternative Name OID=2.5.4.10;*
b.3 Nombre completo de la persona física responsable del certificado según documento de identidad, sin abreviaturas, en el campo *Subject Alternative Name OID=2.5.4.3*
b.4 número de cédula de identidad policial de la persona física responsable del certificado según documento de identidad, en el campo *Subject Alternative OID=2.5.4.5.*

c) En el caso que el titular sea una persona física
c.1 número de cédula de identidad policial de la persona física, según documento de identidad, en el campo *Subject*, como parte del *SerialNumber*, que compone parte del *Distinguished Name*;

c.2 nombre completo de la persona física responsable del certificado según documento de identidad, sin abreviaturas, en el campo *Subject Alternative Name* OID=2.5.4.3.

Además el titular del certificado, a su criterio y mediante una declaración explícita en el documento de ***solicitud de certificado,*** puede solicitar llenar los campos con las siguientes informaciones:

a) el correo del responsable del certificado;
b) El cargo o título del responsable del certificado en caso de ser persona jurídica.

Para ello, el titular deberá presentar la documentación que respalde la información, caso por caso, en su versión original y una copia autenticada por notario público para dejar agregado al legajo. Debe tenerse un archivo con copias de todos los documentos utilizados.

3.2.5 INFORMACIÓN DEL SUSCRIPTOR NO VERIFICADA

No aplica.

Abog. Nadys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

3.2.6. VALIDACIÓN DE LA AUTORIDAD (CAPACIDAD DE HECHO)

La RA, debe corroborar que el solicitante sea capaz de solicitar un tipo de certificado específico. Además, debe validar que el solicitante no posea impedimentos legales.

En el caso de Certificados de Personas Físicas, debe validar:

- Nombre y documento de identidad; y
- Mayoría de edad.

En el caso que el solicitante sea Persona Jurídica debe verificar:

- Nombre o razón social y número de RUC; y
- Nombre del representante legal y documento de identidad.

La RA vinculada al PSC debe, debe verificar la información suministrada por el solicitante contra los datos oficiales correspondientes.

3.2.7. CRITERIOS PARA INTEROPERABILIDAD

Podrán ser reconocidos los certificados digitales extranjeros de conformidad a la normativa vigente. Para el efecto, el estado paraguayo deberá suscribir Acuerdos Internacionales con sus pares extranjeros, salvo que por protocolo adicional a un tratado vigente, los países suscriptores del mismo hayan acordado el reconocimiento reciproco de los certificados digitales emitidos en los respectivos países.

3.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE RE EMISIÓN DE CLAVES

3.3.1 IDENTIFICACIÓN Y AUTENTICACIÓN PARA RE EMISIÓN DE CLAVES

No se permite la re emisión de claves.

3.3.2 IDENTIFICACIÓN Y AUTENTICACIÓN PARA LA RE EMISIÓN DE CLAVES DESPUÉS DE UNA REVOCACIÓN

No se permite bajo estas circunstancias, la re emisión de claves. Luego del procedimiento de revocación, se debe solicitar la emisión de un nuevo certificado.

3.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN

En este apartado, la CPS debe describir los procedimientos utilizados para confirmar la identidad del solicitante de una revocación de certificado. La CPS debe exigir que las solicitudes de revocación de certificados sean siempre registradas. Si se requieren procedimientos específicos para las CP implementadas, los mismos deben ser descritos en esas CP, en el ítem correspondiente.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

4.1 SOLICITUD DEL CERTIFICADO

En este ítem de la CPS, deben ser descriptos todos los requisitos y procedimientos operacionales establecidos por el PSC y las RA, a ella vinculadas, para la solicitud de emisión de certificado. Esos requisitos y procedimientos deberán comprender, como mínimo:

a) La comprobación de los atributos de identificación que constan en el certificado conforme al ítem 3.
b) Una Solicitud de Certificado firmada por el titular del certificado o por el responsable del uso del certificado, en caso de la persona jurídica, conforme al **TÉRMINO DEL FORMULARIO DE SOLICITUD DE CERTIFICADO** correspondiente.

4.1.1 QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO

En este ítem se detallan las personas que pueden presentar una solicitud de certificado, que en el marco de la PKI Paraguay, son:

- Para el caso de certificado de persona física, toda persona, mayor de edad, sin distinción, con un documento de identidad válido, que será el sujeto a cuyo nombre se emita el certificado.
- Para el caso de certificado de persona jurídica, el representante legal o el responsable del uso del certificado con poder suficiente.
- Para el caso de certificado de equipo o aplicación, el representante legal o el responsable del uso del certificado con poder suficiente si el solicitante es una persona jurídica, o toda persona, mayor de edad, sin distinción, con un documento de identidad válido si el solicitante es una persona física.

4.1.2 PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES

En este ítem de la CPS deben ser descriptos los procesos de inscripción y las responsabilidades de los intervinientes en la emisión de un certificado. En general, es atribución de cada RA determinar la adecuación del tipo de certificado a las características de las funciones del solicitante, de acuerdo con lo previsto en la CP

aplicable en cada caso. La Autoridad de Registro podrá autorizar o denegar la solicitud de certificación. La denegatoria como excepción y en circunstancias debidamente fundadas

Las solicitudes de los certificados, una vez completadas, serán enviadas al PSC responsable.

Como regla general, todo solicitante que desee un certificado deberá:

- Completar el formulario de solicitud del certificado con toda la información que la RA requiera para la emisión del mismo. Cabe destacar que no toda la información solicitada aparecerá en el certificado, asegurándose su conservación integra, de manera confidencial, por la Autoridad de Certificación.
- Entregar la solicitud de firma del certificado (CSR) a la RA, que incluye la clave pública, en el caso de que el par de claves lo haya generado el solicitante, y el certificado se genere directamente a partir de la solicitud. En la correspondiente CP se establecerá el procedimiento de entrega.

La existencia del formulario de solicitud y en general el procedimiento de solicitud de certificados deberá estar definido en la CP correspondiente a cada tipo de certificado.

4.2. PROCESAMIENTO DE LA SOLICITUD DEL CERTIFICADO

4.2.1 EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

La RA vinculada al PSC debe velar por la identificación y autenticación de acuerdo con las disposiciones establecidas en el punto 3.2.

4.2.2 APROBACIÓN O RECHAZO DE SOLICITUDES DE CERTIFICADO

La RA vinculada al PSC responsable, debe rechazar la solicitud de certificado en los casos que no se dé cumplimiento a la normativa vigente y a lo establecido en esta CPS.

4.2.3. TIEMPO PARA PROCESAR SOLICITUDES DE CERTIFICADO

El tiempo de procesamiento de la solicitud del certificado debe ser en el menor tiempo posible. Este plazo podrá ser determinado en cada CP.

Abog. Blanca Bolón A.
DIRECTORA GENERAL
Firma Digital y Comercio Electrónico

4.3 EMISIÓN DEL CERTIFICADO

Las CPS deben indicar que un certificado será considerado valido a partir del momento de su emisión.

4.3.1 ACCIONES DEL PSC DURANTE LA EMISIÓN DE LOS CERTIFICADOS

En esta sección de la CPS, deben ser descriptos, los requisitos operacionales establecidos por el PSC para la emisión de los certificados. En caso que sean requeridos procedimientos específicos para cada CP implementadas, los mismos deben ser descriptos, en el ítem correspondiente.

4.3.2 NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA EMISIÓN DEL CERTIFICADO DIGITAL

En este ítem de la CPS, deben ser descriptos los requisitos operacionales establecidos por el PSC para la notificación al solicitante. En caso que sean requeridos procedimientos específicos para cada CP implementadas, los mismos deben ser descriptos, en el ítem correspondiente.

4.4. ACEPTACIÓN DEL CERTIFICADO

4.4.1 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE CERTIFICADO

En este ítem deben ser descriptos todos los requisitos y procedimientos operacionales referentes a la aceptación de un certificado por su titular. Deben ser apuntadas las implicancias de la aceptación, o de la no aceptación del certificado. En caso que sea requeridos procedimientos específicos para las CP implementadas, los mismos deben ser descriptos en esas CP, en el ítem correspondiente.

Abog. [illegible] Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

La CPS debe garantizar que la aceptación de todo certificado emitido sea declarada expresamente por el respectivo titular en el **acuerdo de suscriptores**. En caso de los certificados emitidos para personas jurídicas, equipo o aplicaciones, la declaración expresa deberá ser de la persona física responsable de ese certificado.

4.4.2 PUBLICACIÓN DEL CERTIFICADO POR EL PSC

En este ítem debe ser descripto el procedimiento que el PSC utiliza para mantener disponible la información de los certificados emitidos, en los repositorios de acceso público.

4.4.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR EL PSC A OTRAS ENTIDADES

No se definen entidades externas que necesiten o requieran ser notificados respecto a los certificados emitidos por el PSC.

4.5 USO DEL PAR DE CLAVES Y DEL CERTIFICADO

4.5.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL SUSCRIPTOR

En este ítem, la CPS debe describir las responsabilidades y limitaciones de uso del par de claves y del certificado. En caso que sean requeridos procedimientos específicos para las CP implementada, los mismos deben ser descriptos en esas CP, en el ítem correspondiente.

En cualquier caso, el titular sólo podrá utilizar la clave privada y el certificado para los usos autorizados en la CP y de acuerdo con lo establecido en los campos 'Key Usage' y 'Extended Key Usage' del certificado. Del mismo modo, el titular solo podrá utilizar el par de claves y el certificado tras aceptar las condiciones de uso, establecidas en la CPS y CP, y sólo para lo que éstas establezcan.

Tras la expiración o revocación del certificado, el titular deberá dejar de usar la clave privada.

4.5.2 USO DE LA CLAVE PÚBLICA Y DEL CERTIFICADO POR LA PARTE QUE CONFÍA

En este apartado, la CPS debe describir las condiciones en las que los terceros que confían, podrán depositar su confianza en los certificados emitidos por el PSC. Este requerimiento debe estar en concordancia con lo establecido en el campo 'Key Usage', 'Extended Key Usage' del certificado, y la normativa vigente.

Abog. Carlos Rolón A.
Dirección General
Firma Digital y Comercio Electrónico

4.6 RENOVACIÓN DEL CERTIFICADO

Este ítem no aplica, pues cuando un certificado requiera ser renovado debe solicitarse uno nuevo, de acuerdo con ítem 4.1.

4.6.1 CIRCUNSTANCIAS PARA RENOVACIÓN DE CERTIFICADO

Este Ítem no aplica.

4.6.2 QUIÉN PUEDE SOLICITAR RENOVACIÓN

Este Ítem no aplica.

4.6.3 PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN DE CERTIFICADO

Este Ítem no aplica.

4.6.4 NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA EMISIÓN DE UN NUEVO CERTIFICADO

Este Ítem no aplica.

4.6.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RENOVADO

Este Ítem no aplica.

4.6.6 PUBLICACIÓN POR EL PSC DEL CERTIFICADO RENOVADO

Este Ítem no aplica.

4.6.7 NOTIFICACIÓN POR EL PSC DE LA EMISIÓN DE UN CERTIFICADO A OTRAS ENTIDADES

Este Ítem no aplica.

4.7 RE-EMISIÓN DE CLAVES DE CERTIFICADO

Esta sección no aplica, pues cuando un certificado requiera ser re-emitido debe solicitarse uno nuevo, de acuerdo con ítem 4.1.

4.7.1 CIRCUNSTANCIAS PARA RE-EMISIÓN DE CLAVES DE CERTIFICADO

Este Ítem no aplica.

4.7.2 QUIÉN PUEDE SOLICITAR LA CERTIFICACIÓN DE UNA CLAVE PÚBLICA

Este Ítem no aplica.

4.7.3 PROCESAMIENTO DE SOLICITUDES DE RE-EMISIÓN DE CLAVES DE CERTIFICADO

Este Ítem no aplica.

Abog. Lucas Rolón A.
Director General
Firma Digital y Comercio Electrónico

4.7.4 NOTIFICACIÓN AL SUSCRIPTOR SOBRE LA RE-EMISIÓN DE UN NUEVO CERTIFICADO

Este Ítem no aplica.

4.7.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RE-EMITIDO

Este Ítem no aplica.

4.7.6 PUBLICACIÓN POR EL PSC DE LOS CERTIFICADOS RE-EMITIDOS

Este Ítem no aplica.

4.7.7 NOTIFICACIÓN POR EL PSC DE LA RE-EMISIÓN DE UN CERTIFICADO A OTRAS ENTIDADES

Este Ítem no aplica.

4.8 MODIFICACIÓN DE CERTIFICADOS

Este Ítem no aplica, pues cuando un certificado requiera ser modificado debe solicitarse uno nuevo, de acuerdo con ítem 4.1. Los PSC podrán disponer precios diferenciados para estos casos.

4.8.1 CIRCUNSTANCIAS PARA MODIFICACIÓN DEL CERTIFICADO

Este Ítem no aplica.

4.8.2 QUIÉN PUEDE SOLICITAR MODIFICACIÓN DEL CERTIFICADO

Este Ítem no aplica.

4.8.3 PROCESAMIENTO DE SOLICITUDES DE MODIFICACIÓN DEL CERTIFICADO

Este Ítem no aplica.

4.8.4 NOTIFICACIÓN AL SUSCRIPTOR DE LA EMISIÓN DE UN NUEVO CERTIFICADO

Este Ítem no aplica.

4.8.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO

Este Ítem no aplica.

4.8.6 PUBLICACIÓN POR EL PSC DE LOS CERTIFICADOS MODIFICADOS

Este Ítem no aplica.

4.8.7 NOTIFICACIÓN POR LA CA DE EMISIÓN DE CERTIFICADO A OTRAS ENTIDADES

Este Ítem no aplica.

4.9 REVOCACIÓN Y SUSPENSIÓN

4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN

En este ítem de la CPS, deben ser consignadas, las circunstancias en la cual un certificado podrá ser revocado. Este ítem también debe establecer que un certificado deberá obligatoriamente ser revocado en las siguientes circunstancias:

a) Que afecten la información contenida en el certificado:
   - Modificación de alguno de los datos contenidos en el certificado;
   - Descubrimiento que algunos de los datos aportados en la solicitud de certificado es incorrecto, así como la alteración o modificación de las circunstancias verificadas para la expedición del certificado;
   - Descubrimiento que algunos de los datos contenidos en el certificado es incorrecto.

b) Que afectan la seguridad de la clave o del certificado

   - Compromiso de la clave privada o de la infraestructura o sistemas de la CA que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de este incidente;
   - Infracción, por el PSC, de los requisitos previstos en los procedimientos de gestión de los certificados, establecidos en su propia CP y CPS ;
   - Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado del titular del certificado;
   - Acceso o utilización no autorizada, por un tercero, de la clave privada del titular;
   - El uso irregular por el titular, o falta de diligencia en la custodia de la clave privada;

c) Circunstancias que afectan la seguridad del dispositivo criptográfico

- Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico;
- Pérdida o inutilización por daños del dispositivo criptográfico;
- Acceso no autorizado, por un tercero, a los datos de activación de la clave privada del titular del certificado;

d) Circunstancias que afectan al suscriptor

- Infracción del titular del certificado en sus obligaciones, responsabilidad y garantías, establecidas en la CP y CPS del PSC que emitió el certificado;
- La incapacidad de hecho sobrevenida o la muerte del titular del certificado;
- La extinción de la persona jurídica titular del certificado;
- Solicitud de revocación del certificado por su titular de acuerdo con lo establecido en la CP y en la CPS.

e) Otras causales especificadas en la normativa y reglamentación vigente.

4.9.2 QUIÉN PUEDE SOLICITAR REVOCACIÓN

En este ítem de la CPS, debe establecer que la revocación de un certificado sólo podrá realizarse:

- por petición del titular del certificado;
- por solicitud del responsable del certificado en el caso de un certificado de persona jurídica o un certificado de maquina o aplicación;
- por solicitud de la empresa u organización, cuando en el certificado se detalla el cargo o función que ocupa en la organización y es proporcionado por la misma al titular, por ser éste, su empleado, funcionario o servidor;
- por el PSC emitente;
- por una RA vinculada al PSC emitente;
- por determinación de la CA Raíz del Paraguay;
- por una autoridad judicial competente.

4.9.3 PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACIÓN

En este apartado, la CPS debe describir los procedimientos establecidos por el PSC para la solicitud de revocación de certificados. El PSC deberá garantizar que quienes están autorizados a solicitar la revocación, conforme al ítem 4.9.2, puedan,

fácilmente y en cualquier tiempo, solicitarla revocación de sus respectivos certificados. En el caso que sean requeridos procedimientos específicos para las CP implementadas, los mismos deben ser descriptos en esas CP, en el ítem correspondiente.

Como directrices generales, las CPS debe establecer que:

a) el Solicitante de revocación de un certificado debe ser identificado;
b) las solicitudes de revocación, así como las acciones resultantes de ellas serán registrada y almacenadas;
c) se documentarán las razones de la revocación de un certificado; y
d) la revocación de un certificado terminará con la generación y publicación de una CRL que contenga los datos del certificado revocado y, en el caso de la utilización de consulta OCSP, con la actualización del estado del certificado en la base de datos del PSC.

El plazo máximo admitido para la conclusión del proceso de revocación del certificado después de la recepción de la respectiva solicitud, para todos los certificados descriptos en esta CPS, será de 12 (doce) horas.

En caso que sean requeridos procedimientos de revocación específicos para las CP implementadas, los mismos deben ser descriptos en esas CP, en el ítem correspondiente.

4.9.4 PERÍODO DE GRACIA PARA SOLICITUD DE REVOCACIÓN

No se estipulan periodo de gracia para revocación de certificados.

4.9.5 TIEMPO DENTRO DEL CUAL EL PSC DEBE PROCESAR LA SOLICITUD DE REVOCACIÓN

En este ítem, la CPS debe referir que la solicitud de revocación, debe ser inmediata cuando están configuradas las circunstancias definidas en el ítem 4.9.1. El plazo máximo admitido para la conclusión del proceso de revocación del certificado después del recibimiento de la respectiva solicitud, para todos los certificados descriptos en esta CPS es de 12 (doce) horas.

En caso que sean requeridos plazos específicos para las CP implementadas, los mismos deben ser descriptos en esas CP, en el ítem correspondiente, que no podrán superar las 12 horas

4.9.6 REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN PARA LAS PARTES QUE CONFÍAN

En este apartado, la CPS debe referir la necesidad de que las partes que confían, evalúen el estado del certificado y el estado de todos los certificados de la CA en la cadena a la que pertenece el mismo, antes de confiar en él. Para ello, las partes que confían pueden verificar el estado del certificado mediante el servicio de: OCSP o CRL más reciente, proveída por el PSC.

4.9.7 FRECUENCIA DE EMISIÓN DEL CRL

En esta sección, se debe establecer la frecuencia de emisión de la CRL referente a los certificados de los usuarios finales, PSC y CA Raíz.

La CRL debe actualizarse y publicarse inmediatamente cuando surja una revocación o:

- con una frecuencia de emisión máxima permitida de 12 (doce) horas para la CRL referente a los usuarios finales.
- con una frecuencia de emisión máxima permitida de 45 (días) para la CRL referente al PSC.

En caso que sean utilizadas frecuencias de emisión específicos de CRL para las CP implementadas, deben ser descriptos en estas CP, en el ítem correspondiente.

4.9.8 LATENCIA MÁXIMA PARA CRL

En este ítem se debe establecer la latencia máxima para la CRL. Este plazo será como máximo de 1 (hora) posterior a su generación.

En caso que sean requeridas la latencia máxima para la CRL, específicas para las CP implementadas, deben ser descriptos en estas CP, en el ítem correspondiente.

4.9.9 REQUISITOS DE VERIFICACIÓN DEL CRL

En este ítem, la CPS debe tener presente que todo certificado deberá tener su validez verificada, en la respectiva CRL, antes de utilizarlo.

La CPS debe tener en cuenta también, que la autenticidad de la CRL deberá también ser confirmada, por medio de la verificación de la firma del PSC emitente en el periodo de validez de la CRL.

4.9.10 DISPONIBILIDAD DE VERIFICACIÓN DE REVOCACIÓN/ESTADO EN LÍNEA

En este ítem, la CPS debe informar, según sea el caso, las disponibilidades de recursos del PSC para la revocación en línea del certificado o para la verificación en línea del estado de los certificados.

La verificación del estado de un certificado deberá ser directamente con el PSC emisora, por medio del protocolo OCSP (On-line Certificate Status Protocol).

4.9.11 REQUERIMIENTOS PARA VERIFICAR LA REVOCACIÓN EN LÍNEA

En este ítem, la CPS debe definir, cuando sea apropiado, los requisitos para la verificación en línea de la información de revocación de certificados por la parte que confía. En caso de ser requeridos procedimientos específicos para las CP implementadas, los mismos deben ser descriptos en esas CP, en el ítem correspondiente.

4.9.12 OTRAS FORMAS DE ADVERTENCIAS DE REVOCACIÓN DISPONIBLES

Este Ítem no aplica.

4.9.13 REQUERIMIENTOS ESPECIALES POR COMPROMISO DE CLAVE PRIVADA

En este ítem de la CPS deben ser definidos los requisitos aplicables para la revocación del certificado provocado por el compromiso de la clave privada. La CPS debe tener en cuenta que, en esta circunstancia, el titular del certificado deberá comunicar el hecho inmediatamente al PSC emitente. En el caso que haya requisitos específicos para las CP implementadas, los mismos deben ser descriptos en esas CP, en el ítem correspondiente.

Debe contener también determinaciones que definan los medios utilizados para comunicar un compromiso o sospecha de compromiso de la clave privada.

4.9.14 CIRCUNSTANCIAS PARA SUSPENSIÓN

Este Ítem no aplica.

4.9.15 QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN

Este Ítem no aplica.

4.9.16 PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN

Este Ítem no aplica.

4.9.17 LÍMITES DEL PERÍODO DE SUSPENSIÓN

Este Ítem no aplica.

4.10 SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADO

4.10.1 CARACTERÍSTICAS OPERACIONALES

En este ítem, la CPS debe informar que el estado de los certificados estará disponible a través de la CRL y la lista de los certificados emitidos publicados en el sitio principal de Internet del PSC. Además el PSC deberá implementar obligatoriamente un servicio de consulta del estado del certificado en línea por medio del protocolo OCSP (On-line Certificate Status Protocol).

4.10.2 DISPONIBILIDAD DEL SERVICIO

En este ítem, se debe establecer el tiempo de disponibilidad del servicio de publicación en el repositorio público de la CRL y lista de certificados emitidos, y el servicio de consulta en línea por medio del protocolo OCSP. Este plazo será como mínimo de 99% anual y un tiempo programado de inactividad máximo de 0.5% anual.

4.10.3 CARACTERÍSTICAS OPCIONALES

Este Ítem no aplica.

4.11 FIN DE LA SUSCRIPCIÓN

En este ítem se deben indicar, las condiciones de la extinción de la validez del certificado, siendo estas:

- por la revocación del certificado, antes de la fecha de expiración.
- Por expiración de la fecha de validez del certificado.

4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1 POLÍTICA Y PRÁCTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES

En este ítem, la CPS debe informar sobre la imposibilidad que tiene el PSC de copiar o almacenar los datos de creación de firma de su suscriptor. Solamente, y al efecto del plan de continuidad de negocio, los datos de creación de firma del mismo PSC deben estar en custodia y respaldadas bajo estrictas normas de seguridad, y almacenadas en dispositivos criptográficos FIPS 140-2 nivel 3, que garanticen la no divulgación de los mismos.

4.12.2 POLÍTICAS Y PRÁCTICAS DE RECUPERACIÓN Y ENCAPSULACIÓN DE CLAVES DE SESIÓN

No aplica.

Abog. Ronny Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

5 CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES

En los ítems siguientes, deben ser descriptos los controles de seguridad implementados por el PSC responsable y por las RA vinculadas, para ejecutar de modo seguro sus funciones de generación de claves, identificación, certificación, auditoria y respaldo de los registros.

5.1 CONTROLES FÍSICOS

En las secciones siguientes, la CPS debe describir los controles físicos referentes a las instalaciones que albergan los sistemas del PSC responsable y de las RA vinculadas.

5.1.1 LOCALIZACIÓN Y CONSTRUCCIÓN DEL SITIO

La CPS debe establecer que la localización de las instalaciones donde se albergan los sistemas de certificación del PSC responsable, no deberá ser públicamente identificada. No deberá haber identificación pública externa de las instalaciones e internamente, no deberá ser admitido ambientes compartidos que permitan la visibilidad de las operaciones de emisión y revocación de los certificados. Esas operaciones deberán ser segregadas en compartimientos cerrados y físicamente protegidos.

En este ítem, la CPS debe también describir los aspectos de la construcción de las Instalaciones del PSC responsable, relevantes para los controles de seguridad física, comprendiendo entre otros:

a) Instalaciones para equipamientos de apoyo, tales como: máquinas de aire acondicionado, grupos de generadores, UPS, baterías, paneles de distribución de energía y de telefonía;
b) Instalaciones para sistemas de telecomunicaciones;
c) Los sistemas de puesta a tierra y protección contra rayos; y
d) Iluminación de emergencia;

Las instalaciones donde se emiten los certificados del PSC, se deben proteger con su propio y único perímetro físico, y las barreras físicas (paredes y barrotes) deben ser sólidas, extendiéndose desde el piso real al techo real.

Abog. Rubén Ríos Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

5.1.2 ACCESO FÍSICO

Todo PSC integrante de la PKI Paraguay deberá implementar un sistema de control de acceso físico que garantice la seguridad de sus instalaciones, conforme a al ítem 9 "control de accesos" de la norma ISO 27002:2013 y los siguientes puntos:

5.1.2.1 NIVELES DE ACCESO FÍSICO

La CPS debe definir por los menos 4(cuatro) niveles de acceso físico a los diversos ambientes del PSC responsable, más 2(dos) niveles relativos a la protección de la clave privada del PSC.

En el primer nivel deberá situarse la primera barrera de acceso a las instalaciones del PSC. Para acceder en el área del nivel 1, cada persona deberá ser identificada y registrada por el personal de seguridad, a partir de ese nivel personas extrañas a la operativa del PSC deberán transitar debidamente identificadas y acompañadas. Ningún tipo de proceso operacional o administrativo del PSC deberá ser ejecutado en ese nivel.

Excepto en los casos previstos por la ley, la posesión de armas no será admitida en las instalaciones del PSC, desde el nivel 1. A partir de ese nivel, equipos de grabación, fotografía, vídeo, sonido o similares, así como los ordenadores portátiles, será controlado su ingreso y sólo pueden ser utilizados mediante la autorización formal y supervisada.

El **segundo nivel** será interno al primero y deberá requerir, de la misma forma que el primero, una identificación individual de las personas que en el accedan. Ese será el nivel mínimo de seguridad requerido para la ejecución de cualquier proceso operacional o administrativo del PSC. El paso del primer al segundo nivel deberá exigir por lo menos 1 (uno) factor de autenticación electrónica y tarjeta de identificación visible.

En el tercer nivel deberá situarse dentro del segundo nivel y será el primer nivel en albergar material y actividades sensibles de la operativa del PSC. Cualquier actividad relativa al ciclo de vida de los certificados digitales deberá estar localizada a partir de este nivel. Personas que no están involucradas con esas actividades no deberán tener permiso para acceder a este nivel. Personas que no

poseen permiso de acceso no podrán permanecer en ese nivel si no estuviesen acompañadas por alguien que tenga permiso de acceso.

En este nivel deberán ser controladas tanto las entradas como las salidas de cada persona autorizada. Los mecanismos de control que deberán ser requeridos para acceder a ese nivel como mínimo requerirán de 2 (dos) factores de autenticación electrónica y tarjeta de identificación visible.

Teléfonos móviles y otros equipos de comunicación portátil, con excepción de los necesarios para el funcionamiento del PSC, no serán aceptadas desde el nivel 3.

En **el cuarto nivel**, interno al tercero, donde han de desplegarse, actividades especialmente sensibles a la operación del PSC, tales como la emisión y revocación de los certificados y la emisión de la CRL. Todos los sistemas y equipamientos necesarios a estas actividades deberán estar localizados a partir de este nivel. El nivel 4 deberán poseer 2 (dos) factores de autenticación como mínimo (uno de ellos biométrico) y tarjeta de identificación visible y, adicionalmente, deberá exigir, en cada acceso a su ambiente, la identificación de, como mínimo, 2 (dos) personas autorizadas. En este nivel, la permanencia de esas personas deberá ser exigida mientras el ambiente estuviera ocupado.

En el cuarto nivel, todas las paredes, piso y techo deberán ser revestidos con material resistente. Las paredes, piso y techo deberán ser realizadas de modo a prevenir las amenazas de acceso no autorizado, agua, vapor, gas y fuego. Las tuberías de refrigeración, de energía o de comunicación no deberán permitir la penetración física en las áreas de cuarto nivel. Adicionalmente, debe tener una protección contra las interferencias electromagnéticas externas.

Este ambiente deberá ser construido según las normas internacionales aplicables.

Podrá existir, en el PSC, varios ambientes del cuarto nivel para albergar y segregar, cuando fuera el caso:

a) Equipamientos de producción on-line y cofre de almacenamiento;
b) Equipamientos de producción of-line y cofre de almacenamiento; y
c) Equipamientos de redes e infraestructura (firewall, ruteadores, switches y servidores)

En el quinto nivel o superior, interno al ambiente del nivel 4, deberá disponerse de un cofre o un gabinete reforzado, donde estarán almacenados:

materiales criptográficos, tales como, claves, datos de activación, sus copias y equipamientos criptográficos

Para garantizar la seguridad del material almacenado, el cofre o el gabinete deberán obedecer las siguientes especificaciones mínimas:

a) Estar hecho de acero o con material de resistencia equivalente; y
b) Poseer cerraduras antirrobo.

En el sexto nivel, interno al ambiente del nivel 4, deberá comprender un cofre o un gabinete reforzado. Los datos de activación de la clave privada del PSC deberán ser almacenados en ese ambiente.

Para garantizar la seguridad del material almacenado, el cofre o el gabinete deberán obedecer las siguientes especificaciones mínimas:

a) estar hecho de acero o con material de resistencia equivalente; y
b) poseer cerraduras antirrobo.

Sistemas físicos de detección: la transición entre los diferentes niveles de acceso, así como la sala de operaciones del nivel 4, deberán ser monitoreadas por cámaras de video ligadas a un sistema de grabación 24x7. El posicionamiento y la capacidad de esas cámaras no deberán permitir recuperar las contraseñas digitadas en los controles de acceso.

Las cintas de vídeo resultantes de grabación 24x7 deberán ser almacenadas, como mínimo, 1(un) año. Ellas deberán ser testeadas (verificación de estrechos aleatorios en el inicio, medio y final de la cinta) por lo menos cada 3(tres) meses, con la elección, como mínimo, de 1(una) cinta referente a cada semana. Esas cintas deberán ser almacenadas en el ambiente del nivel 3.

Todas las puertas de transición entre los ambientes de niveles 3 y 4 deberán ser monitoreadas por un sistema de notificación de alarmas. Donde hubiere, a partir del nivel 2, vidrios separando niveles de acceso, deberá ser implementado un mecanismo de alarma de quiebra de vidrios, que deberá estar funcionando ininterrumpidamente.

En todos los ambientes del cuarto nivel, una alarma de detección de movimientos deberá permanecer activo hasta que se satisfaga el criterio de acceso al ambiente. Así que si, debido a la salida de uno o más empleados, trae como

consecuencia que el criterio mínimo de ocupación deje de ser satisfecha, deberán activarse automáticamente los sensores de presencia.

Los sistemas de notificación de alarmas deberán utilizar por los menos 2(dos) medios de notificación: sonoro y visual.

El sistema de monitoreo de las cámaras de video, así como el sistema de notificación de alarma, deberán ser permanentemente monitoreados por el personal autorizado en el ambiente de nivel 3 deben estar localizados en el nivel 3. Las instalaciones del sistema de monitoreo, a su vez, deben ser monitoreados por cámaras de vídeo cuyo posicionamiento debería permitir el seguimiento de las acciones del personal autorizado.

Sistema de control de acceso: el sistema de control de acceso deberá estar en el ambiente de nivel 4.

Mecanismos de emergencia: mecanismos específicos deberán ser implementados por el PSC para garantizar la seguridad de su personal y de sus equipamientos en situaciones de emergencia. Esos mecanismos deberán permitir el desbloqueo de las puertas por medio de accionamiento mecánico, para la salida de emergencia de todos los ambientes con control de acceso. La salida efectuada por medio de estos mecanismos debe accionar inmediatamente las alarmas de apertura de puertas.

EL PSC podrá especificar e implementar otros mecanismos de emergencia, específicos necesarios para cada tipo de instalación. Todos los procedimientos referentes a esos mecanismos de emergencia deberán se documentados. Los mecanismos y procedimientos de emergencia deberán ser verificados semestralmente, por medio de simulación de situaciones de emergencia.

5.1.3 ENERGÍA Y AIRE ACONDICIONADO

La infraestructura del ambiente de certificación del PSC deberá ser dimensionada con sistemas y dispositivos que garanticen el funcionamiento ininterrumpido de energía eléctrica en las instalaciones. Las condiciones de funcionamiento ininterrumpido de energía deben ser mantenidas de forma de atender los requisitos disponibilidad de los sistemas del PSC y de sus respectivos servicios. Un sistema puesta a tierra deberá ser implantado.

Todos los cables eléctricos deben estar protegidos por tuberías y conductos apropiados.

Deberán ser utilizados tuberías, conductos, canaletas, paneles y cajas (de paso, distribución y terminación) diseñadas y construidas de forma a facilitar la inspección y detección de intentos de manipulación. Deberán ser utilizados conductos separados para los cables de energía, de telefonía y de datos.

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

Deberán ser mantenidos actualizados los registros sobre la topología de la red de cables, de acuerdo a los requisitos de confidencialidad establecidos en el ítem 13 "seguridad en las telecomunicaciones" de la norma ISO 27002/2013. Cualquier modificación en esa red deberá ser previamente documentada.

No deberán ser admitidas instalaciones provisorias, cableados expuestas o directamente conectadas a tomas sin la utilización de conectores adecuados.

El sistema climatización deberá cumplir con los requisitos de temperatura y humedad exigidos por los equipamientos utilizados en el ambiente y disponer de filtros de polvo. En los ambientes de nivel 4, el sistema de climatización deberá ser independiente y tolerable a fallas.

La temperatura de los ambientes atendidos por el sistema de climatización deberá ser permanentemente monitoreada por el sistema de notificación de alarmas.

Los sistemas de aire acondicionados de los ambientes de nivel 4 deberán ser internos, con cambio de aire realizado apenas por la abertura de la puerta.

La capacidad de redundancia de toda la estructura de energía y aire acondicionado deberá ser garantizada, por medio de:

a) Generadores de un tamaño compatible
b) Generadores de reserva;
c) Sistemas de UPS redundantes; y
d) Sistemas redundantes de aire acondicionado.

Abog. Tania Rosa Rolón A.
DIRECTORA GENERAL
Firma Digital y Comercio Electrónico

La estructura interna al ambienta de nivel 4, deberá proveer protección física contra exposición a agua, filtraciones e inundaciones provenientes de cualquier fuente externa.

5.1.5 PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO

El sistema de prevención contra incendios, internos a los ambientes deberán posibilitar alarmas preventivas antes que el humo sea visible, activados solamente con la presencia de partículas que caracterizan el sobrecalentamiento de materiales eléctricos y otros materiales combustibles presentes en las instalaciones.

En las instalaciones del PSC no está permitido fumar o portar objetos que produzcan fuego o chispa.

El nivel 4 deberá poseer un sistema para detección precoz de humo y un sistema de extinción de incendio por gas.

En caso de incendio de las instalaciones del PSC, o el aumento la temperatura interna del ambiente del nivel 4, no deberá exceder 50 grados Celsius, y el ambiente deberá soportar esta condición, como mínimo, 1 (una) hora.

5.1.6 ALMACENAMIENTO DE MEDIOS

El PSC 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 PSC 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

Todos los documentos en papel que contengan informaciones clasificadas como sensibles deberán ser triturados antes de ir como residuo.

Todos los dispositivos electrónicos que ya no son utilizables y que se han utilizado previamente para el almacenamiento de información sensible deberán ser destruidos físicamente.

5.1.8 RESPALDO FUERA DE SITIO

Las instalaciones de respaldo deberán cumplir con los requisitos mínimos establecidos por este documento. Su localización deberá ser tal que, en caso de siniestro que torne inoperante la instalación principal del PSC, las instalaciones de respaldo no se vean afectadas y tomen totalmente las operaciones del PSC en condiciones idénticas en, un máximo, de 48(cuarenta y ocho) horas.

5.1.9. INSTALACIONES TÉCNICAS DE LA RA

Las instalaciones técnicas de la RA deberán cumplir con los requisitos establecidos en el documento **CARACTERÍSTICAS MÍNIMAS DE SEGURIDAD PARA LA AUTORIDADES DE REGISTRO DEL PARAGUAY**

5.2 CONTROLES PROCEDIMENTALES

5.2.1 ROLES DE CONFIANZA

El PSC responsable de la CPS deberá garantizar la segregación de tareas para las funciones críticas, con el fin de evitar que un empleado que asume un rol de confianza utilice incorrectamente su sistema de certificación sin ser detectado. Las acciones de cada uno de los empleados se limitarán de acuerdo a su perfil.

Todos los operadores del sistema de certificación del PSC deberán recibir entrenamiento específico antes de obtener cualquier tipo de acceso. El tipo o nivel de acceso serán determinados, en un documento formal, con base en las necesidades de cada perfil.

Cuando un empleado se desvincula del PSC, sus permisos de acceso deberán ser revocados inmediatamente. Cuando hay un cambio en la posición o función que el empleado ocupa dentro del PSC, deberán ser revisadas sus permisos de acceso. Deberá existir una lista de revocación, con todos los recursos, antes disponibilizados, que el empleado deberá devolver al PSC en el momento de su desvinculación

Los Roles de un PSC, deben contemplar, al menos las siguientes responsabilidades que a continuación serán descriptos:

Abog. Pedro Ruiz Bobadilla
DIRECTOR GENERAL
Dirección General de Firma Digital y Comercio Electrónico

a) **Responsables de seguridad:** deberán llevar a cabo la actualización e implementación de las políticas y procedimientos de seguridad que han sido aprobadas por el PSC, controlar la formalización de los convenios entre el personal y el PSC, comunicar las medidas disciplinarias acordadas, supervisando su cumplimiento. Asimismo, deberá cumplir y hacer cumplir las políticas de seguridad del PSC y deberá encargarse de cualquier aspecto relativo a la seguridad de la PKI, desde la seguridad física hasta la seguridad de las aplicaciones, pasando por la seguridad de la red. Será el encargado de gestionar los sistemas de gestión perimetral y en concreto de verificar la correcta gestión de las reglas de los firewalls. Deberá comprobar la correcta instalación, configuración y gestión de los sistemas de detección de intrusos y de las herramientas asociadas a estos, asimismo deberá resolver o hacer que resuelvan las incidencias de seguridad producidas, de eliminar vulnerabilidades detectadas, etc. y es el encargado de la gestión y control de seguridad física, y de los movimientos de material fuera de las instalaciones del PSC.

b) **Responsables de coordinación de área:** es el responsable de autorizar tecnológicamente la emisión de un certificado o la revocación del mismo. Bajo su control y supervisión, se encuentra el personal adscripto a la misma. Es su responsabilidad:
   - Recibir y dar curso a las denuncias que podrían afectar a su personal, proponiendo las medidas disciplinarias correspondientes
   - Efectuar un control permanente de la adecuación de los recursos materiales y humanos que cuenta el área a su cargo, con el fin de atender las necesidades de servicio que tiene encomendadas

c) **Responsables de sistemas:** los responsables de este rol no deberán estar implicados en tareas de auditoría interna. Serán encargados de la instalación y configuración de sistemas operativos, del mantenimiento y actualización de los programas instalados; con capacidad para configurar, mantener los sistemas, pero sin acceso a los datos. Asimismo, deberán establecer y documentar los procedimientos de monitoreo de los sistemas y de los servicios que prestan. Serán responsables de mantener el inventario de servidores y resto de componentes de los sistemas de certificación del PSC y asumirán la gestión de los servicios de ruteamiento y gestión de reglas de firewall, gestión y mantenimiento de los sistemas de detección de intrusos, etc. Serán encargados de la instalación de hardware criptográfico del PSC y de la eliminación del hardware criptográfico del PSC de producción. Serán responsables del mantenimiento o reparación de equipos

Abog. Rodrigo Rolón A.
Director General
Dirección General de Firma Digital y Comercio Electrónico

criptográficos PSC (incluida la instalación de nuevo hardware, firmware o software), y la eliminación de desmontaje y permanente por el uso.

d) **Responsables de la operación diaria del PSC:** será encargada de realizar las tareas de ejecución y revisión de las copias de seguridad del sistema. Asimismo debe velar para que se lleven a cabo las copias de seguridad local y del traslado de las mismas de acuerdo con lo establecido en la política de seguridad. Serán responsables de mantener la información suficiente como para poder restaurar cualquiera de los sistemas en el menor tiempo posible. Serán encargados de la gestión y mantenimiento de los sistemas de energía, aire acondicionado y prevención de incendios.

e) **Responsables de auditoría interna:** serán los responsables de las tareas de ejecución y revisión de auditoría interna del sistema. Esta auditoría interna deberá realizarse de acuerdo con las normas y criterios de auditoría establecidos la presente CPS. Además deberá tener acceso a todos los registros del sistema.

f) **Responsables del ciclo de vida de claves criptográficas:** se distinguen los siguientes responsables para la gestión del ciclo de vida de las claves criptográficas:

- **Oficial criptográfico:** será el responsable de generar los usuarios que van a hacer uso de las claves del HSM. Participa en la copia de respaldo y recuperación del HSM.
- **Oficial de activación:** será el responsable de activar las claves del HSM para que se pueda hacer uso de las mismas.
- **Usuario:** serán quienes operan el sistema de gestión de certificados y el HSM.
- **Oficial de registro:** realizará funciones de registro, como la generación de certificados o la revocación de los mismos.
- **Oficial de generación de CRL:** Encargado de generar y exportar en ficheros las CRL emitidas por el PSC. Además son responsables de activar los servicios de OCSP y asegurar la disponibilidad del CRL.

g) **Responsables de desarrollo de sistemas del PSC:** serán los encargados del diseño de las arquitecturas de programación, de control y supervisión de los desarrollos encomendados y de la correcta documentación de las aplicaciones.

Abog. Rocío Rolón A. DIRECTORA GENERAL Firma Digital y Comercio Electrónico

5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

La CPS debe establecer el requisito de control multi-usuarios para la generación y la utilización de la clave privada del PSC responsable, de la forma definida en el ítem 6.2.2.

Todas las tareas ejecutadas en el ambiente donde está localizado el equipamiento de certificación del PSC deberá requerir de, como mínimo, 2(dos) de sus empleados con rol de confianza. Las demás tareas del PSC podrán ser ejecutadas por un único empleado.

5.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

La CPS debe garantizar que todo empleado que asume un rol de confianza en el PSC será identificado y su perfil será verificado antes de que:

a) Sean incluido en una lista de acceso a las instalaciones del PSC;
b) Sean incluido en una lista para acceso físico al sistema de certificación del PSC;
c) Reciban un certificado electrónico para ejecutar sus actividades operacionales en el PSC; y
d) Reciban una cuenta de usuario del sistema de certificación del PSC.

Los certificados, cuentas y contraseñas utilizados para la identificación y autenticación de los empleados deberán:

a) Ser directamente asignados a un único empleado;
b) No ser compartidos; y
c) Restringirse a las acciones asociadas con el perfil para el que fueron creados.

5.2.4 ROLES QUE REQUIEREN SEPARACIÓN DE FUNCIONES

En este ítem la CPS describirá aquellos roles que requieren separación de funciones. Los roles que requieren separación de los deberes incluyen (pero no está limitado) a los encargados de ejecutar las siguientes responsabilidades:

- Los responsables del ciclo de vida de claves criptográficas no podrán cumplir funciones de los responsables de auditoría interna.
- Los responsables de sistemas no podrán cumplir funciones de los responsables de seguridad ni de los responsables de auditoría interna.
- Los responsables de seguridad no podrán cumplir funciones de los responsables de sistemas, de los responsables del ciclo de vida de claves criptográficas ni de los responsables de auditoría interna.
- Los responsables de auditoría interna no podrán cumplir otra función o rol.

Abog. Raúl Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Además otras tareas que deben ser segregadas son:

- La validación de información en aplicaciones de certificado y de solicitudes información del suscriptor.
- La aceptación, rechazo, otros procesamientos de la aplicación de certificado, solicitud de revocación.
- La emisión o revocación de los certificados, incluyendo personal con acceso a porciones restringidas del repositorio.
- La emisión o destrucción de los certificados del PSC.
- La puesta en operación del PSC en producción.

5.3. CONTROLES DE PERSONAL

5.3.1. REQUERIMIENTOS DE EXPERIENCIA, CAPACIDADES Y AUTORIZACIÓN

Todo el personal del PSC responsable y de las RA vinculado e involucrado en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados deberá ser seleccionado y admitido, conforme a lo establecido en el ítem 7 "seguridad ligada a los recursos humanos" de la norma ISO 27002/2013 y además deberán:

a) Haber demostrado capacidad para ejecutar sus deberes;
b) Haber suscripto un acuerdo de confidencialidad y disponibilidad;
c) No poseer otros deberes que puedan interferir o causar conflicto con los del PSC;
d) No tener antecedentes de negligencia o incumplimiento de labores; y
e) No tener antecedentes penales.

El PSC responsable podrá definir requisitos adicionales para la admisión.

5.3.2. PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES

Con propósito de resguardar la seguridad y credibilidad de las entidades, todo personal del PSC responsable y de las RA vinculadas involucradas en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados deberá ser sometido a:

- Confirmación de empleos anteriores.
- Verificación de referencias profesionales.
- Título académico obtenido.

Abog. Carlos Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

- Verificación de antecedentes judiciales y policiales.

5.3.3. REQUERIMIENTOS DE CAPACITACIÓN

Todo el personal del PSC responsable y de las RA vinculado, involucrado en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados deberá recibir entrenamientos documentado suficiente para el dominio de los siguientes temas:

- principios y mecanismos de seguridad del PSC y de las RA vinculadas;
- sistema de certificación en uso del PSC;
- procedimientos de recuperación de desastres y continuidad del negocio;
- reconocimiento de firmas y validación de documentos presentados en los ítem 3.2.2., 3.2.3. y 3.2.4.;
- normativa vigente que rige la materia; y
- otros asuntos relacionados con las actividades bajo su responsabilidad.

5.3.4. REQUERIMIENTOS Y FRECUENCIA DE CAPACITACIÓN

Todo el personal del PSC responsable y de las RA vinculado, involucrado en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados deberá ser mantenido y actualizado sobre eventuales cambios o modificaciones tecnológicas de los sistemas del PSC o de las RA.

El PSC responsable y de las RA vinculadas deberá proveer los programas de entrenamiento y actualización a su personal para asegurar que el personal mantenga el nivel requerido de eficiencia para ejecutar sus labores satisfactoriamente.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

5.3.5. FRECUENCIA Y SECUENCIA EN LA ROTACIÓN DE LAS FUNCIONES

En este ítem, la CPS podrá definir una política a ser adoptada por el PSC responsable y por las RA vinculadas, para la rotación del personal en los diversos cargos y perfiles por ellas establecidas. Esa política no deberá contrariar los propósitos establecidos en el ítem 5.2.1.

EL PSC responsable y las RA vinculadas deberán efectuar una rotación de sus roles de confianza como mínimo una vez cada 3 años.

5.3.6. SANCIONES PARA ACCIONES NO AUTORIZADAS

La CPS deberá prever que en la eventualidad de una acción no autorizada, real o sospechada, realizada por una persona encargada del proceso operacional del PSC responsable o de una RA vinculada, el PSC deberá de inmediato, suspender el acceso de esa persona a su sistema de certificación, iniciar un procedimiento administrativo para determinar los hechos y, si es necesario, tomar las medidas legales pertinentes.

El proceso administrativo referido en el párrafo anterior deberá contener, como mínimo, los siguientes puntos.

a) Relato de lo ocurrido con el modo de operación;
b) Identificación de los involucrados;
c) Eventuales perjuicios causados;
d) Las sanciones aplicadas, si fuere el caso; y
e) Conclusiones.

Concluido el proceso administrativo, el PSC responsable deberá comunicar sus conclusiones a la CA Raíz.

Las sanciones que podrían aplicarse como resultado de un procedimiento administrativo son:

a) Advertencia;
b) Suspensión por un plazo determinado; o
c) Impedimento definitivo de ejercer funciones en el ámbito de la PKI Paraguay.

5.3.7.REQUISITOS DE CONTRATACIÓN A TERCEROS

Todo el personal del PSC responsable y de las RA vinculado, involucrado en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados, deberá ser contratado conforme a lo establecido los ítems 7 "seguridad ligada a los recursos humanos" y 15 "relaciones con suministradores" norma ISO 27002/2013 y bajo las siguientes condiciones mínimas:

- que exista un contrato con cláusulas propias de los roles de confianza y estipula sanciones para las acciones no autorizadas.

Abog. Roberto Nolón A.
DIRECTOR GENERAL
Dirección General de Firma Digital y Comercio Electrónico

- que el PSC responsable o RA vinculada no posea personal disponible para llenar los roles de confianza.
- que el personal a contratar cumpla con los mismos requisitos del ítem 5.3.1.
- que una vez finalizado el servicio contratado se revoquen los derechos de acceso.

5.3.8. DOCUMENTACIÓN SUMINISTRADA AL PERSONAL

La CPS debe asegurar que el PSC responsable pone a disposición de todo el personal del PSC y para todo el personal de los RA vinculados al menos:

a) Su CPS;
b) Las CP que implementa;
c) La política de seguridad que implementa el PSC;
d) Documentación operacional relativa a sus actividades; y
e) Contratos, normas y políticas relevantes para sus actividades.

Toda documentación entregada o disponibilizada al personal deberá estar clasificada y deberá ser mantenida actualizada.

5.4. PROCEDIMIENTO DE REGISTRO DE AUDITORÍA

En los siguientes ítems de CPS deben describirse los aspectos de los sistemas de auditoría y registro de eventos implementados por el PSC con el fin de mantener un entorno o ambiente seguro.

5.4.1. TIPOS DE EVENTOS REGISTRADOS

El PSC responsable de la CPS, deberá registrar en archivos de auditoria, todos los eventos relacionados a la seguridad de su sistema de certificación. Entre otros, los siguientes eventos deberán obligatoriamente estar incluidos en los archivos de auditoria:

a) Iniciación y terminación del sistema de certificación;
b) Los intentos de crear, eliminar, establecer contraseñas o cambiar los privilegios del sistema de los operadores del PSC;
c) Los cambios en la configuración del PSC o en sus llaves;
d) Los cambios en las políticas de creación de certificados;
e) Los intentos de acceso (*login*) y de salida del sistema (*logoff*);
f) Los intentos no autorizados de acceso a los archivos del sistema;

Abog. Roberto Solón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

g) La generación de claves propias del PSC o de claves de sus usuarios finales;
h) La emisión y revocación de certificados;
i) La generación de la CRL;
j) Los intentos de iniciar, remover, habilitar y deshabilitar a los usuarios de sistemas y actualizar y recuperar sus claves;
k) Las operaciones fallidas de escritura o lectura en el repositorio de los certificados y de la CRL, en su caso; y
l) Las operaciones de escritura en ese repositorio, en su caso.

EL PSC responsable de la CPS deberá también registrar, electrónicamente o manualmente, informaciones de seguridad no generadas directamente por el sistema de certificación, tales como:

a) Registros de accesos físicos;
b) El mantenimiento y los cambios en la configuración de sus sistemas
c) Los cambios de personal y los cambios de su rol de confianza
d) Los informes de discrepancia y de compromiso
e) El registro de destrucción de los medios de almacenamiento que contienen las claves criptográficas, de datos de activación de certificados o de la información personal de los usuarios.

En este ítem, la CPS debe especificar todas las informaciones que deberán ser registradas por el PSC responsable.

La CPS debe prever que todos los registros de auditoria, electrónicos o manuales, deberán contener la fecha y hora del evento registrado y la identidad del agente que lo causo.

Para facilitar los proceso de auditoría, toda documentación relacionada a los servicios del PSC deberá se almacenada, electrónicamente o manualmente, en un local único, conforme a lo establecido en el ítem 12 "seguridad en la operativa" de la norma ISO 27002/2013.

La RA vinculada al PSC responsable de la CPS, deberá registrar electrónicamente archivos de auditorías de todos los eventos relacionados a la validación y aprobación de la solicitud, así como la revocación de los certificados. Los siguientes eventos deberán obligatoriamente estar incluidos en los archivos de auditoria:

a) Los agentes de registros que realizan las operaciones;
b) fecha y hora de las operaciones;
c) La asociación entre los agentes que realizan la validación, aprobación y y el certificado generado;
d) La firma digital del ejecutante.

EL PSC a la que está vinculada la RA, debe establecer, en un documento que esté disponible en las auditorias de cumplimiento, el local de archivo de las copias de los documentos utilizados para la identificación del suscriptor, presentados en el momento de la solicitud y revocación de certificados. El formulario de solicitud y el acuerdo de suscriptores.

5.4.2 FRECUENCIA DE PROCESAMIENTO DEL REGISTRO (*LOGS*)

La CPS debe establecer el periodo, no superior a 1 (un) mes, con que los registros de auditoria del PSC responsable, serán analizados por el personal operacional. Todos los eventos significativos deberán ser explicados en un informe de auditoría de registros. Tal análisis deberá involucrar una inspección breve de todos los registros, con la verificación de que no fueron alterados, seguida de una investigación más detallada de cualquier alerta o irregularidades en esos registros. Todas las medidas adoptadas como resultado de este análisis deberán ser documentadas.

5.4.3 PERÍODO DE CONSERVACIÓN DEL REGISTRO (*LOGS*) DE AUDITORÍA

En este ítem, la CPS debe establecer que el PSC responsable, mantendrá localmente sus registros de auditoria por los menos 2 (dos) meses y, consecuentemente, deberá almacenarlos de la manera descripta en el ítem 5.6.2.

Además de las revisiones oficiales, los registros de auditoría deben ser revisados en respuesta a una alerta, por irregularidades o Incidentes dentro de los sistemas del PSC.

5.4.4 PROTECCIÓN DEL REGISTRO (*LOGS*) DE AUDITORÍA

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

También deben ser descriptos, los mecanismos obligatorios de protección de información manual de auditoria 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.

5.4.5. PROCEDIMIENTOS DE RESPALDO (*BACKUP*) DE REGISTRO (*LOGS*) DE AUDITORÍA

Es este ítem de la CPS deben ser descriptos los procedimientos adoptados por el PSC responsable para generar copias de seguridad de sus registros de auditorías y su frecuencia, que no debe ser superior a 1 (un) mes.

5.4.6. SISTEMA DE RECOLECCIÓN DE INFORMACIÓN DE AUDITORÍA (INTERNO VS EXTERNO)

En este ítem las CPS deben ser descriptas y localizadas los recursos utilizados por el PSC responsable para la recolección de datos de auditoria.

5.4.7. NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO

La CPS debe tener en cuenta que cuando un evento fuera registrado por el conjunto de sistemas de auditoria del PSC responsable, no se requerirá notificar al causante de dicho evento, a excepción de que el evento sea de índole accidental y resulta probable que pueda volver a ocurrir.

5.4.8. EVALUACIÓN DE VULNERABILIDADES

La CPS debe asegurar que los eventos que indiquen posibles vulnerabilidades, detectados en el análisis periódico de los registros de auditoria del PSC responsable, serán analizadas detalladamente y, dependiendo de su gravedad, registradas por separado. Acciones correctivas que surjan deberán ser implementadas por el PSC y registradas con fines de auditoria.

Abog. Rocío Rolón A.
DIRECTORA GENERAL
Firma Digital y Comercio Electrónico

5.5. ARCHIVOS DE REGISTROS

En los ítems siguientes de la CPS debe ser descripta la política general de archivo de registros, para uso futuro, implementada por el PSC responsable y por las RA a ellas vinculadas

5.5.1. TIPOS DE REGISTROS ARCHIVADOS

En este ítem de la CPS deben ser especificados los tipos de registros archivados, que deberá comprender, entre otros:

Durante el inicio de operaciones del PSC:

a) La Habilitación en caso del PSC responsable o una RA vinculada;
b) La CP y la CPS;
c) Cualquier acuerdo contractual para establecer los límites del PSC o RA vinculada; y
d) La configuración del sistema que requiere el PSC

Durante la operativa del PSC:

a) Modificaciones o actualizaciones de cualquiera de los ítems anteriores;
b) Solicitudes de certificados;
c) Solicitudes de revocación de certificados;
d) Documentación para autenticar la identidad del titular del certificado y del responsable de su uso en el caso de un certificado de persona jurídica o un certificado de equipamiento o aplicaciones ;
e) Documentación de recepción de dispositivos de almacenamiento de claves;
f) Todos los certificados emitidos;
g) Todas las CRL emitidas y publicadas;
h) Notificaciones de compromiso de clave privada;
i) Informaciones de auditorías previstas en el ítem 5.4.1.
j) todos los trabajos comunicados o relacionados a políticas, otras PSC y 5.5.2.

5.5.2. PERÍODOS DE RETENCIÓN PARA ARCHIVOS

En este ítem, la CPS debe establecer los periodos de retención para cada registro archivado, teniendo en cuenta que:

a) La CRL y los certificados emitidos de firma digital deberán ser conservados permanentemente para fines de consulta histórica;
b) Las copias de los documentos para identificación del suscriptor, presentados en el momento de la solicitud y de la revocación de certificados, el formulario de solicitud y el acuerdo de suscriptores, como

Abog. Raúl Rolón A.
Director General
Firma Digital y Comercio Electrónico

mínimo, por 10 (diez) años, a contar desde la fecha de expiración o revocación del certificado; y

c) Las demás informaciones, inclusive los archivos de auditoria, deberán ser almacenadas, como mínimo, 10 años.

5.5.3 PROTECCIÓN DE ARCHIVOS

La CPS debe establecer que todos los registros archivados deberán ser clasificados y almacenados con los requisitos de seguridad compatibles con esta clasificación, conforme a lo establecido en el ítem 12 "seguridad en la operativa" de la norma ISO 27002/2013.

5.5.4 PROCEDIMIENTOS DE RESPALDO (*BACKUP*) DE ARCHIVO

La CPS debe establecer que una segunda copia de todo el material archivado deberá ser almacenada en un local externo al PSC responsable, recibiendo el mínimo tipo de protección utilizada para el archivo principal.

Las copias de seguridad deberán seguir los periodos de retención definidos para los registros de las cuales son copias.

El PSC responsable de la CPS deberá verificar la integridad de esas copias de seguridad, como mínimo, cada 6(seis) meses.

5.5.5 REQUERIMIENTOS PARA SELLADO DE TIEMPO DE REGISTROS

Este Ítem no aplica.

5.5.6 SISTEMA DE RECOLECCIÓN DE ARCHIVO (INTERNO O EXTERNO)

En este ítem de la CPS, deben ser descriptos y localizados los recursos utilizados por el PSC responsable para la recolección de datos de auditoria.

5.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR LA INFORMACIÓN ARCHIVADA

En esta sección de la CPS, deben ser detalladamente descriptos los procedimientos definidos por el PSC responsable y por las RA vinculada para la obtención y verificación de sus informaciones de archivo.

Abog. Boris Barón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

El responsable de las RA vinculada debe realizar pruebas de restauración de la información archivada al menos 1 (una) vez al año.

5.6 CAMBIO DE CLAVE

En este ítem, las CPS debe describir los procedimientos para el suministro, por el PSC responsable, de un nuevo certificado, antes de la expiración de certificado a pedido del titular del certificado.

El PSC debe cambiar su clave de acuerdo con el tiempo de uso y tiempo operacional de los certificados emitidos dentro de la PKI Paraguay, este cambio técnicamente implica la emisión de un nuevo certificado.

El tiempo operacional de un certificado coincide con el descripto en los campos de "Válido desde" y "Válido hasta" del mismo. El tiempo de uso refiere al establecido para los certificados emitidos por la jerarquía de la PKI Paraguay para determinados usos, como se aprecia a continuación:

Tabla N° 5 – Certificados emitidos por la Jerarquía PKI

Nivel de Jerarquía	Tiempo de uso en años	Tiempo operacional en años	Descripción
Certificado de Suscriptores (Módulo Hardware)	2	2	El certificado emitido al usuario final es otorgado por un tiempo máximo de dos años, al finalizar ese período pierde su validez
Certificado de Suscriptores (Módulo Software)	1	1	El certificado emitido al usuario final es otorgado por un tiempo máximo de un año, al finalizar ese período pierde su validez
Certificado de PSC	8	10	El Certificado emitido al PSC tendrá: Un tiempo operacional de 10 años, que

Abog. Rocío Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

			resulta de la suma del tiempo de uso de su certificado (8 años) más el tiempo de validez máximo del certificado de su suscriptor (2 años). Solamente durante el tiempo de uso de su certificado, el PSC podrá emitir certificados a usuarios o suscriptores. En los años restantes del tiempo operacional solo podrá firmar el CRL de usuarios o suscriptores.
Certificado CA Raíz	10	20	El Certificado emitido a la CA Raíz tendrá: Un tiempo operacional de 20 años, que resulta de la suma del tiempo de uso de su certificado (10 años) más el tiempo de validez máximo del certificado de su suscriptor (10 años). Solamente durante el tiempo de uso de su certificado, la CA Raíz podrá emitir certificados a un PSC. En los años restantes del tiempo operacional solo podrá firmar el CRL de PSC.

Abog. Ramón Polón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

Del cuadro anterior, se deduce que en determinado momento, puede haber dos certificados del mismo nivel y tipo activos, donde el tiempo de vigencia simultánea de los certificados debe ser de al menos el tiempo operacional del certificador

Por lo tanto, el certificado anterior podrá ser utilizado únicamente para firmar la CRL correspondiente y validar la cadena de confianza de la PKI Paraguay; el nuevo certificado emitido, será utilizado para emitir nuevos certificados y firmar la nueva lista de CRL.

Los responsables del PSC tendrán la obligación de garantizar que el tiempo máximo de uso en años de los certificados de niveles inferiores se ajusta con el tiempo operacional de todos los niveles superiores.

5.7. RECUPERACIÓN DE DESASTRES Y COMPROMISO

5.7.1. PROCEDIMIENTO PARA EL MANEJO DE INCIDENTE Y COMPROMISO

En este ítem de la CPS, deben ser descriptos, los requisitos relacionados a los procedimientos de notificación y de recuperación de desastres, previstos en el plan de continuidad del negocio del PSC responsable, establecido 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.

5.7.2 CORRUPCIÓN DE DATOS, SOFTWARE Y/O RECURSOS COMPUTACIONALES

En este apartado, de la CPS, deben ser descriptos los procedimientos de recuperación utilizados por el PSC responsable cuando los recursos computacionales, software y/o corrupción de datos estuvieren comprometidos o en sospecha de corrupción.

Además, en este ítem la CPS debe describir los procedimientos de recuperación utilizados en caso de la revocación del certificado del PSC responsable.

5.7.3. PROCEDIMIENTOS DE COMPROMISO DE CLAVE PRIVADA DE LA ENTIDAD

En este ítem de la CPS, deben ser descriptos los procedimientos de recuperación utilizados en caso de compromiso del PSC responsable.

5.7.4. CAPACIDAD DE CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

En este ítem de la CPS, deben ser descriptos los procedimientos de recuperación utilizados por el PSC conforme a lo establecido en el ítem 17 "aspectos de seguridad de la información en la gestión de la continuidad del

Abog. Rubén Ruiz Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

negocio" de la norma ISO 27002:2013 después de la ocurrencia de un desastre natural o de otra naturaleza, antes del restablecimiento de un ambiente seguro.

5.7.5. ACTIVIDADES DE LAS AUTORIDADES DE REGISTRO

En este ítem de la CPS, deben ser descriptos los procedimientos previstos en el Plan de continuidad del Negocio de las RA vinculadas para la recuperación, total o parcial de las actividades de las RA, conteniendo, como mínimo las siguientes informaciones:

a) Identificación de eventos que pueden causar interrupciones en los proceso del negocio, por ejemplo falla de equipamientos, inundación e incendios;
b) Identificación y concordancias de todas las responsabilidades y procedimientos de emergencia;
c) Implementación de procedimientos de emergencia que permitan la recuperación y restauración en los plazos necesarios. Se debe prestar especial atención a la evaluación de la recuperación de la documentación almacenada en instalaciones técnicas afectados por el desastre;
d) Documentación de los procesos y procedimientos acordados;
e) Entrenamiento adecuado del personal en los procedimientos y procesos de emergencia definidos, incluido el gerenciamiento de crisis;
f) Prueba y actualización de los planes.

5.8 EXTINCIÓN DE UN PSC

En este ítem la CPS, debe describir los requisitos y los procedimientos que deberán ser adoptados en el caso de la extinción de servicios del PSC responsable o de una RA o PSS a ella vinculada.

Deben ser detallados, los procedimientos para notificación de usuarios y para transferencia de guarda de sus datos de registros y de archivo.

En caso que un PSC responsable, deje de operar deberá cumplir, como mínimo, con lo siguiente:

a) Publicar en su sitio principal de internet la fecha de suspensión de los servicios con al menos 60 días de anticipación;

Abog. Rocío Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

b) Publicar la fecha de suspensión de sus servicios por el plazo de 3 días consecutivos en un diario de gran circulación, 10 días hábiles antes de la suspensión efectiva o cese de las operaciones;
c) Notificar a sus suscriptores por lo menos 30 días antes de la suspensión efectiva o cese de sus operaciones
d) Proceder a la eliminación y destrucción de la clave privada mediante un mecanismo que impida su reconstrucción.

En caso que el PSC, deje de operar, no podrá bajo ningún sentido emitir ningún certificado pero deberá continuar dando soporte a las operaciones de revocación de certificados y publicación de CRL. Recién una vez vencidos o revocados todos los certificados emitidos, y cuya revocación esté publicada, cesa automáticamente la responsabilidad del PSC.

El titular del certificado, podrá seguir utilizando el certificado emitido hasta que se extinga el plazo de vigencia o hasta que fuera revocado. En caso que el certificado llegue a su fecha de expiración no se podrá confiar en dicho certificado.

El MIC custodiará toda la información referida al cese de operación del PSC, además publicará el cese de actividades o finalización del servicio del PSC responsable en su sitio principal de internet.

Abog. Jays Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

6. CONTROLES TÉCNICOS DE SEGURIDAD

En los ítems siguientes, la CPS debe definir las medidas de seguridad implementadas por el PSC responsable para proteger sus claves criptográficas y sus datos de activación, así como las claves criptográficas de los titulares de certificado. Deben también se definidos otros controles técnicos de seguridad utilizados por el PSC y por RA vinculadas en la ejecución de sus funciones operacionales.

6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

6.1.1. GENERACIÓN DEL PAR DE CLAVES

En este ítem, la CPS debe describir los requisitos y procedimientos referentes los procesos de generación de las claves criptográficas del PSC responsable. El par de claves criptográficas del PSC responsable para la CPS deberá ser generado por el propio PSC, posterior a la habilitación otorgada por el MIC vía resolución ministerial.

La CPS debe describir también los requisitos y procedimientos referentes al proceso de generación del par de calves criptográficas de las entidades solicitantes de certificado. El par de claves deberá ser generado solamente por el titular del certificado correspondiente. Los procedimientos específicos deben ser descriptos en cada CP implementada.

Cada CP implementada por el PSC responsable, debe definir el medio utilizado para el almacenamiento de la clave privada, en base a los requerimientos establecidos en el documento DIRECTIVAS OBLIGATORIAS PARA LA FORMULACIÓN Y ELABORACIÓN DE LA POLÍTICA DE CERTIFICACIÓN DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN (PSC)

6.1.2. ENTREGA DE LA CLAVE PRIVADA AL SUSCRIPTOR

Ítem no aplicable. La CPS debe indicar que la generación y guarda de una clave privada será responsabilidad exclusiva del titular del certificado correspondiente.

6.1.3. ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

En este ítem, la CPS debe describir los procedimientos utilizados por el PSC responsable para la entrega de su clave pública a la CA raíz encargada de la emisión de su certificado.

La CPS debe también describir los procedimientos utilizados para la entrega de la clave pública de un solicitante de certificado al PSC responsable. Los procedimientos específicos aplicables deben ser detallados en cada CP implementada.

6.1.4. ENTREGA DE LA CLAVE PÚBLICA DE LA CA A LAS PARTES QUE CONFÍAN

En este ítem, la CPS debe definir las formas para la disponibilización del certificado del PSC responsable, y de todos los certificados de la cadena de certificación, para los usuarios de la PKI Paraguay, la cual podrá comprender, entre otras:

a) En el momento de disponibilización de un certificado para su titular, usando el formato definido en el documento **NORMAS Y ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.**
b) Un directorio
c) Una página WEB del PSC; y
d) Otros medios seguros aprobados por el MIC.

6.1.5. TAMAÑO DE LA CLAVE

En este ítem, la CPS debe indicar que cada CP implementada por el PSC responsable definirá el tamaño de las claves criptográficas asociadas a los certificados emitidos, en base a los requerimientos aplicables establecidos por el documento **DIRECTIVAS OBLIGATORIAS PARA LA FORMULACIÓN Y ELABORACIÓN DE LA POLÍTICA DE CERTIFICACIÓN DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN (PSC)**

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

6.1.6. GENERACIÓN DE PARÁMETROS DE CLAVE ASIMÉTRICAS Y VERIFICACIÓN DE CALIDAD

La CPS debe prever que los parámetros de generación de claves asimétricas del PSC responsable adoptara el padrón definido en el documento **NORMAS Y ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.**

Los parámetros de verificación de calidad, deberán ser verificados de acuerdo con las normas establecidas por el patrón definido en el documento **NORMAS DE ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.**

6.1.7. PROPÓSITOS DE USOS DE CLAVE (CAMPO KEY USAGE X509 V3)

En este ítem, la CPS debe especificar los propósitos para los cuales podrán ser utilizadas las claves criptográficas de los titulares de los certificados emitidos por el PSC responsable, así como las posibles restricciones aplicables, de conformidad con las aplicaciones definidas para los certificados correspondientes. Cada CP implementada debe especificar los propósitos específicos aplicables.

La clave privada del PSC responsable deberá ser utilizada solamente para la firma de los certificados por ella emitidos y de sus CRL.

6.1.8. GENERACIÓN DE CLAVE POR HARWARE O SOFTWARE

En este ítem, la CPS debe indicar que el proceso de generación del par de claves del PSC responsable, deberá ser realizado en un módulo criptográfico de hardware que cumpla, como mínimo, con el estándar FIPS 140-2 nivel 3, similar o superior.

Cada CP implementada por el PSC responsable debe caracterizar el proceso utilizado para la generación de claves criptográficas de los titulares de certificados, en base a los requisitos aplicables establecidos por el documento **DIRECTIVAS OBLIGATORIAS PARA LA FORMULACIÓN Y ELABORACIÓN DE LA POLÍTICA DE CERTIFICACIÓN DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN (PSC)**

6.2 CONTROLES DE INGENIERÍA DEL MÓDULO CRIPTOGRÁFICO Y PROTECCIÓN DE LA CLAVE PRIVADA

En los ítems siguientes, la CPS debe definir los requisitos para la protección de las claves privada del PSC Responsable. Las claves privadas deberán ser

Abog. Rocío Rolón A.
DIRECTORA GENERAL
Firma Digital y Comercio Electrónico

cifradas en el envío del módulo que lo generó al medio utilizado para su almacenamiento. Cuando aplique, la CPS deben también definir los requisitos para proteger las claves privadas de las RA vinculadas y de las entidades titulares de certificados emitidos por el PSC. Cada CP implementada debe especificar los requisitos específicos aplicables.

6.2.1 ESTÁNDARES Y CONTROLES DEL MÓDULO CRIPTOGRÁFICO

La CPS debe prever que el módulo criptográfico de generación de claves asimétricas del PSC responsable adoptará los patrones definidos en el documento NORMAS Y ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.

La CPS debe también, cuando sea el caso, especificar los patrones - como por ejemplo, aquellas definidas en el documento NORMAS Y ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY - requerido para los módulos de generación de claves criptográficas de los titulares de certificado. Cada CP implementada debe especificar los requisitos adicionales aplicables.

6.2.2 CONTROL MULTI-PERSONA DE CLAVE PRIVADA

En este ítem, cuando sea el caso, debe ser definida la forma de control múltiple, de tipo "N" personas de un grupo "M", requerido para la utilización de las claves privadas.

La CPS debe establecer la exigencia de control multi-persona para la utilización de la clave privada del PSC responsable. Como mínimo serán requeridos 3(tres) de "M" titulares de activación de clave, formalmente designada por el PSC.

6.2.3 CUSTODIA/RECUPERACIÓN DE LA CLAVE PRIVADA

En este ítem, la CP debe indicar que no se permitirá, en el ámbito de la PKI Paraguay, almacenar clave privada del titular del certificado de firma digital (tipo F) emitido por el PSC.

6.2.4. RESPALDO/COPIA DE LA CLAVE PRIVADA

La CPS debe observar que, como directriz general, cualquier entidad titular de certificado, podrá, a su criterio, mantener una copia de su propia clave privada.

Abog. Rocio Rojón A.
DIRECTORA
Firma Digital y Comercio Electrónico

El PSC responsable de la CPS deberá mantener una copia de seguridad de su propia clave privada.

EL PSC no podrá mantener copia de seguridad de la clave privada del titular de certificado de firma digital por ella emitida.

Por solicitud del respectivo titular, o empresa u organización, cuando el titular del certificado es su empleado o cliente, el PSC podrá mantener una copia de seguridad de la clave privada correspondiente al certificado de cifrado por ella emitida. Cada CP debe definir los requisitos específicos aplicables.

En cualquier caso, la copia de seguridad deberá ser almacenada cifrada por un algoritmo simétrico definido en el documento **NORMAS Y ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY**, y protegida con un nivel de seguridad no inferior a aquel definido para la calve original.

6.2.5. ARCHIVADO DE LA CLAVE PRIVADA

En este ítem de la CPS, deben ser definidos, cuando sea el caso, los requisitos para el archivado de las claves privadas de cifrado. Las claves deberán ser archivadas en un nivel de seguridad no inferior a aquella definida para la clave original. No deben ser archivadas las claves privadas de la firma digital.

Defínase archivado como el almacenamiento de la clave privada para su uso futuro, después del periodo de validez del certificado correspondiente.

6.2.6. TRANSFERENCIA DE CLAVE PRIVADA HACIA O DESDE UN MÓDULO CRIPTOGRÁFICO

En este ítem de la CPS, deben ser descriptos los requisitos de transferencia de la clave privada del PSC responsable de un módulo criptográfico a otro. La RFC 2510 podrá ser utilizada para ese fin. Cada CP implementada debe definir, cuando sea aplicable, los requisitos de transferencia de la clave privada de los titulares del certificado de un módulo criptográfico a otro.

6.2.7. ALMACENAMIENTO DE LA CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO

La CPS debe indicar que el PSC responsable debe mantener almacenada su clave privada original y su copia de seguridad en módulos criptográficos de hardware que cumplan, como mínimo, con el estándar FIPS140-2 nivel 3.

El PSC no podrá mantener almacenada la clave privada del titular de certificado de firma digital por ella emitida.

Por solicitud del respectivo titular, o empresa u organización, cuando el titular del certificado es su empleado o cliente, el PSC podrá mantener almacenada una copia de la clave privada correspondiente al certificado de cifrado por ella emitida. Cada CP debe definir los requisitos específicos aplicables.

En cualquier caso, la clave privada deberá ser almacenada cifrada por un algoritmo simétrico definido en el documento **NORMAS Y ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.**

6.2.8. MÉTODO DE ACTIVACIÓN DE CLAVE PRIVADA

En este ítem de la CPS deben ser descriptos los requisitos y procedimientos necesarios para la activación de la clave privada del PSC responsable. Deben ser definidos los agentes autorizados a activar esa clave, el método de confirmación de identidad de esos agentes (contraseñas, tokens o biometría) y las acciones necesarias para la activación. Cada CP implementada debe describir los requisitos y procedimientos necesarios para la activación de la clave privada de la entidad titular de certificado.

6.2.9. MÉTODOS DE DESACTIVACIÓN DE LA CLAVE PRIVADA

En este ítem de la CPS, deben ser descriptos los requisitos y procedimientos necesarios para la desactivación de la clave privada del PSC responsable. Deben ser definidos los agentes autorizados a activar esa clave, el método de confirmación de identidad de esos agentes y las acciones necesarias. Cada CP implementada debe describir los requisitos y procedimientos necesarios para la desactivación de la clave privada de la entidad titular de certificado.

6.2.10. DESTRUCCIÓN DE CLAVE PRIVADA

En este ítem de la CPS, deben ser descriptos los requisitos y procedimientos necesarios para la destrucción de la clave privada del PSC responsable y de sus copias de seguridad. Deben ser definidos los agentes autorizados, el método de confirmación de identidad de esos agentes y las acciones necesarias, tal como la destrucción física, la sobre-escritura o la eliminación de los medios de almacenamiento. Cada CP implementada debe describir los requisitos y

procedimientos necesarios para destrucción de la clave privada de la entidad titular de certificado.

6.2.11. CLASIFICACIÓN DEL MÓDULO CRIPTOGRÁFICO

En este ítem la CPS debe indicar que la capacidad del módulo criptográfico del PSC responsable deberá ser expresada en cumplimiento como mínimo del estándar FIPS 140-2, nivel 3. Cuando sea el caso, la CP implementada debe describir la clasificación del módulo criptográfico utilizado por las entidades titulares de los certificados.

6.3. OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES

6.3.1. ARCHIVO DE LA CLAVE PÚBLICA

La CPS debe prever que las claves públicas del PSC responsable y de los titulares de los certificados de firma digital, así como las CRL emitidas, serán almacenadas por el PSC emisor, después de la expiración de los certificados correspondientes, permanentemente, para la verificación de firmas generadas durante su periodo de validez.

6.3.2. PERÍODO OPERACIONAL DEL CERTIFICADO Y PERÍODO DE USO DEL PAR DE CLAVES

La clave privada del PSC responsable de la CPS y de los titulares de certificados de firma digital, deberá ser utilizada únicamente durante el periodo de validez estipulado en el ítem 5.6. La clave pública podrá ser utilizada durante todo el periodo de tiempo determinado por la normativa vigente, para la verificación de firmas generadas durante el plazo de validez de los respectivos certificados.

Los periodos de uso de las claves correspondientes a los certificados de cifrado emitidos por el PSC responsable de la CPS deben ser definidos en las respectivas CP.

Cada CP implementada por el PSC responsable debe definir el periodo máximo de validez del certificado que define, con base a los requisitos aplicables establecidos en el documento DIRECTIVAS OBLIGATORIAS PARA LA FORMULACIÓN Y ELABORACIÓN DE LA POLÍTICA DE CERTIFICACIÓN DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN (PSC)

6.4 DATOS DE ACTIVACIÓN

En los siguientes ítems de la CPS, deben ser descriptos los requerimientos generales de seguridad referentes a los datos de activación. Los datos de activación, distintos a las claves criptográficas, son aquellas requeridas para la operación de algunos módulos criptográficos, la CP implementada debe describir los requisitos específicos aplicables.

6.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

La CPS debe garantizar que los datos de activación de la clave privada del PSC responsable, serán únicos y aleatorios.

La CP debe garantizar que los datos de activación de la clave privada del titular del certificado, serán únicos y aleatorios.

6.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

La CPS debe garantizar que los datos de activación de la calve privada del PSC responsable, serán protegidos contra el uso no autorizado, por medios de criptografía y de control físico.

Cada CP implementada debe garantizar que los datos de activación de la clave privada

6.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

En este ítem de la CPS, deben ser definidos, otros aspectos referentes a los datos de activación. Entre esos otros aspectos pueden ser considerados algunos de aquellos tratados, en relación de las claves, en los ítems 6.1 al 6.3.

6.5 CONTROLES DE SEGURIDAD DEL COMPUTADOR

6.5.1 REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS

La CPS debe prever que la generación del par de claves del PSC responsable será realizada offline para impedir el acceso remoto no autorizado.

En este ítem, la CPS debe también describir los requisitos generales de seguridad computacional del equipamiento donde será generado el par de claves

criptográficas de los titulares de certificados emitidos por el PSC responsable. Los requisitos específicos aplicables deben ser descriptos en cada CP implementada.

Cada computador del PSC responsable, relacionado directamente con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificado, deberá implementar, entre otras, las siguientes características:

a) Control de acceso a los servicios y perfiles del PSC;
b) Clara segregación de tareas y atribuciones relacionadas con cada rol de confianza del PSC;
c) Uso de criptografía para seguridad de base de datos, cuando sea requerido por la clasificación de su información;
d) Generación y almacenamiento de registros de auditoria dl PSC;
e) Mecanismos internos de seguridad para garantizar la integridad de datos y procesos críticos; y
f) Mecanismos para copias de seguridad (*backup*).

Estas características deberán ser implementadas por el sistema operativo o por medio de combinación de este con el sistema de certificación y con mecanismos de seguridad física.

Cualquier equipo o parte del mismo, para ser sometidos a mantenimiento deberán haber borrado la información confidencial que contenga y controlar su número de serie y las fechas de envío y recepción. Al regresar a las instalaciones del PSC, el equipo que fue sometido a mantenimiento debe ser inspeccionado. Cualquier equipo que ya no se utilice de forma permanente, deberán ser destruidas de él, de manera definitiva, todas las informaciones sensibles almacenadas, relativas a la actividad del PSC. Todos estos eventos deberán ser registrados con fines de auditoría.

Cualquier equipo incorporado en el PSC será preparado y configurado según lo previsto en la política de seguridad implementada u otro documento relevante con el fin de mostrar el nivel de seguridad requerido para su propósito.

6.5.2 CLASIFICACIÓN DE LA SEGURIDAD DEL COMPUTADOR

En este apartado de la CPS, debe ser informado, cuando esté disponible, la calificación atribuida a la seguridad computacional de la CA responsable, de acuerdo con criterios tales como: *Trusted System Evaluation Criteria* (TCSEC),

Canadian Trusted Products Evaluation Criteria, European Information Technology Security Evaluation Criteria (ITSEC) o *Common Criteria*.

6.5.3. CONTROLES DE SEGURIDAD PARA AS AUTORIDADES DE REGISTRO

En este ítem, la CPS debe describir los requisitos de seguridad computacional de las estaciones de trabajo y de los computadores portátiles utilizados por la RA para los procesos de validación y aprobación de certificados.

Deben ser incluidos, por lo menos, los requisitos especificados en el documento **CARACTERÍSTICAS MINÍMAS DE SEGURIDAD PARA LAS RA DE LA PKI PARAGUAY.**

6.6 CONTROLES TÉCNICOS DEL CICLO DE VIDA

En los ítems siguientes de la CPS, deben ser descriptos, cuando sea aplicable, los controles implementados por el PSC responsable y por las RA a ella vinculadas en el desarrollo de sistemas y en la gestión de la seguridad.

6.6.1 CONTROLES PARA EL DESARROLLO DEL SISTEMA

En esta sección de la CPS, deben ser abordados aspectos tales como: seguridad del ambiente y del personal de desarrollo, prácticas de ingeniería del software adoptadas, metodología de desarrollo de software, entre otros, aplicados al software del sistema de certificación del PSC responsable o cualquier otro software desarrollado o utilizado por el PSC responsable.

Los procesos de proyecto de desarrollo conducidos por el PSC, deberá proveer documentación suficiente para soportar evaluaciones de seguridad externas de los componentes del PSC.

6.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD

En este ítem de la CPS deben ser descriptos, las herramientas y los procedimientos empleados por el PSC responsable y por las RA vinculadas, para garantizar que sus sistemas y redes operacionales, implementen los niveles de configuración de seguridad.

Una metodología formal de gerenciamiento de configuración deberá ser usada para la instalación y el continuo mantenimiento del sistema de certificación del PSC.

6.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

En este ítem, la CPS debe informar, cuando esté disponible, el nivel de madurez asignado al ciclo de vida de cada sistema, basado en criterios tales como: *Trusted Software Development Methodology* (TSDM) ou o *Capability Maturity Model* do *Software Engineering Institute* (CMM-SEI).

6.6.4. CONTROLES EN LA GENERACIÓN DE CRL

Antes de su publicación, todas las CRL generadas por el PSC, debe ser comprobada la consistencia de su contenido, comparándolo con el contenido esperado en relación al número de CRL, la fecha / hora de emisión y otra informaciones relevantes.

6.7 CONTROLES DE SEGURIDAD DE RED

6.7.1. DIRECTRICES GENERALES

En este ítem de la CPS, deben ser descriptos los controles relativos a la seguridad de red del PSC responsable, incluidos firewalls y recursos similares.

En los servidores del sistema de certificación del PSC, sólo los servicios estrictamente necesarios para el funcionamiento de la aplicación deben estar habilitados.

Todos los servidores y elementos de la infraestructura y protección de redes, tales como ruteadores, hubs, switches, firewalls y sistemas de detección de intrusos (IDS), localizados en el segmento de red en que se hospeda el sistema de la certificación del PSC, deberán estar localizados y operar en un ambiente de nivel, como mínimo, 4(cuatro).

Las últimas versiones de los sistemas operativos y servidores de aplicaciones, así como las eventuales correcciones (parches), disponibilizadas por los respectivos fabricantes deberán ser implementadas inmediatamente después del testeo en el ambiente de homologación.

El acceso lógico a los elementos de la infraestructura y protección de la red deberán restringirse por medio de un sistema de autenticación y autorización de acceso. Los Routeadores conectados a redes externas deberán implementar filtros

de paquetes de datos, que sólo permitan conexiones a los servicios y servidores previamente definidos como objeto de acceso externo.

6.7.2. FIREWALL

Mecanismos de firewall se deberán implementar en equipos de uso específico, configurados exclusivamente para esa función. Un firewall deberá promover el aislamiento, en subredes específicas, de los equipos servidores con acceso externo - la denominada "zona desmilitarizada" (DMZ) - en relación a los equipos con acceso exclusivamente interno al PSC.

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

6.7.3. SISTEMA DE DETECCIÓN DE INTRUSO (IDS)

El sistema de detección de intruso deberá tener la capacidad de ser configurado para reconocer ataques en tiempo real y responder automáticamente, con medidas tales como: enviar traps SNMP, ejecutar programas definidos por la administración de redes, enviar e-mail a los administradores, enviar mensajes de alerta al firewall o al terminal de gerenciamiento, promover la desconexión automática de conexiones sospechosas, o la reconfiguración del firewall.

El sistema de detección de intrusiones deberá ser capaz de reconocer diferentes patrones de ataques, incluso contra el propio sistema, con la posibilidad de actualizar su base de reconocimiento.

El sistema de detección de intruso deberá proveer un registro de los eventos en logs, recuperables en archivos de tipo texto, e implementar una gestión de la configuración.

6.7.4. REGISTRO DE ACCESO NO AUTORIZADO A LA RED

Las tentativas de acceso no autorizado en routeadores, Firewall u IDs- deberán ser registradas en archivos para posterior análisis, que podrá ser automatizada. La frecuencia de examen de los archivos de registro deberá ser, como mínimo, diario y todas las acciones tomadas como resultado de este examen debe ser documentada.

6.8. CONTROLES DE INGENIERÌA DEL MODULO CRIPTOGRÀFICO

En este ítem, la CPS deberá describir los requisitos aplicables para el módulo criptográfico utilizado para almacenar la clave privada del PSC responsable. Podrán ser indicados patrones de referencia, tales como los definidos en el documento **NORMAS Y ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.**

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

7. PERFILES DE CERTIFICADOS, CRL Y OCSP

En los siguientes ítems de la CPS, deben ser descriptos los aspectos de los certificados y CRL emitidos por el PSC responsable.

Cada CP implementada por el PSC responsable, deberá especificar los formatos de los certificados generados y las correspondientes CRL, deben ser incluidos informaciones sobre los patrones adoptados, sus perfiles, versiones y extensiones.

7.1. PERFIL DEL CERTIFICADO

Todos los certificados emitidos por el PSC responsable deberán estar en conformidad con el formato definido por el estándar ITU X.509 o ISO/IEC 9594-8.

7.1.1. NÚMERO DE VERSIÓN

Todos los certificados emitidos por el PSC responsable deberán implementar la versión 3 (tres) del estándar ITU X.509, de acuerdo con el perfil establecido en la RFC 5280.

7.1.2. EXTENSIONES DEL CERTIFICADO

La PKI Paraguay define como obligatorias las siguientes extensiones para los certificados del PSC (PSC):

a) "***Authority Key Identifier***", **no crítica:** el campo key Identifier debe contener el hash SHA- 1 de la clave pública del PSC que emite el certificado;
b) "***Subject Key Identifier***", **no crítica**: debe contener el hash SHA- 1 de la clave pública del PSC titular do certificado;
c) "***Key Usage***", **crítica**: solamente los bits keyCertSign e cRLSign deben estar activados;
d) "***Certificate Policies***", **no crítica**: el campo debe contener el OID de la CP que el PSC titular del certificado implementa y/o la dirección la dirección URL donde se encuentra disponible.
e) "***Basic Constraints***", **crítica**: debe contener el campo SubjectType CA=True y el campo PathLenConstraint debe tener valor cero; y
f) "**CRL Distribution Points**", **no crítica**: debe contener la URL donde está disponible el certificado de CRL.

Abog. Rocys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

7.1.3. IDENTIFICADORES DE OBJETO DE ALGORÍTMOS

Los certificados del PSC deben ser firmados utilizando el algoritmo definido en el documento **NORMAS Y ALGORÍTMOS CRIPTOGRÁFICOS DE LA PKI PARAGUAY.**

7.1.4. FORMAS DEL NOMBRE

Los nombres del PSC titular del certificado, que consta el campo *"Subject"*, deberá adoptar el *"Distinguished Name"* (DN) del estándar ITU X.500/ISO 9594, como ejemplo, la siguiente forma:

Tabla N° 6 – Formas de nombre.

Campo	Ejemplo	Descripción
Country (C)	PY	Código de país es asignado de acuerdo al estándar ISO 3166
Organization (O)	Firma Fiel SA	Denominación o Razón Social de la Persona Jurídica habilitada como PSC
Common Name (CN)	CA – Firma Fiel SA	CA + Nombre de la CA
Serial Number {OID: 2.5.4.5}	RUC 99999999-9	RUC Número de Cédula Tributaria correspondiente al PSC. Debe ser validada durante el proceso de registro.

7.1.5. RESTRICCIONES DEL NOMBRE

En este ítem de la CPS, deben ser descriptas las restricciones aplicables para los nombres del PSC, titulares de certificados, de conformidad con las restricciones generales establecidas por la PKI Paraguay en el documento **DIRECTIVAS OBLIGATORIAS PARA LA FORMULACIÓN Y ELABORACIÓN DE LA POLÍTICA DE CERTIFICACIÓN DEL LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN (PSC)**

Abog. Rocys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

7.1.6. IDENTIFICADOR DE OBJETO DE POLÍTICA DE CERTIFICADO

En este ítem, debe ser informado el OID de la CPS.

7.1.7. USO DE LA EXTENSIÓN RESTRICCIONES DE POLÍTICA (POLICY CONSTRAINTS)

Este Ítem no aplica.

7.1.8. SEMÁNTICA Y SINTAXIS DE LOS CALIFICADORES DE POLÍTICA (POLICY QUALIFIERS)

En los certificados del PSC, la extensión *"Certificate Policies"*, deberá contener la URL de la CPS del PSC que emite el certificado.

7.1.9. SEMÁNTICA DE PROCESAMIENTO PARA LA EXTENSIÓN DE POLÍTICAS DE CERTIFICADO (CERTIFICATE POLICIES)

Este Ítem no aplica.

7.2. PERFIL DE LA CRL

7.2.1 NÚMERO (S) DE VERSIÓN

Las CRL generadas por el PSC responsable deberán implementar la versión 2 del estándar ITU X.509, de acuerdo con el perfil establecido en el RFC 5280.

7.2.2 CRL Y EXTENSIONES DE ENTRADAS DE CRL

7.2.2.1 Número CRL (CRL Number)

En este ítem, la CPS debe indicar que utiliza una orden secuencial de emisión de CRL. Esta extensión es crítica

7.2.2.2 Identificador de clave de Autoridad

En este ítem, la CPS debe indicar que el método para la generación del identificador está basado en la clave pública del PSC responsable contenida en el certificado, de acuerdo a lo descrito por el RFC 5280. La extensión no es crítica.

7.3 PERFIL DE OCSP

El servicio de validación de certificados en línea OCSP (Online Certificate Status Protocol) es una forma para obtener información reciente sobre el estado de un certificado. El servicio OCSP que implemente el PSC responsable, debe cumplir con lo estipulado en el RFC-2560 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

7.3.1 NÚMERO (S) DE VERSIÓN

Debe cumplir al menos con la versión 1 del RFC2560 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".

7.3.2 EXTENSIONES DE OCSP

Sin estipulaciones.

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

El Art. 42 de la Ley Nro. 4017/2010 establece que los PSC, deben ser auditados periódicamente, de acuerdo con el sistema de auditoría que diseñe y apruebe el MIC.

Por Resolución Ministerial se establece el sistema de auditoría al cual será sometido el PSC.

Todo PSC está obligado al cumplimiento de las auditorías, éstas permiten establecer una confianza razonable en el marco de la PKI Paraguay. El proceso de auditoría incluye entre otras: Revisión de seguridad y de prácticas, las cuales incluyen instalaciones, documentos de seguridad, declaración de prácticas de certificación, acuerdos entre las partes, política de privacidad y validación de los planes para asegurar el cumplimiento de estándares.

El MIC o terceros designados por él, será responsable de ejecutar las auditorias, de acuerdo a lo estipulado en la normativa vigente.

Cada PSC, debe implementar un programa de auditorías internas conforme a lo estipulado en el sistema de auditoria que diseñe el MIC y lo establecido en el ítem 18 "cumplimiento" de la norma ISO 27002/2013 para la verificación de su sistema de gestión.

La disposición o resolución que ordena una Auditoría o evaluación no será recurrible.

8.1 FRECUENCIA O CIRCUNSTANCIAS DE EVALUACIÓN

En este ítem, la CPS deben indicar que la auditoría externa al PSC responsable se deberá ejecutar al menos una vez al año y los costos deben ser asumidos por este PSC.

Además la CPS debe indicar de conformidad al programa de auditoría interna de cada PSC, la frecuencia o circunstancias de su realización, que como mínimo, deberán ser ejecutadas al menos vez al año.

8.2 IDENTIDAD/CALIDADES DEL EVALUADOR

En este ítem, la CPS debe describir las cualidades del equipo de Auditoría (Interna o externa), que de modo general debe estar conformado por personal calificado con experiencia en tecnología de la información, seguridad, tecnología de PKI y criptografía.

Abog. Dario Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

8.3 RELACIÓN DEL EVALUADOR CON LA ENTIDAD EVALUADA

En este ítem, la CPS debe indicar que para el caso de las auditorías externas, los auditores deberán ser independientes e imparciales y que deberán ejecutar las evaluaciones acorde a los procedimientos establecidos.

En este ítem, la CPS también debe indicar que para el caso de las auditorías internas, los auditores deberán ser independientes funcionalmente del área objeto de evaluación.

8.4 ASPECTOS CUBIERTOS POR LA EVALUACIÓN

En este ítem, la CPS debe también describir los aspectos cubiertos por la evaluación, que como mínimo, deberá contemplar:

a) Controles de seguridad física y estándares técnicos de seguridad;
b) Confidencialidad y calidad de los sistemas de control;
c) Integridad y disponibilidad de los datos;
d) Cumplimiento de los estándares tecnológicos;
e) Seguridad del personal;
f) Cumplimiento de la política y declaración de prácticas de certificación;
g) Procesos de certificación de clave pública;
h) Política de seguridad y privacidad;
i) Controles administrativos del PSC;
j) Administración de los servicios del PSC; y
k) Revisión de contratos.

8.5 ACCIONES TOMADAS COMO RESULTADO DE UNA DEFICIENCIA

En este ítem, la CPS debe describir los procedimientos que el PSC responsable y las RA vinculadas a ella, deben ejecutar para realizar acciones correctivas en base a las deficiencias detectadas tanto en las Auditorías externas como en las internas.

En caso de detectarse una irregularidad en la Auditoría externa realizada al PSC, podrán tomarse entre otras las siguientes acciones dependiendo de la gravedad de la misma:

a) indicar las irregularidades, pero permitir al PSC responsable o a las RA vinculadas que continúen sus operaciones hasta la próxima auditoría programada;
b) permitir al PSC responsable o a las RA vinculadas que continúen sus

operaciones con un máximo de treinta días corridos, tiempo durante el cual deberá subsanar la irregularidad detectada, caso contrario se procederá a la suspensión; o

c) Suspender la operación del PSC responsable o a las RA vinculadas.

En caso que se ordene la suspensión de actividades del PSC Responsable, esta solo podrá realizar servicios de soporte técnico y atención a los titulares de certificados ya existentes, en ningún caso podrá seguir brindando servicios de certificación.

8.6 COMUNICACIÓN DE RESULTADOS

En este ítem, la CPS debe indicar que el PSC responsable deberá publicar en su sitio principal de internet los informes relevantes de las auditorías realizadas

Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

9. OTROS ASUNTOS LEGALES Y COMERCIALES

9.1 TARIFAS

En los siguientes ítems, deben ser especificados por el PSC responsable de la CPS, las políticas tarifarias y reembolso aplicables según la norma que rige la materia. Caso que sean aplicadas tarifas específicas para las CP implementadas, las mismas deben ser descriptas en las CP, en el ítem correspondiente.

9.1.1 TARIFAS DE EMISIÓN Y ADMINISTRACIÓN DE CERTIFICADOS

9.1.2 TARIFAS DE ACCESO A CERTIFICADOS

9.1.3 TARIFAS DE ACCESO A INFORMACIÓN DEL ESTADO O REVOCACIÓN

9.1.4 TARIFAS POR OTROS SERVICIOS

9.1.5 POLÍTICAS DE REEMBOLSO

9.2 RESPONSABILIDAD FINANCIERA

9.2.1 COBERTURA DE SEGURO

En este apartado, la CPS debe describir los aspectos relativos a la cobertura de seguro que posee el PSC responsable como un medio de garantía suficiente para cubrir las actividades inherentes a su gestión de conformidad con lo establecido en la normativa vigente.

9.2.2 OTROS ACTIVOS

En este ítem de la CPS, se debe hacer referencia a los recursos financieros suficientes que posee el PSC responsable para mantener sus operaciones y ejecutar sus deberes, asimismo debe ser razonablemente capaz de administrar el riesgo de responsabilidad para los suscriptores y partes que confían.

9.2.3 COBERTURA DE SEGURO O GARANTÍA PARA USUARIOS FINALES

En este ítem de la CPS, en el caso que aplique, deben describirse los aspectos relativos a la cobertura de seguro o garantía disponible para los suscriptores.

Caso que sean aplicadas cobertura de seguro o garantía para usuarios finales específicos para las CP implementadas, las mismas deben ser descriptas en las CP, en el ítem correspondiente.

9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

La clave privada de firma digital del PSC responsable de la CPS, será generada y mantenida por el propio PSC, que será responsable de mantener su confidencialidad. La divulgación o utilización indebida de la clave privada de firma digital por el PSC, será de su entera responsabilidad.

La CPS debe informar que los titulares de certificados emitidos para personas físicas o sus responsables para el uso de los certificados emitidos para personas jurídicas, equipos o aplicaciones, tendrán las atribuciones de generación, y confidencialidad de sus respectivas claves privadas. Además, es responsable de la divulgación o utilización de dichas claves privadas. Cuando existan responsabilidades específicas para las CP implementadas, las mismas deben ser descriptas en esas CP, en el ítem correspondiente.

9.3.1 ALCANCE DE LA INFORMACIÓN CONFIDENCIAL

En este ítem, deben ser identificados los tipos de informaciones consideradas confidenciales por el PSC responsable de la CPS y de las RA vinculadas, de acuerdo con las normas, criterios, prácticas y procedimientos de la PKI Paraguay.

La CPS debe establecer, como principio general, que ningún documento, información o registro entregado al PSC o a las RA vinculada deberán ser divulgados.

9.3.2 INFORMACIÓN NO CONTENIDA EN EL ALCANCE DE INFORMACIÓN CONFIDENCIAL

En este ítem deben ser indicados los tipos de informaciones consideradas NO confidenciales por el PSC responsable de la CPS y por las RA a ellas vinculadas, los cuales deberán comprender, entre otros:

a) los certificados y las CRL emitidas por la CA;
b) Las CP implementadas por el PSC;
c) La CPS del PSC;
d) La versiones públicas de la PSS; y
e) La conclusión de los informes de auditoría.

Abog. Rocys Rolon A.
Dirección General
Firma Digital y Comercio Electrónico

9.4 PRIVACIDAD DE INFORMACIÓN PERSONAL

9.4.1 PLAN DE PRIVACIDAD

En este ítem de la CPS, deben ser descriptas las políticas de privacidad de información, implementadas por el PSC responsable y las RA vinculadas a ella, de

acuerdo con la normativa vigente. No se puede divulgar o vender información de los titulares de los certificados o información de identificación de éstos.

9.4.2 INFORMACIÓN TRATADA COMO PRIVADA

En este ítem deben ser identificados los tipos de informaciones tratadas como privada por el PSC responsable de la CPS y de las RA vinculadas, de acuerdo con las normas, criterios, prácticas y procedimientos de la PKI Paraguay.

La CPS debe establecer, como principio general, que ningún documento, información o registro entregado al PSC o a las RA vinculada deberán ser divulgadas, salvo aquellas que figuran en el certificado.

9.4.3 INFORMACIÓN QUE NO ES CONSIDERADA COMO PRIVADA

En este ítem deben ser identificados los tipos de informaciones consideradas como no privada por el PSC responsable de la CPS y de las RA vinculadas, de acuerdo con las normas, criterios, prácticas y procedimientos de la PKI Paraguay. Algunos de ellos se citan en la sección 9.3.2.

9.4.4 RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA

En este ítem de la CPS, deben ser descriptas las responsabilidades que están consignadas al personal que desempeñe labores en el PSC responsable, RA vinculadas y a toda persona que tenga acceso a los datos considerados privados.

9.4.5 NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA

En este ítem deben ser descriptas las condiciones en que, el titular del certificado, podrá tener acceso a cualquiera de sus datos de identificación, o podrá autorizar la divulgación de sus registros a otras personas.

La CPS debe establecer que cualquier liberación de información por el PSC responsable o por las RA vinculada solamente será permitida mediante autorización formal del titular del certificado. Las formas de presentación de esa autorización deben ser definidas por la CPS.

9.4.6 DIVULGACIÓN DE ACUERDO CON UN PROCESO JUDICIAL O ADMINISTRATIVO

Este ítem, debe establecer el deber del PSC responsable de la CPS de proporcionar documentos, informaciones o registros bajo su custodia, mediante una orden judicial.

Abog. Rocys Rolón A.
Director General
Firma Digital y Comercio Electrónico

9.4.7 OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN

En este ítem de la CPS, deben ser descriptas, cuando sea apropiado, cualquier otra circunstancia en que podrán ser divulgadas informaciones de carácter privado.

9.5 DERECHO DE PROPIEDAD INTELECTUAL

En este ítem de la CPS, deben ser tratadas las cuestiones referentes a los derechos de propiedad intelectual de los certificados, políticas, prácticas de certificación, nombres y claves criptográficas, de acuerdo a la legislación vigente.

9.6 REPRESENTACIONES Y GARANTÍAS

9.6.1 REPRESENTACIONES Y GARANTÍAS DEL PSC

En este ítem, deben ser incluidas las obligaciones del PSC responsable de la CPS, conteniendo, como mínimo, las consideraciones mencionadas a continuación:

a) operar de acuerdo a su CPS y CP que implementa;
b) generar y gestionar sus pares de claves criptográficas;
c) asegurar la protección de sus claves privadas;
d) notificar a la CA raíz, emisor de su certificado, cuando se presenta el compromiso de su clave privada y solicitar la revocación inmediata del correspondiente certificado;
e) notificar a sus usuarios cuando hay una sospecha de compromiso de su clave privada o una nueva emisión de su par de claves o la terminación de prestación de su servicio;
f) distribuir su propio certificado;
g) emitir, expedir y distribuir los certificados de las RA a ellas vinculadas, y de los usuarios finales;
h) informar la emisión del certificado al respectivo solicitante;
i) revocar los certificados por el emitidos;
j) emitir, gerenciar y publicar sus CRL y disponibilizar la consulta online de la situación de los certificados emitidos (OCSP - On-line Certificate Status Protocol);
k) publicar, en su sitio principal internet, su CPS, y las CP aprobadas que implementa;
l) publicar, en su sitio principal de Internet, las informaciones definidas en el ítem 2.2. de este documento;
m) publicar, en su sitio principal internet, las informaciones sobre la desvinculación de una RA, así como la extinción de la instalación técnica.

Abog. Roque Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

n) utilizar protocolo de comunicación segura para proporcionar servicios a los solicitantes y usuarios de certificados digitales a través de la web;
o) identificar y registrar todas las acciones ejecutadas, conformes a las normas, prácticas y reglas establecidas por el MIC.
p) adoptar las medidas de seguridad y de control previstas en la CPS, CP y políticas de seguridad (PS) que se implementa, con sujeción a las normas, criterios, prácticas y procedimientos establecidos por el MIC.
q) mantener el cumplimiento de sus procesos, procedimientos y actividades con las normas, prácticas y reglas establecidos por el MIC y la normativa vigente;
r) mantener y garantizar la integridad, confidencialidad y seguridad de la información por ella tratada;
s) mantener y anualmente realizar prueba de su Plan de Continuidad de Negocios (PCN);
t) mantener el contrato de seguro de responsabilidad civil resultante de las actividades de certificación digital y de registro, con una cobertura suficiente y compatible con el riesgo de estas actividades.
u) informar a terceras partes y los titulares de certificados sobre las garantías, cobertura, condiciones y limitaciones establecidas a la póliza de seguro de responsabilidad civil contraída en los términos indicado en el inciso t) de este ítem;
v) informar a la CA raíz , mensualmente, la cantidad de certificados digitales emitidos y revocados;
w) no emitir el certificado con una fecha de caducidad que se extienda más allá de la fecha de vencimiento de su propio certificado.

9.6.2 REPRESENTACIONES Y GARANTÍAS DE LA RA

En este apartado de la CPS, deben ser incluidas las obligaciones de las RA vinculadas al PSC responsable de la CPS, conteniendo, como mínimo, las consideraciones mencionadas a continuación:

a) recibir las solicitudes de emisión y revocación de los certificados;
b) confirmar la identidad del solicitante y validar la solicitud;
c) comunicar la solicitud de emisión o revocación del certificado al PSC responsable utilizando un protocolo de comunicación segura, conforme al patrón definido en el documento. **CARACTERÍSTICAS MÍNIMAS DE SEGURIDAD PARA LAS RA DE LA PKI PARAGUAY.**
d) informar a los respectivos titulares la emisión o revocación de sus certificados;
e) proporcionar los certificados emitidos por el PSC a sus respectivos solicitantes;

Abog. Pedro Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

f) identificar y registrar todas las acciones ejecutadas, conforme a las normas, prácticas y reglas establecidas por le MIC y la normativa vigente;
g) mantener el cumplimiento de sus procesos, procedimientos y actividades con las normas, criterios, prácticas y reglas establecidas por el PSC vinculado, el MIC y en especial con lo contenido en el documento **CARACTERÍSTICAS MÍNIMAS DE SEGURIDAD PARA LAS RA DE LA PKI PARAGUAY**;
h) mantener y garantizar la seguridad de la información por ella tratada, de acuerdo a lo establecido en las normas, criterio, prácticas y procedimientos establecidos por el MIC;
i) mantener y anualmente realizar prueba de su Plan de Continuidad de Negocios (PCN);
j) proceder al reconocimiento de las firmas y de la validez de los documentos presentados en la forma de los ítems 3.2.2, 3.2.3 y 3.2.4.
k) garantizar que todas las aprobaciones de la solicitud de certificados sean realizadas en las instalaciones técnicas autorizadas para funcionar como RA.

9.6.3 REPRESENTACIONES Y GARANTÍAS DEL SUSCRIPTOR

En este ítem deben ser incluidas las obligaciones de los titulares del certificado, emitidos por el PSC responsable de la CPS, tal como se establece en **el acuerdo de suscriptores**, debiendo incluir, como mínimo, las consideraciones mencionadas a continuación:

a) proporcionar, de manera completa y precisa, toda la información necesaria para su identificación;
b) garantizar la protección y confidencialidad de sus claves privadas, contraseñas y dispositivos criptográficos;
c) utilizar sus certificados y claves privadas de una manera apropiada, según lo dispuesto en la CP correspondiente;
d) conocer sus derechos y obligaciones, contemplados por la CPS y CP correspondiente y otros documentos aplicables la PKI Paraguay; y
e) informar al PSC emisora cualquier compromiso de su clave privada y solicitar la revocación inmediata del certificado correspondiente.

En el caso de certificado emitido a las personas jurídicas, equipo o aplicación, estas obligaciones se aplican al responsable del uso certificado.

9.6.4 REPRESENTACIONES Y GARANTÍAS DE LAS PARTES QUE CONFÍAN

La parte que confía, es aquel que confía en el contenido, validez y aplicabilidad del certificado digital.
Constituyen derechos de la tercera parte:

a) negarse a utilizar el certificado para fines distintos de los previstos en la CP correspondiente.
b) comprobar, en cualquier momento, la validez del certificado. Un certificado emitido por un PSC integrante de la PKI Paraguay es considerado valido cuando:
   I. no figura en la CRL del PSC emisor;
   II. no estuviera expirado; y
   III. se pueda verificar usando el certificado válido del PSC emisor.

La falta de ejercicio de estos derechos no elimina la responsabilidad del PSC responsable y del titular del certificado.

9.6.5 REPRESENTACIONES Y GARANTÍAS DEL REPOSITORIO

En este ítem deben ser incluidas las obligaciones del directorio, entre ellas:

a) disponibilizar, inmediatamente después de su emisión, los certificados emitidos por el PSC y su CRL.
b) estar disponible para consulta durante 24 (veinticuatro) horas al día, siete (7) días a la semana; y
c) aplicar los recursos necesarios para la seguridad de los datos almacenados en él.

9.6.6 REPRESENTACIONES Y GARANTÍAS DE OTROS PARTICIPANTES

Este ítem no aplica.

9.7 EXENCIÓN DE GARANTÍA

En este ítem la CPS debe indicar cualquier exención de responsabilidad que pudiera aplicar un PSC.

9.8 LIMITACIONES DE RESPONSABILIDAD LEGAL

En este ítem, la CPS debe indicar, si es el caso, las limitaciones de responsabilidad legal aplicables, conforme a las normas generales de la responsabilidad civil y lo establecido en la Ley 4017/2010

9.9 INDEMNIZACIONES

En este ítem, la CPS debe indicar cualquier limitación de responsabilidad que pudiera aplicársele considerando las responsabilidades de privacidad, seguridad y diligencia en los procesos de certificación establecidas en su CPS y CP vinculadas.

Abog. Paola Rolón A.
DIRECTORA GENERAL
Firma Digital y Comercio Electrónico

9.10 PLAZO Y FINALIZACIÓN

9.10.1 PLAZO

En este ítem, la CPS debe establecer el plazo en que entra en vigencia la CPS del PSC. De la entrada en vigencia deberá ser posterior a la aprobación del mencionado documento, por el Ministerio de Industria y Comercio por resolución Ministerial.

9.10.2 FINALIZACIÓN

En este ítem, la CPS debe establecer las condiciones en el cual la CPS del PSC estará en vigencia y las condiciones de su derogación o cambio.

9.10.3. EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA

En este ítem la CPS debe indicar los efectos de la finalización de la vigencia de la CPS del PSC.

9.11. NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON PARTICIPANTES

En este ítem de la CPS, deben ser descriptos los métodos de notificación y comunicación utilizados por el PSC responsable y por las RA vinculadas; podrán ser realizados mediante mensaje electrónico o por escrito mediante correo dirigido a cualquiera de las direcciones contenidas en el punto 1.5 Administración de las Políticas.

9.12. ENMIENDAS

9.12.1. PROCEDIMIENTOS PARA ENMIENDAS

En este ítem, deben ser descriptos los procedimientos utilizados por el PSC responsable de la CPS para realizar enmiendas. Estos cambios deben ser revisados y aprobados por el Ministerio de Industria Comercio, antes de ser implementados.

9.12.2. PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN

En este ítem, deben ser descriptos los procedimientos utilizados por el PSC responsable de la CPS para publicar y notificar las enmiendas o modificaciones realizadas a la CPS.

Toda enmienda o modificación de la CPS, deberá ser publicada en el sitio principal de internet del PSC.

9.12.3. CIRCUNSTANCIAS EN QUE LOS OID DEBEN SER CAMBIADOS

Éste ítem no aplica.

Abog. Paola Rolón A.
DIRECTORA GENERAL
Firma Digital y Comercio Electrónico

9.13 DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS

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

Debe también establecerse que la CPS del PSC responsable no prevalecerá sobre las normas, criterios, prácticas y procedimientos establecidos por el MIC.

9.14 NORMATIVA APLICABLE

En este ítem debe ser indicada la legislación en que se ampara la CPS.

9.15 ADECUACIÓN A LA LEY APLICABLE

En este ítem debe indicarse que la responsabilidad del MIC en su calidad de Autoridad de Aplicación es la de velar por el cumplimiento de la legislación aplicable indicada en el apartado anterior.

9.16 DISPOSICIONES VARIAS

9.16.1 ACUERDO COMPLETO

Éste ítem no aplica.

9.16.2 ASIGNACIÓN

Éste ítem no aplica.

9.16.3 DIVISIBILIDAD

En este ítem, la CPS debe indicar que, en el eventual caso que una cláusula de la CPS del PSC responsable, sea declarada inconstitucional por la Corte Suprema de Justicia, el resto de las cláusulas de ese documento se mantendrán vigentes.

9.16.4 APLICACIÓN (HONORARIOS DE ABOGADOS Y RENUNCIA DE DERECHOS)

En ítem no aplica.

9.16.5 FUERZA MAYOR

En este ítem la CPS debe indicar que, obligatoriamente, que el deberá incluir cláusulas de fuerza mayor a los efectos de proteger al PSC.

9.17 OTRAS DISPOSICIONES

En este ítem, la CPS debe indicar, si hubiere, otras disposiciones necesarias a ser implantadas.

Jorge Borja Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

10. DOCUMENTOS DE REFERENCIA

Los siguientes documentos referenciados son aplicados para la confección de las políticas de certificación.

- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
- RFC 3739 "Internet X.509 Public Key Infrastructure Qualified Certificates Profile.
- RFC2560 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".
- RFC 3647: "Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework".
- ISO 3166 "Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países.
- Ley Nro. 4017/2010 "De validez jurídica de la firma electrónica, la firma digital, mensaje de datos y el expediente electrónico"
- Ley Nro. 4610/2012 que modifica y amplía la Ley Nro. 4017/2010
- Decreto Reglamentario Nro. 7369/2011

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico

GUSTAVO ANIBAL TOLEDO IRRAZABAL FIRMA

Firmado digitalmente por GUSTAVO ANIBAL TOLEDO IRRAZABAL FIRMA
Fecha: 2016.11.17 14:47:00 -03'00'