DIRECTIVAS OBLIGATORIAS PARA LA FORMULACIÓN Y ELABORACIÓN DE LA DECLARACIÓN DE PRÁCTICAS PARA EL PCSC QUE PRESTE EL SERVICIO DE GENERACIÓN O GESTIÓN DE DATOS DE CREACIÓN DE FIRMA ELECTRÓNICA Y/O SELLO ELECTRÓNICO EN EL MARCO DE LA ICPP

DOC-ICPP-07

Versión 1.0

Firmado
digitalmente por
PEDRO BENJAMIN
MANCUELLO
PEREZ

CONTROL DOCUMENTAL

Documento	
Título: DIRECTIVAS OBLIGATORIAS PARA LA FORMULACIÓN Y ELABORACIÓN DE LA DECLARACIÓN DE PRÁCTICAS PARA EL PCSC QUE PRESTE EL SERVICIO DE GENERACIÓN O GESTIÓN DE DATOS DE CREACIÓN DE FIRMA ELECTRÓNICA Y/O SELLO ELECTRÓNICO EN EL MARCO DE LA ICPP	**Nombre Fichero:** DOC-ICPP-07 Vers 1.0
Código: DOC-ICPP-07	**Soporte Lógico:** https://www.acraiz.gov.py
Fecha: 04/08/2022	**Versión:** 1.0

Registro de Cambios		
Versión	**Fecha**	**Motivo de Cambio**
1.0	04/08/2022	Versión Inicial

Distribución del documento	
Nombre	**Área**
Ministerio de Industria y Comercio (MIC)	Dirección General de Comercio Electrónico (DGCE)
Autoridad Certificadora (AC)	Prestadores Cualificados de Servicios de Confianza (PCSC)
Documento Público	https://www.acraiz.gov.py

Control del documento	
Elaborado por: ***JENNY RUÍZ DÍAZ***	Firmado digitalmente por JENNY ELIZABETH RUIZ DIAZ LEZCANO Fecha: 2022.08.04 16:01:13 -04'00'
Verificado por: ***LUJAN OJEDA***	MARIA LUJAN OJEDA CHAMORRO Digitally signed by MARIA LUJAN OJEDA CHAMORRO Date: 2022.08.04 15:46:02 -04'00'
Aprobado por: ***LUCAS SOTOMAYOR***	LUCAS ATILIO SOTOMAYOR LLANO Firmado digitalmente por LUCAS ATILIO SOTOMAYOR LLANO Fecha: 2022.08.04 17:10:49 -03'00'

Contenido

1. INTRODUCCIÓN

1.1 DESCRIPCIÓN GENERAL

Este documento es parte de un conjunto de normativas creadas para regular a los Prestadores Cualificados de Servicios de Confianza (PCSC) dentro del alcance de la Infraestructura de Claves Públicas de Paraguay (ICPP). Dicho conjunto consta de los siguientes documentos:

a) DOC-ICPP-07 (este documento); y

b) DOC-ICPP-08 [1].

El servicio de generación o gestión de datos de creación de firma electrónica y/o sello electrónico en nombre del firmante o creador del sello por parte del PCSC debe ser habilitada y supervisada por el Ministerio de Industria y Comercio (MIC) y debe prestarse en los términos establecidos en el documento DOC-ICPP-04 [2].

Las claves privadas de los usuarios finales almacenadas en dispositivos estandarizados conforme lo establecido en el documento DOC-ICPP-04 [2], y las firmas sellos electrónicos hechas por la clave privada del usuario en otros sistemas son válidas de conformidad a la Ley N° 6822/2021.

Este documento establece los requisitos mínimos que obligatoriamente deberán ser observados por los PCSC integrantes de la ICPP, para la formulación y la elaboración de su Declaración de Prácticas Certificación (DPC) en el caso que presten el servicio de generación o gestión de datos de creación de firma electrónica y/o sello electrónico en nombre del firmante o creador del sello. La DPC es el documento que describe las prácticas, procedimientos operativos y técnicos empleados por el PCSC para la prestación de sus servicios. Por tanto, el PCSC deberá adecuar su respectiva DPC y Política de Certificación (PC) para el almacenamiento de claves de sus usuarios finales.

El PCSC debe utilizar sistemas y productos fiables, incluidos canales de comunicación electrónicos seguros, aplicar procedimientos y mecanismos técnicos y organizativos adecuados, para garantizar que el entorno sea confiable y que los datos de creación de firma o sellos se utilicen bajo el control exclusivo del titular del certificado. Además, deben custodiar y proteger los datos de creación de firma o sello frente a cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad.

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

Toda DPC elaborada en el ámbito de la ICPP debe obligatoriamente adoptar la misma estructura empleada en este documento.

Las regulaciones previstas en los otros documentos de la ICPP también se aplican a los PCSC que presten servicio de generación o gestión de datos de creación de firma electrónica y/o sello electrónico en nombre del firmante o creador del sello, como integrantes de la referida ICPP, según corresponda:

a) NORMA ISO/IEC 27002:2022. Tecnologías de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información;
b) DOC-ICPP-03 [3];
c) DOC-ICPP-04 [2];
d) DOC-ICPP-06 [4]; y
e) DOC-ICPP-12 [5].

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

1.2 NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

En este ítem debe ser identificada la DPC.

1.3 PARTICIPANTES Y APLICABILIDAD

1.3.1. PRESTADORES CUALIFICADOS DE SERVICIOS DE CONFIANZA

Este ítem debe identificar el PCSC que forma parte del ICPP al que se refiere esta DPC.

En este ítem se deberá identificar la dirección de la página web (URL) donde se encuentran publicados los servicios prestados por el PCSC.

El servicio de generación o gestión de datos de creación de firma electrónica y/o sello electrónico en nombre del firmante o creador del sello por parte del PCSC se clasifican en tres categorías, según el tipo de actividad prevista:

a) almacenamiento de claves privadas de usuarios finales; o

b) servicio de firma y/o sello electrónico cualificado, verificación de firma y/o sello electrónico cualificado; o

c) ambos.

El PCSC mantendrá actualizada en todo momento la información anterior.

Entiéndase el servicio de firma y/o sello electrónico cualificado indicado en el literal b), como el proceso de firma o sello electrónico cualificado realizado por medio de la clave privada del titular de un certificado electrónico emitido por un PCSC cuya clave privada se encuentra almacenada en un dispositivo HSM en custodia del mencionado PCSC.

1.3.2. SUSCRIPTORES

En este ítem, deben ser caracterizadas las personas físicas o jurídicas que podrán solicitar los servicios descritos en esta DPC.

Todo Titular de Certificado deberá manifestar su plena aprobación a los servicios del PCSC y por él contratados, así como el nivel de seguimiento que el PCSC deberá informar al exclusivo efecto de proteger la clave privada del titular, ya sea en la provisión de almacenamiento de claves privadas, servicios de firma y/o sello y verificación de firmas y/o sellos electrónicos cualificados.

Los Titulares de Certificados podrán revocar la autorización otorgada al PCSC para la prestación de los servicios, para lo cual deberá solicitar la revocación de su

certificado. Formalizada la revocación, se procederá a la eliminación de la clave privada del Titular del Certificado almacenada en el dispositivo criptográfico por éste custodiado.

1.3.3. APLICABILIDAD

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

1.4. DATOS DE CONTACTO

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

1.5. PROCEDIMIENTOS DE CAMBIO DE ESPECIFICACIÓN

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

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

1.5.1. POLÍTICAS DE PUBLICACIÓN Y NOTIFICACIÓN.

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

1.5.2. PROCEDIMIENTOS DE APROBACIÓN

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

1.6. DEFINICIONES, SIGLAS Y ACRÓNIMOS

1.6.1 DEFINICIONES

1. **Autenticación:** proceso técnico que permite determinar la identidad de la persona física o jurídica.
2. **Autenticación electrónica:** un proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico.
3. **Autoridad de Aplicación:** Ministerio de Industria y Comercio a través de la Dirección General de Comercio Electrónico, dependiente del Viceministerio de Comercio y Servicios.
4. **Autoridad de Certificación:** entidad que presta servicios de emisión, gestión, revocación u otros servicios de confianza basados en certificados cualificados. En el marco de la ICPP, son Autoridades de Certificación, la AC Raíz-Py y el PCSC.
5. **Autoridad de Certificación Raíz del Paraguay:** órgano técnico, cuya función principal es coordinar el funcionamiento de la ICPP. La AC Raíz-Py tiene los certificados de más alto nivel, posee un certificado autofirmado y es a partir de allí, donde comienza la cadena de confianza. Las funciones de la AC Raíz-Py son ejercidas por la AA.
6. **Gestión de datos de creación de firma o sello electrónico:** El PCSC podrá, en nombre del firmante o creador de sello gestionar los datos de creación de firma o

sello electrónico a los que hayan prestado sus servicios, este servicio deberá ser provisto por un PCSC siempre y cuando cuente con la debida habilitación.

7. **Certificado cualificado de firma electrónica:** un certificado de firma electrónica que ha sido expedido por un PCSC y que cumple los requisitos establecidos en el artículo 43 de la ley Nº 6822/2021.
8. **Certificado cualificado de sello electrónico:** un certificado de sello electrónico que ha sido expedido por un PCSC y que cumple los requisitos establecidos en el artículo 53 de la ley Nº 6822/2021.
9. **Claves criptográficas:** valor o código numérico que se utiliza con un algoritmo criptográfico para transformar, validar, autenticar, cifrar y descifrar datos.
10. **Clave pública y privada:** la criptografía en la que se basa la ICPP, es la criptografía asimétrica. En ella, se emplean 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 electrónico, mientras que a la otra se le denomina privada y está bajo exclusivo control del titular o responsable del certificado.
11. **Compromiso:** violación de la seguridad de un sistema a raíz de una posible divulgación no autorizada de información sensible.
12. **Data center (Centro de Datos):** infraestructura compuesta por espacio físico para la instalación de equipos informáticos y de comunicación con adecuados sistemas de energía, aire acondicionado y seguridad. Es parte de una AC, 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 electrónicos emitidos por la AC.

13. **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.
14. **Declaración de Prácticas de Certificación:** documento en el cual se determina la declaración de las prácticas que emplea una AC al emitir certificados y que define la infraestructura, políticas y procedimientos que utiliza la AC para satisfacer los requisitos especificados en la PC vigente.
15. **Emisión de certificado:** es la autorización de la emisión del certificado en el sistema del PCSC previa comprobación de la concordancia de los datos de solicitud del certificado con los contenidos en los documentos presentados.
16. **Firma electrónica cualificada:** una firma electrónica que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica, la cual deberá estar vinculada al firmante de manera única, permitir la identificación del firmante, haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo y estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.
17. **Firmante:** una persona física que crea una firma electrónica.
18. **Generador:** máquina encargada de generar electricidad a partir de un motor de gasolina o diésel. La instalación de este equipo deberá ser de tal forma que, al interrumpirse el suministro de energía eléctrica del proveedor externo, el mismo debe arrancar automáticamente tomando la carga de las instalaciones del data center de la AC, 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.

19. **Habilitación:** autorización que otorga el MIC, una vez cumplidos los requisitos y condiciones establecidos en la norma.
20. **Infraestructura de Claves Públicas del Paraguay:** conjunto de personas, normas, leyes, políticas, procedimientos y sistemas informáticos necesarios para proporcionar una plataforma criptográfica de confianza que garantiza la presunción de validez legal para actos electrónicos firmados o cifrados con certificados electrónicos cualificados y claves criptográficas emitidas por esta infraestructura.
21. **Integridad:** característica que indica que un mensaje de datos o un documento electrónico no ha sido alterado desde la transmisión por el iniciador hasta su recepción por el destinatario.
22. **Módulo criptográfico**: software o hardware criptográfico que genera y almacena claves criptográficas.
23. **Módulo de Seguridad de Hardware:** dispositivo basado en un módulo criptográfico tipo hardware que genera, almacena y protege claves criptográficas.
24. **Normas Internacionales:** requisitos de orden técnico y de uso internacional que deben observarse en la prestación de los servicios mencionados en la presente DPC.
25. **Organismo de Evaluación de Conformidad:** organismo que desempeña actividades de evaluación de la conformidad a un prestador de servicios de confianza y de los servicios de confianza que este presta conforme a la Ley Nº 6822/2021.
26. **Parte usuaria:** persona física o jurídica que confía en el servicio de confianza.

27. **Prestador Cualificado de Servicios de Confianza:** prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la habilitación.
28. **Política de Seguridad:** es un conjunto de directrices destinadas a definir la protección del personal, seguridad física, lógica y de red, clasificación de la información, salvaguarda de activos de la información, gerenciamiento de riesgos, plan de continuidad de negocio y análisis de registros de eventos de una AC.
29. **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.
30. **Solicitud de certificado:** documento que se instrumenta mediante un formato autorizado de solicitud de certificado o como parte de documento específico denominado Contrato de Prestación de Servicios de Confianza, suscripto por el solicitante en nombre propio en el caso de certificados cualificados de firma electrónica para persona física, o bien en nombre del titular en el caso de certificados cualificados de sello electrónico para persona jurídica.
31. **Solicitud de revocación**: documento que se instrumenta mediante un formato autorizado de solicitud para la revocación de un certificado.
32. **Verificación y validación de firma o sello:** determinación y validación de que la firma o sello electrónico fue creado durante el periodo operacional de un certificado válido, por la clave privada correspondiente a la clave pública que se encuentra en el certificado y que el mensaje no ha sido alterado desde que su creación.

1.6.2 SIGLAS Y ACRÓNIMOS

Tabla Nº 1 - Siglas y Acrónimos

Sigla/Acrónimo	Descripción
AA	Autoridad de Aplicación
AC	Autoridad de Certificación (CA por sus siglas en inglés, Certificate Authority)
AC Raíz-Py	Autoridad Certificadora Raíz del Paraguay
DPC	Declaración de Prácticas de Certificación (DPC por sus siglas en inglés, Certification Practice Statement)
DGCE	Dirección General de Comercio Electrónico dependiente del Viceministerio de Comercio y Servicios.
HSM	Módulo de Seguridad Criptográfico basado en Hardware (HSM por sus siglas en inglés, Hardware Security Module)
ICPP	Infraestructura de Clave Pública del Paraguay
IDS	Sistema de Detección de Intrusos
ISO	Organización Internacional para la Estandarización (ISO por sus siglas en inglés, International Organization for Standardization).

MIC	Ministerio de Industria y Comercio
OEC	Organismo de Evaluación de la Conformidad
PC	Política de certificación (CP por sus siglas en inglés, Certificate Policy)
PCN	Plan de Continuidad del Negocio
PCSC	Prestador cualificado de servicios de confianza
PS	Política de Seguridad
PSS	Prestador de Servicios de Soporte
Py	Paraguay
RFC	Petición de Comentarios (RFC por sus siglas en inglés, Request For Comments)
UPS	Sistemas de alimentación ininterrumpida (UPS por sus siglas en inglés, uninterruptible power supply)
URL	Localizador uniforme de recursos (URL por sus siglas en inglés, Uniform Resource Locator).

2. RESPONSABILIDAD DEL REPOSITORIO Y PUBLICACIÓN

2.1. PUBLICACIÓN

2.1.1. PUBLICACIÓN DE INFORMACIÓN DE PCSC

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

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

a) capacidad de almacenamiento de las claves privadas de los Titulares de Certificados que opera;

b) su DPC;

c) los servicios que implementan;

d) las condiciones generales mediante la cual son prestados los servicios de almacenamiento de claves privadas o servicio de firma y/o sello electrónico cualificado y verificación de firma y/o sello electrónico cualificado.

2.1.2. FRECUENCIA DE PUBLICACIÓN

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

2.1.3. CONTROLES DE ACCESO

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

3. IDENTIFICACIÓN Y AUTORIZACIÓN

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

4. REQUERIMIENTOS OPERACIONALES

4.1. ALMACENAMIENTO Y ACCESO A LAS CLAVES PRIVADAS DEL TITULAR DEL CERTIFICADO

En este ítem de la DPC, además de lo descripto en el documento DOC-ICPP-08 [1], el PCSC debe informar cómo los componentes de software se comunicarán entre la aplicación del Titular del Certificado y el acceso al certificado y sus claves, describiendo:

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

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

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

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

4.2. SERVICIO DE CREACIÓN Y VERIFICACIÓN DE FIRMA Y/O SELLO ELECTRÓNICO CUALIFICADO

En este ítem de la DPC, además de lo descrito en el documento DOC-ICPP-08 [1], el PCSC debe informar sobre el funcionamiento de las plataformas de firma y/o sello electrónico cualificado, y, verificación de firma y/o sello electrónico cualificado.

4.3. PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

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

4.3.1. TIPOS DE EVENTOS REGISTRADOS

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

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

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

a) registros de accesos físicos;
b) el mantenimiento y cambios en la configuración de sus sistemas;
c) los cambios en el personal y de perfiles cualificados;
d) los informes de discrepancia y compromiso; y

e) el registro de destrucción de medios de almacenamiento que contienen claves criptográficas, datos de activación de certificados o información personal de los Titulares de Certificados.

La DPC debe prever que todos los registros de auditoría deberán contener la identidad del agente que los causó, así como la fecha y hora del evento. Los registros de auditoría electrónicos deberán contener la hora *Universal Time Coordinated* (UTC). Los registros manuales en papel podrán contener la hora local siempre que se especifique la ubicación.

Para facilitar los procesos de auditoría, toda la documentación relacionada con los servicios del PCSC deberá ser almacenada, ya sea de forma electrónica o manual, en una única ubicación, conforme a lo establecido ISO 27002/2022.

4.3.2. FRECUENCIA DE AUDITORÍA DE REGISTRO (LOGS)

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

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

Conforme a lo dispuesto en el ítem 5.4.3 del DOC-ICPP-03 [3]

4.3.4. PROTECCIÓN DEL REGISTRO (LOG) DE AUDITORÍA

Conforme a lo dispuesto en el ítem 5.4.4 del DOC-ICPP-03 [3]

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

Conforme a lo dispuesto en el ítem 5.4.5 del DOC-ICPP-03 [3]

4.3.6. SISTEMA DE RECOPILACIÓN DE DATOS DE AUDITORÍA

Conforme a lo dispuesto en el ítem 5.4.6 del DOC-ICPP-03 [3]

4.3.7. NOTIFICACIÓN DE AGENTES CAUSANTES DE EVENTOS

Conforme a lo dispuesto en el ítem 5.4.7 del DOC-ICPP-03 [3].

4.3.8. EVALUACIONES DE VULNERABILIDAD

Conforme a lo dispuesto en el ítem 5.4.8 del DOC-ICPP-03 [3]

4.4. ARCHIVO DE REGISTROS

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

4.4.1. TIPOS DE REGISTROS ARCHIVADOS

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

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

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

4.4.2. PROTECCIÓN DE ARCHIVOS

La DPC debe establecer que todos los registros archivados deben ser clasificados y almacenados con los requisitos de seguridad consistentes con esa clasificación, conforme a lo establecido en la norma ISO 27002/2022.

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

La DPC debe establecer que una segunda copia de todo el material archivado deberá ser almacenada en un ambiente diferente a las instalaciones principales del PCSC

responsable, recibiendo el mismo tipo de protección utilizada por él, en el archivo principal.

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

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

4.4.4. REQUISITOS PARA FECHADO DE REGISTROS

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

4.4.5. SISTEMA DE RECOPILACIÓN DE DATOS DE ARCHIVOS

En este ítem de la DPC, deben ser descriptos y localizados los recursos utilizados por el PCSC responsable para la recopilación de datos del archivo.

4.4.6. PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN DE ARCHIVO

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

4.5. LIBERACIÓN DE ESPACIO DEL SUSCRIPTOR

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

4.6. COMPROMISO Y RECUPERACIÓN ANTE DESASTRES

4.6.1. DISPOSICIONES GENERALES

En los ítems siguientes de la DPC deben ser descriptos los requisitos relacionados con los procedimientos de notificación y de recuperación de desastres, previstas en el PCN del PCSC responsable, conforme a lo establecido en la norma ISO 27002/2022, para garantizar la continuidad de sus servicios críticos.

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

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

En el caso de compromiso de una operación de servicio de firma y/o sello electrónico o verificación de la firma y/o sello electrónico de los documentos firmados o sellados, siempre que sea posible, el PCSC debe disponibilizar a todos los Titulares de Certificados y las terceras partes las informaciones que puedan ser utilizadas para identificar cuáles documentos pudieron haber sido afectados, a menos que viole la

privacidad de los Titulares de Certificados o comprometa la seguridad de los servicios del PCSC.

4.6.2. RECURSOS COMPUTACIONALES, SOFTWARE Y DATOS CORROMPIDOS.

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

4.6.3. SINCRONISMO DEL PCSC

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

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

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

4.7. EXTINCIÓN DE SERVICIOS DE UN PCSC

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

El PCSC debe garantizar que las posibles interrupciones con los Titulares de Certificados y terceras partes, como resultado del cese de los servicios de

almacenamiento de claves privadas o del servicio de firmas y/o sellos electrónicos cualificados y de verificación de las firmas y/o sellos electrónicos cualificados, serán mínimos y, en particular, asegurar el mantenimiento continuo de la información necesaria para que no haya perjuicio para sus Titulares de Certificados y terceras partes.

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

a) disponibilizará a todos los Titulares de Certificados y parte usuaria, informaciones respecto a su extinción;
b) transferirá a otro PCSC, después de la aprobación de AC Raíz-Py, las obligaciones relativas con el mantenimiento del almacenamiento de las claves, de certificados y documentos firmados o sellados, si fuera el caso, y de auditoría necesarios para demostrar el correcto funcionamiento del PCSC, por un periodo razonable;
c) mantendrá o transferirá a otro PCSC, después de la aprobación de AC Raíz-Py, sus obligaciones relativas con la disponibilidad de sus sistemas y hardware, por un período razonable;
d) notificará a todas las entidades afectadas.

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

5. CONTROLES DE SEGURIDAD FÍSICA, DE PROCEDIMIENTO Y PERSONAL

En los ítems siguientes deben ser descriptos los controles de seguridad implementados por el PCSC responsable de la DPC para ejecutar de modo seguro sus funciones, de conformidad con el DOC-ICPP-08 [1].

5.1. SEGURIDAD FÍSICA

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

5.1.1 CONSTRUCCIÓN Y LOCALIZACIÓN DE LAS INSTALACIONES DEL PCSC.

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

a) instalaciones para equipamientos de apoyo, tales como: equipos de aire acondicionado, grupos de generadores, *UPS*, baterías, tableros de distribución de energía y telefonía;
b) instalaciones para sistemas de telecomunicaciones;
c) sistemas de puesta a tierra y de protección contra rayos; e
d) iluminación de emergencia.

5.1.2. ACCESO FÍSICO EN LAS INSTALACIONES DE PCSC.

Todo PCSC integrante de la ICPP deberá implementar un sistema de control de acceso físico que garantice la seguridad de sus instalaciones, conforme con lo establecido en la norma ISO 27002/2022, y los requisitos que siguen.

5.1.2.1. NIVELES DE ACCESO

El PCSC debe describir detalladamente cada nivel de acceso y su conjunto de sistemas, *software* y *hardware* implementados, de acuerdo con las descripciones de los niveles de acceso dispuestos en el documento DOC-ICPP-08 [1].

5.1.2.2. SISTEMAS FÍSICOS DE DETECCIÓN

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

La seguridad se puede lograr mediante:

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

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

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

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

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

5.1.2.3. SISTEMA DE CONTROL DE ACCESO

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

5.1.3. ENERGÍA Y AIRE ACONDICIONADO DE NIVEL 3 DEL PCSC

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

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

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

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

Deberán ser mantenidos actualizados los registros sobre la topología de la red de cableado, sujeto a los requisitos de confidencialidad establecidos en la norma ISO 27002/2022. Cualquier modificación en esta red deberá ser documentada y autorizada previamente.

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

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

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

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

5.1.4. EXPOSICIÓN AL AGUA EN LAS INSTALACIONES DEL PCSC

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

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

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

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

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

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

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

5.1.6. ALMACENAMIENTO DE MEDIOS EN LAS INSTALACIONES DEL PCSC

El PCSC 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 PCSC debe almacenarse de forma segura en armarios ignífugos y cofres de seguridad, según la clasificación de la información en ellos contenida.

5.1.7. ELIMINACIÓN DE RESIDUOS EN LAS INSTALACIONES DEL PCSC

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

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

5.1.8. ARCHIVO EXTERNO (OFF-SITE) DEL PCSC

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

5.2. CONTROLES PROCEDIMENTALES

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

5.2.1. PERFILES CUALIFICADOS

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

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

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

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

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

5.2.2. NÚMEROS DE PERSONAS REQUERIDAS POR TAREA

Todas las tareas realizadas en el cofre o gabinete donde se localizan los servicios del PCSC deberán requerir la presencia de al menos 2 (dos) empleados o funcionarios con perfiles cualificados. Para los casos de copias de las claves de los usuarios, se requerirán al menos 3 (tres) empleados o funcionarios con perfiles distintos y

cualificados. Las otras tareas del PCSC pueden ser realizadas por un solo empleado o funcionario.

5.2.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA PERFIL

La DPC debe garantizar que todo empleado o funcionario del PCSC responsable tendrá su identidad y perfil verificados antes de:

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

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

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

El PCSC debe implementar un estándar para el uso de "contraseñas seguras", definido en su Política de Seguridad y de acuerdo con el correspondiente de la norma ISO 27002/2022, con procedimientos para validar esas contraseñas.

5.3. CONTROLES DE PERSONAL

En los ítems siguientes de la DPC deben ser descriptos los requisitos y procedimientos, implementados por el PCSC responsable en relación a todo su personal, con respecto a aspectos tales como: verificación de antecedentes e idoneidad, capacitación profesional, rotación de cargo, sanciones por acciones no autorizadas, controles de contratación y documentación a proporcionar. La DPC debe garantizar que

todos los empleados del PCSC responsable, a cargo de las tareas operativas, hayan registrado en un documento formal los siguientes términos de responsabilidad:

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

5.3.1. ANTECEDENTES, CUALIFICACIÓN, EXPERIENCIA Y REQUISITOS DE IDONEIDAD

Todo el personal del PCSC responsable involucrado en actividades directamente relacionadas con los procesos de gerenciamiento de los sistemas de almacenamiento de claves privadas, firmas o sellos electrónicos cualificados y verificaciones de firmas o sellos electrónicos cualificados deberán ser admitidos de acuerdo con el ítem correspondiente de la norma ISO 27002/2022. El PCSC responsable podrá definir requisitos adicionales para la admisión.

5.3.2. PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES

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

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

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

5.3.3. REQUISITOS DE ENTRENAMIENTO

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

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

5.3.4. FRECUENCIA Y REQUISITOS PARA CAPACITACIÓN TÉCNICA

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

5.3.5. FRECUENCIA Y SECUENCIA DE ROTACIÓN DE CARGOS

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

5.3.6. SANCIONES POR ACCIONES NO AUTORIZADAS.

La DPC debe estipular, así como en su política de RRHH que, en caso de que una persona a cargo de un proceso operativo lleve a cabo una acción no autorizada, real o sospechosa, el PCSC deberá suspender inmediatamente el acceso de esa persona a los sistemas, instruir procedimientos administrativos para investigar los hechos y, si corresponde, adoptar las medidas legales apropiadas.

El proceso administrativo mencionado anteriormente deberá contener al menos con:

a) informe de la ocurrencia con el modo de operación;
b) identificación de los involucrados;
c) posibles daños causados;

d) sanciones aplicadas, si fuera el caso; y
e) conclusiones.

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

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

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

5.3.7. REQUISITOS PARA CONTRATAR PERSONAL

Todo el personal responsable del PCSC involucrado en actividades directamente relacionadas con los procesos de gerenciamiento de los sistemas de almacenamiento de claves privadas, firmas o sellos electrónicos cualificados y verificación de firmas o sellos electrónicos cualificados deberá ser contratado según lo establecido en el ítem correspondiente de la norma ISO 27002/2022. El PCSC responsable puede definir requisitos adicionales para la contratación.

5.3.8. DOCUMENTACIÓN PROPORCIONADA AL PERSONAL

La DPC debe garantizar que el PCSC responsable pondrá a disposición de todo su personal al menos:

a) su DPC;
b) la norma ISO 27002/2022;
c) documentación operacional relacionada con sus actividades; y
d) contratos, normas y políticas relevantes para sus actividades.

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

6. CONTROLES TÉCNICOS DE SEGURIDAD

En este ítem, la DPC, debe definir las medidas de seguridad implementadas por el PCSC responsable para proteger las claves privadas de los Titulares de Certificados, mantener los servicios relacionados con las firmas y/o sellos electrónicos cualificados, así como el sincronismo de sus sistemas con la fuente de tiempo confiable. También deben ser definidos otros controles técnicos de seguridad utilizados por el PCSC en el desempeño de sus funciones operacionales.

6.1. CONTROLES DE SEGURIDAD COMPUTACIONAL

6.1.1. DISPOSICIONES GENERALES

En este ítem, la DPC debe indicar los mecanismos utilizados para proporcionar seguridad a sus estaciones de trabajo, servidores y otros sistemas y equipamientos, de conformidad con las disposiciones establecidas en los ítems correspondientes de la norma ISO 27002/2022.

6.1.2. REQUISITOS TÉCNICOS ESPECÍFICOS PARA LA SEGURIDAD COMPUTACIONAL

La DPC debe prever que los sistemas y los equipamientos del PCSC responsable, utilizados en los procesos de gerenciamiento de los sistemas de almacenamiento de claves privadas, firmas o sellos electrónicos cualificados y verificaciones de firmas o sellos electrónicos cualificados, deberán implementar, entre otras, las siguientes características:

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

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

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

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

6.1.3. CLASIFICACIÓN DE SEGURIDAD COMPUTACIONAL

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

6.2. CONTROLES TÉCNICOS DEL CICLO DE VIDA

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

6.2.1. CONTROLES DE DESARROLLO DEL SISTEMA

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

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

6.2.2. CONTROLES DE GESTIÓN DE LA SEGURIDAD

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

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

6.2.3. CICLO CLASIFICACIONES DE SEGURIDAD VIDA

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

6.3. CONTROLES DE SEGURIDAD DE REDES

6.3.1. DISPOSICIONES GENERALES

En este ítem de la DPC deben ser descriptos los controles relacionados con la seguridad de la red, incluyendo el firewall y recursos similares, observando las disposiciones establecidas en el ítem correspondiente de la norma ISO 27002/2022.

Todos los servidores y elementos de la infraestructura y protección de red, tales como: enrutadores, hubs, switches, firewalls y sistemas de detección de intrusos (IDS),

localizados en el segmento de red que aloja los sistemas del PCSC, deberán estar ubicados y en funcionamiento al menos en el nivel 3.

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

El acceso lógico a los elementos de la infraestructura y protección de red deberá ser restringido a través de un sistema de autenticación y autorización de acceso. Los enrutadores conectados a redes externas deberán implementar filtros de paquetes de datos, que permitan solamente conexiones a los servicios y servidores previamente definidos como sujeto a acceso externo.

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

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

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

b) por el Titular del Certificado, para el almacenamiento y acceso a la clave privada y servicios de firma y/o sello electrónico cualificado y verificación de la firma o sello electrónico cualificado.

6.3.2. FIREWALL

Los mecanismos de *firewall* deberán ser implementados en equipos para usos específicos, configurados exclusivamente para esa función. Los *firewalls* deberán estar

dispuestos y configurados de forma a promover el aislamiento, en sub-redes específicas, los equipos servidores con acceso externo (denominada "zona desmilitarizada" (DMZ)) en relación a los equipos con acceso exclusivamente interno al PCSC.

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

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

6.3.3. SISTEMA DE DETECCIÓN DE INTRUSOS (IDS)

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

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

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

6.3.4. REGISTRO DE ACCESO NO AUTORIZADO A LA RED.

Las tentativas de acceso no autorizado en ruteadores, Firewall o 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 deben ser documentadas.

6.3.5. OTROS CONTROLES DE SEGURIDAD DE RED

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

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

6.4. CONTROLES DE INGENIERÍA DEL MÓDULO CRIPTOGRÁFICO

En este ítem la DPC se debe describir los requisitos aplicables al módulo criptográfico utilizado para el almacenamiento de la clave privada de los Titulares de Certificados del PCSC responsable. Podrán ser indicados estándares de referencia, como los definidos en el documento**,** DOC-ICPP-06 [4].

7. POLÍTICAS DE FIRMA y/o SELLO

En este ítem de la DPC, el PCSC en el caso que ofrezca el servicio de firma o sello electrónico cualificado debe informar las Políticas de Firma y/o Sello que practica.

8. AUDITORÍAS Y EVALUACIONES DE CONFORMIDAD

8.1. INSPECCIÓN DE CUMPLIMIENTO Y AUDITORÍA

En este ítem, la DPC debe indicar que los PCSC serán auditados, al menos cada veinticuatro (24) meses, corriendo con los gastos que ello genere, por un OEC. La finalidad de la auditoría es confirmar que tanto los PCSC, como los servicios de confianza cualificados que prestan cumplen con los requisitos establecidos en esta DPC y en la normativa vigente. Los PCSC enviarán el informe de evaluación de la conformidad correspondiente a la AC Raíz-Py en el plazo de 3 (tres) días hábiles tras su recepción.

Sin perjuicio de lo dispuesto en el párrafo anterior, la AC Raíz-Py podrá en cualquier momento auditar o solicitar a un OEC que realice una evaluación de conformidad de los PCSC, corriendo con los gastos dichos PCSC, para confirmar que tanto ellos como los servicios de confianza cualificados que prestan cumplen los requisitos de esta DPC y de la normativa vigente.

Además cada PCSC, deberá implementar un programa de auditorías internas conforme a lo estipulado en el ítem correspondiente de la norma ISO 27002/2022 para la verificación de su sistema de gestión.

Cuando la AC Raíz-Py requiera a un PCSC que corrija el incumplimiento de requisitos de esta DPC o de la normativa vigente, y este prestador no actúe en consecuencia, en su caso, en el plazo fijado por la AC Raíz-Py, la AC Raíz-Py, teniendo en cuenta en particular el alcance, la duración y las consecuencias de este incumplimiento, puede retirar la cualificación al prestador o al servicio que este presta y actualizar la lista de confianza. La AC Raíz-Py comunicará al PCSC la retirada de su cualificación o de la cualificación del servicio de que se trate.

Tales supervisiones deberán ser efectuadas conforme a las disposiciones en materia de auditoría, reglamentadas por la AC Raíz-Py.

Todo PCSC está obligado al cumplimiento de las auditorías, éstas permiten establecer una confianza razonable en el marco de la ICPP.

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

9. OTROS ASUNTOS COMERCIALES Y LEGALES

9.1. OBLIGACIONES Y DERECHOS

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

9.1.1. OBLIGACIONES DEL PCSC

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

a) operar de acuerdo con su DPC y la descripción de los servicios que realiza;
b) gestionar y garantizar la protección de las claves privadas de los Titulares de Certificados;
c) mantener el PCSC sincronizado con una fuente confiable de tiempo ajustado con la fecha y hora oficial paraguaya;
d) tomar las medidas apropiadas para garantizar que los Titulares de Certificados y demás entidades involucradas conozcan sus respectivos derechos y obligaciones;
e) supervisar y controlar el funcionamiento de los servicios prestados;
f) notificar al Titular del Certificado, cuando su clave privada se ve comprometida y solicitar la revocación inmediata del certificado correspondiente o la finalización de sus actividades;

g) publicar en su sitio web la DPC y las Políticas de Seguridad (PS) aprobadas que implementa;

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

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

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

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

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

m) mantener y probar anualmente su PCN;

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

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

p) informar a AC Raíz-Py, mensualmente, el número de claves privadas o los certificados electrónicos correspondientes almacenados y las firmas y sellos realizados y verificados.

9.1.2. OBLIGACIONES DEL SUSCRIPTOR

El Titular del Certificado debe asegurarse, a través de las aplicaciones disponibles al aceptar el servicio de un PCSC, que su par de claves y/o certificados electrónicos se hayan almacenado correctamente y que la clave privada utilizada para firmar o sellar esté funcional.

9.1.3 DERECHOS DEL TERCERO (RELYING PARTY)

Se considera que el tercero es la parte usuaria que confía en el contenido, la validez y la aplicabilidad del servicio de firma y/o sello electrónico, y de la verificación de la firma y/o sello electrónico.

Constituyen derechos de tercera parte:

a) rehusarse a utilizar el servicio de firma y/o sello electrónico cualificado y de verificación de la firma y/o sello electrónico cualificado de documentos electrónicos prestados por el PCSC para fines distintos de su propósito de uso en el marco de la ICPP.
b) verificar, en cualquier tiempo, la validez de firma o sello electrónico cualificado. Una firma o sello electrónico cualificado en el marco de la ICPP se considera válido cuando:

    i. el certificado electrónico no aparece en la CRL del PCSC emisor;

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

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

    iv. el propósito del uso está de acuerdo con lo definido en la política del certificado electrónico de los firmantes o creadores del sello.

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

9.2. RESPONSABILIDADES

9.2.1. RESPONSABILIDADES DEL PCSC

El PCSC responsable debe responder por cualquier daño causado.

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

9.3. RESPONSABILIDAD FINANCIERA

9.3.1. INDEMNIZACIONES A TERCEROS (RELYING PARTY)

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

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

9.3.2. RELACIONES FIDUCIARIAS

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

9.3.3. PROCEDIMIENTOS ADMINISTRATIVOS

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

9.4. INTERPRETACIÓN Y EJECUCIÓN

9.4.1. LEGISLACIÓN

En este ítem, se debe indicar la legislación que acompaña la DPC.

9.4.2. FORMA DE INTERPRETACIÓN Y NOTIFICACIÓN.

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

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

9.4.3. PROCEDIMIENTOS DE RESOLUCIÓN DE DISPUTAS

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

También debe ser establecido que la DPC del PCSC responsable no prevalece sobre las reglas, criterios, prácticas y procedimientos establecidos por la AC Raíz-Py.

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

9.5. LAS TASAS DE SERVICIO

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

a) almacenamiento de claves privadas para los usuarios finales;
b) de firma y/o sello electrónico cualificado y de verificación de firma y/o sello electrónico cualificado;
c) otras tarifas.

9.6. CONFIDENCIALIDAD

9.6.1. DISPOSICIONES GENERALES

La clave privada de los Titulares de Certificados será mantenida por el PCSC, que será responsable de su confidencialidad, manteniendo registros de auditoría con la hora y fecha de acceso disponibles para el Titular del Certificado.

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

Los documentos firmados o sellados electrónicamente por los Titulares de Certificados podrán ser conservados por el PCSC, siempre que se acuerde expresamente con el Titular del Certificado y de conformidad con la legislación vigente.

9.6.2. TIPOS DE INFORMACIONES CONFIDENCIALES

En este ítem, deben ser identificados los tipos de informaciones consideradas confidenciales por el PCSC responsable de la DPC, de acuerdo con los estándares, criterios, prácticas y procedimientos de la ICPP.

La DPC, debe establecer, como principio general, que no se deben divulgar documentos, información o registros proporcionados por el Titular del Certificado al PCSC, excepto cuando se haga un acuerdo con el Titular del Certificado.

9.6.3. TIPOS DE INFORMACIÓN NO CONFIDENCIALES

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

a) los certificados del Titular del Certificado;
b) la DPC del PCSC;
c) versiones públicas de su Política de Seguridad; y
d) la conclusión de los informes de auditoría.

9.6.4. INCUMPLIMIENTO DE LA CONFIDENCIALIDAD POR RAZONES LEGALES

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

9.6.5. INFORMACIÓN A TERCEROS

Este ítem de la DPC, deberá establecer como una guía general que ningún documento, información o registro bajo la custodia del PCSC responsable de la DPC se proporcionará a ninguna persona, excepto cuando la persona que lo solicite, por medio

de un instrumento debidamente constituido, esté autorizado para hacerlo y esté correctamente identificado.

9.6.6. OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN

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

9.7. DERECHOS DE PROPIEDAD INTELECTUAL

En este ítem de la DPC, deben abordarse los problemas relacionados con los derechos de propiedad intelectual de los certificados, políticas, especificaciones de prácticas y procedimientos, nombres y claves criptográficas y documentos firmados o sellados electrónicamente de acuerdo con la legislación vigente.

10. DOCUMENTOS DE REFERENCIA

10.1 REFERENCIAS

- Ley Nº 6822/2021 "De los servicios de confianza para las transacciones electrónicas, del documento electrónico y los documentos transmisibles electrónicos."
- RFC 4210: Internet X.509 Public Key Infrastructure. Certificate Management Protocol (CMP).
- RFC 4211: Internet X.509 Public Key Infrastructure. Certificate Request Message Format (CRMF).
- RFC 2030: Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI.
- RFC 3447: Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography. Specifications Version 2.1.
- RFC 3647: Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework.
- Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo del 23 de julio de 2014 - relativo a la identificación electrónica y los servicios de confianza

para transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

- NORMA ISO/IEC 27002:2022

10.2. REFERENCIAS A DOCUMENTOS QUE COMPONEN LA ICPP

Tabla Nº2 – Documentos Referenciados

REF.	NOMBRE DEL DOCUMENTO	CÓDIGO
[1]	Procedimientos operacionales mínimos para el servicio de generación o gestión de datos de creación de firma electrónica y/o sello electrónico.	DOC-ICPP-08
[2]	Directivas obligatorias para la formulación y elaboración de la política de certificación de los Prestadores Cualificados de Servicios de Confianza de la ICPP.	DOC-ICPP-04

[3]	Directivas obligatorias para la formulación y elaboración de la declaración de prácticas de certificación de los prestadores cualificados de servicios de confianza de la ICPP.	DOC-ICPP-03
[4]	Normas de algoritmos criptográficos de la ICPP	DOC-ICPP-06
[5]	Criterios y procedimientos para realización de auditorías en las entidades miembros de la ICPP	DOC-ICPP-12