REQUISITOS MÍNIMOS PARA LA DECLARACIÓN DE PRÁCTICAS DE SELLO CUALIFICADO DE TIEMPO ELECTRÓNICO DE LA ICPP

DOC-ICPP-25

Versión 1.0

CONTROL DOCUMENTAL

Documento	
Título: REQUISITOS MÍNIMOS PARA LA DECLARACIÓN DE PRÁCTICAS DE SELLOS CUALIFICADOS DE TIEMPO ELECTRÓNICO DE LA ICPP	**Nombre Archivo:** DOC-ICPP-25 Vers 1.0
Código: DOC-ICPP-25	**Soporte Lógico:** https://www.acraiz.gov.py/
Fecha: 28/11/2023	**Versión:** 1.0

Registro de cambios		
Versión	**Fecha**	**Motivo de cambio**
1.0	28/11/2023	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	JENNY ELIZABETH RUIZ DIAZ LEZCANO Nombre de reconocimiento (DN): cn=JENNY ELIZABETH RUIZ DIAZ LEZCANO, o=PERSONA FISICA, c=PY, givenName=JENNY ELIZABETH, sn=RUIZ DIAZ LEZCANO, serialNumber=CI1227372, ou=FIRMA F2 Fecha: 2023.11.24 12:22:34 -03'00'
Verificado por: OSCAR ROA	OSCAR GABRIEL ROA BERNAL Firmado digitalmente por OSCAR GABRIEL ROA BERNAL
Aprobado por: LUCAS SOTOMAYOR	LUCAS ATILIO SOTOMAYOR LLANO Nombre de reconocimiento (DN): cn=LUCAS ATILIO SOTOMAYOR LLANO, serialNumber=CI2304026, givenName=LUCAS ATILIO, sn=SOTOMAYOR LLANO, ou=F3, o=CERTIFICADO CUALIFICADO DE FIRMA ELECTRONICA, c=PY Fecha: 2023.11.24 15:50:40 -03'00'

MARIA LORENA MENDEZ DE GUSTAFSON
Firmado digitalmente por MARIA LORENA MENDEZ DE GUSTAFSON
Fecha: 2023.11.28 17:47:33 -03'00'

Contenido

1. INTRODUCCIÓN 9
1.1. DESCRIPCIÓN GENERAL 9
1.2 NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO 11
1.3 PARTICIPANTES 11
1.3.1 PRESTADORES CUALIFICADOS DE SERVICIOS DE CONFIANZA (PCSC) 11
1.3.2 AGENTE DE ATENCIÓN DEL SERVICIO 11
1.3.3 SUSCRIPTORES 11
1.3.4 PARTE QUE USUARIA 11
1.3.5 PRESTADOR DE SERVICIOS DE SOPORTE (PSS) 11
1.4 USO DEL CERTIFICADO 12
1.5 ADMINISTRACIÓN DE LA POLÍTICA 12
1.5.1 ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO 12
1.5.2 PERSONA DE CONTACTO 12
1.5.3 PERSONA QUE DETERMINA LA ADECUACIÓN DE LA DPC-SCTE A LA PC 13
1.5.4 PROCEDIMIENTOS DE APROBACIÓN DE LA DPC-SCTE 13
1.6 DEFINICIONES Y ACRÓNIMOS 13
1.6.1 DEFINICIONES 13
1.6.2 SIGLAS Y ACRÓNIMOS 18
2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO ..20
2.1 REPOSITORIOS 20
2.2 TIEMPO O FRECUENCIA DE PUBLICACIÓN 21
2.3 CONTROLES DE ACCESO A LOS REPOSITORIOS 21
3. IDENTIFICACIÓN Y AUTENTICACIÓN 21
4. REQUERIMIENTOS OPERACIONALES 21
4.1 SOLICITUD DE SCTE 22
4.1.1 QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE SCTE 22
4.1.2 PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES 22
4.1.2.1 RESPONSABILIDADES Y OBLIGACIONES DEL PCSC 22
4.1.2.2 OBLIGACIONES DEL SUSCRIPTOR 24
4.2 EMISIÓN DEL SCTE 24
4.3 ACEPTACIÓN DE SCTE 26
4.4. CARACTERÍSTICAS DEL SCTE 27
5. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES 27
5.1. SEGURIDAD FÍSICA 27
5.1.1. CONSTRUCCIÓN Y UBICACIÓN DE LAS INSTALACIONES DEL PCSC 27
5.1.2. ACCESO FÍSICO A LAS INSTALACIONES DEL PCSC 28

5.1.2.1. NIVELES DE ACCESO FÍSICO 28
5.1.2.2. SISTEMAS FÍSICOS DE DETECCIÓN 30
5.1.2.3. SISTEMAS DE CONTROL DE ACCESO 31
5.1.3. ENERGÍA Y AIRE ACONDICIONADO DEL AMBIENTE DE NIVEL 3 DEL PCSC 31
5.1.4. EXPOSICIÓN AL AGUA 32
5.1.5. PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO 32
5.1.6. ALMACENAMIENTO DE MEDIOS 33
5.1.7. ELIMINACIÓN DE RESIDUOS 33
5.1.8. RESPALDO FUERA DE SITIO 33
5.2. CONTROLES PROCEDIMENTALES 34
5.2.1. ROLES DE CONFIANZA 34
5.2.2. NÚMERO DE PERSONAS REQUERIDAS POR TAREA 35
5.2.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL 35
5.3. CONTROLES DE PERSONAL 35
5.3.1. REQUERIMIENTOS DE EXPERIENCIA Y CAPACIDAD 36
5.3.2. PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES 36
5.3.3. REQUERIMIENTOS DE CAPACITACIÓN 36
5.3.4. REQUERIMIENTOS Y FRECUENCIA DE CAPACITACIÓN 37
5.3.5. FRECUENCIA Y SECUENCIA EN LA ROTACIÓN DE LAS FUNCIONES 37
5.3.6. SANCIONES PARA ACCIONES NO AUTORIZADAS 37
5.3.7. REQUISITOS DE CONTRATACIÓN A TERCEROS 38
5.3.8. DOCUMENTACIÓN SUMINISTRADA AL PERSONAL 38
5.4. PROCEDIMIENTO DE REGISTRO DE AUDITORÍA 39
5.4.1. TIPOS DE EVENTOS REGISTRADOS 39
5.4.2. FRECUENCIA DE PROCESAMIENTO DEL REGISTRO (LOGS) 40
5.4.3. PERÍODO DE CONSERVACIÓN DEL REGISTRO (LOGS) DE AUDITORÍA 41
5.4.4. PROTECCIÓN DEL REGISTRO (LOGS) DE AUDITORÍA 41
5.4.5. PROCEDIMIENTOS DE RESPALDO (BACKUP) DE REGISTRO (LOGS) DE AUDITORÍA 41
5.4.6. SISTEMA DE RECOLECCIÓN DE INFORMACIÓN DE AUDITORÍA (INTERNO O EXTERNO) 41
5.4.7. NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO 42
5.4.8. EVALUACIÓN DE VULNERABILIDADES 42
5.5. ARCHIVOS DE REGISTROS 42
5.5.1. TIPOS DE REGISTROS ARCHIVADOS 42

5.5.2. PERÍODOS DE RETENCIÓN PARA ARCHIVOS 42
5.5.3. PROTECCIÓN DE ARCHIVOS 43
5.5.4. PROCEDIMIENTOS DE RESPALDO (BACKUP) DE ARCHIVO 43
5.5.5. REQUERIMIENTOS PARA SELLADO DE TIEMPO DE REGISTROS 43
5.5.6. SISTEMA DE RECOLECCIÓN DE DATOS DE ARCHIVO (INTERNO O EXTERNO) 43
5.5.7. PROCEDIMIENTOS PARA OBTENER Y VERIFICAR LA INFORMACIÓN ARCHIVADA 43
5.6 CAMBIO DE CLAVE 43
5.7. COMPROMISO Y RECUPERACIÓN DE DESASTRES 44
5.7.1. DISPOSICIONES GENERALES 44
5.7.2 RECURSOS COMPUTACIONALES, SOFTWARE Y/O CORRUPCIÓN DE DATOS 45
5.7.3. PROCEDIMIENTOS EN EL CASO DE COMPROMISO DE LA CLAVE PRIVADA DEL PCSC 45
5.7.3.1. CERTIFICADO DE ENTIDAD ES REVOCADO 45
5.7.3.2. CLAVE DEL PCSC ESTÁ COMPROMETIDA 45
5.7.3.3 PERDIDA DE CALIBRACION Y SINCRONISMO DEL SSTE 45
5.7.4. CAPACIDAD DE CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE 45
5.8. EXTINCIÓN DE LOS SERVICIOS DE UN PCSC O PSS 45
6. CONTROLES TÉCNICOS DE SEGURIDAD 46
6.1. CICLO DE VIDA DE LA CLAVE PRIVADA DEL SSTE 47
6.1.1. GENERACIÓN DEL PAR DE CLAVES 47
6.1.2. GENERACIÓN DE SOLICITUD DE CERTIFICADO 48
6.1.3. EXCLUSIÓN DE SOLICITUD DE CERTIFICADO 48
6.1.4. INSTALACIÓN DEL CERTIFICADO 48
6.1.5. RENOVACIÓN DEL CERTIFICADO 48
6.1.6. DISPONIBILIZACIÓN DE CLAVE PÚBLICA DEL PCSC PARA USUARIOS 48
6.1.7. TAMAÑO DE LA CLAVE 49
6.1.8. GENERACIÓN DE PARÁMETROS DE CLAVES ASIMÉTRICAS 49
6.1.9. VERIFICACIÓN DE CALIDAD DE LOS PARÁMETROS 49
6.1.10. GENERACIÓN DE CLAVES POR HARDWARE O SOFTWARE 49
6.1.11. PROPÓSITOS DE USOS DE CLAVE 49
6.2. PROTECCIÓN DE LA CLAVE PRIVADA 49
6.2.1. ESTÁNDARES Y CONTROLES DEL MÓDULO CRIPTOGRÁFICO 49
6.2.2. CONTROL MULTIPERSONA DE LA CLAVE PRIVADA 50

6.2.3. CUSTODIA (ESCROW) DE LA CLAVE PRIVADA 50
6.2.4. RESPALDO/COPIA DE SEGURIDAD LA CLAVE PRIVADA 50
6.2.5. ARCHIVADO DE LA CLAVE PRIVADA 50
6.2.6. TRANSFERENCIA DE CLAVE PRIVADA HACIA O DESDE UN MÓDULO CRIPTOGRÁFICO 50
6.2.7. MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA 50
6.2.8. MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA 51
6.2.9. MÉTODO DE DESTRUCCIÓN DE CLAVE PRIVADA 51
6.3. OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES 51
6.3.1. ARCHIVO DE LA CLAVE PÚBLICA 51
6.3.2. PERÍODO DE USO DEL PAR DE CLAVES (PÚBLICA Y PRIVADA) 51
6.4. DATOS DE ACTIVACIÓN DE CLAVE DEL SSTE 51
6.4.1. GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN 51
6.4.2. PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN 52
6.4.3. OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN 52
6.5. CONTROLES DE SEGURIDAD COMPUTACIONAL 52
6.5.1. REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS 52
6.5.2. CLASIFICACIÓN DE LA SEGURIDAD DEL COMPUTADOR 53
6.5.3. CARACTERÍSTICAS DEL SERVIDOR DE SELLO DE TIEMPO (SSTE) 53
6.5.4. CICLO DE VIDA DE MÓDULOS CRIPTOGRÁFICOS ASOCIADOS AL SSTE 54
6.5.5. AUDITORÍA Y SINCRONIZACIÓN DE RELOJES DEL SSTE 54
6.6. CONTROLES TÉCNICOS DEL CICLO DE VIDA 55
6.6.1. CONTROLES PARA EL DESARROLLO DEL SISTEMA 55
6.6.2. CONTROLES DE GESTIÓN DE SEGURIDAD 55
6.6.3. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA 56
6.7. CONTROLES DE SEGURIDAD DE RED 56
6.7.1. DIRECTRICES GENERALES 56
6.7.2. FIREWALL 57
6.7.3. SISTEMA DE DETECCIÓN DE INTRUSOS (IDS) 57
6.7.4. REGISTRO DE ACCESOS NO AUTORIZADOS A LA RED 57
6.7.5. OTROS CONTROLES DE SEGURIDAD DE LA RED 58
6.8. CONTROLES DE INGENIERÍA DEL MÓDULO CRIPTOGRÁFICO 58
7. PERFILES DE SELLO CUALIFICADO DE TIEMPO ELECTRÓNICO 58
7.1. DIRECTRICES GENERALES 58
7.2. PERFIL DEL SELLO CUALIFICADO DE TIEMPO ELECTRÓNICO 58

7.2.1. REQUISITOS PARA UN CLIENTE DE SCTE 59
7.2.2. REQUISITOS PARA UN SERVIDOR DE SCTE 59
7.2.3. PERFIL DEL CERTIFICADO SSTE 60
7.2.4. FORMAS DEL NOMBRE 62
7.3. PROTOCOLO DE TRANSPORTE 62
8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES 62
8.1. FRECUENCIA O CIRCUNSTANCIAS DE EVALUACIÓN 62
8.2. IDENTIDAD / CALIDAD DEL EVALUADOR 63
8.3. RELACIÓN DEL EVALUADOR CON LA ENTIDAD EVALUADA 63
8.4. ASPECTOS CUBIERTOS POR LA EVALUACIÓN 64
8.5. ACCIONES TOMADAS COMO RESULTADO DE UNA DEFICIENCIA 64
8.6. COMUNICACIÓN DE RESULTADOS 64
9. OTROS ASUNTOS LEGALES Y COMERCIALES 64
9.1. TARIFAS 64
9.2. RESPONSABILIDAD FINANCIERA 65
9.2.1. COBERTURA DE SEGURO 65
9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL 65
9.3.1. ALCANCE DE LA INFORMACIÓN CONFIDENCIAL 65
9.3.2. INFORMACIÓN FUERA DEL ALCANCE DE LA INFORMACIÓN CONFIDENCIAL 65
9.3.3. RESPONSABILIDAD DE PROTEGER LA INFORMACIÓN CONFIDENCIAL 66
9.4. PRIVACIDAD DE LA INFORMACIÓN PERSONAL 66
9.4.1. PLAN DE PRIVACIDAD 66
9.4.2. INFORMACIÓN TRATADA COMO PRIVADA 66
9.4.3. INFORMACIÓN QUE NO ES CONSIDERADA COMO PRIVADA 66
9.4.4. RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA 66
9.4.5. NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA 66
9.4.6. DIVULGACIÓN DE ACUERDO CON UN PROCESO JUDICIAL O ADMINISTRATIVO 67
9.4.7. OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN 67
9.4.8. INFORMACIÓN A TERCEROS 67
9.5. DERECHO DE PROPIEDAD INTELECTUAL 67
9.6. REPRESENTACIONES Y GARANTÍAS 68
9.6.1. REPRESENTACIONES Y GARANTÍAS DE TERCERAS PARTES 68
9.6.2. CONSENTIMIENTO DE LOS SUSCRIPTORES 68
9.7. EXENCIÓN DE GARANTÍA 68

9.8. LIMITACIONES DE RESPONSABILIDAD LEGAL 68
9.9. INDEMNIZACIONES 68
9.10. PLAZO Y FINALIZACIÓN 69
9.10.1. PLAZO 69
9.10.2. FINALIZACIÓN 69
9.10.3. EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA 69
9.11. NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON PARTICIPANTES 69
9.12. ENMIENDAS 69
9.12.1. PROCEDIMIENTOS PARA ENMIENDAS 69
9.12.2. PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN 69
9.12.3. CIRCUNSTANCIAS EN QUE LOS OID DEBEN SER CAMBIADOS 70
9.13. DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS 70
9.14. NORMATIVA APLICABLE 70
9.15. ADECUACIÓN A LA LEY APLICABLE 70
9.16. DISPOSICIONES VARIAS 70
9.16.1. ACUERDO COMPLETO 70
9.16.2. ASIGNACIÓN 70
9.16.3. INDEPENDENCIA DE LAS DISPOSICIONES 70
10. DOCUMENTOS DE REFERENCIA 71
10.1. REFERENCIA EXTERNA 71
10.2. REFERENCIAS A DOCUMENTOS QUE COMPONEN LA ICPP 72

1. INTRODUCCIÓN

1.1. DESCRIPCIÓN GENERAL

Este documento establece los requisitos mínimos que deben ser obligatoriamente cumplidos por los Prestadores de Cualificados de Servicios de Confianza (PCSC) en su carácter de Autoridad de Certificación Intermedia (ACI), miembros de la Infraestructura de Clave Pública del Paraguay (ICPP) para la elaboración de su Declaración de Prácticas de Certificación relativa al servicio de creación, verificación y validación de sellos cualificados de tiempo electrónico (SCTE). Este documento forma parte de un conjunto de normas de la ICPP y en él se referencian.

Para la prestación del servicio el Prestador requerirá contar con un certificado emitido por la AC Raíz-Py.

Aprobada la habilitación del servicio de Sello Cualificado de Tiempo Electrónico (SCTE), el PCSC deberá emitir un certificado electrónico para el Servidor de Sello de Tiempo Electrónico (SSTE) conforme al perfil indicado en el ítem 7 del presente documento.

El PCSC Sello de tiempo electrónico, conforme la Ley N.° 6.822/2021, se define como datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante.

Sello Cualificado de Tiempo Electrónico (SCTE) se denomina a un sello de tiempo electrónico que debe vincular la fecha y hora con los datos de forma que se elimine razonablemente la posibilidad de modificar los datos sin que se detecte, basarse en una fuente de información temporal vinculada al Tiempo Universal Coordinado y haber sido firmada mediante el uso de una firma electrónica o sellada con un sello electrónico del PCSC o por cualquier método equivalente. El SCTE garantiza y da certeza de exactitud de la fecha y hora que indican y de la integridad de los datos a los que la fecha y hora estén vinculadas.

Este servicio no tiene acceso a la información sobre la cual se crea el SCTE. La prestación de este servicio requiere una petición previa por parte del suscriptor de SCTE (remisión de conjunto de datos) a lo que se debe contestar con la evidencia electrónica correspondiente.

Los SCTE son emitidos por los PCSC, cuyas operaciones deben ser debidamente documentadas y auditadas por un OEC acreditado en el marco de la ICPP y cumplir con los requisitos siguientes:

a) Vincular la fecha y hora con los datos de forma que se elimine razonablemente la posibilidad de modificar los datos sin que se detecte.

b) Basarse en una fuente de información temporal vinculada al Tiempo Universal Coordinado.

c) Haber sido firmada mediante el uso de una firma electrónica o sellada con un sello electrónico de un PCSC.

El PCSC debe declarar en este documento la Fuente Confiable de Tiempo (FCT) que utiliza, la misma podrá consumirse de una fuente oficial de tiempo establecida en la República del Paraguay o extranjera y al igual que su Servidor de Sello de Tiempo (SSTE) deben contar con la autorización correspondiente de la Autoridad de Aplicación. Los relojes de los SSTE deben ser auditados y sincronizados por el PCSC conforme lo dispuesto en el ítem 6.5.5.

El uso de SCTE en el ámbito de ICPP es opcional. El documento firmado o sellado con firma electrónica cualificada o sello electrónico cualificado con una clave privada correspondiente a certificados cualificados en el ámbito de la ICPP son válidos con o sin sello cualificado de tiempo electrónico.

La DPC-SCTE es el documento que describe las prácticas y procedimientos empleados por el PCSC en el desempeño de sus funciones y en la prestación del servicio de expedición de SCTE. De modo general, la política de SCTE indica "lo que debe lograrse", mientras que una declaración de práctica indica “cómo cumplir”, es decir, los procesos que utilizará el PCSC para crear sellos de tiempo y mantener su reloj preciso.

Este documento se basa en las reglas de RFC 3628 y 3161, del IETF y los estandares ETSI EN 319 422 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles y ETSI EN 319 421 V1.2.1 (2023-05) Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

Toda DPC-SCTE elaborada en el ámbito de la ICPP, debe adoptar obligatoriamente la misma estructura utilizada en este documento.

1.2 NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

En este ítem se debe identificar la DPC-SCTE e indicar el OID (Identificador de Objeto) del documento.

1.3 PARTICIPANTES

1.3.1 PRESTADORES CUALIFICADOS DE SERVICIOS DE CONFIANZA (PCSC)

En este ítem debe ser identificado el PCSC integrante de la ICPP a la que se refiere esta DPC-SCTE.

1.3.2 AGENTE DE ATENCIÓN DEL SERVICIO

En este ítem se especifica la figura del Agente de atención al servicio que es el Personal vinculado al PCSC mediante un contrato cuya función es la recepción y trámite de solicitudes vinculadas al servicio.

1.3.3 SUSCRIPTORES

En este ítem se especifican las personas físicas o jurídicas que podrán solicitar SCTE emitidos por el PCSC, de conformidad con esta DPC-SCTE y que acepta los términos del servicio.

1.3.4 PARTE QUE USUARIA

Este ítem se refiere a un tercero (persona física o jurídica) que confía en el contenido, vigencia y aplicabilidad del SCTE emitido en el marco de la ICPP. La Parte Usuaria debe verificar la validez de los certificados en la cadena de certificación.

1.3.5 PRESTADOR DE SERVICIOS DE SOPORTE (PSS)

En 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 PCSC. Los PSS son entidades externas a las que recurre el PCSC para desempeñar todas o parte de las actividades descritas en esta DPC-SCTE o en una PC. Los PSS se clasifican en tres categorías, conforme al tipo de actividades prestadas;

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

El funcionamiento de un PSS vinculado a un PCSC mediante un acuerdo operacional deberá ser autorizado por la AC Raíz-Py.

El PCSC deberá mantener las informaciones arriba citadas siempre actualizadas. El funcionamiento de un PSS vinculado a un PCSC mediante un acuerdo operacional deberá ser autorizado por la AC Raíz-Py. El PCSC deberá igualmente publicar información referente a:

- Lista de todos los PSS habilitados
- Lista de los PSS que se han inhabilitados por el PCSC, indicando la fecha de la inhabilitación.

1.4 USO DEL CERTIFICADO

En este ítem de la DPC-SCTE se debe enumerar e identificar las Políticas de Sello Cualificado de Tiempo Electrónico (PC-SCTE) implementadas por el PCSC, que define ¿cómo los integrantes de la ICPP utilizarán los SCTE emitidos?. En las PC-SCTE se enumeran las aplicaciones o usos para las que son aptos los sellos emitidos por el PCSC y, en su caso, las aplicaciones para las que existan restricciones o prohibiciones en el uso de estos sellos.

1.5 ADMINISTRACIÓN DE LA POLÍTICA

En este ítem se debe incluir el nombre, la dirección y otra información del PCSC responsable de la DPC-SCTE. Igualmente se debe informar nombre, números de teléfono y la dirección de correo electrónico de una persona de contacto.

1.5.1 ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

Nombre del PCSC:

1.5.2 PERSONA DE CONTACTO

Teléfono:
Dirección:
Fax:

Página web:
Correo electrónico:
Otros:

1.5.3 PERSONA QUE DETERMINA LA ADECUACIÓN DE LA DPC-SCTE A LA PC

Nombre:
Teléfono:
Correo electrónico:
Otros:

1.5.4 PROCEDIMIENTOS DE APROBACIÓN DE LA DPC-SCTE

Toda DPC-SCTE debe ser presentada para su aprobación ante la AC Raíz-Py de la ICPP:

- durante el proceso de habilitación como PCSC
- cuando sufriera modificaciones/actualizaciones, presentando la solicitud correspondiente. Cada ítem objeto de modificación/actualización debe ser detallado en el apartado correspondiente del propio documento o en la solicitud pertinente.

1.6 DEFINICIONES 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 Autoridad de Aplicación.

6. **Agente de Atención del Servicio**: personal vinculado al PCSC mediante un contrato cuya función es la recepción y trámite de solicitudes vinculadas al servicio.

7. **Cadena de certificación:** lista ordenada de certificados que contiene un certificado del firmante o creador de sello y certificados de la AC, que termina en un certificado raíz. El emisor del certificado del firmante o creador de sello es el titular del certificado del PCSC y a su vez, el emisor del certificado del PCSC es el titular del certificado de AC Raíz-Py. El firmante, creador de sello o la parte usuaria debe verificar la validez de los certificados en la cadena de certificación.

8. **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.

9. **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.

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

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

12. **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.

13. **Contrato de prestación de servicios de sello cualificado de tiempo electrónico**: Acuerdo entre el PCSC y el suscriptor del servicio que contiene información relativa al solicitante del servicio y además establece los derechos, obligaciones y responsabilidades de las partes con respecto a la prestación del servicio. Este contrato, requiere la aceptación explícita de las partes intervinientes.

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

15. **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.

16. **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.

17. **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.
18. **Documento de identidad:** documento válido y vigente que permite acreditar la identidad de la persona, a los efectos del proceso de emisión, suspensión o revocación del certificado cualificado electrónico será considerada la cédula de identidad civil o el pasaporte del solicitante.

19. **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.

20. **Firmante:** una persona física que crea una firma electrónica.

21. **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.

22. **Habilitación:** autorización que otorga el MIC, una vez cumplidos los requisitos y condiciones establecidos en la norma.

23. **Identificador de Objeto:** 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.

24. **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.

25. **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.

26. **Lista de Certificados Revocados:** lista emitida por una AC, publicada periódicamente y que contiene los certificados que han sido revocados antes de sus respectivas fechas de vencimiento.

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

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

29. **Normas Internacionales:** requisitos de orden técnico y de uso internacional que deben observarse en la prestación de los servicios mencionados en la presente DPC.

30. **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.

31. **Organismo de Supervisión:** organismo que concede y retira la cualificación a los prestadores de servicios de confianza y a los servicios de confianza que prestan además de las funciones establecidas en el artículo 17 de la Ley Nº 6822/2021.

32. **Parte usuaria:** persona física o jurídica que confía en el servicio de confianza.

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

34. **Política de Certificación:** documento en el cual la AC 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.

35. **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.

36. **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.

37. **Prestador de Servicios de Soporte:** entidad externa vinculada a un PCSC mediante un acuerdo operacional a la que recurre la AC o la AR y autorizada por la AC Raíz-Py para desempeñar actividades descritas en la DPC o en una PC.

38. **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.

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

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

41. **Sello de tiempo electrónico:** datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante.

42. **Sello cualificado de tiempo electrónico:** sello cualificado de tiempo electrónico que debe vincular la fecha y hora con los datos de forma que se elimine razonablemente la posibilidad de modificar los datos sin que se detecte, basarse en una fuente de información temporal vinculada al Tiempo Universal Coordinado y haber sido firmada mediante el uso de una firma electrónica o sellada con un sello electrónico del prestador cualificado de servicios de confianza o por cualquier método equivalente.

43. **Suscriptor:** persona física o jurídica que adquiere y utiliza el servicio de sello cualificado de tiempo electrónico.

44. **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.

45. **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.

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

1.6.1 SIGLAS Y ACRÓNIMOS

Tabla Nº 1 - Siglas y Acrónimos

Sigla/Acrónimo	Descripción
AC	Autoridad de Certificación (CA por sus siglas en inglés, Certificate Authority)
AC Raíz-Py	Autoridad Certificadora Raíz del Paraguay
CCTV	Circuito cerrado de TV
DPC-SCTE	Declaraciones de prácticas de sello cualificado de tiempo electrónico
LCR	Lista de certificados revocados (CRL por sus siglas en inglés, Certificate Revocation List)
DGCE	Dirección General de Comercio Electrónico dependiente del Viceministerio de Comercio y Servicios.
ISO	Organización Internacional para la Estandarización (ISO por sus siglas en inglés, International Organization for Standardization).
FCT	Fuente confiable de tiempo

MIC	Ministerio de Industria y Comercio
MSC	Módulo de seguridad criptográfico
OID	Identificador de Objeto (OID por sus siglas en inglés, Object Identifier)
OU	Unidad Organizacional (OU por sus siglas en inglés, Organization Unit)
PKI	Infraestructura de Clave Pública (PKI por sus siglas en inglés, Public Key Infrastructure).
ICPP	Infraestructura de Clave Pública del Paraguay
OEC	Organismo de Evaluación de la Conformidad
OS	Organismo de Supervisión
PCSC	Prestador cualificado de servicios de confianza
PCN	Plan de Continuidad de negocio
PC-SCTE	Política de certificación de sello cualificado de tiempo electrónico
PS	Política de Seguridad
PSS	Prestador de Servicios de Soporte
RFC	Petición de Comentarios (RFC por sus siglas en inglés, Request For Comments)
SCTE	Sello cualificado de tiempo electrónico
SSTE	Servidor de Sello de tiempo electrónico
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).
ETSI	European Telecommunication Standard Institute
ITSEC	European Information Technology Security Evaluation Criteria
ITU	International Telecommunications Union
SNMP	Simple Network Management Protocol
TSP	Protocolo de Sello de Tiempo (TSP por sus siglas en inglés, Time Stamp Protocol)
TSQ	Solicitud de Sello de Tiempo (URL por sus siglas en inglés, Timestamp Request)

2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO

2.1 REPOSITORIOS

Este ítem se deben incluir las siguientes informaciones como mínimo y ser publicadas por el PCSC responsable de la DPC-SCTE en el repositorio:

A. el certificado del SSTE con el que opera;
B. los sellos emitidos a solicitud del suscriptor;
C. su DPC-SCTE;
D. las PC-SCTE que implementa;
E. las condiciones generales bajo las cuales se prestan los servicios de SCTE;
F. la exactitud del sello de tiempo con respecto al FCT;
G. algoritmos hash que pueden utilizar los suscriptores y el algoritmo hash utilizado por el PCSC;
H. una lista actualizada regularmente de los PSS vinculados al PCSC.
I. la resolución del MIC que habilita la prestación de servicios como Prestador Cualificado de SCTE.
J. proforma de contrato de prestación de servicios de sello cualificado de tiempo electrónico.

2.2 TIEMPO O FRECUENCIA DE PUBLICACIÓN

En este ítem, se debe describir la frecuencia de publicación de la información tratada en el punto anterior, con el fin de asegurar la disponibilidad siempre actualizada de su contenido.

El servicio de publicación de información de un PCSC debe estar disponible durante las veinticuatro (24) horas, los siete (7) 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 (24) horas, garantizando la disponibilidad del servicio con un mínimo de 99,5% anual, un tiempo programado de inactividad máximo de 0.5% anual.

2.3 CONTROLES DE ACCESO A LOS REPOSITORIOS

Este ítem debe describir los controles y eventuales restricciones de acceso, lectura y redacción de la información publicada por el PCSC, de conformidad con lo dispuesto en las normas, criterios, prácticas y procedimientos de la ICPP.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

En este ítem, el PCSC responsable deberá describir la forma utilizada para identificar y autenticar a los solicitantes de SCTE, en caso de ser necesario para la realización de dichos trámites.

La TSQ no identifica al solicitante, por lo tanto, en situaciones cuando el PCSC necesite conocer la identidad del solicitante, se deben utilizar medios alternativos de identificación y autenticación.

4. REQUERIMIENTOS OPERACIONALES

Como primer mensaje de este mecanismo, el suscriptor solicita un SCTE enviando una solicitud (que es o incluye TSQ) al PCSC.

Como segundo mensaje, el PCSC responde enviando una respuesta (que es o incluye un sello de tiempo) al suscriptor.

4.1 SOLICITUD DE SCTE

Para solicitar un SCTE en un documento electrónico, el suscriptor debe enviar un TSQ que contiene el hash a firmar o sellar.

Este ítem debe describir todos los requisitos y procedimientos operativos relacionados con la solicitud de un sello de tiempo indicando el protocolo a implementar para el envío de la TSQ, definido en el RFC 3161.

Cada PC-SCTE implementada por el PCSC responsable debe definir los procedimientos específicos para la solicitud de sellos de tiempo emitidos bajo la PC-SCTE, con base a los requisitos aplicables establecidos por el documento DOC-ICPP-26 [4].

4.1.1 QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE SCTE

En este ítem, se deben indicar las personas físicas o jurídicas que puedan solicitar sellos de tiempo emitidos de conformidad con esta DPC-SCTE.

4.1.2 PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES

Los siguientes ítems deben describir las obligaciones generales de las entidades involucradas. Si existen obligaciones específicas para las PC-SCTE implementadas, se deben describir en dichas PC-SCTE, en el ítem correspondiente.

4.1.2.1 RESPONSABILIDADES Y OBLIGACIONES DEL PCSC

Responsabilidades del PCSC

A. Los PCSC deben responder por los daños y perjuicios que causen a cualquier persona en el ejercicio de sus actividades cuando incumplan las obligaciones que les impone la normativa vigente.

B. Los PCSC deben asumir toda la responsabilidad frente a terceros por la actuación de las personas u otros prestadores en los que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios de confianza, incluyendo las actuaciones de comprobación de identidad previas a la expedición de un certificado cualificado.

Obligaciones del PCSC

Este ítem debe incluir las obligaciones del PCSC responsable de la DPC-SCTE, conteniendo, al menos lo siguiente:

a) operar de acuerdo con su DPC-SCTE y las PC-SCTE que implementan;
b) generar, administrar y asegurar la protección de las claves privadas del SSTE;
c) mantener el SSTE sincronizado (con una FCT autorizada por la AA);
d) tomar las medidas apropiadas para asegurar que los usuarios y otras entidades involucradas tengan conocimiento de sus respectivos derechos y obligaciones;
e) monitorear y controlar el funcionamiento de los servicios prestados;
f) asegurar que sus relojes están sincronizados, con autenticación, con la fuente confiable de tiempo establecido por la Autoridad de Aplicación;
g) En marco de la auditoría permitir el acceso del OEC al SSTE de su propiedad;
h) notificar a la AC Raíz-Py cuando su clave privada se vea comprometida y solicitar la revocación inmediata del certificado correspondiente;
i) notificar a sus usuarios cuando exista la sospecha de compromiso de su clave privada, la emisión de un nuevo par de claves y certificado correspondiente o la terminación de sus actividades;
j) publicar en su sitio web, las informaciones definidas en el ítem 2.1, y en la frecuencia establecida en el ítem 2.2 de este documento.
k) identificar y registrar todas las acciones realizadas, de conformidad con las normas, prácticas y reglas establecidas por la AC Raíz-Py de la ICPP;
m) adoptar las medidas de seguridad y control previstas en la DPC-SCTE, PC-SCTE, PS que implementan, involucrando en sus procesos, procedimientos y actividades, observadas las normas, criterios, prácticas y procedimientos de la ICPP;
n) mantener el cumplimiento de sus procesos, procedimientos y actividades con las normas, prácticas y reglamentos de la ICPP y legislación vigente;
o) mantener y garantizar la integridad, la confidencialidad y la seguridad de la información que maneja;
p) mantener y probar anualmente su PCN;
q) mantener un contrato de seguro que cubra la responsabilidad civil derivada de la actividad de emisión de SCTE, con cobertura suficiente y compatible con el riesgo de sus actividades en concordancia con lo dispuesto en el artículo 10 numeral 3 inciso b) de la Ley N° 6822/21;
r) informar a la parte usuaria y suscriptores de SCTE sobre las garantías, coberturas, condiciones y limitaciones estipuladas en la póliza de seguro de responsabilidad civil contraída en los términos señalados en el párrafo anterior; y
s) informar a la AC Raíz-Py, mensualmente, la cantidad de SCTE emitidos.
t) suscribir el contrato de prestación de servicio de sello cualificado de tiempo electrónico y almacenarlo en el dossier del suscriptor

4.1.2.2 OBLIGACIONES DEL SUSCRIPTOR

Al recibir un SCTE, el suscriptor debe verificar que se haya firmado o sellado el SCTE correctamente y que la clave privada utilizada para firmar o sellar el SCTE no se haya visto comprometida.

Deberá suscribir el Contrato de Prestación de Servicio de sello cualificado de tiempo electrónico.

4.2 EMISIÓN DEL SCTE

En este punto se debe describir todos los requisitos y procedimientos operativos relacionados con la emisión de un SCTE y el protocolo a implementar, entre los definidos en el RFC 3161.

Como principio general, el PCSC debe proporcionar a los suscriptores acceso a un **Servidor de Aplicaciones**, reenviar las TSQ recibidas al SSTE y luego devolver al suscriptor los SCTE recibidos en respuesta a las TSQ.

El Servidor de Aplicaciones puede consistir en:

a) sistema instalado en el equipo que realiza las funciones de SSTE;

b) sistema instalado en equipos del PCSC distintos al SSTE;

c) sistema instalado en la estación de trabajo del suscriptor;

d) una combinación de las soluciones anteriores.

En cualquiera de los casos anteriores, la provisión y correcto funcionamiento del Servidor de Aplicaciones es responsabilidad del PCSC.

El Servidor de Aplicaciones deberá realizar al menos las siguientes tareas:

a) identificar y validar, en su caso, el usuario que accede al sistema;

b) recibir los hash que serán sellados;

c) enviar los hash a sellar al SSTE

d) recibir de vuelta los hash debidamente sellados;

e) comprobar la firma o sello electrónico cualificado del SSTE;

f) comprobar el hash recibido de vuelta del SSTE con el hash enviado al SSTE;

g) devolver el hash al usuario debidamente firmado o sellado;

h) enviar automáticamente al SSTE alterno, en caso de avería del SSTE principal;

i) enviar alarmas por correo electrónico a los responsables cuando existan problemas de acceso al SSTE.

El SSTE, al recibir el TSQ, deberá realizar la siguiente secuencia:

a) verificar si la solicitud está de acuerdo con las especificaciones de la norma RFC 3161. En caso de que esté, realizando las operaciones descritas a continuación. Si la solicitud no cumple con las especificaciones, el SSTE debe responder de acuerdo con el punto 2.4.2 de la RFC 3161, con un valor de estado diferente de 0 o 1, e indicar en el campo “PKIFailureInfo” cuál fue el fallo ocurrido sin emitir, en este caso, una estampa de tiempo y finalizando sin ejecutar las siguientes etapas;

b) generar SCTE solo para solicitudes válidas;
c) usar una FCT;
d) incluir un valor de tiempo confiable para cada sello de tiempo;
e) incluir en la respuesta un identificador único para cada sello de tiempo emitido;
f) incluir en cada SCTE un identificador de la política bajo la cual fue creada el sello de tiempo;
g) solo sellar el hash de los datos y no los datos en sí;
h) verificar si el tamaño del hash recibido está de acuerdo con la función hash utilizada;
i) no examinar el hash que está siendo sellado, de ninguna manera excepto para verificar su cumplimiento, de acuerdo con el artículo anterior;
j) no incluir en el SCTE algún tipo de información que pueda identificar al solicitante de sello de tiempo;
k) firmar o sellar cada SCTE con una clave única generada exclusivamente para ese objetivo;
l) la inclusión de información adicional a pedido del solicitante debe realizarse en los campos de extensión soportados y en caso de que no sea posible, se debe responder con un mensaje de error;
m) encadenar el SCTE actual con el anterior, en caso de que el PCSC haya adoptado el mecanismo de encadenamiento.

El PCSC responsable deberá informar en su PC-SCTE la disponibilidad de sus servicios de SCTE. Esta disponibilidad deberá ser, como mínimo, del 99,5% (noventa y nueve coma cinco por ciento) del mes, las 24 horas del día, los 7 días de la semana.

4.3 ACEPTACIÓN DE SCTE

Este punto debe describir todos los requisitos y procedimientos operativos relacionados con la aceptación de un SCTE recibido por el suscriptor.
Una vez recibida la respuesta (que es o incluye un TimeStampResp, que normalmente contiene un sello de tiempo electrónico), el suscriptor debe verificar el estado de error devuelto por la respuesta y, si no hay ningún error presente, debe verificar los campos contenidos en el SCTE y la validez de la firma electrónica cualificada del SCTE.

En particular, debe verificarse la correspondencia entre lo que se selló y lo recibido para sellar, efectivamente. El suscriptor también debe verificar que el SCTE fue firmado o sellado por un PCSC habilitado y que el hash de los datos y el OID del algoritmo hash son correctos. Luego debe verificar el tiempo de la respuesta analizándolo contra una fuente de tiempo local confiable, si la hay, o el valor del número de control incluido en la respuesta, contra el número incluido en la solicitud. Si alguna de las comprobaciones anteriores falla, el SCTE debe ser rechazado.

Además, dado que el certificado del SSTE pudo haber sido revocado, se debe verificar el estado del certificado (por ejemplo, consultando la LCR correspondiente) para comprobar que el certificado sigue siendo válido.

Posteriormente, el suscriptor debe verificar el campo “política” para determinar si la política bajo la cual fue emitida el sello es aceptable o no para la solicitud.

Cada PC-SCTE implementada por el PCSC responsable debe definir los procedimientos específicos para la aceptación de SCTE emitidos bajo la PC-SCTE, con base en los procesos anteriores y en los requisitos aplicables establecidos por el documento DOC-ICPP-26 [4].

4.4. CARACTERÍSTICAS DEL SCTE

En este ítem se deberá informar las características de los sellos de tiempo que serán emitidos según PC-SCTE, que contenga al menos:

a) la exactitud o precisión mínima de la hora registrada en el sello;
b) la unidad utilizada en el campo genTime del SCTE (segundos, milisegundos o microsegundos).

5. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES

Los siguientes puntos deben describir los controles de seguridad implementados por PCSC responsable del DPC-SCTE y de los PSS vinculados a ella para desempeñar sus funciones de manera segura.

5.1. SEGURIDAD FÍSICA

En los siguientes ítems de la DPC-SCTE, se deben describir los controles físicos relacionados con las instalaciones que albergan los sistemas del PCSC responsable y el PSS vinculado.

5.1.1. CONSTRUCCIÓN Y UBICACIÓN DE LAS INSTALACIONES DEL PCSC

La DPC-SCTE debe establecer que la localización de las instalaciones donde se albergan los sistemas relativos a la expedición del SCTE del PCSC responsable, no deberá ser públicamente identificada.

La localización administrativa/operacional, entiéndase una AR, podrá ser accesible al público, para los casos en que el solicitante presente en soporte magnético los documentos electrónicos que requieran el servicio, ya que el mismo no sólo puede ser provisto a través de Internet u otra red de datos. De considerarse esta posibilidad deberá el PCSC contemplar en su respectiva DPC y PC.

5.1.2. ACCESO FÍSICO A LAS INSTALACIONES DEL PCSC

Todo PCSC integrante de la ICPP debe implementar un sistema de control de acceso físico que garantice la seguridad de sus instalaciones, conforme al ítem 9 “control de accesos” de la norma ISO 27002:2022 y los requisitos que siguen.

5.1.2.1. NIVELES DE ACCESO FÍSICO

La DPC-SCTE deberá definir al menos 3 (tres) niveles de acceso físico a los distintos ambientes del PCSC responsable y 1 (un) cuarto nivel relacionado con la protección del SSTE.

El primer nivel o nivel 1 debe estar ubicado después de la primera barrera de acceso a instalaciones del PCSC. El ambiente de nivel 1 de los PCSC de la ICPP cumple la función de interfaz con el cliente que quiere usar el servicio de SCTE y necesita asistir personalmente al PCSC.

El segundo nivel o nivel 2 será interno al primero y deberá requerir la identificación individual de las personas que ingresan al mismo. Este será el nivel mínimo de seguridad, necesarios para la ejecución de cualquier proceso operativo o administrativo de PCSC. El paso del primer al segundo nivel debe requerir factor de autenticación electrónica y tarjeta de identificación visible.

El ambiente del nivel 2 debe estar separado del nivel 1 por paredes divisorias de mampostería o de cartón de yeso prefabricado. No debe haber ventanas u otro tipo de apertura al exterior, excepto la puerta de acceso.

Sólo se debe permitir el acceso a este nivel, a las personas que trabajan directamente con las actividades de sellado de tiempo o con la persona responsable del mantenimiento de sistemas y equipos del PCSC, como administradores de red y técnicos de soporte de informática. No será admitido el acceso a este nivel de otras personas ajenas a las actividades, salvo que estén acompañadas por alguien que tenga acceso autorizado.

Equipos como UPS, generadores y otros componentes de la infraestructura física deben estar alojados en este nivel, para evitar el acceso al ambiente de nivel 3 por parte de los proveedores de servicios de mantenimiento.

Salvo en los casos previstos en la ley, no se admitirá portar armas en Instalaciones del PCSC, a partir del nivel 2. El ingreso y uso de equipos de grabación, fotografía, vídeo, sonido o similar, así como ordenadores portátiles requeridos en este nivel, será permitido con autorización formal y bajo supervisión; igualmente, dicho ingreso deberá ser registrado previo al acceso.

El tercer nivel o nivel 3 deberá estar ubicado dentro del segundo y será el primer nivel para albergar material sensible y actividades de la operación del PCSC. Cualquier actividad relacionada con la emisión de SCTE se realizará a este nivel. Solo personas autorizadas pueden permanecer en ese nivel.

En el tercer nivel, se deberá llevar registro de tanto las entradas como las salidas de cada persona autorizada. Se requerirán dos factores de autenticación para la entrada a este nivel: algún tipo de identificación individual, como una tarjeta electrónica, y la identificación de datos biométricos o acceso mediante contraseña.

Las paredes que delimitan el ambiente del nivel 3 deben ser sólidas y de mampostería o material fuerza equivalente o superior. No debe haber ventanas u otro tipo de abertura al exterior, excepto la puerta de acceso.

Si el ambiente correspondiente al Nivel 3 cuenta con un techo o piso falso, es necesario implementar medidas para prevenir el acceso no autorizado a dicho medio a través de estos elementos. Estas medidas podrían incluir la instalación de rejillas de hierro, las cuales se extenderían desde las paredes hasta las losas de hormigón que conforman tanto la parte superior como la inferior de la estructura.

Deberá haber una sola puerta de acceso al ambiente de nivel 3, que se abre solo después de que el empleado se haya autenticado electrónicamente en el sistema de control de acceso. La puerta debe estar equipada con bisagras que permitan la apertura hacia el exterior, para facilitar la salida y dificultar la entrada al ambiente, así como un mecanismo de cierre automático, para evitar que permanezca abierta más tiempo del necesario.

El PCSC podrá tener varios ambientes en el nivel 3 para albergar y segregar, cuando corresponda:

a) equipo de producción y cofre de almacenamiento; y
b) equipos e infraestructura de red (firewall, enrutadores, conmutadores y servidores).

El cuarto nivel, o nivel 4, interno al ambiente de nivel 3, debe comprender por lo menos 2 cofres o armarios reforzados, que albergarán por separado:

a) los SSTE y equipo criptográfico;
b) otros materiales criptográficos, tales como tarjetas, claves, datos de activación y sus copias.

Para garantizar la seguridad del material almacenado, las cajas fuertes o gabinetes deben cumplir con las siguientes especificaciones mínimas:

a) ser de acero o de un material de resistencia equivalente; y
b) tener una cerradura con llave.

El cofre o gabinete que albergará el SSTE deberá estar bajo llave para que su apertura sólo sea posible con la presencia de dos empleados de confianza del PCSC.

5.1.2.2. SISTEMAS FÍSICOS DE DETECCIÓN

La seguridad de todos los ambientes del PCSC debe realizarse bajo vigilancia 24X7 (las veinticuatro horas del día, los siete días de la semana).

La seguridad puede ser realizada por:

a) guardia armada, uniformada, debidamente entrenada y capacitada para realizar tareas de vigilancia; o
b) CCTV, sensores de intrusión instalados en todas las puertas y ventanas y sensores de movimiento, monitoreados local o remotamente por una empresa de seguridad especializada.

El ambiente de nivel 3 debe estar adicionalmente equipado con circuito cerrado de TV conectado a un sistema de grabación local 24x7. La ubicación y capacidad de estas cámaras no debe permitir la captura de contraseñas tecleadas en los sistemas.

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

El PCSC deberá contar con mecanismos que permitan, en caso de corte de energía:

a) Iluminación de emergencia en todos los ambientes, activado automáticamente;
b) Continuidad de funcionamiento de los sistemas de alarma y del CCTV.

5.1.2.3. SISTEMAS DE CONTROL DE ACCESO

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

5.1.3. ENERGÍA Y AIRE ACONDICIONADO DEL AMBIENTE DE NIVEL 3 DEL PCSC

La infraestructura del ambiente nivel 3 del PCSC, debe estar dimensionada con sistemas y dispositivos que garanticen el suministro ininterrumpido de energía eléctrica a las instalaciones. Las condiciones de suministro de energía deben mantenerse para cumplir con los requisitos de disponibilidad de los sistemas del PCSC y sus respectivos servicios. Un sistema de puesta a tierra debe ser implementado.

Todos los cables eléctricos deben estar protegidos por tuberías o ductos 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, en el menos cada 6 (seis) meses, en busca de evidencias 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 27002/2022. Cualquier modificación en esa red deberá ser previamente documentada.

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

El sistema de climatización deberá cumplir con los requisitos de temperatura y humedad exigidos por los equipos utilizados en el medio ambiente.

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

La capacidad de redundancia de toda la estructura de energía y de climatización del ambiente de nivel 3 del PCSC debe garantizar por medio de UPS y generadores de tamaño compatible.

5.1.4. EXPOSICIÓN AL AGUA

El entorno del PCSC del nivel 3 debe instalarse en un lugar protegido contra la exposición al agua, filtraciones e inundaciones.

5.1.5. PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO

No se permitirá fumar ni portar objetos que produzcan fuego o chispa, a partir del nivel 2.

Los extintores de clase B y C deben estar dentro del ambiente de nivel 3, para apagar incendios en combustibles y equipos eléctricos, dispuestos de tal manera que faciliten su acceso y manipulación. Si hay un sistema de rociadores en el edificio, el ambiente de nivel 3 del PCSC no debe tener salidas de agua, para evitar daños al equipamiento.

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

En los demás ambientes del PCSC, deberá haber extintores para todas las clases de fuego, dispuestos en lugares que faciliten su acceso y manipulación.

El PCSC debe implementar mecanismos específicos para garantizar la seguridad de su personal y de su equipamiento en situaciones de emergencia. Estos mecanismos deben permitir el desbloqueo de puertas mediante accionamiento mecánico, para la salida de emergencia de todos ambientes con control de acceso. La salida realizada a través de estos mecanismos debe activar inmediatamente la apertura de las puertas.

5.1.6. ALMACENAMIENTO DE MEDIOS

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 se debe almacenar 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 información clasificada como sensible deben ser triturados antes de ser desechados.

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

5.1.8. RESPALDO FUERA DE SITIO

Se debe utilizar una sala de almacenamiento fuera de la instalación técnica principal del PCSC para el almacenamiento y la retención de copias de seguridad de datos. Esta sala debe estar disponible al personal autorizado, 24X7 (las veinticuatro horas del día, los 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 siguientes artículos de la DPC-SCTE, deben ser descriptos los requisitos para la caracterización y el reconocimiento de los Roles de Confianza del PCSC responsable y las PSS vinculadas a ella, con las responsabilidades definidas para cada perfil. También se debe establecer el número de personas necesarias para la ejecución de cada tarea asociada a los roles o perfiles definidos.

5.2.1. ROLES DE CONFIANZA

El PCSC responsable de la DPC-SCTE debe garantizar la segregación de tareas para las funciones críticas, con el fin de evitar que un empleado utilice indebidamente el SSTE sin ser detectado. Las acciones de cada empleado deben estar limitadas de acuerdo a su perfil.
El PCSC deberá establecer un mínimo de 3 (tres) roles o perfiles distintos para su funcionamiento, descriptos a continuación:

a) Administrador del sistema: autorizado para instalar, configurar y mantener sistemas confiables para gestionar el SCTE, así como administrar la implementación de las prácticas de seguridad del PCSC;
b) Operador del Sistema: responsable por la operación diaria de los sistemas confiables del PCSC. Autorizado para realizar copias de seguridad (backup) y recuperación del sistema.
c) Auditor del sistema: autorizado para ver archivos y auditar los registros de los sistemas confiables del PCSC.

Todos los empleados del PCSC deben recibir capacitación específica antes de obtener cualquier tipo de acceso. El tipo y nivel de acceso será determinado, en un documento formal, con base en las necesidades de cada rol o perfil.

Cuando un empleado se desvincula del PCSC, sus permisos de acceso deben ser revocados inmediatamente. Cuando se produzca un cambio en el puesto o función que ocupe el empleado dentro del PCSC, se deben revisar sus permisos de acceso. Debe existir una lista de revocación, con todos los recursos previamente puestos a su disposición, que el empleado deberá devolver al PCSC en el acto de su desvinculación.

5.2.2. NÚMERO DE PERSONAS REQUERIDAS POR TAREA

La DPC-SCTE debe establecer el requisito de control multiusuario para la generación de claves de los SSTE operados por el PCSC responsable, conforme definido en el ítem 6.1.1.

Todas las tareas realizadas en el cofre o gabinete donde se encuentran los SSTE deben requerir la presencia de al menos 2 (dos) empleados con roles de confianza. Las demás tareas del PCSC pueden ser realizadas por un solo empleado.

5.2.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

La DPC-SCTE debe garantizar que todo empleado del PCSC responsable tendrá su identidad y perfil comprobado antes de que:

a) sean incluidos en una lista de acceso físico a las instalaciones del PCSC;
b) sean incluidos en la lista de acceso lógico a los sistemas de confianza del PCSC
c) sean incluido en una lista para acceso lógico a los SSTE del PCSC;

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

a) ser directamente asignados a un único empleado;
b) no ser compartidos; y
c) ser restringidas las acciones asociadas con el perfil para los cuales fueron creados.

El PCSC deberá implementar una política para el uso de "contraseñas seguras", definidas en su PS, con procedimientos de validación de estas contraseñas.

5.3. CONTROLES DE PERSONAL

En los siguientes ítems de la DPC-SCTE deben ser descritos los requisitos y procedimientos, implementados por el PCSC responsable y PSS vinculados en relación a todo su personal, referente a aspectos como: verificación de antecedentes e idoneidad, capacitación, rotación de puestos, sanciones por acciones no autorizadas, controles para contratación y documentación a ser proporcionada.

La DPC-SCTE debe garantizar que todos los empleados del PCSC responsable y PSS vinculados, a cargo de las tareas operativas tengan registrado en un contrato o término de responsabilidad:

a) los términos y condiciones del perfil que ocupan;
b) el compromiso de observar las normas, políticas y reglas aplicables al ICPP; y
c) el compromiso de no divulgar información confidencial a quienes tengan acceso.

5.3.1. REQUERIMIENTOS DE EXPERIENCIA Y CAPACIDAD

Todo el personal responsable del PCSC y los PSS vinculados e involucrado en las actividades directamente relacionados con los procesos de emisión, expedición, distribución, revocación y gestión de certificado deberá ser seleccionado y admitido conforme a lo establecido en el ítem 7 "seguridad ligada a los recursos humanos" de la norma ISO 27002/2022. El PCSC responsable puede definir requisitos adicionales para la admisión.

5.3.2. PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES

Con el propósito de resguardar la seguridad y credibilidad de las entidades, todo el personal del PCSC responsable y PSS vinculados e involucrados en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gestión de certificado de sellos de tiempo debe ser sometido a:

a) confirmación de empleos anteriores;
b) verificación de referencias profesionales;
c) título académico obtenido; y
d) verificación de antecedentes judiciales y policiales.

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

5.3.3. REQUERIMIENTOS DE CAPACITACIÓN

Todo el personal del PCSC responsable y los PSS vinculados e involucrados en las actividades directamente relacionados con la emisión, expedición, distribución, revocación y gestión del certificado deberá recibir capacitación o entrenamiento documentado, suficiente para el dominio de los siguientes temas:

a) principios y tecnologías de sello de tiempo y sistema de sello de tiempo en uso en el PCSC;
b) ICPP;
c) principios y tecnologías de certificación electrónica y firma/sello electrónico;
d) principios y mecanismos de seguridad de red y seguridad del PCSC;
e) procedimientos de recuperación de desastres y continuidad del negocio;
f) familiaridad con los procedimientos de seguridad, para personas con responsabilidad de Oficial de Seguridad;
g) familiaridad con los procedimientos de auditoría en sistemas informáticos, para personas con la responsabilidad de Auditores de Sistemas;
h) otros asuntos relacionados con las actividades bajo su responsabilidad.

5.3.4. REQUERIMIENTOS Y FRECUENCIA DE CAPACITACIÓN

Todo el personal del PCSC responsable y los PSS vinculados e involucrados en las actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gestión de los SCTE deben ser mantenidos actualizados sobre eventuales cambios o modificaciones tecnológicas de los sistemas del PCSC.

5.3.5. FRECUENCIA Y SECUENCIA EN LA ROTACIÓN DE LAS FUNCIONES

En este ítem, la DPC-SCTE podrá definir una política a ser adoptada por el PCSC responsable y por el PSS vinculado, para la rotación del personal en los diversos cargos y perfiles establecidos por los mismos. Esta política no debe contradecir los propósitos establecidos en el ítem 5.2.1 para la definición de roles de confianza.

5.3.6. SANCIONES PARA ACCIONES NO AUTORIZADAS

La DPC-SCTE deberá prever que, ante una acción no autorizada, real o sospechosa, realizado por una persona encargada del proceso operativo del PCSC responsable o de un PSS vinculado, el PCSC deberá suspender de inmediato el acceso de esa persona al SSTE, iniciar el procedimiento administrativo para determinar los hechos y, si es necesario, adoptar las medidas legales pertinentes.

El procedimiento administrativo a que se refiere el párrafo anterior deberá contener, al menos, los siguientes elementos:

a) relato de lo ocurrido con el modo de operación o “modus operandis”;
b) identificación de los involucrados;

c) descripción de eventuales perjuicios causados;
d) sanciones aplicadas, en su caso; y
e) conclusiones.

Concluido el procedimiento administrativo, el PCSC responsable deberá comunicar sus conclusiones a la AC Raíz-Py.

Las sanciones que se pueden aplicar, como resultado de un procedimiento administrativo, son:

a) una advertencia;
b) suspensión por un plazo determinado; o
c) cese de sus funciones.

5.3.7. REQUISITOS DE CONTRATACIÓN A TERCEROS

Todo el personal del PCSC responsable y los PSS vinculados e involucrados en las actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gestión de los sellos de tiempo deberá ser contratado conforme lo establecido en los ítems 7 “seguridad ligada a los recursos humanos” y 15 “relaciones con suministradores” norma ISO 27002/2022. El PCSC responsable puede definir requisitos adicionales para contratar.

5.3.8. DOCUMENTACIÓN SUMINISTRADA AL PERSONAL

La DPC-SCTE deberá asegurar que el PCSC responsable pone a disposición de todo su personal y para el personal vinculado al PSS, al menos:

a) su DPC-SCTE;
b) las PC-SCTE que implementa;
c) la Política de Seguridad (PS) que implementa el PCSC;
d) documentación operacional relativa a sus actividades; y
e) contratos, normas y políticas relevantes para sus actividades.

Toda la documentación entregada al personal debe clasificarse de acuerdo con la PS, clasificación de la información definida por el PCSC y deberá mantenerse actualizada.

5.4. PROCEDIMIENTO DE REGISTRO DE AUDITORÍA

En los siguientes ítems de la presente DPC-SCTE, se deben describir aspectos de los sistemas de auditoría y registro de eventos implementados por el PCSC responsable con el fin de mantener un ambiente seguro.

5.4.1. TIPOS DE EVENTOS REGISTRADOS

El PCSC responsable de la DPC-SCTE debe registrar en archivos de auditoría todos los eventos relacionados a la seguridad de su sistema. Entre otros, los siguientes eventos deben incluirse en los archivos de auditoría:

a) inicio y cierre del SSTE;
b) intentos de crear, eliminar, establecer contraseñas o cambiar los privilegios del sistema de los operadores del PCSC;
c) cambios en la configuración de la SSTE o en sus claves;
d) cambios en las políticas de creación de SCTE;
e) intentos de acceso (login) y salida del sistema (logoff);
f) intentos no autorizados de acceso a los archivos del sistema;
g) generación de claves propias del SSTE y otros eventos relacionados con el ciclo de vida estos certificados;
h) emisión de SCTE;
i) intentos de iniciar, eliminar, habilitar y deshabilitar usuarios del sistema y actualizar y recuperar sus claves;
j) operaciones fallidas de escritura o lectura, cuando corresponda; y
k) todos los eventos relacionados con la sincronización de los relojes de los SSTE con la FCT; eso incluye como mínimo:

i. la propia sincronización;
ii. desvío de tiempo o retardo de propagación por encima de un valor especificado;
iii. falta de señal de sincronización;
iv. intentos fallidos de autenticación;
v. detección de pérdida de sincronización.

El PCSC responsable de la DPC-SCTE también deberá registrar, electrónica o manualmente, información de seguridad no generada directamente por su sistema, como:

a) registros de accesos físicos;
b) mantenimiento y cambios en la configuración de sus sistemas;
c) cambios en el personal y de su rol de confianza;
d) informes de discrepancias y compromisos; y
e) registros de destrucción de medios de almacenamiento que contengan las claves criptográficas, los datos activación de certificados o de la información personal de los usuarios.

En este ítem, la DPC-SCTE deberá especificar todas las informaciones que deberán ser registradas por el PCSC responsable.

La DPC-SCTE debe prever que todos los registros de auditoría, electrónicos o manuales contengan la identidad del agente que lo provocó, así como la fecha y hora del evento. Los registros electrónicos de auditoría deben contener la hora UTC. Los registros manuales en papel pueden contener la hora local especificando la ubicación.

Para facilitar los procesos de auditoría, toda la documentación relacionada con los servicios del PCSC debe almacenarse, electrónica o manualmente, en un único lugar, de acuerdo con la PS del PCSC.

5.4.2. FRECUENCIA DE PROCESAMIENTO DEL REGISTRO (LOGS)

La DPC-SCTE debe establecer el periodo, no superior a una (1) semana, con que los registros de auditoría del PCSC 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 acciones adoptadas como resultado de este análisis deberán ser documentadas.

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

En este punto, la DPC-SCTE deberá establecer que el PCSC responsable mantendrá localmente sus registros de auditoría durante al menos 2 (dos) meses y posteriormente almacenarlos en la forma descrita en el ítem 5.5.2.

5.4.4. PROTECCIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

En este ítem, la DPC-SCTE deberá describir los mecanismos obligatorios incluidos de registro de eventos del PCSC responsable para proteger sus registros de auditoría contra la lectura, modificación y eliminación no autorizadas.

También se deben describir los mecanismos obligatorios de protección de la información manual de auditoría contra la lectura, modificación y eliminación no autorizadas.

Los mecanismos de protección descritos en este ítem deben obedecer a lo dispuesto en el ítem 12 “seguridad en la operativa” de la norma ISO 27002/2022.

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

Este ítem de la DPC-SCTE debe describir los procedimientos adoptados por el PCSC responsable para generar copias de seguridad (backup) de sus registros de auditoría y su frecuencia, que no debe exceder de una (1) semana.

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

En este ítem de la DPC-SCTE se deben describir y ubicar los recursos utilizados por el PCSC responsable para la recolección de datos de auditoría.

5.4.7. NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO

La DPC-SCTE deberá tener en cuenta que de ser registrado un evento por el conjunto de sistemas de seguridad auditoría del PCSC responsable, no se requerirá notificar a ninguna persona, organización, dispositivo o aplicación que causó el evento.

5.4.8. EVALUACIÓN DE VULNERABILIDADES

La DPC-SCTE debe asegurar que los eventos que indiquen una posible vulnerabilidad, detectados en el análisis periódico de los registros de auditoría del PCSC responsable, se analizarán detalladamente y, dependiendo de su gravedad, serán registradas por separado.

Las acciones correctivas que surjan serán implementadas por el PCSC y registradas con fines de auditoría.

5.5. ARCHIVOS DE REGISTROS

En los siguientes ítems de la DPC-SCTE, se debe describir la política general de archivo de registros, para su uso futuro, implementada por el PCSC responsable y los PSS vinculados a él.

5.5.1. TIPOS DE REGISTROS ARCHIVADOS

En este ítem de la DPC-SCTE, se deben especificar los tipos de registros archivados, los cuales deben comprender, entre otros:

a) notificaciones de compromiso de clave privada del SSTE;
b) sustituciones de claves privadas del SSTE;
c) información de auditoría prevista en el ítem 5.4.1.

5.5.2. PERÍODOS DE RETENCIÓN PARA ARCHIVOS

En este punto, la DPC-SCTE deberá establecer los plazos de conservación de cada registro archivado, señalando que los SCTE emitidos y otras informaciones, incluyendo archivos de auditoría, deberán conservarse como mínimo por diez (10) años.

5.5.3. PROTECCIÓN DE ARCHIVOS

La DPC-SCTE deberá establecer que todos los registros archivados deberán ser clasificados y almacenados con requisitos de seguridad compatibles con esta clasificación, conforme a lo establecido en el ítem 12 “seguridad en la operativa” de la norma ISO 27002/2022.

5.5.4. PROCEDIMIENTOS DE RESPALDO (BACKUP) DE ARCHIVO

La DPC-SCTE deberá establecer que una segunda copia de todo el material archivado deberá ser almacenado fuera de las instalaciones principales del PCSC responsable, recibiendo los mismos tipos de protección que se utiliza en el archivo principal.

Las copias de seguridad deben seguir los períodos de retención definidos para los registros de las cuales son copias.

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

5.5.5. REQUERIMIENTOS PARA SELLADO DE TIEMPO DE REGISTROS

En este punto, la DPC-SCTE deberá establecer los formatos y estándares de fecha y hora contenidos en cada tipo de registro.

5.5.6. SISTEMA DE RECOLECCIÓN DE DATOS DE ARCHIVO (INTERNO O EXTERNO)

Este ítem de la DPC-SCTE deben ser descritos y localizados los recursos utilizados por el PCSC responsable para la recolección de datos de archivo.

5.5.7. PROCEDIMIENTOS PARA OBTENER Y VERIFICAR LA INFORMACIÓN ARCHIVADA

En este ítem de la DPC-SCTE, deben ser descritos los procedimientos definidos por el PCSC responsable y los PSS vinculados para la obtención o verificación de sus informaciones de archivo.

5.6 CAMBIO DE CLAVE

En este ítem, la DPC-SCTE deberá describir los procedimientos técnicos y operativos que serán utilizados por el PCSC responsable para garantizar que se generará e instalará un nuevo par de claves en el SSTE cuando el ciclo de vida del par de claves que está en uso, expire.

La generación de un nuevo par de claves y la instalación del certificado respectivo en el SSTE deberán ser realizadas únicamente por empleados con roles de confianza, a través de un doble control, en un ambiente físico seguro.

5.7. COMPROMISO Y RECUPERACIÓN DE DESASTRES

5.7.1. DISPOSICIONES GENERALES

En los siguientes ítems de la DPC-SCTE, deben ser descritos los requisitos relacionados con los procedimientos de notificación y de recuperación de desastres, previstos en el PCN del PCSC responsable, establecido de conforme a su POLÍTICA DE SEGURIDAD el cual debe considerar el ítem 17 “aspectos de seguridad de la información en la gestión de la continuidad del negocio” de la norma ISO 27002/2022, para asegurar la continuidad de los servicios críticos.

El PCSC debe garantizar, que en caso de compromiso de su operación por cualquiera de las razones enumeradas en los puntos a continuación, las informaciones relevantes estén disponibles para los suscriptores y para la parte usuaria. Igualmente, el PCSC debe poner a disposición de todos los suscriptores y de la parte usuaria una descripción del compromiso ocurrido.
En caso de compromiso de una operación del SSTE (por ejemplo, compromiso de la clave privada del SSTE), sospecha de compromiso o pérdida de calibración, el SSTE no debe emitir un SCTE hasta que se tomen medidas para recuperación del compromiso.

En caso de deterioro grave de la operación o funcionamiento del PCSC, siempre que sea posible, se deberá poner a disposición de todos los suscriptores y de terceros, informaciones que permitan identificar los SCTE que pueden haber sido afectados, a menos que tales informaciones violen la privacidad de los suscriptores o comprometan la seguridad de los servicios del PCSC.

5.7.2 RECURSOS COMPUTACIONALES, SOFTWARE Y/O CORRUPCIÓN DE DATOS

En este ítem, la DPC-SCTE debe describir los procedimientos de recuperación utilizados por el PCSC responsable cuando los recursos computacionales, el software y/o los datos comprometidos o estuvieren en sospecha de corrupción.

5.7.3. PROCEDIMIENTOS EN EL CASO DE COMPROMISO DE LA CLAVE PRIVADA DEL PCSC

5.7.3.1. CERTIFICADO DE ENTIDAD ES REVOCADO

Este ítem de la DPC-SCTE debe describir los procedimientos de recuperación utilizados en caso de revocación del certificado del SSTE del PCSC responsable.

5.7.3.2. CLAVE DEL PCSC ESTÁ COMPROMETIDA

Este ítem de la DPC-SCTE debe describir los procedimientos de recuperación utilizados en caso de compromiso de la clave privada del SSTE, y, en su caso, los medios que se pueden utilizar para distinguir entre sellos auténticos y sellos con fechas y horas adulteradas.

5.7.3.3 PERDIDA DE CALIBRACION Y SINCRONISMO DEL SSTE

En este ítem, la DPC-SCTE deberá describir los procedimientos de recuperación previstos por el PCSC para uso en casos de pérdida de calibración y sincronismo SSTE.

5.7.4. CAPACIDAD DE CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

Este ítem de la DPC-SCTE debe describir los procedimientos de recuperación utilizados por el PCSC responsable después de la ocurrencia de un desastre natural o de otra índole, antes del restablecimiento de un ambiente seguro.

5.8. EXTINCIÓN DE LOS SERVICIOS DE UN PCSC O PSS

Este ítem de la DPC-SCTE debe describir los requisitos y procedimientos que deben ser adoptados en los casos de extinción de los servicios del PCSC responsable o de un PSS vinculado a éste.

El PCSC debe garantizar que se minimicen las posibles interrupciones con los suscriptores y parte usuaria, en consecuencia del cese de los servicios de sello de tiempo del PCSC y, en particular, asegurar el mantenimiento continuo de la información necesaria para verificar la exactitud de los sellos de tiempo que ha emitido.

Antes de que un PCSC cese sus servicios de sellado de tiempo, se deberán llevar a cabo como mínimo, los siguientes procedimientos:

a) El PCSC deberá poner a disposición de todos los suscriptores y partes receptoras información sobre el cese respectivo;

b) El PCSC revocará la autorización de todos los PSS y subcontratistas que actúen en su nombre para el desempeño de cualquier función relacionada con el proceso de emisión de los SCTE;
c) el PCSC trasladará a otro PCSC, previa aprobación de la AC Raíz-Py, las obligaciones relativas al mantenimiento de archivos de registro y de auditoría necesarios para demostrar el funcionamiento correcto del PCSC, por un periodo razonable;
d) el PCSC deberá mantener o transferir a otro PCSC, previa aprobación de la AC Raíz-Py, sus obligaciones relativas a la disponibilización de su clave pública o de sus certificados a terceras partes, por un período razonable;
e) las claves privadas del SSTE deberán ser destruidas de tal forma que no puedan ser recuperadas;
f) el PCSC deberá solicitar la revocación de sus certificados del SSTE;
g) el PCSC deberá notificar a todas las entidades afectadas.

El PCSC deberá proporcionar los medios para cubrir los costos de cumplimiento de estos requisitos mínimos en caso de quiebra u otras causales, se vea incapaz de cubrir los costos.

6. CONTROLES TÉCNICOS DE SEGURIDAD

En los siguientes ítems, la DPC-SCTE deberá definir las medidas de seguridad implementadas por el PCSC responsable para proteger sus claves criptográficas y mantener sincronizado su SSTE. También se pueden definir otros controles técnicos de seguridad utilizados por el PCSC y PSS vinculados en el desempeño de sus funciones operativas.

6.1. CICLO DE VIDA DE LA CLAVE PRIVADA DEL SSTE

El SSTE debe permitir:

a) generación del par de claves criptográficas;
b) generación de solicitud de certificado electrónico;
c) exclusión de solicitud de certificado electrónico;
d) instalación de certificados electrónico;
e) renovación del certificado electrónico (con la generación de un nuevo par de claves);
f) protección de las claves privadas.

6.1.1. GENERACIÓN DEL PAR DE CLAVES

En este ítem, la DPC-SCTE deberá describir los requisitos y procedimientos relacionados con el proceso de generación del par de claves criptográficas del PCSC responsable. El par de claves criptográficas del SSTE del PCSC responsable de la DPC-SCTE debe ser generado por el propio PCSC, posterior a la habilitación otorgada por la AC Raíz-Py vía resolución ministerial.

El PCSC deberá garantizar que todas las claves criptográficas sean generadas en circunstancias controladas. En particular:

a) la generación de la clave firma o sello del SSTE se realizará en un ambiente físico seguro, mediante personal con roles de confianza bajo al menos doble control. El Personal autorizado para el desempeño de esta función se limitará a quienes se les ha encomendado esta responsabilidad de acuerdo con las prácticas del PCSC;

b) la generación de la clave de firma o sello del SSTE se realizará dentro de un MSC que cumpla con los requisitos establecidos en el documento DOC-ICPP-06 [2];

c) el algoritmo de generación de claves del SSTE, la longitud de la clave de firma resultante y el algoritmo de firma utilizado para firmar o sellar el sello cualificado de tiempo electrónico serán los contenidos en el DOC-ICPP-06 [2].

El PCSC deberá garantizar que las claves privadas se generarán de tal forma que no puedan ser exportables.

6.1.2. GENERACIÓN DE SOLICITUD DE CERTIFICADO

En este punto, la DPC-SCTE deberá informar que el SSTE deberá contar con un mecanismo para generar solicitud de certificado electrónico correspondiente a la clave privada generada en el módulo criptográfico asociado al SSTE, que cumple con el formato definido por la ICPP.

6.1.3. EXCLUSIÓN DE SOLICITUD DE CERTIFICADO

El SSTE deberá garantizar que la exclusión de una solicitud de certificado electrónico, por desistimiento de emitir el certificado, implica necesariamente la exclusión de la clave privada correspondiente.

6.1.4. INSTALACIÓN DEL CERTIFICADO

El SSTE debe por lo menos verificar los elementos descritos a continuación antes de la instalación del certificado:

a) comprobar si la clave privada correspondiente al certificado está en su módulo criptográfico asociado;
b) comprobar si el certificado incorpora las extensiones obligatorias;
c) validar la ruta de certificación.

6.1.5. RENOVACIÓN DEL CERTIFICADO

El SSTE deberá permitir la renovación de su certificado electrónico, mediante la generación de una solicitud de certificado electrónico siempre que se genere un nuevo par de claves, diferente al actual.

6.1.6. DISPONIBILIZACIÓN DE CLAVE PÚBLICA DEL PCSC PARA USUARIOS

En este ítem, la DPC-SCTE deberá definir las formas de hacer disponible el certificado del PCSC responsable y de todos los certificados de la cadena de certificación para los usuarios de ICPP.

Estas formas pueden incluir, entre otros:

a) la disponibilización de un SCTE para el suscriptor, conteniendo la cadena de certificación, conforme el formato definido en el documento DOC-ICPP-06 [2];
b) el sitio web del PCSC; y
c) otros medios seguros aprobados por la AC Raíz-Py.

6.1.7. TAMAÑO DE LA CLAVE

En este ítem, la DPC-SCTE debe señalar que cada PC-SCTE implementada por el PCSC responsable definirá el tamaño de las claves criptográficas del SSTE que opera, en concordancia con los requerimientos aplicables establecidos por el documento DOC-ICPP-06 [2].

6.1.8. GENERACIÓN DE PARÁMETROS DE CLAVES ASIMÉTRICAS

La DPC-SCTE debe prever que los parámetros de generación de claves asimétricas del PCSC responsable adoptarán las normas definidas en el documento DOC-ICPP-06 [2].

6.1.9. VERIFICACIÓN DE CALIDAD DE LOS PARÁMETROS

Los parámetros deberán ser verificados de acuerdo con las normas establecidas en el documento DOC-ICPP-06 [2].

6.1.10. GENERACIÓN DE CLAVES POR HARDWARE O SOFTWARE

La DPC-SCTE debe indicar que el proceso de generación del par de claves del PCSC responsable es realizado por hardware.

6.1.11. PROPÓSITOS DE USOS DE CLAVE

En este ítem, la DPC-SCTE deberá especificar que las claves privadas de los STE operados por el PCSC responsable sólo pueden ser utilizados para firmar o sellar los sellos cualificados de tiempo electrónicos por él emitidos.

6.2. PROTECCIÓN DE LA CLAVE PRIVADA

En los puntos siguientes, la DPC-SCTE deberá establecer los procedimientos de seguridad que adoptará para la protección de la clave privada de su SSTE.

6.2.1. ESTÁNDARES Y CONTROLES DEL MÓDULO CRIPTOGRÁFICO

La DPC-SCTE deberá prever que el módulo criptográfico de generación y almacenamiento de claves asimétricas del PCSC responsable adoptará las normas definidas en el documento DOC-ICPP-06 [2].

6.2.2. CONTROL MULTIPERSONA DE LA CLAVE PRIVADA

No aplica.

6.2.3. CUSTODIA (ESCROW) DE LA CLAVE PRIVADA

En este ítem, la DPC-SCTE debe indicar que no está permitido, en el ámbito de la ICPP, recuperación de claves privadas, es decir, no se permite que terceros puedan obtener legalmente una clave privada sin el consentimiento de su titular.

6.2.4. RESPALDO/COPIA DE SEGURIDAD LA CLAVE PRIVADA

En este ítem, la DPC-SCTE debe describir que no está permitido, en el ámbito de la ICPP, la generación de copia de seguridad (backup) de claves privadas de firma o sello del SSTE.

6.2.5. ARCHIVADO DE LA CLAVE PRIVADA

En este ítem de la DPC-SCTE, se debe describir que el PCSC no archivará claves privadas de firma o sello de su SSTE.

Defínase archivado como el almacenamiento de la clave privada para uso futuro, posterior al período de validez del certificado correspondiente.

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

No aplica.

6.2.7. MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

En este ítem de la DPC-SCTE, deben ser descritos los requisitos y procedimientos necesarios para la activación de la clave privada del PCSC responsable. Se deben definir los agentes autorizados para activar esta clave, el método de confirmación de la identidad de estos agentes (contraseñas, tokens o biometría, etc) y las acciones necesarias para la activación.

6.2.8. MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

Este ítem de la DPC-SCTE debe describir los requisitos y procedimientos necesarios para la desactivación de la clave privada del PCSC responsable. Los agentes autorizados deben ser definidos, así como el método de confirmación de la identidad de estos agentes y las acciones necesarias para la desactivación.

6.2.9. MÉTODO DE DESTRUCCIÓN DE CLAVE PRIVADA

Este ítem de la DPC-SCTE debe describir los requisitos y procedimientos necesarios para la destrucción de la clave privada del SSTE. Los agentes autorizados, el método de confirmación de la identidad de estos agentes y las acciones necesarias, tales como destrucción física, sobrescritura o borrado de los medios de almacenamiento.

6.3. OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES

6.3.1. ARCHIVO DE LA CLAVE PÚBLICA

La DPC-SCTE deberá disponer que las claves públicas del SSTE del PCSC responsable, posterior a la expiración de los certificados correspondientes, serán conservados de manera permanente por el PCSC que los emitió, para verificación de firmas o sellos electrónicos generados durante su vigencia.

6.3.2. PERÍODO DE USO DEL PAR DE CLAVES (PÚBLICA Y PRIVADA)

Las claves privadas del SSTE del PCSC responsable de la DPC-SCTE sólo deben ser utilizadas durante el período de validez de los certificados correspondientes. Las claves públicas correspondientes podrán ser utilizadas durante todo el período de tiempo determinado por la legislación aplicable, para verificación de firmas o sellos electrónicos generados durante el período de vigencia de los respectivos certificados.

El sistema de generación de SCTE deberá rechazar cualquier intento de emisión de SCTE si su clave privada de firma o sello está vencida o revocada.

6.4. DATOS DE ACTIVACIÓN DE CLAVE DEL SSTE

No aplica.

6.4.1. GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

No aplica.

6.4.2. PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

No aplica.

6.4.3. OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

No aplica.

6.5. CONTROLES DE SEGURIDAD COMPUTACIONAL

En este ítem, la DPC-SCTE deberá indicar los mecanismos utilizados para brindar la seguridad de sus estaciones de trabajo, servidores y demás sistemas y equipos, conforme a la PS del PCSC responsable.

6.5.1. REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS

La DPC-SCTE deberá disponer que el SSTE y los equipos del PCSC responsable, utilizados en los procesos de emisión, expedición, distribución, y gestión de los SCTE deben implementar, entre otras, las siguientes funcionalidades:

a) control de acceso a los servicios y perfiles del PCSC;
b) clara segregación de tareas y atribuciones relacionadas con cada rol de confianza o perfil del PCSC;
c) uso de criptografía para la seguridad de la base de datos, cuando así lo exija 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) mecanismos para copias de seguridad (backup).

Estas características serán implementadas por el sistema operativo o por medio de combinación de este, con el sistema de gestión de sellos de tiempo y con mecanismos de seguridad física.

Cualquier equipo, o parte del mismo, para ser sometido a mantenimiento deberá haber eliminado toda información confidencial contenida en el mismo y controlar su número de serie junto con las fechas de envío y recepción Al regresar a las instalaciones del PCSC, el equipo que fue sometido a mantenimiento debe ser inspeccionado.

Cuando un equipo que ya no será utilizado de forma permanente, deberá tener destruida toda la información confidencial en él almacenado, que guarde relación con la actividad del PCSC. Todos estos eventos deben registrarse con fines de auditoría.

Cualquier equipo incorporado al PCSC debe estar preparado y configurado conforme lo previsto en la PS implementada u otro documento aplicable, con el fin de mostrar el nivel de seguridad necesario para su propósito.

6.3.1. CLASIFICACIÓN DE LA SEGURIDAD DEL COMPUTADOR

En este ítem de la DPC-SCTE, debe ser informado cuando esté disponible, la clasificación atribuida a la seguridad computacional del PCSC, de acuerdo con criterios como: Trusted System Evaluation Criteria*(TCSEC), Canadian Trusted Products Evaluation Criteria, European Information Technology Security Evaluation Criteria (ITSEC) o Common Criteria.*

6.3.2. CARACTERÍSTICAS DEL SERVIDOR DE SELLO DE TIEMPO (SSTE)

El Sistema de SSTE es un sistema de hardware y software que realiza la generación de SCTE, cumpliendo las especificaciones descritas en este apartado.

El SSTE debe mantener su reloj interno sincronizado con una fuente confiable de tiempo (FCT). El MSC asociado al SSTE es aquel que, conectado de forma segura al SSTE, se encuentra interna o externamente a éste, almacena las claves criptográficas utilizadas para las firmas o sellos electrónicos del SSTE. Cualquier MSC asociado externamente con un SSTE deberá ser instalado y operar dentro del mismo ambiente de nivel 4 de acceso físico que el SSTE. El SSTE deberá asegurarse de que los SCTE sean emitidos de conformidad con el tiempo constante de su reloj interno y que la firma o sello electrónico del sello de tiempo será realizada por un MSC asociado. En este ítem de la DPC-SCTE se deben definir las características del SSTE utilizados por el PCSC. El SSTE debe tener mínimamente las siguientes características:

a) emitir sellos de tiempo en el mismo orden en que se reciben las solicitudes;
b) permitir la gestión y protección de claves privadas;
c) utilizar un certificado cualificado electrónico válido emitido por un PCSC habilitado para dicho servicio;

d) permitir la identificación y registro de todas las acciones realizadas y sellos de tiempo emitidos;
e) garantizar la no retroactividad en la emisión de sellos de tiempo;
f) proporcionar los medios necesarios para que el OEC pueda auditar y verificar la sincronización de su reloj interno:
h) poseer un certificado de especificación emitido por el fabricante;
i) emitir un sello de tiempo únicamente si:

i. garantiza que la exactitud de la sincronización de su reloj está de acuerdo con el reloj de una FCT.
ii. está firmado o sellado por un certificado cualificado electrónico válido emitido por un PCSC habilitado en el marco de la ICPP.

6.5.2. CICLO DE VIDA DE MÓDULOS CRIPTOGRÁFICOS ASOCIADOS AL SSTE

En este ítem de la DPC-SCTE, deben ser descritos los requisitos y procedimientos necesarios para la seguridad de los módulos criptográficos del SSTE a lo largo de su ciclo de vida. Particularmente, el PCSC debe asegurarse de que la instalación y activación de un módulo criptográfico solo se realicen por personal formalmente designado, involucrando a más de una persona simultáneamente, en un ambiente seguro.

6.5.3. AUDITORÍA Y SINCRONIZACIÓN DE RELOJES DEL SSTE

El PCSC debe realizar operaciones de sincronismo al menos una vez cada veinticuatro (24) horas.

El PCSC debe asegurarse de que su SSTE estén sincronizados con la FCT dentro de la exactitud declarada en las respectivas PC-SCTE y, en particular, que:

a) los valores de tiempo utilizados por el SSTE en la emisión de SCTE sean rastreables hasta el tiempo del FCT;
b) la calibración del reloj del SSTE se mantenga de tal manera que no se desvíe de la precisión declarada en la PC-SCTE;
c) Los relojes del SSTE deben estar protegidos contra ataques, incluida la manipulación y las imprecisiones causadas por señales eléctricas o señales de radio, evitando que sean mal calibradas y permitiendo detectar cualquier modificación;
d) la ocurrencia de pérdida de sincronización del valor de tiempo indicado en un sello de tiempo con el FCT siendo detectado por los controles del sistema;
e) el SSTE debe dejar de emitir sellos de tiempo cuando el reloj SSTE se encuentra fuera de precisión y exactitud en relación al tiempo UTC conforme a lo establecido en el PC-SCTE correspondiente, y en caso de que la AC Raíz-Py así lo determine;
f) la sincronización de los relojes del SSTE debe mantenerse incluso cuando ocurra la inserción de un segundo de transición (leap second);
g) el OEC tenga acceso con un perfil de auditoría a los registros resultantes de la Autenticación y Sincronización de Reloj.

6.6. CONTROLES TÉCNICOS DEL CICLO DE VIDA

Los siguientes ítems de la DPC-SCTE deben describir, cuando corresponda, los controles implementados por el PCSC responsable y por los PSS vinculados a ella en el desarrollo de sistemas y en la gestión de seguridad.

6.6.1. CONTROLES PARA EL DESARROLLO DEL SISTEMA

En este ítem de la DPC-SCTE, deben ser abordados aspectos tales como: seguridad ambiental y del personal de desarrollo, prácticas de ingeniería de software adoptadas, metodología de desarrollo de software, entre otros, aplicado al software del sistema de PCSC o cualquier otro software desarrollado o utilizado por el PCSC responsable.

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

6.6.2. CONTROLES DE GESTIÓN DE SEGURIDAD

Este ítem de la DPC-SCTE debe describir las herramientas y procedimientos utilizados por el PCSC responsable y los PSS vinculados para garantizar que sus sistemas y redes operacionales implementen los niveles de seguridad configurados.

Se debe utilizar una metodología formal de gestión de la configuración para la instalación y mantenimiento continuo del sistema del PCSC.

6.6.3. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

En este ítem, la DPC-SCTE 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) o el *Capability Maturity Model* do *Software Engineering Institute* (CMM-SEI).

6.7. CONTROLES DE SEGURIDAD DE RED

6.7.1. DIRECTRICES GENERALES

Este ítem de la DPC-SCTE debe describir los controles relacionados con la seguridad de la red del PCSC responsable, incluyendo firewall y recursos similares, teniendo en cuenta lo dispuesto en la PS implementada por el PCSC.
Todos los servidores y elementos de infraestructura y protección de redes, tales como: routers, hubs, switches, firewall y sistemas de detección de intrusos (IDS), ubicados en el segmento de red que aloja el SSTE, se debe ubicar y operar desde un ambiente de nivel 3 como mínimo.

Las últimas versiones de los sistemas operativos y aplicaciones de servidores, así como cualquier corrección (patches) provistos por los respectivos fabricantes debe ser implementados inmediatamente después de la prueba en un ambiente de desarrollo u homologación.

El acceso lógico a los elementos de infraestructura y protección de red, deberá restringirse por medios de autenticación y sistema de autorización de acceso. Los routers conectados a redes externas deben implementar filtros de paquetes de datos, que permitan sólo conexiones a servicios y servidores previamente definidos como pasibles a acceso externo.

El acceso a Internet debe ser proporcionado por al menos dos líneas de comunicación de distintos sistemas autónomos.

El acceso a la red del SSTE y los sistemas de gestión del PCSC solo se permitirá para los siguientes servicios:

a) por el OEC, para la auditoría del reloj del SSTE;
b) por el PCSC, para la administración del SSTE y sistemas de gestión desde equipos conectados a través de una red interna o VPN establecida por direcciones IP fija registrada previamente en la AC Raíz-Py;
c) por PSS del PCSC, para la administración de los SSTE y sistemas de gestión de equipo conectado a través de red interna o VPN establecida a través de direccionamiento IP fija previamente registrada en la AC Raíz-Py;
d) por el suscriptor, para solicitar y recibir sellos electrónicos de tiempo.

6.3.1. FIREWALL

Se deben implementar mecanismos de firewall en los equipos de uso específico, configurado exclusivamente para tal función. Los firewalls deben ser organizados y configurados de manera a promover el aislamiento, en subredes específicas, de los equipos servidores con acceso externo, la llamada “zona desmilitarizada” (DMZ), en relación con los equipos con acceso exclusivamente interno al PCSC.

6.3.2. SISTEMA DE DETECCIÓN DE INTRUSOS (IDS)

El IDS debe tener la capacidad de ser configurado para reconocer ataques en tiempo real y responder a ellos de forma automática, con medidas como: envío de trap de SNMP, ejecutar programas definidos por la administración de red, enviar correo electrónico a administradores, enviar mensajes de alerta al cortafuegos o al terminal de gestión, promover la desconexión automática de conexiones sospechosas, o la reconfiguración del cortafuegos.

El IDS debe tener la capacidad de reconocer diferentes patrones de ataques, incluso contra el propio sistema, presentando la posibilidad de actualizar su base de reconocimiento.

El IDS debe registrar eventos en registros o logs, recuperable en archivos de texto, además de implementar la gestión de configuración.

6.3.1. REGISTRO DE ACCESOS NO AUTORIZADOS A LA RED

Los intentos de acceso no autorizados (en routers, firewalls o IDS) deben registrarse en archivos para un análisis posterior, que se podrá automatizar. La frecuencia del examen de los archivos de registro deben ser al menos semanales y todas las acciones tomadas como resultado deben ser documentadas.

6.3.2. OTROS CONTROLES DE SEGURIDAD DE LA RED

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

Las estaciones de trabajo y los servidores deben estar cubiertos con antivirus, antispyware y otras herramientas de protección contra las amenazas provenientes de la red a la que están conectados.

Los relojes de los SSTE deben estar protegidos contra ataques, incluida la manipulación e imprecisiones causadas por señales eléctricas o señales de radio, para evitar que estén mal calibradas. Cualquier modificación ocurrida en estos relojes debe ser detectada y registrada.

6.4. CONTROLES DE INGENIERÍA DEL MÓDULO CRIPTOGRÁFICO

Este ítem DPC-SCTE debe describir los requisitos aplicables al módulo criptográfico utilizado para almacenar la clave privada de los SSTE del PCSC responsable. Podrán estar indicados estándares de referencia, como los definidos en el documento DOC-ICPP-06 [2].

7. PERFILES DE SELLO CUALIFICADO DE TIEMPO ELECTRÓNICO

7.1. DIRECTRICES GENERALES

En los siguientes ítems de la DPC-SCTE, se deben describir los aspectos de los sellos de tiempo emitidos por el PCSC responsable, así como las solicitudes que se les envíen.

7.2. PERFIL DEL SELLO CUALIFICADO DE TIEMPO ELECTRÓNICO

Todos los SCTE emitidos por el PCSC responsable deben cumplir con el formato definido por el perfil de sello de tiempo establecido en el estándar ETSI EN 319 422 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ETSI); Time-stamping protocol and time-stamp token profiles y deben seguir las definiciones contenido en RFC 3161.

7.2.1. REQUISITOS PARA UN CLIENTE DE SCTE

Perfil para formato de pedido

a) Parámetros a soportar: no es necesario que esté presente ninguna extensión.
b) Algoritmos a utilizar: ver documento DOC-ICPP-06 [2].

Perfil de formato de respuesta

a) Parámetros a soportar:

i. el campo *accuracy* (de precisión) debe ser soportado y entendido;
ii. incluso cuando no existe o se configura como FALSO, el campo *ordering* (de orden) debe ser soportado;

iii. el campo *nonce* debe ser soportado y verificado con el valor constante de la solicitud correspondiente para que la respuesta sea validada de forma correcta;
iv. ninguna extensión necesita ser manejada o soportada.

b) Algoritmos a soportar: ver documento DOC-ICPP-06 [2].
c) Tamaños de clave a soportar: consultar documento DOC-ICPP-06 [2].

7.2.2. REQUISITOS PARA UN SERVIDOR DE SCTE

Perfil para formato de pedido

a) Parámetros a soportar:

i. no necesita admitir ninguna extensión;
ii. debe poder manejar campos opcionales reqPolicy, nonce, certReq.

b) Algoritmos a soportar: ver documento DOC-ICPP-06 [2].

Perfil de formato de respuesta

a) Parámetros a soportar:

i. el campo *genTime* debe estar representado hasta la unidad especificada en la PC-SCTE;
ii. debe haber una precisión mínima como se define en la PC-SCTE;
iii. el campo *ordering (*de pedido) debe ser configurado como falso o no debe incluirse en la respuesta;
iv. extensión, no crítica, que contiene información sobre la cadena de sellos de tiempo, si el PCSC adopta este mecanismo;
v. otras extensiones, si se incluyen, no deben marcarse como críticas;

b) Algoritmos a soportar: ver documento DOC-ICPP-06 [2].
c) Tamaños de clave a soportar: consultar documento DOC-ICPP-06 [2].

7.2.3. PERFIL DEL CERTIFICADO SSTE

El PCSC necesita firmar o sellar cada mensaje de SCTE con una clave privada específica para este uso. El PCSC puede usar diferentes claves para acomodar, por ejemplo, diferentes políticas, diferentes algoritmos, diferentes tamaños de claves privadas o para aumentar el rendimiento.

El certificado correspondiente debe contener sólo una instancia del campo de extensión, como se define en RFC 5280, con el subcampo KeyPurposeID que contiene el valor id-kptimeStamping. Esta extensión debe ser crítica.

El siguiente OID identifica el KeyPurposeID, que contiene el valor id-kp-timeStamping: 1.3.6.1.5.5.7.3.8.

Nombre del campo	Valor	Crítico
Version	Versión 3	
Serial Number	Valor único para todos los certificados emitidos por el PCSC	
Signature Algorithm	sha256withRSAEncryption (1.2.840.113549.1.1.11)	
Issuer	Common Name(CN)	DN del PCSC emisor conforme figura en el certificado (Ítem 7.2.4)
	Organizacional Unit Name	
	Organization Name	
	Country	
Not before (Fecha de inicio de la validez del certificado)	Valor UTC (Universal Time Coordinated) Fecha de inicio del periodo de validez del certificado	
Not Alter (Fecha de finalización de la validez del certificado)	Valor UTC (Universal Time Coordinated) Fecha de finalización del periodo de validez del certificado	
Subject (D<istinguished Name)	**OID=2.5.4.6 C= PY**; **OID=2.5.4.10 O= ICPP** **OID=2.5.4.11 OU= Prestador Cualificado de Sello cualificado de tiempo electrónico** **OID: 2.5.4.3 CN= [***denominación o razón social de la física o persona jurídica habilitada como PCSC en mayúsculas y sin tildes, según documento de identificación***]**; **OID=2.5.4.11 OU= SERVICIO - SELLO CUALIFICADO DE TIEMPO ELECTRONICO [***denominación del servicio habilitado del PCSC en mayúsculas y sin tildes, según documento de identificación***];**	
Subject Public Key Info	Codificado de acuerdo al RFC 5280, contiene información de la clave publica RSA. Tamaño mínimo 2048 bits	
Signature	Certificado de firma. Generado y codificado acorde al RFC 5280	
Uso de la clave	Firma digital Sin rechazar Codificar claves	SI
Uso extendido de la clave	TimeStamping	SI

7.2.4. FORMAS DEL NOMBRE

El nombre del PCSC titular del certificado, que consta el campo "*Subject*", deberá adoptar el "*Distinguished Name"* (DN) del estándar ITU X.500/ISO 9594 de la siguiente forma:

OID=2.5.4.6 C= PY;
OID=2.5.4.10 O= ICPP
OID=2.5.4.11 OU= Prestador Cualificado de Servicios de Confianza;
OID: 2.5.4.3 CN= [*denominación o razón social de la física o persona jurídica habilitada como PCSC en mayúsculas y sin tildes, según documento de identificación***]**;
OID: 2.5.4.5 SERIAL NUMBER=[conforme al formato descripto en el ítem 3.1.4.1 del DOC-ICPP-03]

7.3. PROTOCOLO DE TRANSPORTE

Como mínimo, se debe admitir el siguiente protocolo definido en el RFC 3161: Time Stamp Protocol (Sello cualificado de tiempo electrónico) vía HTTP.

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

8.1. FRECUENCIA O CIRCUNSTANCIAS DE EVALUACIÓN

En este ítem la DPC-SCTE 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-SCTE 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 18 “cumplimiento” 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-SCTE 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.

8.2. IDENTIDAD / CALIDAD DEL EVALUADOR

Las inspecciones del PCSC y PSS de la ICPP son realizadas por la AC Raíz-Py, a través de su propio personal, en cualquier momento, sin previo aviso.

Las auditorías de los PCSC de la ICPP y de su PSS se realizan en materia de procedimientos operativos y en cuanto a la autenticación y sincronización de los SSTE, por un OEC, a través de su personal, por sí misma, o por terceros autorizados por ella.

8.3. RELACIÓN DEL EVALUADOR CON LA ENTIDAD EVALUADA

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

La AC Raíz-Py, aplicará el procedimiento de acreditación de los OEC conforme al DOC-ICPP-11 [3] para la recepción del informe de evaluación de la conformidad. Respecto a las disposiciones en materia de auditoría, los OEC deberán realizar un informe lo suficientemente detallado y respaldado sobre la evaluación de la conformidad de los PCSC con el objeto de confirmar que tanto el Prestador como los servicios de confianza cualificados que presta, cumplen con los requisitos establecidos en la normativa vigente que resulte aplicable.

8.4. ASPECTOS CUBIERTOS POR LA EVALUACIÓN

Las inspecciones y auditorías realizadas en el ámbito de la ICPP tienen como objetivo verificar si los procesos, procedimientos y actividades de las entidades que componen la ICPP están en cumplimiento de sus respectivos DPC-SCTE, PC-SCTE, PSS y demás normas y procedimientos establecidos por ICPP.

En este punto de la DPC-SCTE, el PCSC responsable debe informar que ha recibido una auditoría previa por parte del OEC para fines de habilitación del servicio por parte de la AC Raíz-Py y que es auditado al menos cada veinticuatro (24) meses.

En este ítem de la DPC-SCTE, el PCSC responsable debe informar que recibieron una auditoría previa, de un OEC para fines de habilitación del servicio por parte de la AC Raíz-Py, a efectos de continuidad de operación.

En este ítem de la DPC-SCTE, el PCSC responsable debe informar que las entidades del ICPP empresas directamente vinculadas también recibieron una auditoría previa, con fines de acreditación, y que el PCSC es responsable de realizar auditorías anuales a estas entidades, con fines de mantenimiento. de acreditación, según lo dispuesto en el documento mencionado en el numeral 8.2.2.

8.5. ACCIONES TOMADAS COMO RESULTADO DE UNA DEFICIENCIA

El PCSC debe contar con procedimientos para ejecutar acciones correctivas para las deficiencias detectadas como resultado de una Auditoría.

8.6. COMUNICACIÓN DE RESULTADOS

El PCSC debe remitir el informe de evaluación de la conformidad (IEC) resultante de la Auditoría al Organismo de Supervisión en el plazo de tres días hábiles tras su recepción.

9. OTROS ASUNTOS LEGALES Y COMERCIALES

9.1. TARIFAS

En los siguientes ítems, deben ser especificados por el PCSC responsable de la DPC-SCTE, las políticas tarifarias y de reembolso aplicables según la normativa que rige la materia.

Tarifas de emisión de SCTE.
Tarifas de acceso a SCTE.
Tarifas por revocación o acceso a la información de estado
Tarifas por otros servicios
Política de reembolso.

9.2. RESPONSABILIDAD FINANCIERA

En este ítem de la DPC-SCTE se debe indicar sobre los recursos financieros suficientes para mantener las operaciones y cumplir con las obligaciones así como para afrontar riesgos de conformidad a la normativa vigente.

9.2.1. COBERTURA DE SEGURO

Conforme al ítem 4 de esta DPC-SCTE.

9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

9.3.1. ALCANCE DE LA INFORMACIÓN CONFIDENCIAL

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

La DPC-SCTE debe establecer, como principio general, que ningún documento, información o registro entregado al PCSC o PSS vinculadas deberán ser divulgados, excepto que se establezca un acuerdo con el suscriptor para su mayor difusión.

9.3.2. INFORMACIÓN FUERA DEL ALCANCE DE LA INFORMACIÓN CONFIDENCIAL

9.3.3.

En este ítem deben ser indicados los tipos de informaciones consideradas no confidenciales por el PCSC responsable de la DPC-SCTE y por los PSS a ellas vinculadas, los cuales deberán comprender, entre otros:

a) los certificados de los SSTE;

b) las PC-SCTEs implementadas por el PCSC;

c) la DPC-SCTE del PCSC;

d) versión pública de la PS; y

e) la conclusión de los informes de auditoría

9.3.4. RESPONSABILIDAD DE PROTEGER LA INFORMACIÓN CONFIDENCIAL

Los participantes que reciban o tengan acceso a información confidencial deberán contar con mecanismos que aseguren la protección y confidencialidad, evitando su uso o divulgación a terceros, bajo pena de responsabilidad, de acuerdo con la ley.

La clave privada de los SSTE deben ser generadas y mantenidas por el propio PCSC, quien será responsable de su confidencialidad.

9.4. PRIVACIDAD DE LA INFORMACIÓN PERSONAL

9.4.1. PLAN DE PRIVACIDAD

El PCSC debe garantizar la protección de los datos personales de conformidad con su Política de Privacidad. Dicha política debe de contemplar aspectos y procedimientos de seguridad organizativos con el fin de garantizar que los datos personales a los que tenga acceso son protegidos ante su pérdida, destrucción, daño y procesamiento no autorizado.

9.4.2. INFORMACIÓN TRATADA COMO PRIVADA

Como principio general, todo documento, información o registro que contenga datos personales proporcionados al PCSC se considerará confidencial, salvo disposición normativa en contrario, o cuando esté expresamente autorizado por el respectivo titular, de conformidad con la legislación aplicable.

9.4.3. INFORMACIÓN QUE NO ES CONSIDERADA COMO PRIVADA

En este ítem de la DPC-SCTE se debe de indicar que el tratamiento de la información que no es considerada como privada, si corresponde.

9.4.4. RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA

En este ítem de la DPC-SCTE se debe de indicar que el PCSC es responsable por la divulgación indebida de información confidencial, por lo que deben asegurar que no pueda ser comprometida o divulgada a terceros.

9.4.5. NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA

La información privada obtenida por el PCSC podrá ser utilizada o divulgada a terceros, previa notificación al titular o responsable del certificado y con su autorización expresa.

El titular o responsable del certificado tendrán amplio acceso a cualquiera de sus propios datos e identificaciones, y podrán autorizar la divulgación de sus registros a otras personas.

La autorización formal se podrá formalizar:

a) por medios electrónicos, conteniendo una firma o sellos válidos garantizados por un certificado reconocido por la ICPP; o
b) mediante solicitud por escrito con firma autenticada.

9.4.6. DIVULGACIÓN DE ACUERDO CON UN PROCESO JUDICIAL O ADMINISTRATIVO

En este ítem de la DPC-SCTE se debe de indicar que ningún documento, información o registro en poder del PCSC será prestado a cualquier persona, excepto el titular o su representante legal, debidamente constituida por instrumento público o privado, con facultades específicas, prohibida la sustitución.

La información privada o confidencial en poder del PCSC solamente podrá divulgarse en el marco de un procedimiento administrativo o judicial, cuya solicitud emane de una orden judicial o autoridad administrativa competente.

9.4.7. OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN

Este ítem de la DPC-SCTE deberá describir, en su caso, cualquier otra circunstancia donde se puede divulgar información confidencial.

9.4.8. INFORMACIÓN A TERCEROS

Este artículo de la DPC-SCTE debe establecer como lineamiento general que ningún documento, información o registros en poder del PSS o el PCSC responsable de la DPC-SCTE deben ser entregado a cualquier persona, salvo que quien lo solicite, mediante instrumento debidamente constituido, está autorizado para ello y correctamente identificado.

9.5. DERECHO DE PROPIEDAD INTELECTUAL

Conforme la legislación vigente

9.6. REPRESENTACIONES Y GARANTÍAS

9.6.1. REPRESENTACIONES Y GARANTÍAS DE TERCERAS PARTES

Los derechos del tercero son:

a) negarse a utilizar el SCTE para fines distintos a los previstos en la PC-SCTE correspondiente;

b) verificar, en cualquier momento, la vigencia del sello de tiempo.

Un SCTE emitido por un PCSC se considera válido cuando:

a) haya sido correctamente firmado o sellado, utilizando un certificado ICPP específico para servidores de sellado de tiempo;

b) la clave privada utilizada para firmar o sellar el sello de tiempo no se ha visto comprometida hasta que tiempo de la verificación;

La falta de ejercicio de estos derechos no exime de responsabilidad al PCSC y al suscriptor.

9.6.2. CONSENTIMIENTO DE LOS SUSCRIPTORES

Este ítem de la DPC-SCT, el PCSC debe indicar que implementa un Contrato de prestación de servicios de sello cualificado de tiempo electrónico para la expresión del consentimiento del suscriptor del servicio.

9.7. EXENCIÓN DE GARANTÍA

Este ítem no aplica.

9.8. LIMITACIONES DE RESPONSABILIDAD LEGAL

En este ítem de la DPC-SCTE, se deberá indicar que el PCSC en el marco de su actividad como prestador cualificado la limitación de su responsabilidad será conforme a las disposiciones de la Ley Nº 6822/2021, sus modificaciones y reglamentaciones.

9.9. INDEMNIZACIONES

En este ítem, la DPC-SCTE se se debe indicar que el PCSC es responsable por los daños causados y que le fueran imputables, conforme a lo establecido en la normativa vigente.

9.10. PLAZO Y FINALIZACIÓN

9.10.1. PLAZO

En este ítem, se debe establecer que la DPC entra en vigencia a partir de la fecha establecida en el instrumento que la aprueba y expedido por la AC Raíz-Py.

9.10.2. FINALIZACIÓN

Esta DPC tendrá una vigencia indefinida, manteniéndose vigente y eficaz hasta que sea revocada o sustituida, expresa o tácitamente.

9.10.3. EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA

Los actos realizados durante la vigencia de esta DPC-SCTE son válidos y eficaces a todos los efectos legales, produciendo efectos incluso después de su revocación o sustitución.

9.11. NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON PARTICIPANTES

Las notificaciones, citaciones, solicitudes o cualquier otra comunicación necesaria sujeta a las prácticas descritas en la presente DPC-SCTEse realizarán, preferentemente, mediante sistema de información firmado o sellado electrónicamente, o, en su defecto, mediante oficio de la autoridad competente.

9.12. ENMIENDAS

9.12.1. PROCEDIMIENTOS PARA ENMIENDAS

En este ítem de la DPC-SCTE se debe indicar el procedimiento para enmiendas y que propuestas de modificación de la DPC-SCTE deben ser revisadas y aprobadas por la AC Raíz-Py antes de ser implementadas. Las modificaciones deben documentarse y mantenerse actualizadas a través de versiones.

9.12.2. PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN

En este ítem, deben ser descriptos los procedimientos utilizados para publicar y notificar las enmiendas o modificaciones realizadas a la DPC-SCTE. Toda enmienda o modificación de la DPC-SCTE, deberá ser publicada en el repositorio del PCSC.

9.12.3. CIRCUNSTANCIAS EN QUE LOS OID DEBEN SER CAMBIADOS

No aplica.

9.13. DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS

En este ítem, se debe indicar que las controversias derivadas de la presente DPC-SCTE se resolverán de conformidad con la legislación vigente. Debe también establecerse que la DPC-SCTE del PCSC responsable no prevalecerá sobre las normas, criterios, prácticas y procedimientos establecidos por la AC Raíz-Py.

9.14. NORMATIVA APLICABLE

Esta DPC-SCTE se rige por la legislación de la República del Paraguay, en particular por la Ley Nº 6822/2021, reglamentaciones y la legislación que la sustituya o modifique, así como las demás leyes y normas vigentes en el Paraguay.

9.15. ADECUACIÓN A LA LEY APLICABLE

En este ítem se debe indicar que la DP-SCTE se adecua a la legislación aplicable y que el PCSC responsable se compromete a cumplir y observar las disposiciones previstas en ella.

9.16. DISPOSICIONES VARIAS

9.16.1. ACUERDO COMPLETO

Esta PC-SCTE representa las obligaciones y deberes aplicables al PCSC y autoridades vinculadas.

En caso de conflicto entre esta PC-SCTE y otras resoluciones de la AC Raíz-Py, prevalecerá siempre la última editada.

9.16.2. ASIGNACIÓN

Los derechos y obligaciones previstos en esta DPC-SCTE son públicos e indisponibles, y no pueden ser cedidos o transferidos a terceros.

9.16.3. INDEPENDENCIA DE LAS DISPOSICIONES

La nulidad, nulidad o ineficacia de cualquiera de las disposiciones de este DPCT no afectará a las demás disposiciones, las cuales permanecerán plenamente válidas y eficaces. En este caso, la disposición inválida, nula o ineficaz se tendrá por no escrita, por lo que el presente DPCT se interpretará como si no la contuviera y, en lo posible, manteniendo la intención original de las restantes disposiciones.

10. DOCUMENTOS DE REFERENCIA

10.1. REFERENCIA EXTERNA

- Ley Nº 6822/2021 "De los servicios de confianza para las transacciones electrónicas, del documento electrónico y los documentos transmisibles electrónicos."
- RFC 3161, IETF - Public Key Infrastructure Time Stamp Protocol (TSP), agosto de 2001.
- RFC 3628, IETF - Policy Requirements for Time Stamping Authorities, november 2003.
- RFC 3647: "Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework".
- ETSI TS 101861 - v 1.2.1 Technical Specification / Time Stamping Profile, março de 2002
- ETSI EN 319 401 General Policy Requirements for Trust Service Providers
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

10.2. REFERENCIAS A DOCUMENTOS QUE COMPONEN LA ICPP

Tabla Nº 7– Documentos Referenciados

REF.	NOMBRE DEL DOCUMENTO	CÓDIGO
[1]	Directivas obligatorias para la formulación de la Declaración de Prácticas de Certificación de los Prestadores Cualificados de Servicios de Confianza de la ICPP	DOC-ICPP-03
[2]	Normas de algoritmos criptográficos de la ICPP.	DOC-ICPP-06
[3]	Guía para la acreditación de los organismos de evaluación de la conformidad	DOC-ICPP-11
[4]	Requisitos Mínimos para Políticas de Sello Cualificado de Tiempo Electrónico de los PCSC de la ICPP	DOC-ICPP-26