CONFIRMA

PROCEDIMIENTOS OPERACIONALES MINIMOS PARA EL SERVICIO DE GENERACION O GESTION DE DATOS DE CREACION DE FIRMA ELECTRONICA

CONFIRMA S.A.

CONTROL DOCUMENTAL

NOMBRE DEL ARCHIVO:	
Procedimientos Operacionales Mínimos para el Servicio de Generación o Gestión de los Datos de Creación de Firma Electrónica	
CÓDIGO: POMSGC -CF	**VERSIÓN: 1.0**
UBICACIÓN FÍSICA: CONFIRMA S.A.	**FECHA: 14/04/2023**
CLASIFICACIÓN DE SEGURIDAD: Público	

CONTROL DE VERSIONES			
FECHA	**VERSIÓN**	**RESPONSABLES**	**MOTIVO DE CAMBIO**
14/04/2023	1.0	CONFIRMA S.A.	Primera Edición del Documento

DISTRIBUCIÓN DEL DOCUMENTO	
ÁREA	**NOMBRES**
Personal con Rol de Confianza establecidos en la DPC del PCSC CONFIRMA S.A..	PCSC CONFIRMA S.A..
Documento Público	https://www.confirma.com.py/wpcontent/uploads/2023/01/Declaracion_de_politicas_prestacion_del_servicios_generacion_datos_firma_electronica.pdf

PREPARADO POR:	**REVISADO POR:**	**APROBADO POR:**
UANATACA	CONFIRMA S.A.	CONFIRMA S.A.

ÍNDICE

1. DESCRIPCIÓN GENERAL

El objetivo de este documento es regular los requisitos mínimos de seguridad y los procedimientos operacionales que debe adoptar el Prestador Cualificado de Servicios de Confianza (PCSC) CONFIRMA S.A., que forma parte de la Infraestructura de Claves Públicas del Paraguay (ICPP) para prestar el servicio de generación o gestión de datos de creación de firma electrónica.

El presente documento se ha elaborado en el ámbito de la ICPP y adopta la estructura definida en el documento DOC-ICPP-08 [5]

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

Los requisitos contenidos en este documento fueron acreditados por el PCSC CONFIRMA S.A. en el proceso de habilitación para ser autorizados a prestar el servicio de generación o gestión de datos de creación de firma electrónica y/o sello electrónico en nombre del firmante o creador del sello, los cuales se mantendrán actualizados durante su operación y mientras la entidad se encuentre habilitada e integre la ICPP.

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

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

El PCSC CONFIRMA S.A. cuenta con una Política de Seguridad de la Información compuesta por directrices, normas y procedimientos que describen los controles de seguridad que deben seguirse en sus dependencias y actividades, en consonancia con la norma ISO 27002/2022.

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

Este documento define los estándares operacionales y de seguridad se aplican en las áreas internas del PCSC CONFIRMA S.A., así como en el tránsito de informaciones, en el almacenamiento de claves privadas, en los servicios de firma y/o sello electrónico cualificado y verificación de firma y/o sello electrónico cualificado y en materiales con entidades externas.

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

1.1DEFINICIONES, SIGLAS Y ACRÓNIMOS

1.1.1 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 Comercio Electrónico, dependiente del Viceministerio de Comercio y Servicios.

4) Autoridad de Certificación Raíz del Paraguay: órgano técnico, cuya función principal es coordinar el funcionamiento de la ICPP. La AC Raíz-Py tiene los certificados de más alto nivel, posee un certificado autofirmado y es a partir de allí, donde comienza la cadena de confianza. Las funciones de la AC Raíz-Py son ejercidas por la AA.

5) Gestión de datos de creación de firma o sello electrónico: El PCSC podrá, en nombre del firmante o creador de sello gestionar los datos de creación de firma o sello electrónico a los que hayan prestado sus servicios, este servicio deberá ser provisto por un PCSC siempre y cuando cuente con la debida habilitación.

6) Certificado cualificado de firma electrónica: un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el artículo 43 de la ley N° 6822/2021.

7) 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 N° 6822/2021.

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

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

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

11) Creador de un sello: una persona jurídica que crea un sello electrónico.

12) 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.

13) Firmante:una persona física que crea una firma electrónica.

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

15) 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.

16) 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.

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

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

19) Normas Internacionales :requisitos de orden técnico y de uso internacional que deben observarse en la prestación de los servicios mencionados en el presente documento.

20) Prestador Cualificado de Servicios de Confianza: un prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido habilitación.

21) 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.

22) 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 firma digital fue creada.

23) 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.

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

1.1.2 SIGLAS Y ACRÓNIMOS

Sigla/Acrónimo	Descripción
AA	Autoridad de Aplicación
AC	Autoridad de Certificación
ACI	Autoridad de Certificación Intermedia
AC Raíz-Py	Autoridad Certificadora Raíz del Paraguay
DGCE	Dirección General de y Comercio Electrónico dependiente del Viceministerio de Comercio y Servicios.
HSM	Módulo de Seguridad Criptográfico basado en Hardware (HSM por sus siglas en inglés, Hardware Security Module)
ISO	Organización Internacional para la Estandarización (ISO por sus siglas en inglés, International Organization for Standardization).
MIC	Ministerio de Industria y Comercio
PCN	Plan de Continuidad del Negocio

PKI	Infraestructura de Clave Pública (PKI por sus siglas en inglés, Public Key Infrastructure).
ICPP	Infraestructura de Claves Públicas del Paraguay
PCSC	Prestador Cualificado Servicios de Confianza
PS	Política de Seguridad
RFC	Petición de Comentarios (RFC por sus siglas en inglés, Request For Comments)
UPS	Sistemas de alimentación ininterrumpida (UPS por sus siglas en inglés, uninterruptible power supply)
URL	Localizador uniforme de recursos (URL por sus siglas en inglés, Uniform Resource Locator).

2. SEGURIDAD PERSONAL

El PCSC CONFIRMA S.A. tiene una Política de Gestión de Talento Humano que disponga sobre los procesos de contratación, despido, descripción del cargo, evaluación del desempeño y capacitación.

La comprobación de la capacidad técnica del personal involucrado en los servicios prestados por el PCSC CONFIRMA S.A., está disponible para eventuales auditorías e inspecciones.

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

El acuerdo de confidencialidad de la información deberá contener una cláusula explícita de responsabilidad en caso de incumplimiento de las normas o regulaciones que rigen en el marco de la ICPP. El acuerdo de confidencialidad de la información se aplicará a cualquier otra entidad que pueda tener acceso a información interna y de terceros proveniente de los proyectos coordinados por el PCSC CONFIRMA S.A.
El PCSC CONFIRMA S.A. tiene procedimientos formales para la verificación y la rendición de cuentas en caso de incumplimiento de las normas establecidas por sus políticas o por las normas que rigen en el marco de la ICPP.

Todo el personal del PCSC CONFIRMA S.A. cuenta con un dossier que contenga los siguientes documentos:

i. contrato de trabajo o instrumento formal de vinculación;
ii. currículum vitae donde consten antecedentes de contratación;
iii. certificado original de antecedentes policiales;
iv. certificado original de antecedentes judiciales;
v. currículum vitae que incluya histórico de empleos anteriores y formación educativa con respaldo documental;

vi. certificado original de vida y residencia;

vii. comprobante de capacidad técnica;

viii. resultado de la entrevista inicial, con la firma del entrevistador;

ix. declaración en la que afirma conocer sus atribuciones y en la que asume el deber de cumplir con las normas aplicables en el marco de la ICPP;

x. acuerdo de confidencialidad; y

xi. documento formal de asignación de rol y asignación de mecanismos de control de acceso.

No serán admitidos pasantes en el ejercicio de las actividades del PCSC CONFIRMA S.A. A su desvinculación, dicho dossier debe contener los siguientes documentos:

i. evidencia de exclusión de acceso físico y lógico en entornos del PCSC CONFIRMA S.A.; y

ii. declaración firmada por el personal desvinculado de que no posee pendientes, conforme lo dispuesto en el punto ítem 7 "seguridad ligada a los recursos humanos" de la norma ISO 27002/2022.

3. SEGURIDAD FISICA

Serán definidos al menos 4 (cuatro) niveles de acceso físico a los diferentes ambientes del PCSC CONFIRMA S.A.

El primer nivel, o nivel 1, deberá ubicarse después de la primera barrera de acceso a las instalaciones del PCSC. El ambiente de nivel 1 del PCSC en la ICPP desempeña una función de interfaz con clientes o proveedores que necesitan asistir al PCSC CONFIRMA S.A.

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

a) el ambiente del nivel 2 deberá estar separado del nivel 1 por paredes divisorias de oficinas, mampostería o placas premoldeadas de yeso acartonado. No debe haber ventanas ni ningún otro tipo de abertura al exterior, excepto la puerta de acceso;

b) el acceso a este nivel sólo deberá ser permitido a las personas que trabajan directamente con las actividades de servicios de almacenamiento de claves para usuarios finales y servicios de firma electrónica cualificada y de verificación de firma electrónica cualificada o el personal responsable del mantenimiento de los sistemas y equipos del PCSC, como administradores de red y técnicos de soporte de informática. Los demás empleados/funcionarios del PCSC no deberán acceder a este nivel;

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

d) excepto en los casos previstos por la ley, no se permitirá la posesión de armas en las instalaciones del PCSC, comenzando en el nivel 2. A partir de ese nivel, equipos de grabación, fotografía, video, sonido o equipo

similar, así como computadoras portátiles, tendrán ingreso controlado y solo se puede usar con autorización formal y bajo supervisión.

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

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

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

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

d) debe haber una única puerta de acceso al entorno de nivel 3, deberá abrirse solamente después de que el empleado o funcionario se haya autenticado electrónicamente en el sistema de control de acceso. La puerta deberá estar equipada con bisagras que permitan la apertura

para el lado externo, para facilitar la salida y dificultar el ingreso al ambiente, así como un mecanismo de cierre automático, para evitar que permanezca abierto más tiempo del necesario.

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

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

ii. Poseer una cerradura con llave.

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

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

constituyen las llamadas salas cofre, deberán tener protección contra la interferencia electromagnética externa.

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

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

a) equipamientos de producción on-line; y
b) equipamientos de red e infraestructura (firewall, enrutadores, switches y servidores).
Todos los servidores y elementos de la infraestructura y protección del segmento de red, tales como ruteadores, hubs, switches y firewall deben:
a) operar en un ambiente con seguridad equivalente, al menos, en el tercer nivel avanzado, para el caso del PCSC que presta servicios de firma electrónica cualificada, o en el cuarto nivel, en el caso del PCSC que presta servicios de almacenamiento de clave privada citados en este documento; y

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

Los PCSC también deben cumplir los siguientes requisitos:

a) el ambiente físico del PCSC deberá contener dispositivos que autentiquen y registren el acceso de personas informando la fecha y hora de esos accesos;

b) el PCSC deberá contener imágenes que garanticen la identificación de las personas cuando acceden físicamente a cualquier parte de su ambiente;

c) la sincronización de la fecha y la hora entre los mecanismos de seguridad física es obligatoria, garantizando el seguimiento de auditoría entre los dispositivos de control de acceso físico y de imagen;

d) todos los que transitan en el ambiente físico del PCSC deben llevar credenciales de identificación, incluidos los visitantes;

e) el tránsito de material de terceros a través de los ambientes físicos del PCSC sólo se permitirá mediante el registro, garantizando el seguimiento de la auditoría con informaciones sobre dónde pasó el material, la fecha y la hora en que ocurrió el tránsito y quién fue responsable de manejarlo;

f) el PCSC deberá contener dispositivos de prevención y control de incendios, temperatura, humedad, iluminación y fluctuaciones en la corriente eléctrica en todo su ambiente físico;

g) todo material crítico inutilizable, desechable o que ya no se pueda utilizar deberá tener un tratamiento de destrucción especial, garantizando la confidencialidad de la información contenida en el mismo. Los equipamientos enviados para mantenimiento deberán tener sus datos borrados, irreversiblemente, antes de ser retirados del ambiente físico del PCSC;

h) las computadoras personales, servidores y dispositivos de redes, y sus respectivos softwares, deberán ser inventariados con información que permitan la identificación inequívoca;

i) en caso de inoperancia de los sistemas automáticos, el control de acceso físico debe realizarse provisionalmente por medio de un libro de registro donde conste quién accedió a él, la fecha, la hora y el motivo del acceso;

j) deberán ser proporcionados mecanismos para garantizar la continuidad del suministro de energía en áreas críticas, manteniendo los activos críticos de información en funcionamiento hasta que todos los procesos y datos estén asegurados en caso de que se agote el suministro de emergencia;

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

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

4. SEGURIDAD LOGICA

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

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

Los equipamientos deberán tener mecanismos para bloquear sesiones inactivas.

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

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

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

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

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

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

5. SEGURIDAD RED

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

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

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

6. REQUISITOS PARA ALMACENAMIENTO DE CLAVES PRIVADAS

6.1. ALMACENAMIENTO DE CLAVES PRIVADAS Y CERTIFICADOS ELECTRONICOS

Las claves privadas de los usuarios finales, para los certificados del Tipo F3 o S3 son generados y almacenados en hardware criptográficos tipo HSM. Las mismas están almacenadas dentro de los espacios de la frontera criptográfica, o equivalente dentro del contexto de seguridad del HSM. Las claves serán activadas y utilizadas únicamente dentro del hardware

físico de dicho HSM bajo control exclusivo del usuario titular del certificado.

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

Los HSM cumplen los siguientes requisitos:
1) garantizan, por medios técnicos y de procedimiento adecuados, que:
a) esté garantizada razonablemente la confidencialidad de los datos de creación de firma utilizados para la creación de firmas electrónicas;
b) los datos de creación de firma electrónica utilizados para la creación sólo puedan aparecer una vez en la práctica;
c) exista la seguridad razonable de que los datos de creación de firma utilizados para la creación de firma electrónica no pueden ser hallados por deducción y de que la firma está protegido con seguridad contra la falsificación mediante la tecnología disponible en el momento; y

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

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

Los espacios para el almacenamiento de las claves privadas de los usuarios finales podrán ser liberados desde que no haya renovación por parte del usuario o revocación de las claves, sin embargo, el registro de almacenamiento de claves debe mantenerse de acuerdo con el DOC-ICPP-07 [4].

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

6.2. MECANISMO DE AUTENTICACION PARA ACCESO A LA CLAVE PRIVADA

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

El PCSC CONFIRMA S.A. proporciona mecanismos de doble factor de autenticación al titular del certificado para el acceso a su clave privada, debiendo:

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

ii. ambos dentro del límite de la frontera criptográfica del HSM.

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

i) Usuario y contraseñas: de acuerdo con las reglas que establezca la AC Raíz-Py;

ii) PIN de firma (PIN/PUK): de acuerdo con las reglas que establezca la CARaíz- Py

iii) OTP: de acuerdo con las reglas de RFC 6238 (TOTP), RFC 6287, RFC 4226 (HOTP);

iv) Biometría: de acuerdo con las reglas que establezca la CA Raíz-Py;

v) Certificado electrónico: de acuerdo a las normas establecidas en el marco de la ICPP;

vi) Notificación Push: de acuerdo con las reglas del protocolo de extensión XMPP o similar; o vii) Otras autenticaciones semánticas de acuerdo con este documento y previamente aprobadas por la AC Raíz-Py.

6.3. PROTOCOLOS

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

a) ejecutar los algoritmos que sean parte de las funciones core de una firma electrónica en forma interna al hardware del HSM;

b) generar y destruir claves simétricas y asimétricas en forma interna al hardware del HSM;

c) activar y desactivar claves en forma interna al hardware del HSM cuando su titular lo autorice;

d) proteger las claves privadas y sólo habilitar su activación y uso en forma interna del hardware del HSM; y

e) habilitar el uso de punteros, manejadores, alias o tokens de claves privadas a las aplicaciones que se conecten, evitando el uso directo de las mismas en claro desde el exterior en forma interna al hardware del HSM

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

6.4. REDES Y DISPONIBILIDAD

El PCSC CONFIRMA S.A. disponibiliza mecanismos para asegurar a los usuarios finales la disponibilidad del sistema para uso de sus claves privadas y certificados.

Entre dichos mecanismos para asegurar la disponibilidad se citan:

a) hacer una copia de las claves de los usuarios finales, en otro ambiente de contingencia física o disponer de mecanismos de recuperación de claves, observando los mismos requisitos de almacenamiento que el ambiente principal. El ambiente de contingencia debe estar listo para operar dentro de las 48 horas;

b) podrá ser diseñado un pool o clúster de HSM para operación, replicación y gerenciamiento de las claves de los usuarios finales, debiendo seguir, además de los descritos en este documento, los siguientes requisitos.

i. especificación y establecimiento de comunicación segura (sesión SSL/TLS) o equivalente entre los HSM;

ii. los HSM podrán estar en diferentes ambientes/entornos siempre que los mecanismos de acceso y seguridad se mantengan como se describe en este documento; y

iii. el número de conjuntos de datos duplicados no podrá superar el mínimo necesario para garantizar la continuidad del servicio.

El PCSC CONFIRMA S.A. cuenta, además de las exigencias relacionadas a sus instalaciones, con:

a) procedimientos e indicaciones de recuperación de claves y del esquema de disponibilidad de las mismas;

b) controles de seguridad para recuperación de claves y para el funcionamiento de esquema de disponibilidad de claves; y

c) pruebas de recuperación y funcionamiento de esquema de disponibilidad de claves.

El PCSC CONFIRMA S.A. cumple con el criterio de 99.95% de "nivel de tiempo de actividad" (uptime) que se verificará por mes.

6.5. REQUISITOS PARA SERVICIOS DE USO DE CLAVES PRIVADA

6.5.1. DEFINICIONES PARA LA INTERFAZ DE LOS SERVICIOS

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

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

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

6.5.2. DEFINICIONES PARA EL URI DE BASE PARA SERVICIOS

El URI de base (URI-base) definirá el estilo y el formato de las direcciones HTTPS de servicios del PCSC CONFIRMA S.A.

El URI-base deberá ser registrado ante la AC Raíz-Py bajo la ICPP. Ejemplo de URI-base: https://servicio.prestador_de_almacenamiento.com.py
Obs. La dirección servicio.prestador_de_almacenamiento.com.py representa en este ejemplo la porción de autoridad del URI en el dominio utilizado por el PCSC CONFIRMA S.A.
Las porciones restantes del URI de los servicios registrados del PCSC CONFIRM S.A. deben concatenarse con el URI-base.

6.5.3. LISTA DE SERVICIOS PROPORCIONADOS POR EL PCSC

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

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

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

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

2) Firma: servicio de firma electrónica conforme al ítem 6, para el cual deberá tener un token de acceso válido; y

3) Registro de Aplicaciones: servicio de registro de una aplicación en el PCSC a través de un servicio o una operación administrativa en la plataforma.

b) Servicios Opcionales

1) Recuperación de Certificado: servicio para recuperar un certificado almacenado en el PCSC. La aplicación deberá tener un token de acceso válido;

2) Localización del Titular: servicio para encontrar a un titular a través del número CI, PAS o RUC; y

3) Autorización con credencial de titular: servicio para obtener autorización del titular del certificado para utilizar su clave privada, con solicitud de factores de autenticación.

6.5.4. AUTORIZACION Y AUTENTICACION PARA SOLICITUD DE SERVICIOS

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

Dichos servicios son consumidos por las aplicaciones cliente de firma electrónica.

6.5.4.1. Flujo básico para Uso de Servicios

a) Seguido del flujo de autorización establecido por el RFC 6749, el uso de claves privadas en el PCSC CONFIRMA S.A. deberá ir precedido de una solicitud exitosa, por parte de las aplicaciones. Este requerimiento se aplica para los siguientes servicios:

i. Servicio de Autorización (Código de Autorización y Token de Acceso); y
ii. Firma.

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

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

b) Cuando fuera necesario utilizar un servicio destinado únicamente a la autenticación del titular, es decir, sin el uso de una clave privada, deberá ir precedido de una solicitud exitosa, por parte de las aplicaciones. Este requerimiento se aplica para los siguientes servicios:

i. Servicios de Autorización (Código de Autorización y Token de Acceso); y

ii. Recuperación de certificado.

6.5.4.2. Tránsito de los Factores de Autenticación

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

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

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

6.5.4.3. Autenticación de aplicaciones de Firma

Para que una aplicación pueda utilizar los servicios del PCSC CONFIRMA S.A. tiene que solicitar el registro en la plataforma de firma y obtener un

mecanismo de acceso para su conexión. Por tanto, en cuanto a la autenticación de aplicaciones de firma: para obtener acceso a los servicios, el PCSC CONFIRMA S.A. implementa un Servicio de Registro de Aplicaciones.

El Servicio de Registro de Aplicaciones podrá estar basado en certificados electrónicos en mecanismos sin certificados pero que utilicen una API Key dentro del modelo OAuth. En este último caso, como resultado del registro, la aplicación obtendrá un identificador (identificador de cliente), un secreto compartido con la plataforma (secreto de cliente) y una API-Key. La aplicación deberá utilizar la API Key como credencial de autenticación en todas las peticiones que dirija al servicio de autenticación y autorización para obtener un token de acceso a cualquiera de los recursos protegidos de la plataforma (datos de un usuario y de su proceso de autenticación, identidades de firma de un usuario, etc.). Para ello, tal como establece OAuth 2.0, pondrá la API Key en la cabecera de autorización de dichas peticiones.

El PCSC CONFIRMA podrá implementar, para las aplicaciones, otros métodos de acceso a sus servicios, siempre que se evalúen los riesgos asociados y se permita la trazabilidad.

7. SERVICIO DE FIRMA ELECTRÓNICA CUALIFICADA Y VERIFICACIÓN DE FIRMA ELECTRÓNICA CUALIFICADA

7.1. INTRODUCCION

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

El PCSC CONFIRMA S.A. deberá disponer de documentación para desarrolladores para la integración a su servicio de firma electrónica estableciendo las condiciones para su uso y/o integración en concordancia con lo dispuesto en este documento. Independientemente de la implementación del servicio de firma, en todo momento se deberá asegurar el exclusivo control del firmante sobre su clave privada de firma electrónica en custodia.

7.2. CREACION DE FIRMAS

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

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

i. firmante que quiere crear una firma en un documento electrónico;

ii. una aplicación conductiva que representa un ambiente de usuario (por ejemplo, una aplicación

comercial) que el suscriptor usa para acceder a la funcionalidad de firma y
iii. un sistema de creación de firma, que implementa la funcionalidad de firma, ubicado en el PCSC CONFIRMA S.A.
Antes de procesar la petición de firma, el PCSC garantiza que el usuario titular del certificado sea autenticado y debe verificar la validez de dicho certificado.
La participación humana de un firmante no siempre es necesaria.

La firma electrónica puede ser un proceso automatizado e implementado en la aplicación en el entorno del usuario.

7.3. DISPOSITIVOS PARA LA CREACION DE FIRMAS

Son sistemas o equipos configurados para implementar códigos y/u otros mecanismos que permiten la activación de la clave privada del firmante para la creación de firmas. Los dispositivos para creación de firmas, además de poder verificar los datos de autenticación del firmante, deben contener:
i) la clave privada del firmante; y
ii) el correspondiente certificado electrónico relacionado a esa clave privada o tener una referencia inequívoca a él.
El PCSC CONFIRMA S.A. utiliza un HSM y sistemas de software correspondiente autorizados por el MIC para brindar los servicios que expone, permitiendo que el titular del certificado tenga acceso, control y uso exclusivo de sus datos de creación de firma. Dichos componentes

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

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

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

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

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

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

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

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

7.5. SUITES DE FIRMA

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

7.6. FORMATOS DE FIRMA

Los formatos CAdES, XAdES y PAdES son compatibles con los certificados generados por CONFIRMA S.A., utilizado en el firmado de estos; las firmas electrónicas se basan conforme al DOC-ICPP-06 [3].

7.7. LA FIRMA ELECTRONICA CON EL SELLO DE TIEMPO

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

Los PCSC CONFIRMA S.A. podrá utilizar políticas de firma que requieran el uso de la marca de tiempo basadas en normas internacionales.

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

● RFC 2030, IETF - Simple Network Time Protocol (SNTP) version 4.0

● RFC 2527, IETF - Internet X-509 Public Key Infrastructure Certificate Policy and Certifications Practices Frame work, março de 1999.

● RFC 3161, IETF - Public Key Infrastructure Time Stamp Protocol (TSP), Agosto de 2001.

● RFC 3628, IETF - Policy Requirements for Time Stamping Authorities, November 2003.

● ETSI TS 101.861 Technical Specification/Time Stamping Profile.
● ETSI TS 102.023 Technical Specification / Policy Requirements for Time Stamping Authorities

7.8. VALIDACION DE FIRMAS

Consiste en primer lugar, determinación y validación de que la firma o electrónica 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 firma electrónica fue creado.

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

El firmante crea una firma de acuerdo con una política de firma y el verificador evalúa la validez de una firma utilizando la misma política de firma o utilizada en la creación de esa firma.

7.9. ACUERDO DE NIVEL DE SERVICIO

El acuerdo de nivel de servicio para todos los servicios acreditados por el PCSC CONFIRMA S.A. son de al menos 99.95%.

8. CLASIFICACION DE LA INFORMACION

Toda la información generada y custodiada por el PCSC CONFIRMA S.A. se clasifica de acuerdo con su contenido crítico y grado de confidencialidad, de acuerdo con su propia Política de Clasificación de Información.

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

La información se puede clasificar en:

i. pública: cualquier activo de información, propiedad del PCSC o no, que pueda ponerse a disposición del público sin consecuencias perjudiciales para el funcionamiento normal del PCSC. Cualquier persona puede acceder a este, ya sea interno o externo al PCSC. La integridad de la información no es vital.

ii. personal: Cualquier activo de información relacionado con información personal. Por ejemplo: mensaje de correo electrónico personal, archivo personal, datos personales, entre otros.

ii. interna: cualquier activo de información, propiedad del PCSC o no, que no se considere público. La divulgación no autorizada del activo de la información podría afectar la imagen del PCSC. Por ejemplo: código

fuente del programa, cronograma de actividades, actas de reuniones, entre otros.

iv. confidencial: cualquier activo de información que sea crítico para las actividades del PCSC. en relación con la confidencialidad y la integridad.

9. SALVAGUARDA DE ACTIVOS DE INFORMACION

El PCSC CONFIRMA S.A., en su Política de Seguridad de la Información, define cómo se guardarán los activos de información en formato electrónico, también denominado backup.

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

i. Procedimientos de backup;
ii. Indicaciones para usar los métodos de backup;
iii. Tabla de temporalidad;
iv. Ubicación y restricciones de almacenamiento y salvaguarda en función a la fase de uso;
v. Tipos de medios;
vi. Controles ambientales de almacenamiento;
vii. Controles de seguridad;
viii. Prueba de restauración de backup.
El PCSC tiene una política de recepción, manejo, depósito y descarte de materiales de terceros.

10. GESTION DE RIESGOS

El PCSC tiene un proceso de gestión de riesgos actualizado para evitarlos, incluidos los derivados de las nuevas tecnologías, con el objetivo de

elaborar planes de acción adecuados para proteger los componentes amenazados, actualizados al menos anualmente.

11. PLAN DE CONTINUIDAD DE NEGOCIOS

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

12. ANALISIS DE REGISTRO DE EVENTOS

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

13. PLAN DE CAPACIDAD OPERACIONAL (PCO)

El PCSC CONFIRMA S.A. mantiene un PCO anualmente para determinar la capacidad de producción actual y futura con niveles de rendimiento satisfactorios para responder a las nuevas demandas, proporcionando niveles satisfactorios de servicios a los usuarios, con el objetivo de escalar los sistemas para soportar el crecimiento orgánico, uso máximo y estacionalidad. El PCO deberá, como mínimo:

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

14. DOCUMENTOS DE REFERENCIAS

14.1. REFERENCIAS

● Ley No 6822/2021 "De los servicios de confianza para las transacciones electrónicas, del documento electrónico y los documentos transmisibles electrónicos."

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

Trust-service status information.
● RFC 2030: Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OS.
● RFC 2527: Internet X.509 Public Key Infrastructure. Certificate Policy and Certification

Practices Framework.
● RFC 3161: Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP)
● RFC 3628: Policy Requirements for Time-Stamping Authorities (TSAs)
● RFC 5246: The Transport Layer Security (TLS) Protocol. Version 1.2
● RFC 6749: The OAuth 2.0 Authorization Framework.
● RFC 7636: Proof Key for Code Exchange by OAuth Public Clients
● ETSI TS 101.861 - Technical Specification/Time Stamping Profile.
● ETSI TS 102.023 - Technical Specification/Policy Requirements for Time Stamping Authorities.

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

● ETSI. XML Format for Signature Policies. Number TR 102 038.

● ETSI. Electronic Signatures and Infrastructures; PDF Advanced Electronic Signature Profiles;

Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles. TS 102 778-3. V1.2.1. 2010.

● ETSI. Electronic Signatures and Infrastructures; PDF Advanced Electronic Signature Profiles;

Part 4: PAdES Long Term - PAdES-LTV Profile. TS 102 778-4. V1.1.1. 2009.

● Política de recepción, manejo, depósito y descarte de materiales de terceros.

14.2. REFERENCIAS A DOCUMENTOS QUE COMPONEN LA ICPP

REF.	NOMBRE DEL DOCUMENTO	CÓDIGO
[1]	Directivas obligatorias para la formulación y elaboración de la declaración de prácticas de certificación de los prestadores cualificados de servicios de confianza de la ICPP.	DOC-ICPP-03
[2]	Directivas obligatorias para la formulación y elaboración de la política de certificados de los Prestadores Cualificados de Servicios de Confianza de la ICPP.	DOC-ICPP-04
[3]	Normas de Algoritmos criptográficos de la ICPP	DOC-ICPP-06

[4]	Directivas obligatorias para la formulación y elaboración de la declaración de prácticas de certificación del PCSC CONFIRMA S.A. que genera o gestiona datos de creación de firma electrónica y/o de sello electrónico.	DOC-ICPP-07
[5]	Procedimientos operacionales mínimos para el servicio de generación o gestión de datos de creación de firma electrónica y/o sello electrónico de la ICPP	DOC-ICPP-08