CONFIRMA

DECLARACIÓN DE PRÁCTICAS DE SELLO CUALIFICADO DE TIEMPO ELECTRÓNICO DEL PCSC CONFIRMA S.A.

VERSIÓN: 1.0

CLASE: PÚBLICO

CONTROL DOCUMENTAL

NOMBRE DEL ARCHIVO:	
DECLARACIÓN DE PRÁCTICAS DE SELLO CUALIFICADO DE TIEMPO ELECTRÓNICO DEL PCSC CONFIRMA S.A.	
CÓDIGO: **DPC –SCTE**	**VERSIÓN:** **1.0**
UBICACIÓN FÍSICA: **CONFIRMA S.A.**	**FECHA:** 18/03/2024
CLASIFICACIÓN DE SEGURIDAD: **Público**	

CONTROL DE VERSIONES			
FECHA	**VERSIÓN**	**RESPONSABLES**	**MOTIVO DE CAMBIO**
18/03/2024	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/wp-content/uploads/2024/03/Declaracion_de_practicas_de_sellotiempo_Confirma_SA.pdf

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

INDICE

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) CONFIRMA S.A. que presta el Servicio de creación, verificación y validación de sellos cualificados de tiempo electrónico (SCTE) en su carácter de Autoridad de Certificación Intermedia (ACI), y como miembro de la Infraestructura de Clave Pública del Paraguay (ICPP).

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 Sello de tiempo electrónico, conforme la Ley N.° 6822/2021, 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.

Confirma declara en este documento la Fuente Confiable de Tiempo (FCT) que utiliza es la del servidor ntp.cesca.cat, con el nivel de referencia horaria Stratum 1. la misma podrá consumirse de una fuente oficial de tiempo establecida en la República del Paraguay o extranjera. 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

Nombre del Documento	DECLARACIÓN DE PRÁCTICAS DE SELLO CUALIFICADO DE TIEMPO ELECTRÓNICO DEL PCSC CONFIRMA S.A.
Versión del Documento	1.0
Estado del Documento:	Versión Inicial
Fecha de Emisión	18/03/2024
OID	1.3.6.1.4.1.58404.1.3.1.1
Ubicación de la DPC	https://www.confirma.com.py/wp-content/uploads/2024/03/Declaracion_de_practicas_de_sellotiempo_Confirma_SA.pdf

1.3 PARTICIPANTES

1.3.1 PRESTADORES CUALIFICADOS DE SERVICIOS DE CONFIANZA (PCSC)

El Prestador Cualificado de Servicios de Confianza, en adelante "PCSC" es la persona, física o jurídica, que presta uno o más servicios de confianza. Asimismo, CONFIRMA es un prestador cualificado de servicios de confianza, que actúa de acuerdo con lo dispuesto en la LEY Nro 6822/2021 DE LOS SERVICIOS DE CONFIANZA PARA LAS TRANSACCIONES ELECTRÓNICAS, DEL DOCUMENTO ELECTRÓNICO Y LOS DOCUMENTOS TRANSMISIBLES ELECTRÓNICOS.

1.3.2 AGENTE DE ATENCIÓN DEL SERVICIO

La figura del Agente de atención al servicio 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

Todas las personas físicas o jurídicas 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

Se refiere a parte usuaria 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 PRESTADORES DE SERVICIOS DE SOPORTE (PSS)

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 mantiene publicada información referente a:

- Lista de todos los PSSs habilitados

https://www.confirma.com.py/prestadores-de-servicios-de-soporte/

- Lista de los PSSs que se han inhabilitado por el PCSC, indicando la fecha de la inhabilitación.

1.4. USOS DEL CERTIFICADO

El PCSC COMFIRMA S.A. implementa las siguientes políticas de certificación:

https://www.confirma.com.py/wp-content/uploads/2024/03/PC_Politica_de_Certificacion_SelloTiempo_Confirma_SA.pdf

1.5. ADMINISTRACIÓN DE LA POLÍTICA

1.5.1 ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

Nombre del PCSC: CONFIRMA S.A.

Dirección: Ruiz Díaz de Melgarejo Nro. 985 c/ Antonio Taboada

Correo Electrónico: info@confirma.com.py

Página Web: https://www.confirma.com.py/

1.5.2 PERSONA DE CONTACTO

Nombre: GERENTE DE CONFIRMA S.A.

Teléfono: (+595 21) 218 0 218

Página web: https://www.confirma.com.py/

E-mail: info@confirma.com.py

Dirección: Ruiz Díaz de Melgarejo Nro. 985 c/ Antonio Taboada

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

Nombre: GERENTE DE CONFIRMA S.A.

Teléfono: (+595 21) 218 0 218

Página web: https://www.confirma.com.py/

E-mail: info@confirma.com.py

Dirección: Ruiz Díaz de Melgarejo Nro. 985 c/ Antonio Taboada

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 que firma electrónicamente, en función del mensaje firmado por ésta, y al cual se le vincula. Este proceso no otorga certificación notarial ni fe pública.

2. Autenticación electrónica: 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 auto firmado 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 al 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 de usuario final y certificados de las AC, que termina en un certificado raíz. El emisor del certificado del usuario final 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 usuario final 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 Nro. 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 Nro. 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 servicio de confianza**: Acuerdo entre la AC Raíz-Py y el PCSC, o entre el PCSC y el titular o responsable del certificado 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 de la 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**: es 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, el 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 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 Hardware**: 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 DP.

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 Nro. 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 Nro. 6822/2021.

32. **Parte usuaria**: la 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. **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.

36. **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 la habilitación.

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 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 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 existan 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 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.

SIGLAS Y ACRÓNIMOS

1. **AC**: Autoridad de Certificación (CA por sus siglas en inglés, Certificate Authority)
2. **AC Raíz-Py**: Autoridad Certificadora Raíz del Paraguay
3. **CCTV**: Circuito cerrado de TV
4. **DPC-SCTE**: Declaración de prácticas de sello cualificado de tiempo electrónico
5. **DGCE**: Dirección General de Comercio Electrónico dependiente del Viceministerio de Comercio y Servicios.
6. **FCT**: Fuente confiable de tiempo
7. **ISO**: Organización Internacional para la Estandarización (ISO por sus siglas en inglés, International Organization for Standardization).

8. **LRC**: Lista de certificados revocados (CRL por sus siglas en inglés, CertificateRevocation List)
9. **MIC**: Ministerio de Industria y Comercio
10. **MSC**: Módulo de seguridad criptográfico
11. **OID**: Identificador de Objeto (OID por sus siglas en inglés, Object Identifier)
12. **OU**: Unidad Organizacional (OU por sus siglas en inglés, Organization Unit)
13. **PKI**: Infraestructura de Clave Pública (PKI por sus siglas en inglés, Public Key Infrastructure).
14. **ICPP**: Infraestructura de Claves Públicas del Paraguay
15. **OEC**: Organismo de Evaluación de la Conformidad
16. **OS**: Organismo de Supervisión
17. **PCSC**: Prestador cualificado de Servicios de confianza
18. **PCN**: Plan de Continuidad del negocio
19. **PC-SCTE**: Política de certificación de sello cualificado de tiempo electrónico
20. **PS**: Política de Seguridad
21. **PSS**: Prestador de Servicios de Soporte
22. **RFC**: Petición de Comentarios (RFC por sus siglas en inglés, Request For Comments)
23. **SCTE**: Sello cualificado de tiempo electrónico
24. **SSTE**: Servidor de Sello de tiempo electrónico
25. **UPS**: Sistemas de alimentación ininterrumpida (UPS por sus siglas en inglés, uninterruptible power supply)
26. **URL**: Localizador uniforme de recursos (URL por sus siglas en inglés, UniformResource Locator).
27. **ETSI**: European Telecommunication Standard Institute

28. **ITSEC**: European Information Technology Security Evaluation Criteria
29. **ITU**: International Telecommunications Union
30. **SNMP**: Simple Network Management Protocol
31. **TSP**: Protocolo de Sello de Tiempo (TSP por sus siglas en inglés, Time Stamp Protocol)
32. **TSQ**: Solicitud de Sello de Tiempo (TSQ Por sus suglas en inglés, Time Stamp Request)

2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO

2.1 REPOSITORIOS

El PCSC CONFIRMA S.A. mantiene un repositorio disponible conforme a las siguientes obligaciones:

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

La información del Prestador Cualificado de Servicios de Certificación, incluyendo las políticas y la Declaración de Prácticas de Certificación, se publica tan pronto como está disponible.

Los cambios en la Declaración de Prácticas de Certificación se rigen por lo establecido en la sección 1.5 de este documento. El repositorio del PCSC CONFIRMA S.A. está disponible las veinticuatro (24) horas del día, los siete (7) días de la semana. En caso de interrupción debido a fuerza mayor, el servicio se restablecerá en un plazo no superior a veinticuatro (24) horas, asegurando una disponibilidad del servicio de al menos un 99,5% anual y un tiempo máximo de inactividad programada del 0,5% anual.

2.3 CONTROLES DE ACCESO A LOS REPOSITORIOS

El acceso permanente, irrestricto y gratuito a la información publicada en el repositorio de PCSC CONFIRMA S.A. está garantizado.

Se han implementado medidas de seguridad lógicas y físicas para evitar que personas no autorizadas puedan agregar, eliminar o modificar el contenido del repositorio.

El Servicio de Publicación de CONFIRMA S.A. cuenta con un sistema de seguridad que controla de manera efectiva el acceso a la información y previene que personas no autorizadas puedan realizar modificaciones o eliminaciones de registros. Este proceso asegura la integridad y autenticidad de la información almacenada, garantizando que:

- Solo las personas autorizadas puedan hacer anotaciones y modificaciones.
- Se pueda verificar la autenticidad de la información.

- Los certificados solo estén disponibles para consulta si el suscriptor ha dado su consentimiento formal en el contrato de suscripción correspondiente.
- Los servidores que almacenan la información del repositorio público de PCSC CONFIRMA S.A. están en el nivel 4 de seguridad física y requieren un control de acceso con doble factor de autenticación.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

La TSQ no incluye información sobre el solicitante, por lo tanto, en situaciones en las que PCSC CONFIRMA S.A. requiera conocer la identidad del solicitante, implementa métodos alternativos de identificación y autenticación.

4. REQUERIMIENTOS OPERACIONALES

4.1 SOLICITUD DE SCTE

Para solicitar un SCTE en un documento electrónico, el suscriptor debe enviar un TSQ que contenga el hash a ser firmado o sellado.

A continuación, se detallan 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, tal como se define en el RFC 3161.

La PC-SCTE implementada por PCSC CONFIRMA S.A. define los procedimientos específicos para la solicitud de sellos de tiempo emitidos bajo la PC-SCTE, conforme a los requisitos aplicables establecidos en el documento DOC-ICPP-26 [4].

Una vez que la solicitud ha sido aceptada, registrada y se han llevado a cabo las verificaciones pertinentes, se genera la marca de tiempo y se envía al solicitante.

4.1.1 QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO

El solicitante, ya sea una persona física o jurídica, puede realizar la solicitud de emisión de sellos cualificados de tiempo electrónico directamente a CONFIRMA S.A. Una vez que la solicitud ha sido aceptada, registrada y se han realizado las verificaciones pertinentes, se genera la marca de tiempo y se envía al solicitante.

4.1.2 PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES

En los siguientes ítems se describen las obligaciones generales de las entidades involucradas.

4.1.2.1. RESPONSABILIDADES Y OBLIGACIONES DEL PCSC

Responsabilidades:

A. El PCSC es responsable 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:

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.
Suscribirá el Contrato de Prestación de Servicio de sello cualificado de tiempo electrónico.

4.2 EMISIÓN DEL SCTE

A continuación, se describen los requisitos y procedimientos operativos relacionados con la emisión de un SCTE y el protocolo a implementar, según lo definido en el RFC 3161. CONFIRMA S.A. proporciona a sus suscriptores acceso a un Servidor de Aplicaciones para reenviar las TSQ recibidas al SSTE y luego devolver al suscriptor los SCTE recibidos en respuesta a las TSQ.
El Servidor de Aplicaciones consiste 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.
El Servidor de Aplicaciones mínimamente realiza 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 *hashes 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:

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.

La disponibilidad de sus servicios de SCTE del PCSC CONFIRMA S.A. es de 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

A continuación, se detallan los requisitos y procedimientos operativos relacionados con la aceptación de un SCTE recibido por el suscriptor.

Después de recibir la respuesta (que normalmente contiene un sello de tiempo electrónico en un TimeStampResp), el suscriptor debe verificar si hay errores en la respuesta. Si no hay errores, debe verificar los campos del SCTE y la validez de la firma electrónica cualificada del mismo. Es crucial verificar que lo que se selló coincide con lo recibido para sellar. Además, se debe verificar que el SCTE fue emitido por CONFIRMA S.A., y que el hash de los datos y el OID del algoritmo hash son correctos. Luego, se debe verificar el tiempo de la respuesta comparándolo con una fuente de tiempo local confiable o el número de control incluido en la solicitud. Si alguna de estas verificaciones falla, el SCTE debe ser rechazado.

Además, se debe verificar el estado del certificado del SSTE, por ejemplo, consultando la Lista de Certificados Revocados (LCR), para asegurarse de que el certificado sigue siendo válido. El suscriptor también debe analizar el campo "política" para determinar si la política bajo la cual se emitió el sello es aceptable para la solicitud.

La PC-SCTE implementada por PCSC CONFIRMA define los procedimientos específicos para la aceptación de SCTE emitidos bajo esta política, basados en los procesos mencionados y los requisitos aplicables establecidos por el documento DOC-ICPP-26 [4].

4.4 CARACTERÍSTICAS DEL SCTE

Las características de los sellos de tiempo que serán emitidos según PC-SCTE, contienen:

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

5.1. SEGURIDAD FÍSICA

A continuación, se detallan los controles físicos relacionados con las instalaciones que albergan los sistemas de PCSC CONFIRMA S.A. y el PSS vinculado.

5.1.1 CONSTRUCCIÓN Y UBICACIÓN DE LAS INSTALACIONES DEL PCSC

Las instalaciones que albergan los sistemas relacionados con la expedición del SCTE de PCSC CONFIRMA S.A. no están públicamente identificadas. Sin embargo, la ubicación administrativa/operacional, como una AR, puede ser accesible al público en casos donde el solicitante presente los documentos electrónicos en soporte magnético

que requieran el servicio. Esto se debe a que el servicio no solo puede ser proporcionado a través de Internet u otra red de datos.

5.1.2 ACCESO FÍSICO A LAS INSTALACIONES DEL PCSC

El PCSC CONFIRMA S.A. implementa un sistema de control de acceso físico que garantiza 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

El PCSC CONFIRMA S.A. define 3 (tres) niveles de acceso físico a los distintos ambientes del PCSC y 1 (un) cuarto nivel relacionado con la protección del SSTE.

El primer nivel o nivel 1 está ubicado después de la primera barrera de acceso a las instalaciones del PCSC. El ambiente de nivel 1 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 es interno al primero requiere la identificación biométrica individual de las personas que ingresan al mismo. Este es el nivel de seguridad para la ejecución de cualquier proceso operativo o administrativo de PCSC. El paso del primer al segundo nivel requiere de factor de autenticación electrónica y tarjeta de identificación visible.

El ambiente del nivel 2 está separado del nivel 1 por paredes divisorias de mampostería, no posee ventanas u otro tipo de apertura al exterior, excepto la puerta de acceso.

Sólo se permite 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 está 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 lleva un registro de tanto las entradas como las salidas de cada persona autorizada. Se requerirán dos factores de autenticación para la entrada a este nivel como identificación por tarjeta electrónica e identificación de datos biométricos o contraseñas.

Las paredes que delimitan el ambiente del nivel 3 son sólidas y de mampostería. No poseen ventanas u otro tipo de abertura al exterior, excepto la puerta de acceso.

El PCSC CONFIRMA S.A. posee 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 se encuentra 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 en el nivel 3 para alberga y segrega:

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, comprende 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 cumplen 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 alberga el SSTE se encuentra 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 se realiza bajo vigilancia 24X7 (las veinticuatro horas del día, los siete días de la semana).

La seguridad es realizada por 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 se encuentra equipado con circuito cerrado de TV conectado a un sistema de grabación local 24x7. La ubicación y capacidad de estas cámaras no permite la captura de contraseñas tecleadas en los sistemas.

Los medios resultantes de esta grabación son almacenados 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 PCSC CONFIRMA S.A. posee sistema de control de acceso desde el Nivel 1.

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

La infraestructura del ambiente nivel 3 del PCSC CONFIRMA S.A., esta dimensionada con sistemas y dispositivos que garantizan el suministro ininterrumpido de energía eléctrica a las instalaciones. Las condiciones de suministro de energía se mantienen para cumplir con los requisitos de disponibilidad de los sistemas del PCSC CONFIRMA S.A. y sus respectivos servicios. Un sistema de puesta a tierra debe ser implementado.
Todos los cables eléctricos están protegidos por tuberías o ductos apropiados.

Son 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. Son utilizados conductos separados para los cables de energía, de telefonía y de datos.

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

Son mantenidos actualizados los registros sobre la topología de la red de cables, de acuerdo con los requisitos de confidencialidad establecidos en el ítem 13 "seguridad en las telecomunicaciones" de la norma ISO 27002/2022. Cualquier modificación en la red es previamente documentada.

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

El sistema de climatización cumple 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 es permanentemente monitoreada por el sistema de notificación de alarmas.

La capacidad de redundancia de toda la estructura de energía y aire acondicionado es garantizada,

por medio de Generadores de un tamaño compatible y Sistemas de UPS redundantes.

5.1.4 EXPOSICIÓN AL ALGUA

Las instalaciones del PCSC CONFIRMA S.A. están protegidas para evitar exposiciones al agua, filtraciones e inundaciones provenientes de fuentes externas.

5.1.5 PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO

Dentro de las Instalaciones del PCSC CONFIRMA S.A. no se permite fumar ni portar objetos que produzcan fuego o chispa, a partir del nivel 1.

Los extintores de clase B y C están dentro del ambiente de nivel 3, para apagar incendios en combustibles y equipos eléctricos, dispuestos de tal manera que faciliten su acceso y manipulación.

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

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

El PCSC CONFIRMA S.A. implementa mecanismos específicos descriptos en su Procedimiento de Salida de Emergencia, el cual está diseñado para *garantizar la* seguridad de su personal y de su equipamiento en situaciones de emergencia. Estos mecanismos permiten 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 activa inmediatamente la apertura de las puertas.

5.1.6 ALMACENAMIENTO DE MEDIOS

PCSC CONFIRMA S.A. se compromete a garantizar el manejo adecuado y la protección efectiva de los medios de almacenamiento que contengan datos críticos o sensibles del sistema. Esto incluye la prevención de daños accidentales debido a factores como agua, fuego o electromagnetismo, así como la detección y prevención de cualquier uso no autorizado, acceso o divulgación de esta información.

Para lograr este objetivo, la información relacionada con la infraestructura de PCSC CONFIRMA S.A. se almacena de manera segura

en armarios ignífugos y cofres de seguridad. La elección de estos dispositivos se basa en la clasificación de la información que contienen, garantizando así un nivel adecuado de protección en función de la sensibilidad de los datos almacenados.

5.1.7 ELIMINACIÓN DE RESIDUOS

Los soportes de información, tanto en papel como magnéticos, se eliminan utilizando mecanismos que aseguran que la información no pueda ser recuperada. En el caso de los soportes magnéticos, se destruyen físicamente después de ser desechados, o se reutilizan después de un proceso de borrado permanente o formateo. En el caso de la documentación en papel, se utilizan trituradoras o papeleras específicamente designadas para su destrucción, asegurando un control adecuado durante todo el proceso.

5.1.8 RESPALDO FUERA DE SITIO

CONFIRMA S.A. cuenta con un almacén externo seguro para la custodia de documentos, dispositivos magnéticos y electrónicos, los cuales son independientes del centro de operaciones principal. Esta instalación solo está accesible para el personal autorizado las 24 horas del día, los 7 días de la semana (24X7) y cumple con los requisitos mínimos establecidos en este documento para ser considerada un ambiente de nivel 2.

5.2 CONTROLES PROCEDIMENTALES

A continuación, se detallan en los siguientes apartados de esta DPC los requisitos para la identificación y definición de los Roles de Confianza en el PCSC CONFIRMA S.A., así como de las PSS vinculadas a estos roles, junto con las responsabilidades asignadas a cada perfil. Asimismo, se

especifica la cantidad de personal requerido para llevar a cabo cada tarea relacionada con los roles o perfiles establecidos.

5.2.1. ROLES DE CONFIANZA

CONFIRMA S.A. asegura la segregación de tareas en las funciones críticas para prevenir el uso indebido del SSTE por parte de un empleado sin ser detectado. Las acciones de cada empleado están restringidas de acuerdo con su perfil asignado.

Se establecen 3 (tres) 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 colaboradores de CONFIRMA S.A. reciben formación específica antes de obtener cualquier tipo de acceso. El nivel y tipo de acceso se establecen en un documento oficial, de acuerdo con los requisitos de cada rol o perfil.

Cuando un colaborador se desvincula de CONFIRMA S.A., se revocan de inmediato sus permisos de acceso. Además, cualquier cambio en el puesto o función de un colaborador dentro del PCSC requiere una revisión de sus permisos de acceso. Se mantiene una lista de revocación que detalla todos los recursos que el colaborador debe devolver al PCSC CONFIRMA S.A. al momento de su desvinculación.

5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

El PCSC CONFIRMA S.A. tiene un requisito de control multiusuario para la generación y el uso de claves del SSTE, según lo definido en el punto 6.1.1. Para todas las actividades llevadas a cabo en el cofre o gabinete que almacena los SSTE, se requiere la presencia de al menos dos colaboradores con roles de confianza. En cambio, las demás tareas en PCSC CONFIRMA S.A. son realizadas por un único empleado.

5.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

El PCSC CONFIRMA S.A. garantiza que la identidad y el perfil de cada empleado serán verificados antes de que:

a) sean incluidos en una lista de acceso físico a las instalaciones del PCSC CONFIRMA S.A.;

b) sean incluidos en la lista de acceso lógico a los sistemas de confianza del PCSC CONFIRMA S.A.

c) sean incluido en una lista para acceso lógico a los SSTE del PCSC CONFIRMA S.A.;

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.

CONFIRMA S.A. implementa una política para el uso de "contraseñas seguras", definidas en su PS, con procedimientos de validación de estas contraseñas.

5.3 CONTROLES DE PERSONAL

Los siguientes ítems de esta DPC describen los requisitos y procedimientos establecidos por el PCSC CONFIRMA S.A. y los PSS asociadas con respecto a su personal. Estos aspectos incluyen la verificación de

antecedentes y competencias, la formación, la rotación de puestos, las sanciones por conductas no autorizadas, los controles durante el proceso de contratación y la documentación requerida.

Todos los colaboradores del PCSC CONFIRMA S.A. y de los PSS vinculadas, responsables de las tareas operativas, han sido registrados mediante 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 CONFIRMA S.A. y los PSS vinculados e involucrado en las actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gestión de certificado es 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 objetivo de salvaguardar la seguridad y la credibilidad de las entidades, todos los colaboradores del PCSC CONFIRMA S.A. y las PSS vinculadas que participen en actividades relacionadas con la emisión, expedición, distribución, revocación y gestión de certificados de sellos de tiempo deben someterse a:

a) confirmación de empleos anteriores;

b) verificación de referencias profesionales;

c) título académico obtenido; y

d) verificación de antecedentes judiciales y policiales.

5.3.3. REQUERIMIENTOS DE CAPACITACIÓN

Todo el personal del PCSC CONFIRMA S.A. y los PSS vinculados e involucrados en las actividades directamente relacionados con la emisión, expedición, distribución, revocación y gestión del certificado reciben 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

El personal de PCSC CONFIRMA S.A. y las PSS vinculadas que participan en actividades relacionadas con la emisión, expedición, distribución, revocación y gestión de los SCTE, se mantiene al día respecto a posibles cambios o modificaciones tecnológicas en los sistemas de PCSC CONFIRMA S.A.

5.3.5. FRECUENCIA Y SECUENCIA EN LA ROTACIÓN DE LAS FUNCIONES

CONFIRMA S.A. establece una política para la rotación del personal en diferentes cargos y perfiles definidos por la organización. Esta política está alineada con los objetivos establecidos en el ítem 5.2.1. Además, PCSC CONFIRMA S.A. lleva a cabo una rotación de sus roles de confianza al menos una vez cada cinco años.

5.3.6. SANCIONES PARA ACCIONES NO AUTORIZADAS

En caso de detectarse una acción no autorizada, ya sea confirmada o sospechosa, realizada por un individuo responsable del proceso operativo de PCSC CONFIRMA S.A. o de un PSS asociado, el PCSC procederá de inmediato a suspender el acceso de dicha persona al SSTE. Posteriormente, se iniciará un procedimiento administrativo para esclarecer los hechos y, de ser necesario, se tomarán las medidas legales pertinentes.

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

a) relato de lo ocurrido con el modo de operación o "modus operandi";

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 CONFIRMA S.A. comunicará 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 CONFIRMA S.A. 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 es contratado conforme lo establecido en los ítems 7 "seguridad ligada a los recursos humanos" y 15 "relaciones con suministradores" norma ISO 27002/2022.

5.3.8. DOCUMENTACIÓN SUMINISTRADA AL PERSONAL

El PCSC CONFIRMA S.A. pone a disposición de todo su personal y para el personal vinculado al PSS:

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 proporcionada al personal está clasificada de acuerdo con la Política de Seguridad (PS), que define la clasificación de la información establecida por el PCSC CONFIRMA S.A. Además, esta documentación se mantiene actualizada de forma regular.

5.4 PROCEDIMIENTO DE REGISTRO DE AUDITORÍA

En los siguientes ítems se describen los aspectos de los sistemas de auditoría y registro de eventos implementados por el PCSC CONFIRMA S.A con el fin de mantener un ambiente seguro.

5.4.1 TIPOS DE EVENTOS REGISTRADOS

El PCSC CONFIRMA S.A. registra en archivos de auditoría todos los eventos relacionados a la seguridad de su sistema. Los siguientes eventos están incluidos 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 CONFIRMA S.A. registra, 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.

El PCSC CONFIRMA S.A. establece que todos los registros de auditoría ya sean electrónicos o manuales, deben incluir la identificación del agente responsable, así como la fecha y hora del evento. Los registros electrónicos de auditoría deben mostrar la hora en formato UTC, mientras que los registros en papel deben indicar la hora local junto con la ubicación específica.

Para facilitar los procesos de auditoría, toda la documentación relacionada con los servicios de PCSC CONFIRMA S.A. se almacena de

manera electrónica o manual en un único lugar, conforme a la Política de Seguridad (PS) establecida por el PCSC.

5.4.2 FRECUENCIA DE PROCESAMIENTO DEL REGISTRO (LOGS)

El PCSC CONFIRMA S.A. establece un plazo máximo de una semana para que el personal operativo analice los recursos de auditoría.

Todos los eventos significativos serán detallados en un informe de auditoría de registros. El procesamiento de los registros de auditoría implica una revisión exhaustiva que incluye la verificación de que no han sido manipulados, una inspección breve de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad detectada en los registros. Las acciones tomadas como resultado de la revisión de auditoría son documentados.

5.4.3 PERÍODO DE CONSERVACIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

El PCSC CONFIRMA S.A. ha determinado que los registros de auditoría se conservarán localmente durante un período mínimo de dos meses, luego serán almacenados según lo indicado en el ítem 5.5.2.

5.4.4 PROTECCIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

Los registros de auditoría del PCSC CONFIRMA S.A. están protegidos de manipulación mediante la firma de los archivos que los contienen. Además, son almacenados en dispositivos ignífugos y se garantiza su disponibilidad al ser almacenados en instalaciones externas al centro principal.

El acceso a los archivos de registros está restringido únicamente a personas autorizadas, y el manejo de los dispositivos está a cargo de personal autorizado en todo momento. Existe un procedimiento interno

que detalla los procesos de gestión de los dispositivos que contienen los registros de auditoría.

Estos mecanismos de protección cumplen con los requisitos establecidos en el ítem 12 "seguridad en la operativa" de la norma ISO 27002/2022.

5.4.5 PROCEDIMIENTO DE RESPALDO (BACKUP) DE REGISTRO (LOGS) DE AUDITORÍA

El PCSC CONFIRMA S.A. cuenta con un procedimiento eficiente de copias de seguridad para garantizar la disponibilidad de archivos relevantes en caso de pérdida o destrucción. Se ha implementado un procedimiento de copia de seguridad semanal para los registros de auditoría, donde se realiza una copia de todos los logs en un medio externo. Además, se mantiene una copia de respaldo en un centro de custodia externo.

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

La información de la auditoría de eventos se recopila internamente de manera automatizada por el sistema operativo, las comunicaciones de red y el software de sellado de tiempo, además de los datos generados manualmente, los cuales serán almacenados por personal debidamente autorizado. Estos elementos conforman el sistema de acumulación de registros de auditoría.

5.4.7 NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO

No es necesario notificar al individuo, organización, dispositivo o aplicación que causó un evento registrado por el sistema de acumulación de registros de auditoría.

5.4.8 EVALUACIÓN DE VULNERABILIDADES

Las actividades de análisis de vulnerabilidades del PCSC CONFIRMA S.A. están integradas en los procesos de auditoría. Estos análisis deben ser ejecutados, revisados y examinados mediante una evaluación de los eventos monitorizados, y en caso de ser relevantes, serán registrados por separado según su gravedad.

Las acciones correctivas que surjan serán implementadas por PCSC CONFIRMA S.A. y documentadas para fines de auditoría. Estos análisis deben llevarse a cabo periódicamente según el procedimiento interno establecido para tal fin.

Los datos de auditoría de los sistemas se almacenan con el propósito de ser utilizados en la investigación de incidencias y para identificar vulnerabilidades.

5.5 ARCHIVOS DE REGISTROS

En los siguientes ítems se describe la política general de archivo de registros, para su uso futuro, implementada por el PCSC CONFIRMA S.A. y los PSS vinculados a él.

5.5.1 TIPOS DE REGISTROS ARCHIVADOS

Los tipos de registros archivados comprenden lo siguiente:

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

El PCSC CONFIRMA S.A. establece 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

Los archivos del PCSC CONFIRMA S.A. están protegido de manera que solo las personas debidamente autorizadas puedan acceder a él. Está protegido contra visualización, modificación, borrado u cualquier otra manipulación al ser almacenado en un sistema fiable.

Se garantiza la protección adecuada de los archivos mediante la asignación de personal calificado para su manejo y su almacenamiento en instalaciones externas seguras. Los archivos están clasificados y almacenados con requisitos de seguridad compatibles con esta clasificación, según lo establecido en el ítem 12 "seguridad en la operativa" de la norma ISO 27002/2022.

5.5.4. PROCEDIMIENTO DE RESPALDO (BACKUP) DE ARCHIVO

El PCSC CONFIRMA S.A. dispone de un centro de Almacenamiento Externo que se establece con el fin de asegurar la disponibilidad de las copias de los archivos de ficheros electrónicos. Los documentos físicos están resguardados en sitios seguros con acceso restringido exclusivamente para el personal autorizado. Se lleva a cabo, como mínimo, una copia de respaldo incremental diaria de todos los documentos electrónicos, y de forma semanal se realiza una copia de respaldo completa para el caso de recuperación de datos.

Adicionalmente, en situaciones donde se requiera conservar copias de documentos en formato físico, estos se guardan en un lugar seguro. Es necesario verificar la integridad de estas copias de seguridad al menos cada seis meses.

5.5.5. REQUERIMIENTOS PARA SELLADO DE TIEMPO DE REGISTROS

Los registros se fechan utilizando una fuente confiable a través del Protocolo de Tiempo de Red (NTP). Estos registros se almacenan en una carpeta renombrada siguiendo el formato yyyy-mm-dd, donde cada carpeta abarca desde el primer día hasta el último día de la semana correspondiente.

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

PCSC CONFIRMA S.A. cuenta con un sistema centralizado para recopilar información sobre la actividad de los equipos involucrados en el servicio de gestión de datos de archivo.

5.5.7. PROCEDIMIENTOS PARA OBTENER Y VERIFICAR LA INFORMACIÓN ARCHIVADA

El PCSC CONFIRMA S.A. cuenta con un procedimiento que detalla el proceso para verificar la exactitud y accesibilidad de la información archivada. Además, durante las auditorías, CONFIRMA S.A. proporciona al Organismo de Evaluación de la Conformidad (OEC) la información y los medios necesarios para la verificación.

5.6 CAMBIO DE CLAVE

Cada par de claves de los Certificados utilizados en el servicio de sellado de tiempo está exclusivamente asociado al sistema que proporciona dicho servicio. Antes de que la clave privada de los Certificados caduque, se llevará a cabo un cambio de claves previo a la caducidad o revocación de las claves actuales. La generación de un nuevo par de claves y la instalación del certificado correspondiente en el SSTE son

realizadas únicamente por empleados con roles de confianza, mediante un proceso de doble control, en un entorno físico seguro.

5.7 RECUPERACIÓN DE DESASTRES Y COMPROMISO

5.7.1 Disposiciones Generales

En los siguientes ítems se describen los requisitos relacionados con los procedimientos de notificación y de recuperación de desastres, previstos en el PCN de CONFIRMA S. A, establecido de conforme a su POLÍTICA DE SEGURIDAD el cual considera 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.

CONFIRMA S.A. garantiza, que en caso de compromiso de su operación por cualquiera de las razones enumeradas en los puntos a continuación, las informaciones relevantes estarán disponibles para los suscriptores y para la parte usuaria. Igualmente, se podrá 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 emitirá un SCTE hasta que se tomen medidas necesarias 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 caso de que ocurra un evento de corrupción de recursos, aplicaciones o datos, se seguirán los procedimientos de gestión correspondientes según las políticas establecidas de seguridad y gestión de incidentes. Estos procedimientos incluyen escalado, investigación y respuesta al incidente.

5.7.3 PROCEDIMIENTOS DE COMPROMISO DE LA CLAVE PRIVADA DEL PCSC

5.7.3.1 CERTIFICADO DE ENTIDAD ES REVOCADO

En caso de que el certificado de SCTE del PCSC CONFIRMA S.A. sea revocado, se notificará a todos sus suscriptores que el proceso de SCTE no estará disponible hasta nuevo aviso.

5.7.3.2 CLAVE DEL PCSC ESTA COMPROMETIDA

En caso de sospecha o confirmación de compromiso, CONFIRMA activará los procedimientos de compromiso de claves conforme a las políticas de seguridad, gestión de incidentes y continuidad del negocio. Estos procedimientos facilitarán la recuperación de los sistemas críticos, si es necesario, en el centro de datos secundario. Además, se notificará de inmediato al MIC la situación y se solicitará la revocación del certificado correspondiente. Asimismo, se informará a todos los suscriptores que el proceso de SCTE no estará disponible hasta nuevo aviso.

5.7.3.3 PERDIDA DE CALIBRACION Y SINCRONISMO DEL SSTE

A continuación, se describen los procedimientos que realiza el PCSC CONFIRMA S.A. en caso de pérdida de calibración y sincronismo del SSTE.

a) Detección del problema: Identificar y confirmar que ha ocurrido una pérdida de calibración y sincronismo en el SSTE.
b) Aislamiento del sistema: Si es posible, aislar el SSTE afectado para evitar que el problema se propague o afecte a otros sistemas o servicios relacionados.
c) Notificación: Informar de inmediato a los responsables de seguridad de la información y al equipo técnico encargado de la gestión del SSTE sobre la pérdida de calibración y sincronismo.
d) Investigación y Análisis: Realizar una investigación detallada para determinar la causa raíz de la pérdida de calibración y sincronismo.
e) Recuperación de calibración y sincronismo: Tomar las medidas necesarias para restaurar la calibración y sincronismo del SSTE. Esto puede incluir la recalibración del sistema, la corrección de desviaciones de tiempo y la sincronización con las fuentes de tiempo confiables.
f) Validación y pruebas: Una vez restaurada la calibración y sincronismo, realizar pruebas exhaustivas para verificar que el sistema funcione correctamente y que los sellos de tiempo electrónicos (SCTE) generados sean precisos y confiables.
g) Monitoreo: monitoreo continuo del SSTE para detectar cualquier anomalía o desviación en la calibración y sincronismo en el futuro.

h) Actualización de Políticas y Procedimientos: Si es necesario, revisar y actualizar las políticas y procedimientos relacionados con la gestión de la calibración y sincronismo del SSTE para prevenir futuros incidentes similares.

i) Registro: Es importante documentar todos los detalles del incidente, así como las acciones tomadas para su resolución. Además, si se determina que los sellos de tiempo emitidos durante el período de pérdida de calibración y sincronismo podrían verse afectados, puede ser necesario comunicarse con los suscriptores para informarle sobre la situación.

5.7.4 CAPACIDAD DE CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

El PCSC CONFIRMA S.A. restablecerá los servicios críticos conforme al plan de incidencias y continuidad de negocio vigente, garantizando la recuperación de la operación normal en un plazo máximo de 24 horas tras el desastre. Además, cuenta con un centro de datos secundario preparado para poner en funcionamiento los sistemas de certificación según lo descrito en el plan de continuidad de negocio, en caso de ser necesario.

5.8 EXTINCIÓN DE UN PCSC O ENTIDADES VINCULADAS

El PCSC CONFIRMA S.A. asegura que cualquier interrupción para los suscriptores del servicio y terceras partes debido al cese de los servicios sea mínima. En este sentido, garantiza un mantenimiento continuo de los

registros según lo establecido en la Declaración de Prácticas de Certificación de Sellado de Tiempo durante el tiempo definido.

Antes de llevar a cabo el cese de sus actividades, CONFIRMA S.A. implementará un plan de terminación que incluirá las siguientes disposiciones:

a) Pondrá a disposición de todos los suscriptores y partes receptoras información sobre el cese respectivo;

b) 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) 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)Mantendrá o transferirá 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 serán destruidas de tal forma que no puedan ser recuperadas;

f) Deberá solicitar la revocación de sus certificados del SSTE;

g) Deberá notificar a todas las entidades afectadas.

CONFIRMA S.A. proporcionará 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

Los siguientes ítems describen las medidas utilizadas por sistemas y productos confiables, protegidos contra cualquier tipo de alteración, para garantizar la seguridad técnica y criptográfica de los procesos de certificación que respaldan.

6.1 CICLO DE VIDA DE LA CLAVE PRIVADA DEL SSTE

El SSTE permite:

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

El PCSC CONFIRMA S.A. genera el par de claves del Certificado conforme a su Declaración de Prácticas de Certificación y su texto de divulgación, los cuales están disponibles en su página web.

El par de claves criptográficas del SSTE de PCSC CONFIRMA S.A. debe ser generado por CONFIRMA S.A., previa autorización otorgada por la AC Raíz-Py a través de una resolución ministerial. Para garantizar la seguridad, se seguirán rigurosamente los procedimientos de ceremonia de claves

dentro de un área de alta seguridad designada para esta tarea. Durante la ceremonia de generación de claves, todas las actividades serán registradas, fechadas y firmadas por todos los participantes, con la supervisión de un Auditor. Estos registros están bajo custodia para su posterior auditoría y seguimiento.

CONFIRMA S.A. garantizará que todas las claves criptográficas serán 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.

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].

Las claves privadas se generarán de tal forma que no puedan ser exportables.

6.1.2 GENERACIÓN DE SOLICITUD DEL CERTIFICADO

El PCSC CONFIRMA S.A. cuenta 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 garantiza que, al excluir una solicitud de certificado electrónico debido a un desistimiento en la emisión del certificado, se excluye automáticamente la clave privada correspondiente.

6.1.4 INSTALACION DEL CERTIFICADO

El SSTE debe 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 permite 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 LA CLAVE PÚBLICA DEL PCSC PARA USUARIOS

El PCSC CONFIRMA S.A. establece los métodos para hacer disponibles los certificados, incluyendo todos los de la cadena de certificación, para los usuarios de ICPP. Estos métodos incluyen:

a) A través del sitio web de CONFIRMA S.A.

6.1.7 TAMAÑO DE CLAVE

CONFIRMA S.A.A define el tamaño de las claves criptográficas del SSTE, en concordancia con los requerimientos aplicables establecidos por el documento DOC-ICPP-06 [2].

6.1.8 GENERACIÓN DE PARÁMETROS DE CLAVES ASIMÉTRICAS

Los parámetros de generación de claves asimétricas adoptan las normas definidas en el documento DOC-ICPP-06 [2].

6.1.9 VERIFICACIÓN DE CALIDAD DE LOS PARÁMETROS

Los parámetros serán 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 generación del par de claves del PCSC CONFIRMA S.A. es realizado por hardware.

6.1.11 PROPÓSITOS DE USOS DE CLAVE

Las claves privadas de los STE operados por el PCSC CONFIRMA S.A. 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, se establecen 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

Los módulos criptográficos de generación de claves asimétricas del PCSC CONFIRMA S.A. adoptan las normas definidas en el documento DOC-ICPP-06 [2].

6.2.2 CONTROL MULTI-PERSONA DE CLAVE PRIVADA

No aplica.

6.2.3 CUSTODIA (ESCROW) DE LA CLAVE PRIVADA

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 DE LA CLAVE PRIVADA

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

PCSC CONFIRMA S.A. no archivara 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

Los procedimientos de gestión de la clave privada del Certificado de CONFIRMA S.A. se activan a través de la ejecución del procedimiento de inicio seguro del módulo criptográfico. Esto lo llevan a cabo personas con funciones fiables, quienes verifican su identidad mediante métodos como contraseñas, tokens o biometría, entre otros, y realizan las acciones necesarias para la activación.

6.2.8 MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

Antes de proceder con la destrucción de las claves, se emitirá una revocación del certificado de las claves públicas asociadas a estas. Posteriormente, se llevará a cabo la destrucción física o el reinicio a bajo nivel de los dispositivos que contengan cualquier parte de las claves privadas de CONFIRMA S.A, siguiendo los pasos detallados en el manual del administrador del equipo criptográfico. Por último, se eliminarán de forma segura las copias de seguridad.

6.2.9 MÉTODO DE DESTRUCCIÓN DE CLAVE PRIVADA

Antes de proceder con la destrucción de las claves, se emitirá una revocación del certificado de las claves públicas asociadas a estas. Posteriormente, se llevará a cabo la destrucción física o el reinicio a bajo nivel de los dispositivos que contengan cualquier parte de las claves privadas de CONFIRMA S.A, siguiendo los pasos detallados en el manual del administrador del equipo criptográfico. Por último, se eliminarán de forma segura las copias de seguridad.

6.3 OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES

6.3.1 ARCHIVO DE LA CLAVE PÚBLICA

Las claves públicas del SSTE del PCSC CONFIRMA S.A. serán conservados de manera permanente a su expiración, 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 CONFIRMA S.A. 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 rechazará 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, se indican los mecanismos utilizados para brindar la seguridad de sus estaciones de trabajo, servidores y demás sistemas y equipos, conforme a la PS del PCSC CONFIRMA S.A.

6.5.1 REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS

Los equipos del PCSC CONFIRMA S.A., utilizados en los procesos de emisión, expedición, distribución, y gestión de los SCTE implementan, entre otras, las siguientes funcionalidades:

a) control de acceso a los servicios y perfiles del PCSC CONFIRMA S.A.;

b) clara segregación de tareas y atribuciones relacionadas con cada rol de confianza o perfil del PCSC CONFIRMA S.A.;

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 CONFIRMA S.A;

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 son implementadas por el sistema operativo y por medio de combinación de este, con el sistema de gestión de sellos de tiempo y con mecanismos de seguridad física.

Antes de someter cualquier equipo, o parte de él, a mantenimiento, es necesario eliminar toda la información confidencial que pueda contener y registrar su número de serie junto con las fechas de envío y recepción. Al regresar a las instalaciones de PCSC CONFIRMA S.A., se debe realizar una inspección del equipo que fue sometido a mantenimiento.

Cuando un equipo que ya no será utilizado de forma permanente debe ser completamente eliminada toda la información confidencial relacionada con la actividad de PCSC CONFIRMA S.A. Todos estos procesos deben ser registrados con fines de auditoría.

Todo equipo que sea incorporado al PCSC CONFIRMA S.A. debe ser preparado y configurado según lo establecido en la Política de

Seguridad (PS) implementada u otro documento aplicable, con el objetivo de cumplir con el nivel de seguridad requerido para su función.

6.5.2 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 CONFIRMA S.A., 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.

6.5.3 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 mantiene 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.

El SSTE tiene 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 PCSC CONFIRMA S.A. 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 el PCSC CONFIRMA S.A.

6.5.4 CICLO DE VIDA DE MÓDULOS CRIPTOGRÁFICOS ASOCIADOS AL SSTE

CONFIRMA S.A. se asegura de que el hardware criptográfico utilizado para el servicio de sellado de tiempo no se manipule durante su transporte mediante la inspección del material entregado. Este hardware criptográfico se transporta sobre soportes diseñados para evitar cualquier manipulación y se registra toda la información relevante del dispositivo para agregarla al catálogo de activos.

El uso del hardware criptográfico de sellado de tiempo requiere la participación de al menos dos empleados que tengan rol de confianza. Además, se realizan pruebas periódicas para garantizar el correcto

funcionamiento del dispositivo, el cual solo es manipulado por personal con rol de confianza.

Una vez que se retira el dispositivo, se elimina la clave privada del certificado almacenada en el hardware criptográfico. Todas las configuraciones del sistema, así como sus modificaciones y actualizaciones, son documentadas y controladas. Los cambios o actualizaciones son autorizados por el responsable de seguridad y se registran en las actas de trabajo correspondientes, realizadas por al menos dos personas con rol de confianza.

6.5.5 AUDITORÍA Y SINCRONIZACIÓN DE RELOJES DEL SSTE

El PCSC CONFIRMA S.A. realiza operaciones de sincronismo al menos una vez cada veinticuatro (24) horas.

CONFRIMA S.A. se asegurar que su SSTE está 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 se describen, cuando corresponda, los controles implementados por el PCSC CONFRIMA S.A. 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

Este ítem no aplica.

6.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD

El PCSC CONFIRMA S.A. lleva a cabo actividades específicas para la formación y concienciación de sus empleados en materia de seguridad. Los materiales utilizados para la formación y los documentos que describen los procesos son actualizados después de su aprobación por un grupo encargado de la gestión de la seguridad. Además, CONFIRMA S.A. cuenta con un plan de formación anual para llevar a cabo estas funciones.

Además, CONFIRMA S.A. exige contractualmente que cualquier proveedor externo involucrado en las labores de servicios electrónicos de certificación cumpla con medidas de seguridad equivalentes.

6.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

En este ítem, el PCSC CONFIRMA S, A. informará, 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

PCSC CONFIRMA S.A. protege el acceso físico a sus dispositivos de gestión de red y cuenta con una arquitectura que organiza el tráfico en función de sus características de seguridad, creando secciones de red claramente definidas mediante el uso de cortafuegos. Para garantizar la seguridad de la información confidencial transferida a través de redes no seguras, se utiliza cifrado mediante protocolos SSL o el sistema VPN con autenticación de doble factor.

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, están ubicados y operando desde un ambiente de nivel 3.

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

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

El acceso a Internet es proporcionado por dos líneas de comunicación de distintos sistemas autónomos.

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

a) por el OEC, para la auditoría del reloj del SSTE;

b) por el CONFIRMA S.A., 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.

6.7.2 FIREWALL

El PCSC CONFRIMA S.A. implementa mecanismos de firewall en los equipos de uso específico, configurado exclusivamente para tal función. Los firewalls están 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.

6.7.3 SISTEMA DE DETECCIÓN DE INTRUSOS (IDS)

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

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

6.7.4 REGISTRO DE ACCESO NO AUTORIZADO A LA RED

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

6.7.5 OTROS CONTROLES DE SEGURIDAD DE LA RED

El PCSC CONFRIMA S.A. implementa 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 están 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 están 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 es detectada y registrada.

6.8 CONTROLES DE INGENIERÍA DEL MÓDULO CRIPTOGRÁFICO

La clave privada de los SSTE de PCSC CONFIRMA S.A. se almacena siguiendo estándares definidos en el documento DOC-ICPP-06 [2].

7. PERFILES DE SELLO CUALIFICADO DE TIEMPO ELECTRÓNICO

7.1 DIRECTRICES GENERALES

En los siguientes ítems, describen los aspectos de los sellos de tiempos emitidos por el PCSC CONFIRMA S.A., así como las solicitudes que se les envíen.

7.2 PERFIL DEL SELLO CUALIFICADO DE TIEMPO ELECTRÓNICO

Todos los SCTE emitidos por el PCSC CONFRIMA S.A. cumplen 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 timestamp token profiles y siguen 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: conforme a lo establecido en el documento DOC-ICPP-06 [2].

Perfil de formato de respuesta

a) Parámetros a soportar:

1- el campo accuracy (de precisión) debe ser soportado y entendido;

2- incluso cuando no existe o se configura como FALSO, el campo ordering (de orden) debe ser soportado;

3- 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;

4- ninguna extensión necesita ser manejada o soportada.

b) Algoritmos a soportar: conforme a lo establecido en el documento DOC-ICPP-06 [2].

C) Tamaños de clave a soportar: conforme a lo establecido en el 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) conforme a lo establecido en documento DOC-ICPP-06 [2].

Perfil de formato de respuesta

c) 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;

d) Algoritmos a soportar: conforme a lo establecido en documento DOC-ICPP-06 [2].

e) Tamaños de clave a soportar: conforme a lo establecido en el 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. CONFIRMA S.A. utiliza 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 idkptimeStamping. 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	CRITICO
Versión	Versión	
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) Organizacional Unit Name Organization Name Country SERIAL NUMBER= RUC80113823-0	DN del PCSC emisor que conforma figura en el certificado (Item 7.2.4)
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 (Distinguished 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**= CONFIRMA S.A. [denominación o razón social de la física o persona jurídica habilitada como PCSC en mayúsculas y sin tildes, según documento de identificación]; **OID=**1.3.6.1.4.1.58404.1.3.1.1 **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 con el RFC 5280, contiene información de la clave pública 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 CONFIRMA S.A., 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= CONFIRMA S.A.

OID: 2.5.4.5 SERIAL NUMBER= RUC80113823-0

7.3 PROTOCOLO DE TRANSPORTE

CONFIRMA S.A. admite 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

El PCSC CONFIRMA S.A. será auditado, 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

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 DOCICPP-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.

CONFIRMA S.A. ha recibido una auditoría previa por parte del OEC para fines de habilitación del servicio por parte de la AC Raíz-Py y es auditado al menos cada veinticuatro (24) meses.

El PCSC CONFIRMA S.A. informa que recibió una auditoría previa, de un OEC para fines de habilitación del servicio por parte de la AC RaízPy, a efectos de continuidad de operación.

CONFIRMA S.A. informa que las entidades del ICPP directamente vinculadas a ella también fueron sometidas a una auditoría previa con fines de acreditación. Además, CONFIRMA S.A. es responsable de llevar a cabo auditorías anuales a estas entidades con el objetivo de mantener su acreditación.

8.5 ACCIONES TOMADAS COMO RESULTADO DE UNA DEFICIENCIA

El PCSC CONFIRMA S.A. cuenta con procedimientos de acciones correctivas resultantes de una auditoría, para ejecutar acciones correctivas para las deficiencias detectadas como resultado de una Auditoría.

8.6 COMUNICACIÓN DE RESULTADOS

CONFIRMA S.A. remitirá 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

El PCSC CONFIRMA S.A. comunicará al interesado en adquirir el servicio todos los costos que debe asumir para obtener el certificado y los posibles reembolsos aplicables según la normativa vigente:

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

CONFIRMA S.A. dispone de 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.

9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

9.3.1 ALCANCE DE LA INFORMACIÓN CONFIDENCIAL

CONFIRMA S.A. mantiene como confidenciales las siguientes informaciones:

1- Solicitudes de servicio y cualquier otra información personal obtenida para su prestación, excepto la información detallada en la siguiente sección.
2- Registros de transacciones, tanto completos como de auditoría.
3- Registros de auditoría interna y externa.
4- Planes de continuidad de negocio y de emergencia.
5- Planes de seguridad
6- Documentación de operaciones, archivos, monitoreo y similares.
7- Cualquier otra información designada como "Confidencial".

Como principio general, ningún documento, información o registro entregado al PCSC o PSS vinculadas serán divulgados, excepto que se establezca un acuerdo con el suscriptor para su mayor difusión.

9.3.2 INFORMACIÓN FUERA DEL ALCANCE DE INFORMACIÓN CONFIDENCIAL

El PCSC CONFIRMA S.A. considera como información pública:

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.

9.3.3 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 debe ser generadas y mantenidas por CONFIRMA S.A., quien será responsable de su confidencialidad.

9.4 PRIVACIDAD DE INFORMACIÓN PERSONAL

9.4.1 PLAN DE PRIVACIDAD

CONFIRMA S.A. garantiza la protección de los datos personales de conformidad con su Política de Privacidad. Dicha política contempla *los* 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

Todo documento, información o registro que contenga datos personales proporcionados a CONFIRMA S.A. 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

El tratamiento de la información que no es considerada como privada, estará sujero a lo que dispone la normativa al efecto.

9.4.4 RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA

El PCSC CONFIRMA S.A. es responsable por la divulgación indebida de información confidencial, por lo que se asegura que no pueda ser comprometida o divulgada a terceros.

9.4.5 NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA

La información privada obtenida por CONFIRMA S.A. 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 *tendrá 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

Ningún documento, información o registro en poder de CONFIRMA S.A. 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 de CONFIRMA S.A. 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

Sin estipulaciones.

9.4.8 INFORMACIÓN A TERCEROS

El PCSC CONFIRMA S.A. establece como lineamiento general que ningún documento, información o registros en poder del PSS o CONFIRMA S.A. responsable de esta DPC-SCTE debe 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

Según 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

El PCSC CONFIRMA S.A. implementa un Contrato de prestación de servicios de sello cualificado de tiempo electrónico para la expresión del consentimiento del suscriptor del servicio.

9.7 EXTENSION DE GARANTIA

Este ítem no aplica.

9.8 LIMITACIONES DE RESPONSABILIDAD LEGAL

El PCSC CONFIRMA S.A. en el marco de su actividad como prestador cualificado de servicios de confianza, la limitación de su responsabilidad será conforme a las disposiciones de la Ley N° 6822/2021, sus modificaciones y reglamentaciones.

9.9 INDEMNIZACIONES

El PCSC CONFIRMA S.A. 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

Esta DPC entra en vigor 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-SCTE 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 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 sujetan a las prácticas descritas en la presente DPC se 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

El PCSC CONFIRMA S.A. posee un procedimiento para enmiendas en el cual establece que las modificaciones a este documento 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

Toda enmienda o modificación de la DPC luego de la aprobación por parte de la AC Raíz-Py, *es 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

Las controversias derivadas de la presente DPC se resolverán de conformidad con la legislación vigente. También establece que la DPC de CONFIRMA S.A. 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 N° 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

Esta DPC-SCTE se adecua a la legislación aplicable y el PCSC CONFIRMA S.A. se compromete a cumplir y observar las disposiciones previstas en ella.

9.16 DISPOSICIONES VARIAS

9.16.1 ACUERDO COMPLETO

Esta DPC-SCTE representa las obligaciones y deberes aplicables a CONFIRMA S.A. y autoridades vinculadas.

En caso de conflicto entre esta DPC-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 o ineficacia de cualquiera de las disposiciones de este DPC 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 DPC 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

REFERENCIA	NOMBRE DEL DOCUMENTO	CODIGO
[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