CONFIRMA

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO SERVICIOS DE CONFIANZA CONFIRMA S.A.

CONTROL DOCUMENTAL

NOMBRE DEL ARCHIVO:	
Declaración de Prácticas de Certificación del Prestador Cualificado de Servicios de Confianza Confirma S.A.	
CÓDIGO: DPC –CF	**VERSIÓN: 2.0**
UBICACIÓN FÍSICA: CONFIRMA S.A.	**FECHA: 22/08/2023**
CLASIFICACIÓN DE SEGURIDAD: Público	

CONTROL DE VERSIONES			
FECHA	**VERSIÓN**	**RESPONSABLES**	**MOTIVO DE CAMBIO**
14/04/2023	1.0	CONFIRMA S.A.	Primera Edición del Documento
22/08/2023	2.0	CONFIRMA S.A.	4.9.13 Circunstancias para la suspensión. 4.9.14 Quién puede solicitor la suspensión 4.9.15 Procedimiento para la solicitud de suspensión 4.9.16 Límites del periodo de suspensión

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/2023/01/Declaracion_de_practicas_de_certificacion_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 declara las Prácticas de Certificación de CONFIRMA S.A. que estipula el funcionamiento y operaciones como Prestador Cualificado de Servicios de Confianza (PCSC) en su carácter de Autoridad de Certificación Intermedia (ACI), miembros de la Infraestructura de la Clave Pública del Paraguay (ICPP)

La presente Declaración de Prácticas de Certificación de CONFIRMA S.A. fue elaborada teniendo en cuenta las recomendaciones establecidas de la (Request for comments) RFC 3647 "Internet X. 509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework", de IETF que contiene los principios y reglas relativos a la gestión de certificados digitales, las normas mínimas y básicas que debe cumplir El PCSC CONFIRMA S.A. para mantener actualizada toda la información de su DPC.

Este documento compone el conjunto normativo de la ICPP y en él se referencian otras reglamentaciones previstas en las demás normas del ICPP.

En la Declaración de Prácticas de Certificación se establecen las normas y condiciones generales de los servicios de certificación que presta el PCSC CONFIRMA S.A. relacionadas, con la gestión de los datos de los certificados, las condiciones aplicables a la solicitud, expedición, uso, hasta la extinción de vigencia de los certificados, las medidas de seguridad adoptadas tanto físicas, técnicas y organizacionales, y los

mecanismos de resguardo, auditorías y acceso a la información relacionada a la prestación de servicios de certificación.

Los certificados del PCSC CONFIRMA S.A. contienen la clave pública correspondiente a sus claves privadas y están relacionados a los servicios de:

1- Firma Electrónica Cualificada

La firma electrónica cualificada basada en certificados cualificados conforme a la legislación vigente tiene un efecto jurídico equivalente a una firma manuscrita.

Los certificados cualificados de firma electrónica y los certificados cualificados tributarios solo podrán emitirse a personas físicas, los certificados de sello electrónico están reservados para personas jurídicas. Los certificados citados deben ser emitidos por PCSC.

1.2. NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

El Documento es la "Declaración de Prácticas de Certificación de CONFIRMA S.A.

Nombre del Documento	Declaración de Prácticas de Certificación de CONFIRMA S.A.
Versión del Documento	2.0
Estado del Documento:	Versión Inicial
Fecha de Emisión	22/08/2023
OID	1.3.6.1.4.1.58404.1.2.1.1

Ubicación de la DPC	https://www.confirma.com.py/wp-content/uploads/2023/01/Declaracion_de_practicas_de_certificacion_Confirma_SA.pdf

1.3. PARTICIPANTES DE LA ICPP

1.3.1. AUTORIDADES CERTIFICADORAS (AC)

Dentro del marco de la ICPP, son entidades autorizadas a emitir certificados de clave pública:

AC Raíz-Py: En la cúspide de la Jerarquía de la Infraestructura de Clave Pública del Paraguay (ICPP), se ubica la AC Raíz-Py, la misma cuenta con un certificado auto emitido y aceptado por los terceros que confían en la ICPP. Emite certificados a los PCSC y a partir de allí, comienza la cadena de confianza. Los certificados digitales emitidos por la AC Raíz-Py se rigen y ajustan a su Declaración de Prácticas de Certificación (DPC), cuyo cumplimiento es de carácter obligatorio.
ACI; Es una entidad habilitada por la AA, encargada de operar una AC en el marco de la ICPP, debe contar con un certificado digital emitido por la AC Raíz- Py y solo podrá emitir certificados a personas físicas y jurídicas. En el ámbito de la ICPP un PCSC es considerado una ACI.

Un PCSC presta servicios de creación, verificación y validación de firmas electrónicas cualificadas y/ certificados relativos a estos servicios.

El PCSC además podrá ser habilitado para prestar servicios de generación o gestión de datos de creación de firma electrónica en los términos establecidos en el documento *DOC-ICPP-04 [1]* y *DOC-ICPP-07 [2]*.

Un PCSC habilitado para brindar servicios de generación o gestión de datos de creación de firma electrónica y/o datos de creación de sello electrónico en nombre del firmante o creador del sello, debe utilizar sistemas y productos fiables, incluidos canales de comunicación electrónicos seguros, aplicar procedimientos y mecanismos técnicos y organizativos adecuados para garantizar que el entorno sea confiable y que los datos de creación se utilicen bajo el control exclusivo del titular del certificado. Además, deben custodiar y proteger los datos de creación de firma frente a cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad.

Las claves privadas de los firmantes y/o de los creadores de sellos almacenadas en dispositivos estandarizados conforme lo establecido en el documento *DOC- ICPP-04 [1]*, y las firmas electrónicas cualificadas o los sellos electrónicos cualificados realizados con la clave privada del firmante y/o creador del sello son validas de conformidad a la Ley N° 6822/2021.

1.3.2. AUTORIDADES DE REGISTRO (AR)

Es la entidad responsable de la identificación y autenticación de titulares de certificados electrónicos. Las Autoridades de Registro (AR) llevan a cabo la identificación de los solicitantes de certificados conforme a las normas de esta DPC y el acuerdo suscrito con el PCSC CONFIRMA S.A.

Una AR interviene en el proceso de solicitud del certificado, en el proceso de revocación o en ambos.

La AR puede ser propia del PCSC o delegada a un tercero cuyo funcionamiento deberá ser autorizado por la AC Raíz-Py con la habilitación correspondiente.

Las ARs delegadas son autoridades de registro vinculadas a un PCSC mediante un acuerdo operacional.

El PCSC CONFIRMA S.A. mantiene publicado en el sitio web https://www.confirma.com.py/ las siguientes informaciones:

a) La lista de todas las ARs habilitadas;

b) Lista de las ARs que se han inhabilitado por el PCSC, indicando la fecha de la inhabilitación.

1.3.3. AUTORIDADES DE VALIDACIÓN (AV)

La AV puede ser una entidad del PCSC o delegada a un tercero cuyo funcionamiento deberá ser autorizado por la AC Raíz-Py con la habilitación correspondiente. Su función es suministrar información sobre la vigencia de los certificados que a su vez hayan sido registrados por una AR y certificados por el PCSC.

Las AVs delegadas son autoridades de validación vinculadas a un PCSC mediante un acuerdo operacional.

El PCSC mantiene publicada información referente a:

- Lista de todas las AVs habilitadas
- Lista de las AVs que se han inhabilitado por el PCSC, indicando la fecha de la inhabilitación.

1.3.4. TITULARES DEL CERTIFICADO

Toda persona física o jurídica podrá ser titular de los certificados emitidos por el PCSC CONFIRMA S.A. según corresponda a un certificado cualificado de firma electrónica, tributario o de sello electrónico cualificado respectivamente conforme a esta DPC.

1.3.5. PARTE USUARIA

Se entenderá por parte usuaria, toda persona física o jurídica que confía en el servicio de confianza. Es decir, confía en el contenido, validez y aplicabilidad del certificado electrónico y claves emitidas en el marco de la ICPP.

1.3.6. OTROS PARTICIPANTES

1.3.6.1. PRESTADORES DE SERVICIO DE SOPORTE (PSS)

Los PSS son entidades externas a las que recurre el PCSC o la AR para desempeñar actividades descritas en esta DPC o en una PC y se clasifican en tres categorías, conforme al tipo de actividades prestadas;

a) disponibilización de infraestructura física y lógica;

b) disponibilización de recursos humanos especializados; y

c) La disponibilidad de infraestructura física y lógica y de recursos humanos especializados.
El PCSC deberá mantener las informaciones arriba citadas siempre actualizadas.

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

El PCSC 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

Esta sección lista las aplicaciones para las que puede emplearse cada tipo de certificado, establece limitaciones a ciertas aplicaciones y prohíbe ciertas aplicaciones de los certificados.

1.4.1. USOS APROPIADOS DEL CERTIFICADO

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

https://www.confirma.com.py/wp-content/uploads/2023/01/PC_Politica_de_Certificacion_Confirma_SA.pdf

A continuación, se describen el uso apropiado del Certificado del PCSC CONFIRMA S.A.:

Certificado del PCSC CONFIRMA S.A. (Firma de Certificado a sus suscriptores. Firma de LCR de sus titulares de certificados.)

DESCRIPCION DE USO APROPIADO:

1- Firma de Certificado (Certificate Sig-ning).
2- Firma LCR (LCR Singning)
3- Firma LCR sin conexión (Off line LCR Singning)

1.4.2. USOS PROHIBIDOS DEL CERTIFICADO

Los certificados se emplean según su finalidad definida en la correspondiente PC, sin que puedan emplearse en otras funciones y con otras finalidades.

Del mismo modo, los certificados deben emplearse únicamente de acuerdo con la regulación aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

Se deben tener en cuenta los límites indicados en los diversos campos de los perfiles de certificados, disponibles en la web del PCSC CONFIRMA S.A. https://www.confirma.com.py/

El empleo de los certificados en operaciones que contravienen esta Declaración de Prácticas de Certificación, los documentos jurídicos vinculantes con cada certificado, o los contratos con las entidades de registro o con sus firmantes/suscriptores, tiene la consideración de uso indebido a los efectos legales oportunos, eximiéndose por tanto al PCSC CONFIRMA S.A. en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.

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 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. PROCEDIMIENTO DE APROBACIÓN DE LA DPC

Los procedimientos para la aprobación de DPC del PCSC son establecidos a criterio de AC Raíz-Py de la ICPP.

1.6. DEFINICIONES, SIGLAS Y ACRÓNIMOS

1.6.1. DEFINICIONES

- **Agente de registro:** persona responsable de la realización de las actividades inherentes a la AR. Realiza la identificación de los solicitantes en la solicitud de emisión/revocación de certificados de firma electrónica cualificada o sello electrónico cualificado.
- **Autenticación:** proceso técnico que permite determinar la identidad de la persona física o jurídica.
- **Autenticación electrónica:** un proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico.
- **Autoridad de Aplicación:** Ministerio de Industria y Comercio a través de la Dirección General de Comercio Electrónico, dependiente del Viceministerio de Comercio y Servicios.
- **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.
- **Autoridad de Certificación Raíz del Paraguay:** órgano técnico, cuya función principal es coordinar el funcionamiento de la ICPP. La AC Raíz-Py tiene los certificados de más alto nivel, posee un certificado autofirmado y es a partir de allí, donde comienza la cadena de confianza. Las funciones de la AC Raíz-Py son ejercidas por la AA.
- **Autoridad de Certificación Intermedia**: entidad cuyo certificado ha sido emitido por la AC Raíz-Py, es responsable de la emisión de certificados cualificados a personas físicas y jurídicas. Un Prestador

cualificado de Servicios de Confianza es considerado una Autoridad de Certificación Intermedia.

- **Autoridad de Registro:** entidad responsable de tramitar las distintas solicitudes inherentes a certificados cualificados, identificar al solicitante y remitir las solicitudes al PCSC. La AR puede ser propia del PCSC o delegada a un tercero.
- **Autoridad de Validación:** entidad responsable de suministrar información sobre la vigencia de los certificados que a su vez hayan sido registrados por una AR y certificados por la AC. La AV puede ser propia del PCSC o delegada a un tercero.
- **Gestión de datos de creación de firma o sello electrónico:** El PCSC podrá, en nombre del firmante o creador de sello gestionar los datos de creación de firma o sello electrónico a los que hayan prestado sus servicios, este servicio deberá ser provisto por un PCSC siempre y cuando cuente con la debida habilitación.
- **Cadena de certificación:** lista ordenada de certificados que contiene un certificado del firmante o creador de sello y certificados de la AC, que termina en un certificado raíz. El emisor del certificado del firmante o creador de sello es el titular del certificado del PCSC y a su vez, el emisor del certificado del PCSC es el titular del certificado de AC Raíz-Py. El firmante, creador de sello o la parte usuaria debe verificar la validez de los certificados en la cadena de certificación.
- **Certificado cualificado de firma electrónica:** un certificado de firma electrónica que ha sido expedido por un PCSC y que cumple los requisitos establecidos en el artículo 43 de la ley No 6822/2021.
- **Certificado cualificado de sello electrónico:** un certificado de sello electrónico que ha sido expedido por un PCSC y que cumple los requisitos establecidos en el artículo 53 de la ley No 6822/2021.

- **Certificado cualificado tributario:** certificado expedido por un Prestador Cualificado de Servicios de Confianza, el cual podrá ser utilizado para todos los fines convencionales ante el Sistema Marangatu, Sistema Integrado de Facturación Electrónica Nacional, otros Sistemas de Información administrados por la Subsecretaría de Estado de Tributación (SET) así como otros usos afines autorizados por la Autoridad de Aplicación.
- **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.
- **Cifrado asimétrico:** tipo de cifrado que utiliza un par de claves criptográficas diferentes (ejemplo: privado y público) y matemáticamente relacionadas.
- **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 que contiene información relativa al solicitante 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.
- **Claves criptográficas:** valor o código numérico que se utiliza con un algoritmo criptográfico para transformar, validar, autenticar, cifrar y descifrar datos.
- **Clave pública y privada:** la criptografía en la que se basa la 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.

- **Compromiso:** violación de la seguridad de un sistema a raíz de una posible divulgación no autorizada de información sensible.
- **Data center (Centro de Datos):** infraestructura compuesta por espacio físico para la instalación de equipos informáticos y de comunicación con adecuados sistemas de energía, aire acondicionado y seguridad. Es parte de una AC, constituye un recinto seguro que alberga, entre otras cosas, los módulos criptográficos de hardware, protege la infraestructura tecnológica y es el lugar donde se ejecutan servicios del ciclo de vida del certificado. La importancia del data center radica en la protección que brinda a la clave privada y asegura la confianza en los certificados electrónicos emitidos por la AC.
- **Datos de activación:** valores de los datos, distintos al par de claves, que son requeridos para operar los módulos criptográficos y que necesitan estar protegidos.
- **Declaración de Prácticas de Certificación:** 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.
- **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.
- **Dossier del titular del certificado:** conjunto formado por la verificación de los documentos de identificación utilizados para la

emisión, suspensión o revocación del certificado, solicitud de certificado, contrato de prestación de servicios, y por la solicitud de revocación, cuando sea el caso. Este dossier deberá estar en formato de archivo digital, en el cual se escanean los documentos en formato papel, si los hubiere y se firma la solicitud de certificado y contrato de prestación de servicios con la clave privada del titular, después de la autorización del AGR por medio de la firma de dichos documentos, siempre y cuando sea informado y aceptado su contenido por parte de su solicitante y firmada electrónicamente con un certificado cualificado después de la generación de las claves y anterior a la instalación del certificado correspondiente.

- **Emisor del certificado:** persona física o jurídica cuyo nombre aparece en el campo emisor de un certificado.
- **Emisión de certificado:** es la autorización de la emisión del certificado en el sistema del PCSC previa comprobación de la concordancia de los datos de solicitud del certificado con los contenidos en los documentos presentados.
- **Firma electrónica cualificada:** una firma electrónica que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica, la cual deberá estar vinculada al firmante de manera única, permitir la identificación del firmante, haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo y estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.
- **Firmante:** una persona física que crea una firma electrónica.

- **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.
- **Habilitación:** autorización que otorga el MIC, una vez cumplidos los requisitos y condiciones establecidos en la norma.
- **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.
- **Identificación del Solicitante de certificado:** comprende la etapa de la confirmación de la identidad de una persona física o jurídica, realizada a través de la presencia física del interesado o mediante otros medios que aporten una seguridad equivalente en términos de fiabilidad a la presencia física, conforme a los supuestos establecidos en la Ley y en base a los documentos de identificación previstos en la presente DPC.
- **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.

- **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.
- **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.
- **Lista de Confianza**: Lista publicada en el sitio web oficial de la AC Raíz - Py y que contiene información relativa a los Prestadores cualificados de servicios de confianza y a los servicios cualificados que éstos prestan conforme a la Ley No 6822/21.
- **Módulo criptográfico**: software o hardware criptográfico que genera y almacena claves criptográficas.
- **Módulo de Seguridad de Hardware:** dispositivo basado en un módulo criptográfico tipo hardware que genera, almacena y protege claves criptográficas.
- **Normas Internacionales:** requisitos de orden técnico y de uso internacional que deben observarse en la prestación de los servicios mencionados en la presente DPC.
- **Organismo de Evaluación de Conformidad:** organismo que desempeña actividades de evaluación de la conformidad a un prestador de servicios de confianza y de los servicios de confianza que este presta conforme a la Ley No 6822/2021.
- **Organismo de Supervisión:** organismo que concede y retira la cualificación a los prestadores de servicios de confianza y a los servicios de confianza que prestan además de las funciones establecidas en el artículo 17 de la Ley No 6822/2021.

- **Parte usuaria:** persona física o jurídica que confía en el servicio de confianza.
- **Perfil del certificado:** especificación del formato requerido para un tipo particular de certificado (incluyendo requisitos para el uso de los campos estándar y extensiones).
- **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.
- **Prestador Cualificado de Servicios de Confianza:** prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la habilitación.
- **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.
- **Prestador de Servicios de Soporte:** entidad externa vinculada a un PCSC mediante un acuerdo operacional a la que recurre la AC o la AR y autorizada por la AC Raíz-Py para desempeñar actividades descritas en la DPC o en una PC.
- **Registro de Auditoría:** registro cronológico de las actividades del sistema, el cual es suficiente para permitir la reconstrucción, revisión e inspección de la secuencia de los ambientes y de las actividades que rodean o que conducen a cada acontecimiento en la ruta de una transacción desde su inicio hasta la salida de los resultados finales.

- **Repositorio:** sitio principal de Internet confiable y accesible, mantenido por la AC con el fin de difundir su información pública.
- **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.
- **Servicio OCSP:** permite utilizar un protocolo estándar para realizar consultas en línea al servidor de la AC sobre el estado de un certificado.
- **Solicitante de Certificado:** persona física o jurídica que solicita la emisión de un certificado a una AC.
- **Solicitud de Firma de Certificado:** petición de certificado electrónico que se envía a la AC, mediante la información contenida en el CSR, la AC, puede emitir el certificado electrónico una vez realizadas las comprobaciones que correspondan.
- **Solicitud de certificado:** documento que se instrumenta mediante un formato autorizado de solicitud de certificado o como parte de documento específico denominado Contrato de Prestación de Servicios de Confianza, suscripto por el solicitante en nombre propio en el caso de certificados cualificados de firma electrónica para persona física, o bien en nombre del titular en el caso de certificados cualificados de sello electrónico para persona jurídica.
- **Solicitud de revocación**: documento que se instrumenta mediante un formato autorizado de solicitud para la revocación de un certificado.
- **Verificación y validación de firma o sello:** determinación y validación de que la firma o sello electrónico fue creado durante el periodo operacional de un certificado válido, por la clave privada correspondiente a la clave pública que se encuentra en el

certificado y que el mensaje no ha sido alterado desde que su creación.

- **X.500:** estándar desarrollado por la ITU que define las recomendaciones del directorio. Da lugar a la serie de recomendaciones siguientes: X.501, X.509, X.511, X.518, X.519, X.520, X.521, X.525.
- **X.509:** estándar desarrollado por la ITU, que define el formato electrónico básico para certificados electrónicos.

1.6.2. SIGLAS Y ACRÓNIMOS

Tabla Número 1 – Siglas y Acrónimos

Sigla / Acrónimo	Descripción
AA	Autoridad de Aplicación
AGD	Autoridad de Gestión de Datos
AGR	Agente de Registro
P	País (C por su sigla en inglés, Country)
AC	Autoridad de Certificación (CA por sus siglas en inglés, Certificate Authority)
ACI	Autoridad de Certificación Intermedia (CAI por sus siglas en inglés, Certificate Authority Intermediate)
AC Raíz-Py	Autoridad Certificadora Raíz del Paraguay
CI	Cédula de identidad civil
NC	Nombre Común (CN por sus siglas en inglés, Common Name)
PC	Políticas de Certificación (CP por sus siglas en inglés, Certificate Policy)
DPC	Declaración de Prácticas de Certificación (DPC por sus siglas en inglés, Certification Practice Statement)
LCR	Lista de certificados revocados (CRL por sus

	siglas en inglés, Certificate Revocation List)
CSR	Solicitud de firma de Certificado (CSR por sus siglas en inglés, certificate Signing Request)
DGCE	Dirección General de Comercio Electrónico dependiente del Viceministerio de Comercio y Servicios.
HSM	Módulo de Seguridad Criptográfico basado en Hardware (HSM por sus siglas en inglés, Hardware Security Module)
ISO	Organización Internacional para la Estandarización (ISO por sus siglas en inglés, International Organization for Standardization).
MIC	Ministerio de Industria y Comercio.
O	Organización (por su sigla en inglés, Organization)
OCSP	Servicio de validación de certificados en línea (OCSP por sus siglas en inglés, Online Certificate Status Protocol)
OID	Identificador de Objeto (OID por sus siglas en inglés, Object Identifier)
OU	Unidad Organizacional (OU por sus siglas en inglés, Organization Unit)
PAS	Pasaporte
PCN	Plan de Continuidad del Negocio
PKI	Infraestructura de Clave Pública (PKI por sus siglas en inglés, Public Key Infrastructure).
ICPP	Infraestructura de Clave Pública del Paraguay
OEC	Organismo de Evaluación de la Conformidad
PCSC	Prestador cualificado de servicios de confianza
PS	Política de Seguridad
PSS	Prestador de Servicios de Soporte
Py	Paraguay
AR	Autoridad de Registro (RA por sus siglas en inglés, Registration Authority).
RFC	Petición de Comentarios (RFC por sus siglas en inglés, Request For Comments)
RUC	Registro único del Contribuyente.

UPS	Sistemas de alimentación ininterrumpida (UPS por sus siglas en inglés, uninterruptible power supply)
URL	Localizador uniforme de recursos (URL por sus siglas en inglés, Uniform Resource Locator).
AV	Autoridad de validación (VA por sus siglas en inglés, Validation Authority).

2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO

2.1. REPOSITORIOS

El PCSC CONFIRMA S.A., es responsable de las funciones de repositorio

para su AC, las cuales son:

a) poner a disposición, inmediatamente después de su emisión, los certificados emitidos por el PCSC y su LCR/OCSP;

b) Estar disponible para consultas las 24 (veinticuatro) horas del día, los 7 (siete) días de la semana;

c) Implementar los recursos necesarios para la seguridad de los datos allí almacenados; y

d) proporcionar 2 (dos) repositorios, en infraestructuras de red segregada, para la distribución del LCR/OCSP.

El PCSC CONFIRMA S.A. aplica los recursos necesarios para garantizar la seguridad e integridad de los datos almacenados en él.

El PCSC CONFIRMA S.A. posee un repositorio público que se encuentra disponible en un 99,5% anual, durante 24 horas al día, 7 días a la semana.

Es un servicio Web de acceso libre y no contiene ninguna información de naturaleza confidencial.

Las informaciones del repositorio son publicadas en la página web:

https://www.confirma.com.py/ el acceso es vía HTTPS.

El PCSC CONFIRMA S.A proporciona 02 (dos) repositorios, en infraestructuras de red segregadas, para la distribución de LCR / OCSP.

2.2. PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

El repositorio del PCSC CONFIRMA S.A. está disponible durante 24 horas al día, 7 días a la semana. En caso de interrupción por causa de fuerza mayor, el servicio se deberá restablecer en un plazo no mayor a veinticuatro horas, garantizando la disponibilidad del servicio con un mínimo de 99,5% anual, un tiempo programado de inactividad máximo de 0,5% anual.

El PCSC CONFIRMA S.A. mantiene su repositorio en el sitio principal de internet el cual permite a las partes que confían verificar en línea la revocación de un certificado y cualquier otra información necesaria para validar el estado de este.

El PCSC CONFIRMA S.A. mantiene publicada en su repositorio público la versión actualizada de:

a) PC y DPC que implementan;
b) el certificado de la AC Raíz-Py;
c) su propio certificado;
d) la LCR;
e) certificados emitidos;
f) proforma del contrato de prestación de servicios de confianza;
g) las resoluciones que habilitan o revocan al PCSC:
h) leyes, decretos, reglamentos y resoluciones que rigen la actividad de la ICPP;
i) identificación, domicilio y medios de contacto;

j) una lista, actualizada periódicamente, que contiene las ARs propias y delegadas con las respectivas direcciones de sus instalaciones técnicas de operación, autorizadas por la AC Raíz-Py para funcionar;
k) acuerdos operacionales celebrados entre un PCSC y una AR delegada;
l) la lista actualizada de todas las ARs cuya habilitación fue revocada, con la indicación de la fecha de revocación.
m) la lista de todas las AVs habilitadas;
n) para cada AV, las direcciones de todas las instalaciones técnicas, autorizadas por la AC Raíz-Py para funcionar;
o) acuerdos operacionales celebrados entre un PCSC y una AV delegada;
p) la lista de todas las AVs cuya habilitación fue revocada, con la indicación de la fecha de revocación.
q) una lista, actualizada periódicamente de los PSS vinculados a un PCSC;

2.3. 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 en cuanto se encuentra disponible.

Los cambios en la Declaración de Prácticas de Certificación se rigen por lo establecido en la sección 1.5 de este documento.

La información de estado de revocación de certificados se publica de acuerdo con lo establecido en las secciones 4.9.9 y 4.9.10 de esta Declaración de Prácticas de Certificación.

2.4. CONTROLES DE ACCESO A LOS REPOSITORIOS

El PCSC CONFIRMA S.A. garantiza el acceso permanente, irrestricto y gratuito a la información publicada en su repositorio.

El PCSC CONFIRMA S.A. implementa medidas de seguridad lógicas y físicas para evitar que personas no autorizadas puedan añadir, borrar o modificar el contenido del repositorio.

El Servicio de Publicación de CONFIRMA S.A. cuenta con un sistema de seguridad que permite controlar de forma adecuada el acceso a la información.

Este sistema impide además que personas no autorizadas puedan añadir, modificar o borrar registros de este Servicio, este proceso protege la integridad y autenticidad de la información depositada, de modo tal que:

- Únicamente las personas autorizadas puedan hacer anotaciones y modificaciones.
- Puede comprobarse la autenticidad de la información.
- Los certificados sólo estarán disponibles para consulta si el suscriptor ha prestado formalmente su consentimiento en el correspondiente contrato de suscripción.
- Los servidores que almacenan la información del repositorio público del PCSC CONFIRMA S.A. se encuentran en el nivel 4 de seguridad física y requiere de un control de acceso con doble factor de autenticación.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

El PCSC CONFIRMA S.A. comprobará la identidad y/o atributos de las personas físicas y jurídicas antes de incluir estos atributos en un certificado en el marco de la ICPP. Se prohíbe a las personas físicas y jurídicas utilizar en sus certificados nombres que violen los derechos de propiedad intelectual de terceros. El PCSC CONFIRMA S.A. se reserva el derecho, sin responsabilidad ante ningún solicitante, de rechazar solicitudes.

Todo el proceso de identificación del titular del certificado es registrado y firmado electrónicamente por los ejecutantes. Dichos registros son realizados de tal manera que permitan la completa reconstrucción de los procesos realizados, para fines de auditoría.

Se mantiene un archivo con copias de todos los documentos utilizados para confirmar la identidad de una persona física o jurídica y anexar al dossier del Titular del Certificado. Dichas copias podrán conservarse en papel o en formato digital, sujeto a las condiciones definidas en el documento DOC-ICPP-05.

3.1 NOMBRES

3.1.1. TIPOS DE NOMBRES

Todos los certificados emitidos por el PCSC CONFIRMA S.A. contienen un nombre distintivo. Entre los tipos de nombres considerados está el D*istinguished name* según lo establecido en la ITU X.500, direcciones de correos electrónicos o direcciones de página web (URL).

3.1.2. NECESIDAD DE NOMBRES SIGNIFICATIVOS

Los certificados emitidos por el PCSC CONFIRMA S.A. requieren el uso de nombres significativos que permitan determinar de manera única la identidad de la persona u organización que posee el certificado al que se refieren, para identificar a los titulares de los certificados emitidos por CONFIRMA S.A. Este nombre significativo, corresponde al especificado en el documento de identificación presentado por el solicitante en el momento de registro.

3.1.3. ANONIMATO O SEUDÓNIMO DE LOS TITULARES DE CERTIFICADOS

El PCSC CONFIRMA S.A. no admite el uso de seudónimos en los certificados cualificados firma electrónica emitidos por un PCSC y autorizados por la AC Raíz-Py. El PCSC que consigne un seudónimo en un certificado electrónico cualificado deberá constatar la verdadera identidad del titular del certificado y conservar la documentación que la acredite, en el dossier de titular del certificado.

El PCSC CONFIRMA S.A. estará obligado a revelar la identidad cuando lo soliciten los órganos judiciales y otras autoridades públicas para el ejercicio de las funciones.

3.1.4. REGLAS PARA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRES

Los formatos de nombres se interpretarán de acuerdo con la ley del país de establecimiento del titular del certificado, en sus propios términos.

Está prohibido el uso de nombres en certificados que violen los derechos de propiedad intelectual de terceros.

3.1.4.1. CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA O CERTIFICADO CUALIFICADO TRIBUTARIO

La Cédula de Identidad civil es expedida por el Departamento de Identificaciones de la Policía Nacional, y debe cumplir el siguiente formato:

Tabla No 3 - CI Certificado Cualificado de Firma Electrónica o Certificado Cualificado Electrónico.

TIPO DE DOCUMENTO	PREFIJO	FORMATO	DESCRIPCIÓN
Cédula de identidad	CI	CI999999	Siglas CI seguido del número de cédula de identidad cilvil, el cual puede ser alfanumérico.

El Pasaporte es expedido por un órgano nacional competente y en el caso de extranjeros por un órgano de su país de origen, y debe cumplir el siguiente formato:

Tabla No 4 - PAS Certificado Cualificado de Firma Electrónica o Certificado Cualificado Tributario

TIPO DE DOCUMENTO	PREFIJO	FORMATO	DESCRIPCIÓN
Pasaporte	PAS	PASQ999999	Siglas PAS seguido del número de Pasaporte, el

			cual puede ser alfanumérico.

3.1.5 UNICIDAD DE NOMBRES

El "Distinguished Name" (DN), deberán ser únicos para cada titular del certificado, en el ámbito del PCSC CONFIRMA S.A. emitente. Números y letras adicionales podrán ser incluidos al nombre de cada entidad para asegurar la unicidad del campo.

3.1.6 PROCEDIMIENTO PARA RESOLVER DISPUTA DE NOMBRE

El PCSC CONFIRMA S.A.. se reserva el derecho de tomar todas las decisiones en caso de una disputa de nombres que surja de la igualdad de nombres entre varios solicitantes de certificados. Durante el proceso de verificación de identidad, corresponde al solicitante del certificado demostrar su derecho a usar un nombre específico.

3.1.7 RECONOCIMIENTO, AUTENTICACIÓN Y ROL DE LAS MARCAS REGISTRADAS

El PCSC CONFIRMA S.A. establece que los procesos de tratamiento, reconocimiento, autenticación y rol de marcas registradas serán ejecutados de acuerdo con la legislación vigente sobre la materia.

3.2 VALIDACIÓN DE IDENTIDAD

En el Siguiente apartado se detalla la forma, los procedimientos y los requisitos para la primera identificación y registro ante la ICPP de los titulares o responsables de certificados electrónicos, comprendiendo los siguientes procesos:

a) **Identificación y registro del titular del certificado:** identificación de la persona física o jurídica, titular del certificado, con base en los documentos de identificación mencionados en los ítems 3.2.2, 3.2.3, observando lo siguiente:

- Para certificados cualificados de firma electrónica cualificada: prueba de que la persona física que se presenta como titular del certificado, es realmente aquel cuyos datos aparecen en la documentación. Queda prohibido cualquier tipo de poder para tal fin.
- Para certificados cualificados tributarios: se procederá conforme a lo establecido en el ítem i. en el caso que el titular del certificado corresponda a una empresa unipersonal y conforme al ítem ii. en el caso de que el titular del certificado preste servicios en una organización.

b) **Emisión del certificado**: luego de cotejar los datos de la solicitud del certificado con los contenidos en los documentos y biometría presentados, en la etapa de identificación, se procede a la emisión del certificado en el sistema del PCSC. Se considera que la extensión ***Nombre Alternativo del Sujeto (Subject Alternative Name)*** está fuertemente relacionada con la clave pública contenida en el certificado, por lo que todas las partes de esta extensión deben verificarse y el solicitante del certificado debe demostrar que tiene los derechos sobre esta información ante la autoridad competente, o que está autorizado por el titular de la información para utilizarlos.

3.2.1 MÉTODO PARA PROBAR POSESIÓN DE LA CLAVE PRIVADA

En caso de que el par de claves sea generado por el solicitante del certificado, la posesión de la clave privada, correspondiente a la clave pública para la que solicita que se genere el certificado, quedará probada mediante el envío de la petición de certificado (CSR) en formato PKCS#10 u otras demostraciones criptográficas equivalentes, aprobadas por la Autoridad de Aplicación, en la cual se incluirá la clave pública firmada mediante la clave privada asociada.

3.2.2 AUTENTICACIÓN DE IDENTIDAD DE PERSONA JURÍDICA

3.2.2.1 DISPOSICIONES GENERALES

No Aplica

3.2.2.2 DOCUMENTOS REQUERIDOS PARA IDENTIFICAR UNA PERSONA JURÍDICA

No Aplica.

3.2.2.3 INFORMACIÓN CONTENIDA EN UN CERTIFICADO CUALIFICADO DE SELLO ELECTRONICO

No Aplica.

3.2.3 AUTENTICACIÓN DE IDENTIDAD DE PERSONA FÍSICA

En este ítem se definen los procedimientos utilizados por las ARs vinculadas al PCSC CONFIRMA S.A. para la identificación y el registro de una persona física en la ICPP. Esta confirmación deberá realizarse:

La confirmación de la identidad de la persona física responsable del certificado será verificada por el PCSC bien directamente o por medio de un tercero en los siguientes términos:

a) En presencia de la persona física; o,

b) Por medio de un certificado de una firma electrónica cualificada expedido de conformidad con el Art. 36 numeral 5, inc b) de la Ley Nro. 6822/2023.

3.2.3.1 PROCEDIMIENTO PARA LA IDENTIFICACIÓN DE UNA PERSONA

La identificación de la persona física solicitante del certificado debe realizarse de la siguiente manera: a) presentación de la siguiente documentación, en su versión oficial original, física o electrónica:

> i) cédula de Identidad civil o pasaporte, si es paraguayo ii) cédula de Identidad extranjero, si es extranjero domiciliado en Paraguay; o iii) pasaporte, si es extranjero no domiciliado en Paraguay.

Se considera documento de identidad al documento oficial, físico o electrónico, según la legislación específica, emitido por el Ministerio del Interior a través de la Policía Nacional.

Los documentos electrónicos deberán ser verificados a través de fuentes oficiales de organismos competentes. Dicha verificación formará parte del dossier del titular del certificado. En caso de una identificación positiva, se omite el requerimiento de verificación descritos en el siguiente párrafo:

Los documentos en papel, para los cuales no existan formas de verificación a través de fuentes oficiales competentes, deberán verificarse:

a) Por un AGR distinto del que realizó el paso de identificación;

b) Por la AR delegada o AR propia vinculada al PCSC;

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

La emisión de certificados a favor de los absolutamente incapaces y de los relativamente incapaces deberá observar las disposiciones de la ley vigente y las normas emitidas por la ICPP.

3.2.3.2 INFORMACIÓN CONTENIDA EN UN CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA

La información obligatoria contenida en los campos del certificado expedido por el PCSC CONFIRMA S.A. para una persona física debe coincidir exactamente con la información contenida en los siguientes documentos:

a) Nombre completo de la persona física titular del certificado según el documento de identidad; y

b) Número de cédula de identidad civil o número de pasaporte de la persona física, según documento de identidad.

Además, el titular del certificado, a su criterio y mediante una declaración expresa en el documento contrato de prestación de

servicios de confianza, puede solicitar llenar los campos con las siguientes informaciones:

c) El correo del titular del certificado;

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

e) El nombre de la unidad de la organización en el que presta servicio el titular del certificado;

f) El número de RUC de la organización en el que presta servicio el titular del certificado

g) El número de RUC del titular del certificado;

h) Posición o función asignada al titular del certificado en la organización en el que presta servicio; y

i) El título académico del titular del certificado.

Para ello, en el caso del correo electrónico se considerará suficiente la declaración expresa en la correspondiente solicitud. Dado el caso de incorporar otra información, la misma debe contar con respaldo documental en formato original o copia autenticada. Las copias de los mismos deben ser incluidas en el dossier de titular del certificado.

3.2.3.3 INFORMACIÓN CONTENIDA EN UN CERTIFICADO CUALIFICADO TRIBUTARIO

La información obligatoria contenida en los campos del certificado cualificado tributario expedido a una persona física debe coincidir

exactamente con la información contenida en los siguientes documentos:

a) Nombre completo de la persona física titular del certificado según el documento de identidad;

b) Número de cédula de identidad civil o número de pasaporte de la persona física, según documento de identidad;

c) Nombre de la organización en el que presta servicio el titular del certificado o razón social del titular del certificado en caso de tratarse de una organización unipersonal, según cédula tributaria; y

d) Número de RUC correspondiente a la organización en el que presta servicio el titular del certificado o el número de RUC del titular del certificado en caso de tratarse de una organización unipersonal, según cédula tributaria.

Además, el titular del certificado, a su criterio y mediante una declaración expresa en el documento contrato de prestación de servicios de confianza, puede solicitar llenar los campos con las siguientes informaciones:

e) El correo del titular del certificado;

f) El nombre de la unidad de la organización en el que presta servicio el titular del certificado;

g) Posición o función asignada al titular del certificado en la organización en el que presta servicio; y

h) El título académico del titular del certificado.

Para ello, en el caso del correo electrónico se considerará suficiente la declaración expresa en la correspondiente solicitud. Dado el caso de incorporar otra información, la misma debe contar con respaldo documental en formato original o copia autenticada. Las copias de los mismos deben ser incluidas en el dossier de titular del certificado.

3.2.4 INFORMACIÓN NO VERIFICADA DEL TITULAR DEL CERTIFICADO

No Aplica

3.2.5 VALIDACIÓN DE LA AUTORIDAD (CAPACIDAD DE HECHO)

La AR vinculada al PCSC CONFIRMA S.A. debe determinar si el solicitante es apto y cuenta con la capacidad de solicitar un certificado, ademas que no posea impedimentos legales. En el caso de Certificados Cualificados para firma electrónica, debe validar que el solicitante sea mayor de edad.

3.2.6 CRITERIOS PARA INTEROPERABILIDAD

Los servicios de confianza prestados por el prestador cualificado de servicios de confianza CONFIRMA S.A. establecidos fuera del país serán reconocidos como legalmente equivalentes a los servicios de confianza cualificados prestados en la República del Paraguay si los servicios de confianza son reconocidos en virtud de acuerdos de reconocimiento mutuo celebrado entre autoridades oficiales de cada país o con organizaciones internacionales de conformidad a la reglamentación correspondiente.

Los acuerdos a que se refiere el párrafo anterior garantizan, en particular, que:

a) Los prestadores de servicios de confianza establecidos fuera del país u organizaciones internacionales y los servicios de confianza que prestan, cumplen los requisitos aplicables a los PCSC establecidos en el Paraguay y a los servicios de confianza cualificados que prestan.

b) Los servicios de confianza cualificados prestados por PCSC establecidos en Paraguay son reconocidos como legalmente equivalentes a los servicios de confianza prestados por prestadores de servicios establecidos fuera del país u organizaciones internacionales con los que se celebran acuerdos.

3.2.7 PROCEDIMIENTOS COMPLEMENTARIOS

El PCSC CONFIRMA S.A. comprueba la identidad y/o atributos de las personas físicas y jurídicas antes de incluir estos atributos en un certificado en el marco de la ICPP. Se prohíbe a las personas físicas y jurídicas utilizar en sus certificados nombres que violen los derechos de propiedad intelectual de terceros. El PCSC CONFIRMA S.A. se reserva el derecho, sin responsabilidad ante ningún solicitante, de rechazar solicitudes.

El PCSC CONFIRMA S.A. mantiene actualizado sus políticas y procedimientos internos que son revisados periódicamnate para cumplir con los requisitos establecidos por la AC Raíz-Py.

Se debe mantener un archivo con copias de todos los documentos utilizados para confirmar la identidad de una persona física o jurídica. Tales copias podrán ser conservadas en papel o en formato electrónico, sujetas a las condiciones definidas en el documento *DOC-ICPP-05 (4)*.

3.2.8 PROCEDIMIENTOS ESPECÍFICOS

Para el caso de certificado emitido a Empleados del Servicio Exterior Paraguayo, en misión permanente en el exterior, si existen impedimentos para identificación conforme previsto en el ítem 3.2, es posible enviar la documentación por vía diplomática y realizar la identificación por otros medios seguros, que deben ser definidos y aprobados por la AC Raíz-Py.

3.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE NUEVAS CLAVES

El proceso del PCSC CONFIRMA S.A. para la emisión de nuevas claves antes de su expiración puede realizarse de acuerdo con una de las siguientes posibilidades:

- Adopción de los mismos requisitos y procedimientos requeridos en los puntos 3.2.2 o 3.2.3.
- Solicitud, por medio electrónico, firmada electrónicamente utilizando un certificado cualificado de la ICPP válido del solicitante, que sea del mismo nivel de seguridad o superior, limitado a una (1) ocurrencia sucesiva, cuando no hayan sido recolectados los datos biométricos del titular, admitiéndose esta hipótesis únicamente para los certificados cualificados de firma electrónica y a los certificados cualificados tributarios;

3.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN

Los procedimientos aceptados para la autenticación del solicitante de la revocación incluyen algunos de los siguientes medios:

- Mediante el código de revocación que es enviado al suscriptor en el correo consignado en el momento de la emisión del certificado.
- Presencialmente a través de los procesos de autenticación, de identidad (items 3.2.2 y 3.2.3)
- Cualquier otro medio establecido por el PCSC CONFIRMAS.A. y aprobado la AC Raiz-Py, que permita una identificación veraz y segura.

Solamente los agentes descriptos en el ítem 4.9.2 pueden solicitar la revocación del certificado.

Las solicitudes de revocación de certificados son registradas.

4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

4.1 SOLICITUD DEL CERTIFICADO

Los requisitos y procedimientos mínimos establecidos por el PCSC CONFIRMA S.A. y sus ARs vinculadas, para la solicitud de emisión de certificados. Estos requisitos y procedimientos comprenden, en detalles, todas las acciones necesarias tanto del solicitante como del PCSC y la AR vinculadas en el proceso de solicitud del certificado electrónico. La descripción también contempla lo siguiente:

a) La comprobación de los atributos de identificación que constan en el certificado, conforme al ítem 3.2;

b) El uso de un certificado cualificado de firma electrónica y autenticación biométrica del AGR responsable de gestionar las solicitudes de emisión, suspensión y revocación de certificados;.

c) Un *contrato de prestación de servicio de confianza* firmado con firma electrónica cualificada por el titular del certificado o por la persona responsable del certificado, en el caso de un certificado cualificado de sello electrónico.

Ante la imposibilidad técnica de firmar electrónicamente el contrato de prestación de servicio de confianza se aceptará la firma manuscrita del contrato por parte del titular o responsable en el caso de un certificado cualificado de sello electrónico. Para este caso será necesaria la verificación de la firma contra el documento de identificación y se adjuntará al dossier del titular del certificado, el documento manuscrito

digitalizado y firmado con firma electrónica cualificada por el AGR, conforme al *DOC-ICPP-05 [4]*.

El formato del documento contrato de prestación de servicio de confianza según sea el tipo de certificado a ser emitido será establecido por la AC Raiz-Py.

4.1.1 QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO

La presentación de la solicitud para el PCSC CONFIRMA S.A. será siempre a través de una AR.

A continuación, se detallan las personas que pueden presentar una solicitud de certificado, en el marco de la ICPP:

a) Para el caso de certificado cualificado de firma electrónica o tributario, puede ser solicitado por toda persona mayor de edad, sin distinción, con un documento de identidad válido y vigente, que será el sujeto a cuyo nombre se emita el certificado;

4.1.2 PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES

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

4.1.2.1. RESPONSABILIDADES Y OBLIGACIONES DEL PCSC

Responsabilidades:

a) El PCSC CONFIRMA S.A. responde por los daños y perjuicios que causen a cualquier persona en el ejercicio de su actividad cuando incumplan las obligaciones que les impone la normativa vigente;

b) El PCSC CONFIRMA S.A. asume toda la responsabilidad frente a terceros por la actuaciòn de las personas u otros prestadores en los que deleguen la ejecución de alguna/s de las funciones necesarias para prestaciòn de servicios de confianza, incluyendo las actuaciones de comprobaciòn de identidad previas a la expediciòn de un certificado cualificado.

Obligaciones

a) Publicar informaciòn veraz y acorde con las reglamentaciones vigentes, en su sitio principal Internet:

i) Su DPC, y las PC aprobadas que implementa;

ii) Las informaciones definidas en el ítem 2.2. de este documento y

iii) Las informaciones sobre la desvinculación de una AR.

b)No almacenar ni copiar, por sí o a través de un tercero, los datos de creación de firma, de sello de la persona física o jurídica a la que hayan emitido certificados, salvo en caso de su gestión en nombre del firmante o del creador del sello. En este caso, el PCSC tiene la obligación de:

c) Utilizar sistemas y productos fiables, incluidos canales de comunicación electrónica seguros;

d) Aplicar procedimientos y mecanismos técnicos y organizativos adecuados, para garantizar que el entorno sea fiable y se utilice bajo el control exclusivo del titular del certificado;

e) Custodiar y proteger los datos de creación de firma, de sello frente a cualquier alteración, destrucción o acceso no autorizado; y

f) Garantizar su continua disponibilidad.

g) Disponer de un servicio de consulta sobre el estado de validez y revocación de los certificados emitidos, accesible al público;

h) Conservar la información relativa a los servicios prestados por el término de diez años;

i) Constituir un seguro de responsabilidad civil por importe mínimo de quinientos salarios mínimos previstos para actividades diversas no especificadas, excepto si el prestador pertenece al sector público. Si presta más de un servicio de los previstos en la normativa, se añadirán ciento cincuenta salarios mínimos más por cada servicio. La citada garantía puede ser sustituida total o parcialmente por una garantía mediante aval bancario o seguro de caución, de manera que la suma de las cantidades aseguradas sea coherente con lo dispuesto en el párrafo anterior;

j) Informar a la parte usuaria y los titulares de certificados sobre las garantías, cobertura, condiciones y limitaciones establecidas en la póliza de seguro de responsabilidad civil contraída en los términos indicado en el inciso e);

k) En el caso de cese de sus operaciones, comunicar a los que preste sus servicios y al organismo de supervisión con una antelación mínima de dos meses el cese efectivo de la actividad. El plan de cese del PCSC puede incluir la transferencia de clientes a otro prestador cualificado, una vez acreditada la ausencia de oposición de los mismos;

l) Comunicar al organismo de supervisión cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, debe comunicar, en cuanto tenga conocimiento de ello, la apertura de cualquier proceso concursal que se siga contra él;

m) Asegurarse de que el titular del certificado puede controlar el acceso y uso de los datos de creación de firma o sello correspondientes a los de verificación que consten en el certificado, antes de la expedición de un certificado cualificado;

n) Enviar el informe de evaluación de la conformidad a la AC Raíz-Py en el plazo de tres días hábiles tras su recepción. El incumplimiento de esta obligación conlleva la suspensión de la cualificación al prestador y al servicio que éste presta, y su eliminación de la lista de confianza;

o) Notificar, en un plazo de veinticuatro horas tras tener conocimiento de ellas, a la AC Raíz-Py de las violaciones de seguridad que sufran, entendiéndose como violación de seguridad a un evento que afecta de manera crítica la confidencialidad, integridad y/o disponibilidad de los activos de información y tenga un impacto significativo en el servicio de confianza prestado o en los datos personales correspondientes;

p) Gestionar los incidentes de seguridad que les afecten, debiendo prever los mecanismos adecuados para su prevención, detección, análisis y resolución;

q) Ampliar tras la resolución del incidente, la información suministrada en la notificación inicial con arreglo a las directrices que pueda establecer AC Raíz-Py;

r) Facilitar a la AC Raíz-Py toda la información y colaboración precisas para el ejercicio de sus funciones. En particular, deben permitir a sus agentes o al personal inspector el acceso a sus instalaciones y la consulta de cualquier documentación relevante para la inspección de que se trate conforme al servicio que se preste. En sus inspecciones podrán ir acompañados de expertos o peritos en las materias sobre las que versen aquéllas; .

s) Adoptar las medidas técnicas y organizativas adecuadas para gestionar los riesgos para la seguridad de los servicios de confianza que prestan. Habida cuenta de los últimos avances tecnológicos, dichas medidas garantizan un nivel de seguridad proporcional al grado de riesgo. En particular, se adoptarán medidas para evitar y reducir al mínimo el impacto de los incidentes de seguridad e informar a los interesados de los efectos negativos de cualquiera de tales incidentes.

t) Notificar al *organismo de supervisión* y al *centro de respuestas a incidentes Cibernéticos* del Ministerio de Tecnologías de la Información y Comunicación (MITIC), sin demoras indebidas, pero en cualquier caso en un plazo de veinticuatro horas tras tener conocimiento sobre cualquier violación de la seguridad que tenga un impacto significativo en el servicio de confianza prestado o en los datos personales correspondientes.

Cuando la violación de seguridad pueda atentar contra una persona física o jurídica a la que se ha prestado el servicio de confianza, se deberá notificar también a la persona física o jurídica, sin demora indebida, la violación de seguridad. El organismo de supervisión notificado informará al público o exigirá al prestador de servicios de confianza que lo haga, en caso de considerar que la divulgación de la violación de seguridad reviste interés público.

u) Informar al organismo de supervisión de cualquier cambio en la prestación de servicios de confianza cualificados, y de su intención de cesar tales actividades.

v) Contar con personal y, si procede, con subcontratistas, que posean los conocimientos especializados, la fiabilidad, la experiencia y las cualificaciones necesarios y hayan recibido la formación adecuada en materia de seguridad y normas de protección de datos personales y que apliquen procedimientos administrativos y de gestión que correspondan a normas internacionales.

v) Con respecto al riesgo de la responsabilidad por daños, mantener recursos financieros suficientes u obtener pólizas de seguros de responsabilidad adecuadas.

w) Antes de entrar en una relación contractual, informar, de manera clara y comprensible, a cualquier persona que desee utilizar un servicio de confianza cualificado acerca de las condiciones precisas relativas a la utilización de dicho servicio, incluidas las limitaciones de su utilización.

x) Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad y la fiabilidad técnicas de los procesos que sustentan.

y) Utilizar sistemas fiables para almacenar los datos que se les faciliten de forma verificable, de modo que:

i) Estén a disposición del público para su recuperación sólo cuando se haya obtenido el consentimiento de la persona a la que corresponden los datos.

ii) Solo personas autorizadas puedan hacer anotaciones y modificaciones en los datos almacenados.

iii) Pueda comprobarse la autenticidad de los datos.

z) Tomar medidas adecuadas contra la falsificación y el robo de datos.

aa) Registrar y mantener accesible durante un período de tiempo definido por la AC Raíz-Py, incluso cuando hayan cesado las actividades del PCSC, toda la información pertinente referente a los datos expedidos y recibidos por el PCSC, en particular al objeto de que sirvan de prueba en los procedimientos legales y para garantizar la continuidad del servicio. Esta actividad de registro podrá realizarse por medios electrónicos.

bb) Contar con un plan de cese actualizado para garantizar la continuidad del servicio,

cc) Garantizar un tratamiento lícito de los datos personales.

dd) Mantener actualizada una base de datos de certificados.

ee) Cuando los PCSC revocan un certificado, deberán registrar su revocación en su base de datos de certificados y publicar el estado de revocación del certificado oportunamente y, en todo caso, en un plazo de veinticuatro horas después de la recepción de la solicitud.

ff) Recolectar los datos personales directamente de la persona a quien esos datos se refieran. La recolección y procesamiento en general de los datos personales se realizarán solo en la medida en que los mismos sean necesarios para la prestación del servicio de confianza. Los datos personales no pueden ser procesados para otro fin distinto al acordado, sin el consentimiento expreso del titular de los datos.

gg) Constatar la verdadera identidad del firmante o titular del certificado y conservar la documentación que la acredite en caso de expedir certificados que consignen seudónimos.
hh) Revelar la verdadera identidad del firmante o titular del certificado en caso de expedir certificados que consignen seudónimos, cuando lo soliciten los órganos judiciales y otras autoridades públicas para el ejercicio de las funciones.

ii) Proporcionar a cualquier parte usuaria información sobre el estado de validez o revocación de los certificados cualificados expedidos por ellos. Esta información debe estar disponible al menos por cada certificado en cualquier momento y con posterioridad al período de validez del certificado en una forma automatizada que sea fiable, gratuita y eficiente.

jj) Operar de acuerdo a su DPC y PC que implementan;

kk) Generar y gestionar sus pares de claves criptográficas;

ll) Asegurar la protección de sus claves privadas;
mm) Distribuir su propio certificado;

nn) Emitir, expedir y distribuir los certificados de los usuarios finales;
oo) Informar la emisión del certificado al respectivo solicitante;
pp) Revocar o suspender los certificados por él emitidos, de acuerdo con lo establecido en la PC correspondiente y en la DPC;
mm) emitir, gestionar y publicar sus LCRs y disponibilizar la consulta online del estado de los certificados emitidos (OCSP-On-line Certificate Status Protocol);
qq) Utilizar un protocolo de comunicación seguro cuando se preste servicios a través de la web a los solicitantes o usuarios de certificados electrónicos;
rr) Identificar y registrar todas las acciones ejecutadas, conformes a las normas, prácticas y reglas establecidas por AC Raíz-Py;
ss) Adoptar las medidas de seguridad y de control previstas en la DPC, PC que se implementan, con sujeción a las normas, criterios, prácticas y procedimientos establecidos por la AC Raíz-Py.
tt) Mantener el cumplimiento de sus procesos, procedimientos y actividades con las normas, prácticas y reglas establecidos por AC Raíz-Py, y la normativa vigente;
uu) Mantener y garantizar la integridad, confidencialidad y seguridad de la información por él tratado;
ss) Mantener y anualmente realizar prueba de su PCN;
vv) Informar a la AC Raíz-Py, mensualmente, la cantidad de certificados electrónicos emitidos y revocados;
ww) No emitir el certificado con una fecha de caducidad que se extienda más allá de la fecha de vencimiento de su propio certificado.
xx) Someterse a una auditoría al menos una vez cada veinte y cuatro

meses, corriendo con los gastos que ello genere, por un OEC debidamente acreditado, y remitir el informe de evaluación de la conformidad correspondiente al organismo de supervisión en el plazo de tres días hábiles tras su recepción;

yy) Someterse a auditoría o evaluación de conformidad, corriendo con los gastos que ello genere, en cualquier momento, solicitada por el organismo de supervisión; y

zz) Asegurarse de que todas las aprobaciones de solicitudes de certificados sean realizadas por un AGR y en una estación de trabajo declarada.

aa) Cumplir con las demás disposiciones reglamentadas por la AC Raíz-Py para asegurar que el PCSC se ajusta a la normativa vigente.

4.1.2.2. RESPONSABILIDADES Y OBLIGACIONES DE LA AR

Responsabilidades

La AR será responsable de los daños que ocasione.

Obligaciones

A continuación se detallan las Obligaciones de las AR vinculadas al PCSC CONFIRMA S.A. las cuales son:

a) Recibir las solicitudes de emisión y revocación de los certificados;

b) Confirmar la identidad del solicitante y validar la solicitud;

c) Remitir la solicitud de emisión, suspensión revocación del certificado al PCSC responsable, por medio de acceso remoto al ambiente de la AR alojado en las instalaciones del PCSC, utilizando un protocolo de comunicación seguro, conforme al patrón definido en el documento *DOC-ICPP-05 [4]*;

d) Informar a los respectivos titulares la emisión o revocación de sus certificados;

e) Mantener el cumplimiento de sus procesos, procedimientos y actividades con las normas, criterios, prácticas y reglas establecidas por el PCSC vinculado, la AC Raíz-Py y en especial con lo contenido en el documento *DOC-ICPP-05 [4]*;

f) Mantener y anualmente realizar prueba de su PCN;

g) Proceder a la comprobación de las firmas y de la validez de los documentos presentados en la forma de los ítems 3.2.2 y 3.2.3

h) Divulgar sus prácticas, relacionadas con la cadena del PCSC a la que se vincula, de acuerdo a los principios y criterios establecidas por la AC Raiz-Py para las AR.

4.2 PROCESAMIENTO DE LA SOLICITUD DEL CERTIFICADO

4.2.1 EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

El PCSC CONFIRMA S.A. y las ARs vinculadas realizan funciones de identificación y autenticación conforme a lo descrito en el ítem 3 de la presente DPC.

4.2.2 APROBACIÓN O RECHAZO DE LAS SOLICITUDES DE CERTIFICADO

El PCSC CONFIRMA S.A. y las AR vinculadas, con la debida justificación formal, aceptaran o rechazaran solicitudes de certificados de los solicitantes de acuerdo con los procedimientos descriptos en esta DPC y la normativa vigente.

4.2.3 TIEMPO PARA PROCESAR SOLICITUDES DE CERTIFICADO

Las solicitudes de certificados del PCSC CONFIRMA S.A. se atienden por orden de llegada, en un plazo razonable, cumpliendo con los procedimientos determinados por la AC Raíz-Py

No se cuenta con un tiempo máximo para procesar las solicitudes en el marco de la ICPP.

4.3 EMISIÓN DEL CERTIFICADO

Un certificado emitido por el PCSC CONFIRMA S.A. será considerado como válido a partir del momento de su emisión.

4.3.1 ACCIONES DEL PCSC DURANTE LA EMISIÓN DE LOS CERTIFICADOS

La emisión del certificado depende del correcto llenado del **FORMULARIO DE SOLICITUD DE CERTIFICADO**, de la firma del **CONTRATO DE PRESTACIÓN DE SERVICIOS DE CONFIANZA** y de la recepción de otros documentos requeridos de acuerdo con las especificaciones para cada tipo de certificado. Después del proceso de validación de la información

proporcionada por el solicitante, se emite el certificado y el Titular es notificado de la emisión y del método para retirar el certificado.

El certificado se considera válido desde el momento de su emisión.

4.3.2 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO POR PARTE DEL PCSC SOBRE LA EMISIÓN DEL CERTIFICADO

Se notificará al Titular sobre la emisión del certificado y el método para retirar el certificado. El envío de la notificación se realiza al correo electrónico consignado por éste en el Formulario de solicitud de Certificado.

La PC de CONFIRMA S.A. podrá establecer otro procedimientO de notificación mediante el cual se le informará al solicitante de la emisión de su certificado.

4.4 ACEPTACIÓN DEL CERTIFICADO

4.4.1 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE CERTIFICADO

El titular del certificado o la persona física responsable verifica la información contenida en el certificado y la acepta si la información es completa, correcta y verdadera. De lo contrario, el titular del certificado no puede usar el certificado y debe solicitar inmediatamente su revocación. Al aceptar el certificado, el titular del certificado:

a) está de acuerdo con las responsabilidades, obligaciones y deberes estipuladas en esta DPC y la PC correspondiente;

b) asegura que, con su conocimiento, ninguna persona no autorizada tuvo acceso a la clave privada asociada con el certificado;

c) afirma que todas las informaciones contenidas en el certificado, proporcionada en la solicitud, es verdadera y se reproduce en el certificado de manera correcta y completa.

La aceptación del certificado emitido y su contenido es declarada por el titular de este expresamente con la firma del Contrato de prestación de servicios de confianza. En caso de los certificados emitidos para sello electrónico, la declaración expresa deberá ser de la persona física responsable de ese certificado.

El Contrato de prestación de servicios de confianza de CONFIRMA S.A. contiene información relativa al solicitante 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.

4.4.2 PUBLICACIÓN DEL CERTIFICADO POR EL PCSC

El certificado del PCSC CONFIRMA S.A.. y los certificados emitidos a usuarios finales, serán publicados de acuerdo con el punto 2.2 de esta DPC.

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

No se definen entidades externas que necesiten o requieran ser notificados respecto a los certificados emitidos por el PCSC CONFIRMA S.A.

4.5 USO DEL PAR DE CLAVES Y DEL CERTIFICADO

El titular o responsable de un certificado debe usar el par de claves y el certificado correspondiente de acuerdo a la DPC y las PCs que implementa el PCSC CONFIRMA S.A.establecidas de acuerdo con este documento y con el documento *DOC-ICPP-04 [1]*.

4.5.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL TITULAR O RESPONSABLE

El PCSC CONFIRMA S.A. utiliza su clave privada y garantiza la protección de esa clave cumpliendo con lo indicado en su correspondiente DPC.

Obligaciones del Titular del Certificado:

A continuación se detallan las obligaciones de los titulares de certificados emitidos por el PCSC CONFIRMA S.A. contenidas en el contrato de prestación de servicios de confianza referidos en el ítem 4.1 y debe incluir al menos los ítem más abajo:

a) proporcionar al PCSC información veraz, completa y exacta para la prestación del servicio de confianza, en particular, sobre los datos que deban constar en el certificado electrónico o que sean necesarios para su expedición o para la extinción o suspensión de su vigencia;

b) comunicar sin demora al PCSC de cualquier modificación de las circunstancias que incidan en la prestación del servicio de confianza, en particular, aquellas reflejadas en el certificado electrónico;

c) conservar adecuadamente sus datos de creación de firma o sello, asegurar su confidencialidad y proteger de todo acceso o revelación de éstos o, en su caso, de los medios que den acceso a ellos;

d) solicitar la suspensión o revocación del certificado electrónico en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma o sello o, en su caso, de los medios que den acceso a ellos.

e) no utilizar los datos de creación de firma o sello cuando haya expirado el período de validez del certificado electrónico o el PCSC le notifique la extinción o suspensión de su vigencia.

f) utilizar sus certificados y claves privadas de forma adecuada, según lo previsto en la PC correspondiente;

g) conocer sus derechos y obligaciones, contemplados en la DPC y la PC correspondiente y demás documentos aplicables de la ICPP; y

h) informar al PCSC emisor de cualquier compromiso de su clave privada y solicitar la revocación inmediata del certificado correspondiente.

En el caso de un certificado emitido a una persona jurídica, estas obligaciones se aplican a la persona física responsable del certificado.

4.5.2 USO DE LA CLAVE PÚBLICA Y DEL CERTIFICADO POR LA PARTE USUARIA

Conforme a lo estipulado en el ítem 9.6.4 de esta DPC.

4.6 RENOVACIÓN DEL CERTIFICADO

Conforme a lo estipulado en el ítem 3.3 de esta DPC.

4.6.1 CIRCUNSTANCIAS PARA RENOVACIÓN DE CERTIFICADO

Conforme a lo estipulado en el ítem 3. 3 de esta DPC.

4.6.2 QUIÉN PUEDE SOLICITAR RENOVACIÓN

Conforme a lo estipulado en el ítem 4.1.1 de esta DPC.

4.6.3 PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN DE CERTIFICADO

Conforme a lo estipulado en el ítem 4.2 de esta DPC.

4.6.4 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO SOBRE LA EMISIÓN DE UN NUEVO CERTIFICADO.

Conforme a lo estipulado en el ítem 4.3.2 de esta DPC.

4.6.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UNA CERTIFICADO RENOVADO

Conforme a lo estipulado en el ítem 4.4.1 de esta DPC.

4.6.6 PUBLICACIÓN POR EL PCSC DEL CERTIFICADO RENOVADO

Conforme a lo estipulado en el ítem 4.4.2 de esta DPC.

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

Conforme a lo estipulado en el ítem 4.4.3 de esta DPC.

4.7 RE – EMISIÓN DE CLAVES DE CERTIFICADO (RE – KEY)

Este ítem no aplica.

4.7.1 CIRCUNSTANCIAS PARA RE – EMISIÓN DE CLAVES DE CERTIFICADO

Este ítem no aplica.

4.7.2 QUIÉN PUEDE SOLICITAR LA CERTIFICACIÓN DE UNA CLAVE PÚBLICA

Este ítem no aplica.

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

Este ítem no aplica.

4.7.4 NOTIFICACIÓN AL TITULAR DEL CERTIFICADO SOBRE LA RE – EMISIÓN DE UN NUEVO CERTIFICADO

Este ítem no aplica.

4.7.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RE – EMITIDO

Este ítem no aplica.

4.7.6 PUBLICACIÓN POR EL PCSC DE LOS CERTIFICADOS RE – EMITIDOS

Este ítem no aplica.

4.7.7 NOTIFICACIÓN POR EL PCSC DE LA RE – EMISIÓN DE UN CERTIFICADO A OTRAS ENTIDADES

Este Ítem no aplica.

4.8 MODIFICACIÓN DE CERTIFICADOS

Este ítem no aplica.

4.8.1 CIRCUNSTANCIAS PARA MODIFICACIÓN DEL CERTIFICADO

Este ítem no aplica.

4.8.2 QUIÉN PUEDE SOLICITAR MODIFICACIÓN DEL CERTIFICADO

Este ítem no aplica.

4.8.3 PROCESAMIENTO DE SOLICITUDES DE MODIFICACIÓN DEL CERTIFICADO

Este ítem no aplica.

4.8.4 NOTIFICACIÓN AL TITULAR DE LA EMISIÓN DE UN NUEVO CERTIFICADO

Este ítem no aplica.

4.8.5 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO

Este ítem no aplica.

4.8.6 PUBLICACIÓN POR EL PCSC DE LOS CERTIFICADOS MODIFICADOS

Este ítem no aplica.

4.8.7 NOTIFICACIÓN POR EL PCSC DE UNA EMISIÓN DE CERTIFICADOS A OTRAS ENTIDADES

Este ítem no aplica.

4.9 REVOCACIÓN Y SUSPENSIÓN

La revocación de un certificado supone la pérdida de validez definitiva del mismo, y es irreversible.

La suspensión de un certificado supone la pérdida de validez temporal del mismo, y es reversible. Sólo los certificados de entidad final podrán ser suspendidos.

4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN

Un certificado deberá obligatoriamente ser revocado en las siguientes circunstancias:

a) Solicitud formulada por el firmante, la persona física titular o jurídica representada por un tercero autorizado, el creador del sello.

b) Violación o puesta en peligro del secreto de los datos de creación de firma o de sello, o de CONFIRMA S.A., o utilización indebida de dichos datos por un tercero.

c) Resolución judicial o administrativa competente que lo ordene.

d) Fallecimiento del firmante; incapacidad sobrevenida, total o parcial, del firmante y extinción de la personalidad jurídica o disolución del creador del sello.

e) Cese en la actividad del CONFIRMA S.A. salvo que la gestión de los certificados electrónicos expedidos por aquél sea transferida a otro prestador de servicios de confianza.

f) Descubrimiento de la falsedad o inexactitud de los datos aportados para la expedición del certificado y que consten en él, o alteración posterior de las circunstancias verificadas para la expedición del certificado.

g) Cuando se incumpla con el proceso de autenticación y validación del solicitante.

h) Cuando el solicitante no este de acuerdo con el Contrato de Prestación de Servicios de Confianza y no lo suscriba

i) Impago de tarifa por parte del suscripto (ítem 9.1)

En su caso, y de manera previa o simultánea a la indicación de revocación de un certificado electrónico cualificado en el servicio de consulta sobre el estado de validez o revocación de los certificados por él expedidos, CONFIRMA S.A.. informará al firmante acerca de esta circunstancia, especificando los motivos, la fecha y la hora en que el certificado quedará sin efecto.

El PCSC CONFIRMA S.A. revocara, en un plazo definido en el ítem 4.9.3, el certificado de titular del certificado que incumpla con las políticas, estándares, prácticas y reglas establecidas en el marco de la ICPP.

La AC Raíz-Py podrá determinar la revocación del certificado del PCSC CONFIRMA S.A.., si el mismo incumpliese con la legislación vigente o las políticas, estándares, prácticas y reglas establecidas en el marco de la ICPP.

4.9.2 QUIÉN PUEDE SOLICITAR LA REVOCACIÓN

La revocación de los certificados emitidos por el PCSC CONFIRMA S.A. solo podrá realizarse:

a) Por solicitud del firmante, la persona física o jurídica representada por éste, un tercero autorizado o el creador del sello;

b) Resolución judicial o administrativa competente que lo ordene.

c) Por solicitud de la empresa u organización, cuando en el certificado se detalla el cargo o función que ocupa en la organización y es proporcionado por la misma al titular, por ser éste, su empleado o funcionario;

d) Por el PCSC emitente;

e) Por una AR vinculada al PCSC emitente;

4.9.3. PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACIÓN

Se requiere una solicitud de revocación para que la AR responsable inicie el proceso de revocación. Quienes están autorizados a solicitar la revocación, conforme al ítem 4.9.2, pueden, fácilmente y en cualquier tiempo, solicitar la revocación de sus respectivos certificados.

Las instrucciones para solicitar la revocación del certificado se encuentran en el sitio web puesto a disposición por el PCSC CONFIRMA S.A. o por una AR vinculada.

La revocación se lleva a cabo a través de un formulario en línea que contiene el motivo de la solicitud de revocación al proporcionar datos y el PIN de revocación entregado al Titular del Certificado o el responsable en el correo electrónico consignado en el formulario de Solicitud del Certificado.

Como directrices generales, se establece lo siguiente:
a) El solicitante de revocación de un certificado será identificado

b) Las solicitudes de revocación, así como las acciones resultantes de ellas serán registradas y almacenadas;

c) Se documentarán las razones de la revocación de un certificado; y

d) La revocación de un certificado terminará con la generación y publicación de una LCR que contenga los datos del certificado revocado y, en el caso de la utilización de consulta OCSP, con la actualización del estado del certificado en la base de datos del PCSC CONFIRMA S.A.

CONFIRMA S.A. registra su revocación en su base de datos de certificados y publicar el estado del certificado oportunamente y, en todo caso, en un plazo de veinticuatro (24) horas después de la recepción de la solicitud. La revocación será efectiva inmediatamente después de su publicación.

CONFIRMA S.A. responde plenamente por todos los daños causados por el uso de un certificado en el período comprendido entre la solicitud de su revocación y la emisión de la LCR correspondiente.

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

4.9.4. PERIODO DE GRACIA PARA SOLICITUD DE REVOCACIÓN

La solicitud de revocación será inmediata cuando se configuren las circunstancias definidas en el ítem 4.9.1.

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

En el caso de una solicitud formalmente constituida, de acuerdo con las reglas de la ICPP, el PCSC CONFIRMA S.A. procesara la revocación inmediatamente después de analizar la solicitud.

4.9.6. REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN PARA LAS PARTES USUARIAS

Las partes que confían deben comprobar el estado de aquellos certificados en los cuales desean confiar.

Un método por el cual se puede verificar el estado de los certificados es consultando el estado del certificado mediante el servicio de: OCSP o LCR más reciente, proveído por el PCSC CONFIRMA S.A.

Antes de confiar en un certificado, las partes usuarias deben confirmar la validez de cada certificado en la cadena de certificación de acuerdo con los estándares IETF PKIX, incluida la verificación de la validez del certificado, encadenando el nombre del emisor y el titular del certificado, restricciones de uso de claves y políticas de certificación y estado de revocación por medio de la LCR o respuestas OCSP identificadas en cada certificado en la cadena de certificación.

Las Listas de Certificados Revocados se publican en el repositorio público de la Entidad de Certificación, así como en las siguientes direcciones web, indicadas dentro de los certificados:
http://crl1.confirma.com.py/public/pki/crl/confirma.crl

El estado de la vigencia de los certificados también se puede comprobar por medio del protocolo OCSP.
http://ocsp1.confirma.com.py/public/pki/ocsp/

4.9.7. FRECUENCIA DE EMISIÓN DEL LCR

El PCSC CONFIRMA S.A. Publicará una nueva LCR en su repositorio en el momento en que se produzca una revocación. En cualquier caso, publicará una nueva LCR en su repositorio a intervalos no superiores a 12 horas, aunque no se haya revocado ningún certificado desde la última publicación.

La LCR mantiene publicado obligatoriamente:

- El certificado revocado hasta que expire, y
- El certificado suspendido, mientras permanezca tal condición.

La LCR mantiene obligatoriamente el certificado revocado o suspendido hasta que expira.

4.9.8. LATENCIA MÁXIMA PARA LCR

El tiempo máximo entre la generación de una LCR y su correspondiente publicación en el repositorio es de 1 hora.

4.9.9. DISPONIBILIDAD PARA REVOCACIÓN/VERIFICACIÓN DE ESTADO EN LÍNEA

Los recursos disponibles para la revocación/verificación en línea son:

Verificación:

a) Consultando la LCR o Delta-LCR más reciente emitida por el PCSC CONFIRMA S.A. que estará disponible en su sitio principal de internet.

b) Mediante la consulta de certificados en línea, disponible en la pagina web de CONFIRMA S.A.

Revocación:

a)Mediante el portal de revocación en línea, disponible en la pagina web de CONFIRMA S.A.

Todo certificado debe tener su validez verificada, en la respectiva LCR o consulta de certificados en línea, antes de ser utilizado.

Además, debe confirmarse la autenticidad de la LCR mediante la verificación de la firma del PCSC emisor y del período de validez de la LCR.

4.9.10. REQUISITOS DE VERIFICACIÓN DE REVOCACIÓN EN LÍNEA

Resulta obligatorio que la parte que confía debe consultar el estado de los certificados antes de confiar en estos, utilizando los mecanismos de verificación descriptos en el ítem anterior.

4.9.11. OTRAS FORMAS DE ADVERTENCIAS DE REVOCACIÓN DISPONIBLES

Sin Estipulaciones.

4.9.12. REQUERIMIENTOS ESPECIALES POR COMPROMISO DE CLAVE PRIVADA

a) En caso de compromiso de claves del PCSC CONFIRMA S.A., será notificado, en la medida posible, a todos los participantes de la ICPP, en especial a:

i. Todos los titulares de certificados emitidos.

ii. Terceros que confían, los que se tenga conocimiento

b) En caso de compromiso de claves del Titular de Certificado emitido por el PCSC CONFIRMA S.A., el titular deberá notificar al PCSC CONFIRMA S.A., de forma inmediata.

Los métodos para comunicación de compromiso o sospecha de compromiso de claves son:

a) Mediante el correo electrónico consignado en la solicitud de certificado y en el campo "email" del atributo "Nombre alternativo del titular" (SAN por sus siglas en inglés "Subject alternative name").

b) Mediante un teléfono consignado en la solicitud de certificado.

c) Mediante una visita presencial del titular a una AR vinculada al PCSC CONFRIMA S.A.

d) Mediante una fuente de información suficientemente confiable.

4.9.13. CIRCUNSTANCIAS PARA SUSPENSIÓN

Siempre que se prevea la posibilidad de suspender los certificados, el PCSC CONFIRMA S.A. procederá conforme a los siguientes supuestos:

a) Solicitud formulada por el firmante, la persona física o jurídica representada por éste, un tercero autorizado.
b) sospecha o duda de violación o puesta en peligro del secreto de los datos de creación de firma, o del PCSC, o utilización indebida de dichos datos por un tercero.
c) resolución judicial o administrativa competente que lo ordene.

d) sospecha o duda de la falsedad o inexactitud de los datos aportados para la expedición del certificado y que consten en él, o alteración posterior de las circunstancias verificadas para la expedición del certificado.

De manera previa o simultánea a la indicación de la suspensión de un certificado electrónico cualificado en el servicio de consulta sobre el estado de validez de los certificados por él expedidos, el PCSC CONFIRMA S.A. informará al titular de certificado o al responsable del mismo acerca de esta circunstancia, especificando los motivos, la fecha y la hora en que el certificado quedará sin efecto. La vigencia del certificado se extinguirá si transcurrido el plazo de duración de la suspensión, el prestador no la hubiera levantado.

4.9.14. QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN

La suspensión de un certificado sólo podrá realizarse por:

a) por solicitud formulada a través del firmante, la persona física o jurídica representada por éste, un tercero autorizado

b) resolución judicial o administrativa competente que lo ordene.

c) por solicitud de la empresa u organización, cuando en el certificado se detalla el cargo o función que ocupa en la organización y es proporcionado por la misma al titular, por ser éste, su empleado o funcionario;

d) por el PCSC CONFIRMA S.A.;

e) por una AR vinculada al PCSC CONFIRMA S.A.

4.9.15. PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN

El PCSC CONFIRMA S.A. garantiza que quienes están autorizados a solicitar la suspensión conforme al ítem 4.9.14, puedan, fácilmente y en

cualquier momento, solicitar la suspensión de sus respectivos certificados. Como directrices generales, se establece que:

a) el solicitante de suspensión de un certificado será identificado;

b) las solicitudes de suspensión, así como las acciones resultantes de ellas serán registradas y almacenadas;

c) se documentarán las razones de la suspensión de un certificado; y

d) la suspensión de un certificado terminará con la generación y publicación de una LCR que contenga los datos del certificado suspendido y, en el caso de la utilización de consulta OCSP, con la actualización del estado del certificado en la base de datos del PCSC.

El PCSC CONFIRMA S.A., debe registrar la suspensión, en el caso de certificado electrónico cualificado, en su base de datos de certificados y publicar el estado del certificado oportunamente y, en todo caso, en un plazo de veinticuatro (24) horas después de la recepción de la solicitud. La suspensión será efectiva inmediatamente después de su publicación. Se garantiza que el PCSC CONFIRMA S.A. responde plenamente por todos los daños causados por el uso de un certificado en el período comprendido entre la solicitud de su suspensión y la emisión de la LCR correspondiente. En caso de que sean requeridos procedimientos de suspensión específicos para las PCs implementadas, los mismos deberán ser descriptos en esas PCs, en el ítem correspondiente.

4.9.16. LÍMITES DEL PERÍODO DE SUSPENSIÓN

El límite del periodo de suspensión será establecido por el titular del certificado. La vigencia del certificado se extinguirá si transcurrido el plazo de duración de la suspensión, el PCSC no la hubiera levantado.

4.10.SERVICIOS DE ESTADO DEL CERTIFICADO

4.10.1. CARACTERÍSTICAS OPERACIONALES

El PCSC CONFIRMA S.A. proporciona un servicio de estado de certificado en forma de un punto de distribución de LCR en los certificados y OCSP, conforme al ítem 4.9.9

4.10.2. DISPONIBILIDAD DEL SERVICIO

El PCSC CONFIRMA S.A. garantiza la disponibilidad del servicio de publicación durante las veinticuatro horas, los siete días de la semana (24/7). En caso de interrupción por causa de fuerza mayor, el servicio se deberá restablecer en un plazo no mayor a veinticuatro (24) horas, garantizando la disponibilidad del servicio con un mínimo de 99,5% anual, un tiempo programado de inactividad máximo de 0.5% anual.

4.10.3. CARACTERÍSTICAS OPCIONALES

Para hacer uso del servicio de validación en línea es responsabilidad de la parte que confía disponer de un *cliente OCSP* que cumpla el RFC 6960.

4.11. FIN DE ACTIVIDADES

El PCSC CONFIRMA S.A. describe las condiciones en las cuales daría por finalizado el servicio conforme a lo establecido en el ítem 5.8 de esta DPC.

4.12. CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1. POLÍTICA Y PRÁCTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES

El PCSC CONFIRMA S.A. tiene **PROHIBIDO** copiar y almacenar los datos de creación de firma o de la persona física a la que hayan prestado sus

servicios, salvo en caso de su gestión en nombre del firmante o del creador del sello. Además, se custodian y protegen los datos de creación de firma, frente a cualquier alteración, destrucción o acceso no autorizado, así como se garantiza su continua disponibilidad.

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

Este ítem no aplica.

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

El PCSC CONFIRMA S.A. a fin de asegurar la confiabilidad y seguridad de sus operaciones como Prestador Cualificado de Servicios de Confianza ha dispuesto e implantado controles de seguridad física y lógica en todas sus instalaciones, al igual que procedimientos de auditoría, tanto interna como externa, para el seguimiento y verificación del cumplimiento de las políticas, directivas y procedimientos en materia de seguridad.

5.1. CONTROLES FÍSICOS

Se han establecido controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los propios sistemas y los equipamientos empleados para las operaciones para la prestación de los servicios electrónicos de certificación tanto para el PCSC CONFIRMA S.A. como para las ARs vinculadas.

En concreto, la política de seguridad aplicable establece prescripciones sobre lo siguiente:

- Controles de acceso físico.
- Protección frente a desastres naturales.
- Medidas de protección frente a incendios.
- Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)
- Derrumbamiento de la estructura.
- Inundaciones.
- Protección antirrobo.

- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del Proveedor de Servicios de certificación.

Estas medidas resultan aplicables a las instalaciones desde donde se prestan los servicios electrónicos de certificación, en sus entornos de producción y contingencia, las cuales son auditadas periódicamente de acuerdo con la normativa aplicable y a las políticas propias destinadas a este fin.

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año con asistencia en las 24 horas siguientes al aviso.

5.1.1. LOCALIZACIÓN Y CONSTRUCCION DEL SITIO

La localización del edificio donde se ubican los sistemas de certificación del PCSC CONFIRMA S.A. no es públicamente identificada. No existe identificación pública externa de las instalaciones e internamente.

El PCSC CONFIRMA S.A no posee ambientes compartidos que permitan la visibilidad de las operaciones de emisión y revocación de certificados.

Las operaciones de PCSC CONFIRMA S.A. son ser segregadas en compartimientos cerrados y físicamente protegidos.

Los sistemas están físicamente separados de otros existentes en el lugar, de forma que solo el personal autorizado del PCSC CONFIRMA S.A. pueda acceder a ellos, garantizando así la independencia de estos equipos y sistemas de terceros alojados en el lugar.

Las instalaciones relevantes del PCSC CONFIRMA S.A. cuentan al menos con los siguientes aspectos relevantes para los controles de seguridad física:

a) Instalaciones para equipamientos de apoyo, tales como: máquinas de aire acondicionado, grupos de generadores, UPS, baterías, tableros

de distribución de energía y de telefonía, subestaciones, rectificadores, estabilizadores y similares;

b) Instalaciones para sistemas de telecomunicaciones;

c) Los sistemas de puesta a tierra y protección contra rayos; e

d) Iluminación de emergencia;

La protección física se logra mediante la creación de perímetros de seguridad claramente definidos en torno a los servicios. La calidad y solidez de los materiales de construcción de las instalaciones garantiza unos adecuados niveles de protección frente a intrusiones por la fuerza bruta y ubicada en una zona de bajo riesgo de desastres y permite un rápido acceso.

La sala donde se realizan las operaciones criptográficas en el Centro de Proceso de Datos cuenta con redundancia en sus infraestructuras, así como varias fuentes alternativas de electricidad y refrigeración en caso de emergencia.

Se dispone de instalaciones que protegen físicamente la prestación de los servicios de aprobación de solicitudes de certificados y de gestión de revocación, del compromiso causado por acceso no autorizado a los sistemas o a los datos, así como a la divulgación de estos.

5.1.2. ACCESO FÍSICO

El PCSC CONFIRMA S.A. implementa un sistema de control de acceso físico que garantiza la seguridad de sus instalaciones, conforme al punto "control de accesos" de la norma ISO 27002 y los siguientes puntos:

5.1.2.1. NIVELES DE ACCESO FÍSICO

Los centros de datos donde se aloja la infraestructura tecnológica de PCSC CONFIRMA S.A. cuentan con seis niveles de seguridad física:

Primer nivel: Se situa la primera barrera de acceso a las instalaciones del PCSC CONFIRMA S.A. Para acceder al área del nivel 1, cada persona deberá ser identificada y registrada por el personal de seguridad, a partir de ese nivel personas extrañas a la operativa del PCSC deberán transitar debidamente identificadas y acompañadas. Ningún tipo de proceso operacional o administrativo del PCSC es ejecutado en ese nivel.

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

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

Tercer nivel: Nivel interno dentro del segundo nivel y es el primer nivel en albergar material y actividades sensibles de la operativa del PCSC. Cualquier actividad relativa al ciclo de vida de los certificados digitales deberá estar localizada a partir de este nivel. Personas que no están involucradas con esas actividades no cuentan con permiso para acceder a este nivel. Las personas que no posean permiso de acceso no

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

En este nivel son controladas tanto las entradas como las salidas de cada persona autorizada. Los mecanismos de control requeridos para acceder a ese nivel son dos: algún tipo de identificación individual, como una tarjeta electrónica, y la identificación biométrica .

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

Cuarto nivel: nivel de acceso para el area de operaciones críticas del PCSC CONFIRMA S.A. donde se despliegan las actividades especialmente sensibles a la operación del PCSC, tales como la emisión y revocación de los certificados y la emisión de la LCR. Todos los sistemas y equipamientos necesarios a estas actividades se encuentran localizados a partir de este nivel. El nivel 4 deberá poseer 2 (dos) factores de autenticación como mínimo (uno de ellos biométrico) y tarjeta de identificación visible y, adicionalmente, exigir, en cada acceso a su ambiente, la identificación de, como mínimo, 2 (dos) personas autorizadas. En este nivel, la permanencia de esas personas es exigida mientras el ambiente estuviera ocupado.

En el cuarto nivel, todas las barreras físicas (paredes y barrotes) son sólidas, extendiéndose desde el piso real al techo real. Las paredes, piso y techo revestidas de modo a prevenir las amenazas de acceso no autorizado, agua, vapor, gas y fuego. Las tuberías de refrigeración, de energía o de comunicación permiten la penetración física en las áreas

de cuarto nivel. Adicionalmente, debe tener protección contra las interferencias electromagnéticas externas.

Este ambiente esta construido según las normas internacionales aplicables.

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

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

Quinto nivel: interno al ambiente del nivel 4, se dispone de un cofre o un gabinete reforzado, donde se encuentran almacenados: materiales criptográficos, tales como, claves, datos de activación, sus copias y equipamientos criptográficos

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

a) Estar hecho de acero o con material de resistencia equivalente; y

b) Poseer cerraduras antirrobo.

Sexto nivel: interno al ambiente del nivel 4, comprende de un cofre o un gabinete reforzado. Los datos de activación de la clave privada del PCSC CONFIRMA S.A. son almacenados en ese ambiente.

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

a) Estar hecho de acero o con material de resistencia equivalente; y

b) Poseer cerraduras antirrobo.

5.1.2.2. SISTEMAS FÍSICOS DE DETECCIÓN

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

Las cintas de vídeo resultantes de grabación 24x7 deberán ser almacenadas, como mínimo, 4 (cuatro) años. Ellas deberán ser testeadas (verificación de estrechos aleatorios en el inicio, medio y final de la cinta) por lo menos cada 3 (tres) meses, con la elección, como mínimo, de 1 (una) cinta referente a cada semana. Esas cintas deberán ser almacenadas en el ambiente del nivel 3.

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

En todos los ambientes del cuarto nivel, una alarma de detección de movimientos deberá permanecer activa hasta que se satisfaga el criterio de acceso al ambiente. Así que si, debido a la salida de uno o más empleados, trae como consecuencia que el criterio mínimo de ocupación deje de ser satisfecha, deberán activarse automáticamente los sensores de presencia.

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

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

5.1.2.3. SISTEMAS DE CONTROL DE ACCESO

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

5.1.2.4. MECANISMOS DE EMERGENCIA

Mecanismos específicos son implementados por el PCSC del CONFIRMA S.A. para garantizar la seguridad de su personal y de sus equipamientos en situaciones de emergencia.

Esos mecanismos permiten el desbloqueo de las puertas por medio de accionamiento mecánico, para la salida de emergencia de todos los ambientes con control de acceso. La salida efectuada por medio de estos mecanismos acciona inmediatamente las alarmas de apertura de puertas.

El PCSC CONFIRMA S.A. puede especificar e implementar otros mecanismos de emergencia, específicos necesarios para cada tipo de instalación.

Todos los procedimientos referentes a esos mecanismos de emergencia son documentados.

Los mecanismos y procedimientos de emergencia son verificados semestralmente, por medio de simulación de situaciones de emergencia.

Los centros de datos donde se aloja la infraestructura disponen de al menos, los siguientes elementos de seguridad física:

- Muros perimetrales Reforzados.
- Generación de energía redundante.
- Sistema ininterrumpible de energía.
- Sistema de UPS redundante.
- Doble acometida eléctrica.
- Sistema de enfriamiento de precisión redundante.
- Sistema de detección, extinción y supresión automática de fuego.
- Sistema de monitoreo de infraestructura.
- Sistema de tierras físicas y pararrayos.
- Suministro de energía eléctrica regulada y con protección.
- Sistema de aire acondicionado HVAC.
- Seguridad física 24/7 (subsistema de seguridad mediante guardias de seguridad).
- Sistema CCTV con grabación de movimiento.

5.1.3. ENERGÍA Y AIRE ACONDICIONADO

Las áreas donde se ubican los equipos de la infraestructura tecnológica del PCSC CONFIRMA S.A. cuentan con suministros de electricidad y aire acondicionados adecuados a los requisitos de los equipos en ellas instalados. La infraestructura se encuentra protegida contra caídas de tensión o cualquier otra anomalía en el suministro eléctrico

EL PCSC CONFIRMA S.A. dispone de:

- Sistemas de alimentación ininterrumpida (UPS por sus siglas en inglés Uninterruptible Power Supply)

- Grupo electrógeno con potencia suficiente para soportar la carga del Centro de Datos, incluido los equipos informáticos y equipos de refrigeración.
- Doble Acometida eléctrica para los equipos.
- Sistema de puesta a tierra implantado.
- 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.

Todos los cables son catalogados, identificados e inspeccionados periódicamente, al menos (6) meses, en busca de evidencia de violación y anomalías.

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

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

El Sistema de climatización cumple con los requisitos de temperatura y humedad exigidos por los equipamientos utilizados en el ambiente y disponer de filtros de polvos.

En los ambientes del nivel 4, el sistema de climatización es independiente y tolerante a fallas.

La temperatura de los ambientes atendido por los sistemas de climatización es permanentemente monitoreada por el sistema de notificación de alarmas.

Los sistemas de aire acondicionados de los ambientes de nivel 4 son internos, con cambio de aire realizados apenas por la abertura de la puerta.

La capacidad de redundancia de toda la estructura de energía acondicionada está garantizada, por medio de:

- Generadores de un tamaño compatible
- Generadores de reserva;
- Sistemas de UPS redundantes; y
- Sistemas redundantes de aire acondicionado.

La estructura interna al ambiente del nivel 4, provee protección física contra exposición al agua, filtraciones e inundaciones proveniente de cualquier fuente externa.

5.1.4. EXPOSICIÓN AL ALGUA

La infraestructura interna del PCSC de CONFIRMA S.A posee protección física contra exposición al agua, filtraciones e inundaciones provenientes de cualquier fuente externa.

5.1.5. PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO

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

En las instalaciones del PCSC CONFIRMA S.A. no está permitido fumar o portar objetos que produzcan fuego o chispa.

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

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

5.1.6. ALMACENAMIENTO DE MEDIOS

El PCSC CONFIRMA S.A. asegura el adecuado manejo y protección de los medios de almacenamiento de información, que contengan datos críticos o sensibles del sistema, contra daños accidentales (agua, fuego, electromagnetismo) e impide, detecta y previene su uso no autorizado, acceso o su divulgación.

La información relacionada a la infraestructura del PCSC CONFIRMA S.A. es almacenada de forma segura en armarios ignífugos y cofres de seguridad, según su clasificación.

5.1.7. ELIMINACIÓN DE RESIDUOS

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

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

Se ha optado por un procedimiento de eliminación de residuos que establece la eliminación de soportes, tanto papel como magnéticos, se realizan mediante mecanismos que garantizan la imposibilidad de recuperación de la información.

En el caso de soportes magnéticos, se desechan en cuyo caso se destruyen físicamente, o se reutilizan previo proceso de borrado permanente o formateo. En el caso de documentación en papel, mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.

5.1.8. RESPALDO FUERA DE SITIO

El PCSC CONFIRMA S.A. cuenta con una instalación de respaldo con niveles de protección física y ambiental similar al sitio principal y con separación física adecuada.

En caso de siniestro que torne inoperante la instalación principal del PCSC CONFIRMA S.A. la instalación de respaldo tomará totalmente las operaciones en condiciones idénticas en un máximo de 48 (cuarenta y ocho) horas.

5.2. CONTROLES PROCEDIMENTALES

El PCSC CONFIRMA S.A. garantiza que sus sistemas se operan de forma segura, para lo cual ha establecido e implantado procedimientos para las funciones que afectan a la provisión de sus servicios.

El personal al servicio ejecuta los procedimientos administrativos y de gestión de acuerdo con la política de seguridad a fin de evitar que un empleado que asume un rol de confianza utilice incorrectamente su sistema de certificación sin ser detectado. Las acciones de cada uno de los empleados se limitarán de acuerdo con su perfil.

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

Cuando un empleado es desvinculado inmediatamente, sus permisos de accesos serán revocados. Cuando hay un cambio en la posición o función que el empleado ocupa dentro del PCSC, serán revisados y reasignados sus permisos de accesos.

5.2.1. ROLES DE CONFIANZA

El PCSC CONFIRMA S.A. garantiza la segregación de tareas para las funciones críticas a fin de evitar que un funcionario que asuma un rol de confianza utilice incorrectamente los sistemas de certificación sin ser detectado.

Estos Roles contemplan, al menos las siguientes responsabilidades que a continuación serán descriptos:

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

física, y de los movimientos de material fuera de las instalaciones del PCSC;

b) Responsables de sistemas: los responsables de este rol no deberán estar implicados en tareas de auditoría interna. Serán encargados de la instalación y configuración de sistemas operativos, del mantenimiento y actualización de los programas instalados; con capacidad para configurar, mantener los sistemas, pero sin acceso a los datos. Asimismo, deberán establecer y documentar los procedimientos de monitoreo de los sistemas y de los servicios que prestan. Serán responsables de mantener el inventario de servidores y resto de componentes de los sistemas de certificación del PCSC y asumirán la gestión de los servicios de ruteamiento y gestión de reglas de firewall, gestión y mantenimiento de los sistemas de detección de intrusos, etc. Serán encargados de la instalación de hardware criptográfico del PCSC y de la eliminación del hardware criptográfico del PCSC de producción. Serán responsables del mantenimiento o reparación de equipos en general así como de dispositivos criptográficos del PCSC (incluida la instalación de nuevo hardware, firmware o software), Igualmente serán responsables de los desmontajes y la eliminación permanente por el uso;

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

mantenimiento de los sistemas de energía, aire acondicionado y prevención de incendios;

d) Responsables de auditoría: serán los responsables de las tareas de ejecución y revisión de auditoría de los sistemas que conforman la infraestructura tecnológica del PCSC. Esta auditoría deberá realizarse de acuerdo con las normas y criterios de auditoría establecidos en la presente DPC. Además, deberá tener acceso a todos los registros del sistema mencionados;

e) responsables del ciclo de vida de claves criptográficas: son los responsables de la gestión del ciclo de vida de las claves criptográficas (ejemplo: oficial criptográfico, oficial de activación, etc.)

F) responsables de desarrollo de sistemas del PCSC: serán los encargados del diseño de las arquitecturas de programación, de control y supervisión de los desarrollos encomendados y de la correcta documentación de las aplicaciones; y

g) agentes de registros: son los responsables de la realización de las actividades inherentes a una AR, realizan la identificación de los solicitantes en la solicitud de emisión/revocación de un certificado y autoriza en el sistema la emisión o revocación del mismo.

Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de investigación y control específicos. Adicionalmente, se implementan criterios en sus políticas para la segregación de las funciones, como medida de prevención de actividades fraudulentas.

Todos los operadores del sistema de certificación del PCSC CONFIRMA S.A. recibiran entrenamiento específico antes de obtener cualquier tipo

de acceso. El tipo o nivel de acceso serán determinados, en un documento formal, con base en las necesidades de cada perfil.

Cuando un empleado o funcionario se desvincula del PCSC de CONFRIMA S.A, inmediatamente sus permisos de acceso son revocados. Cuando hay un cambio en la posición o función que el empleado o funcionario ocupa dentro del PCSC, deberán ser revisados y actualizados en su caso, sus permisos de acceso. Existe una lista de revocación, con todos los recursos, antes disponibilizados, que el empleado o funcionario deberá devolver al PCSC en el momento de su desvinculación.

5.2.2. NÚMERO DE PERSONAS REQUERIDAS POR TAREA

El PCSC CONFIRMA S.A. garantiza al menos dos personas para realizar las tareas relativas a la generación, recuperación y back-up de la clave privada de las Autoridades de Certificación. Igual criterio se aplica para la ejecución de tareas de emisión y activación de certificados y claves privadas de las Autoridades de Certificación.

Las demás tareas podrán ser ejecutadas por un único empleado o funcionario.

El PCSC mantiene y ejecuta procedimientos de control rigurosos para asegurar la segregación de funciones.
Esta DPC establece el requisito de control multiusuarios para la generación y la utilización de la clave privada del PCSC CONFIRMA S.A. en el punto 6.2.2.

5.2.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Todo empleado que asume un rol de confianza en el PCSC CONFIRMA S.A. es identificado y su perfil es verificado antes de que:

- Sea incluido en la lista de acceso a las instalaciones del PCSC.

- Sea incluido en la lista para acceso físico al sistema de certificación del PCSC.
- Reciba un certificado electrónico para ejecutar sus actividades operacionales en el PCSC.
- Reciba una cuenta de usuario del sistema de certificación del PCSC.

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

- Son directamente asignados a un único empleado.
- No son compartidos.
- Se restringe a las acciones asociadas con el perfil para el que fueron creados.

5.2.4. ROLES DE REQUIEREN SEPARACIÓN DE FUNCIONES

Los roles que requieren separación de los deberes incluyen (pero no está limitado) a los encargados de ejecutar las siguientes responsabilidades:

a) los responsables del ciclo de vida de claves criptográficas no podrán cumplir funciones de los responsables de auditoría;

b) los responsables de sistemas no podrán cumplir funciones de los responsables de seguridad ni de los responsables de auditoría;

c) los responsables de seguridad no podrán cumplir funciones de los responsables de sistemas, de los responsables del ciclo de vida de claves criptográficas, de los agentes de registros ni de los responsables de auditoría; y

d) los responsables de auditoría no podrán cumplir otra función o rol.

Además, otras tareas que deben ser segregadas son:

a) La puesta en operación del PCSC en producción;

b) La emisión o destrucción de los certificados del PCSC; y

c) La validación de información en los sistemas de certificación del PCSC y de solicitudes de emisión/revocación o información del titular o responsable del certifciado.

5.3. CONTROLES DE PERSONAL

Son descriptos los requisitos y procedimientos, implementados por el PCSC CONFIRMA S.A. por las ARs y PSSs vinculadas a todo su personal, refiriéndose a aspectos como: verificación de antecedentes e idoneidad, capacitación, rotación de puestos, sanciones por acciones no autorizadas, controles para contratación y documentación a ser proporcionada.

La DPC debe garantizar de que todos los empleados o funcionarios del PCSC CONFIRMA S.A. de las ARs y de los PSSs vinculados, a cargo de las tareas operativas, se hayan registrado en un contrato o término de responsabilidad:

a) Los términos y condiciones del perfil que ocuparán;

b) El compromiso de observar las reglas, políticas y normas aplicables a la PKI- Paraguay; y

c) El compromiso de no divulgar información confidencial a la que tenga acceso.

5.3.1. REQUERIMIENTOS DE EXPERIENCIA, CAPACIDADES Y AUTORIZACIÓN

Todo el personal del PCSC CONFIRMA S.A. y de las AR vinculadas e involucrado en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados son seleccionados y admitidos, conforme a lo establecido en el ítem 7 "seguridad ligada a los recursos humanos" de la norma ISO 27002 y además debieron:

a) Haber demostrado capacidad para ejecutar sus deberes;

b) Haber suscripto un acuerdo de confidencialidad y disponibilidad;

c) No poseer otros antecedentes que puedan interferir o causar conflicto con los del PCSC;

d) No tener antecedentes de negligencia o incumplimiento de labores; y

e) No tener antecedentes judiciales ni policiales.

El PCSC CONFIRMA S.A. puede definir requisitos adicionales para la admisión.

5.3.2. PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES

Con el propósito de resguardar la seguridad y credibilidad de las entidades, todo personal del PCSC CONFIRMA S.A. y de las ARs vinculadas involucradas en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados son sometido a:

a) Confirmación de empleos anteriores;

b) Verificación de referencias profesionales;

c) Título académico obtenido; y

d) Verificación de antecedentes judiciales y policiales.

El PCSC CONFIRMA S.A. puede definir requisitos adicionales para la verificación de antecedentes.

5.3.3. REQUERIMIENTOS DE CAPACITACIÓN

Todo el personal del PCSC CONFIRMA S.A. y de las AR vinculadas, involucrado en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados reciben entrenamiento documentado suficiente para el dominio de los siguientes temas:

a) Principios y mecanismos de seguridad del PCSC y de las ARs vinculadas;

b) Sistema de certificación en uso del PCSC;

c) Procedimientos de recuperación de desastres y continuidad del negocio;

d) Reconocimiento de firmas y validación de documentos presentados en los ítems 3.2.2., 3.2.3. y 3.2.4.;

e) Normativa vigente que rige la materia; y

f) Otros asuntos relacionados con las actividades bajo su responsabilidad.

5.3.4. REQUERIMIENTOS Y FRECUENCIA DE CAPACITACIÓN

Todo el personal del PCSC CONFIRMA S.A. y de las ARs vinculadas, involucrado en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados deberá son mantenidos y actualizados sobre eventuales cambios o modificaciones tecnológicas de los sistemas del PCSC o de las ARs.

A su vez, el PCSC CONFIRMA S.A. y sus ARs vinculadas proveen de programas de capacitacion para actualizar la formación del personal de acuerdo con las necesidades, y con la frecuencia suficiente para cumplir sus funciones de forma competente y satisfactoria, especialmente cuando se realicen modificaciones sustanciales en las tareas de certificación.

5.3.5. FRECUENCIA Y SECUENCIA EN LA ROTACIÓN DE LAS FUNCIONES

Esta DPC define una política a ser adoptada por el PCSC CONFIRMA S.A. y por las ARs vinculadas, para la rotación del personal en los diversos cargos y perfiles por ellas establecidas. Esa política no contradice los propósitos establecidos en el ítem 5.2.1.

El PCSC CONFIRMA S.A. y las ARs vinculadas efectuan una rotación de sus roles de confianza como mínimo una vez cada 5 años.

5.3.6. SANCIONES PARA ACCIONES NO AUTORIZADAS

Se dispone de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas, las mismas son recogidas en el Reglamento Interno de CONFIRMA S.A. y de acuerdo a lo estipulado en el documento suscripto para los roles de confianza.

El proceso administrativo referido en el párrafo anterior contendra, como mínimo, los siguientes puntos:

a) Relato de lo ocurrido con el modo de operación;

b) Identificación de los involucrados;

c) Eventuales perjuicios causados;

d) Las sanciones aplicadas, si fuere el caso; y

e) Conclusiones.

Concluido el proceso administrativo, el PCSC CONFIRMA S.A. comunica sus conclusiones a la AC Raíz-Py.

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

a) Advertencia;
b) Suspensión por un plazo determinado; o

c) Cese de sus funciones.

5.3.7. REQUISITOS DE CONTRATACIÓN A TERCEROS

El PCSC CONFIRMA S.A. y sus AR vinculadas, pueden contratar personal externo, consultores o terceros, conforme a lo establecido en los Ítems: 7 "Seguridad ligada a los recursos humanos" y 15 "Relaciones con suministradores" norma ISO 27002 bajo las siguientes condiciones mínimas:

a) Que exista un contrato con cláusulas propias de los roles de confianza y estipula sanciones para las acciones no autorizadas;

b) Que el PCPS responsable o AR vinculada no posea personal disponible para llenar los roles de confianza;

c) Que el personal a contratar cumpla con los mismos requisitos del ítem 5.3.1; y

d) Que una vez finalizado el servicio contratado se revoquen los derechos de acceso.

5.3.8. DOCUMENTACIÓN SUMINISTRADA AL PERSONAL

El PCSC CONFIRMA S.A. y sus ARs vinculadas proporcionan a sus personales toda la documentación y buenas prácticas de seguridad de la información necesarias para el correcto desempeño de sus tareas. Entre las documentaciones se encuentran:

a) Su DPC;

b) Las PCs que implementa;

c) La política de seguridad que implementa el PCSC;

d) Documentación operacional relativa a sus actividades; y

e) Contratos, normas y políticas relevantes para sus actividades.

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

5.4. PROCEDIMIENTO DE REGISTRO DE AUDITORÍA

En los siguientes ítems se describen los aspectos de los sistemas de auditorías y registro de eventos a ser implementados por el PCSC CONFIRMA S.A. con el fin de mantener un entorno o 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 de certificación. Entre otros, los siguientes eventos estan obligatoriamente incluidos en los archivos de auditoría:

a) Iniciación y terminación del sistema de certificación;
b) Los intentos de crear, eliminar, establecer contraseñas o cambiar los privilegios del sistema de los operadores del PCSC;
c) Los cambios en la configuración del PCSC o en sus claves;
d) Los cambios en las políticas de creación de certificados;
e) Los intentos de acceso (*login*) y de salida del sistema (*logoff*);
f) Los intentos no autorizados de acceso a los archivos del sistema;
g) La generación de claves propias del PCSC o de claves de sus usuarios finales;
h) La emisión y revocación de certificados;
i) La generación de la LCR;
j) Los intentos de iniciar, remover, habilitar y deshabilitar a los usuarios de sistemas y actualizar y recuperar sus claves;

k) Las operaciones fallidas de escritura o lectura en el repositorio de los certificados y de la LCR, en su caso; y

l) Las operaciones de escritura en ese repositorio, en su caso.

El PCSC CONFIRMA S.A. registra, electrónicamente o manualmente, informaciones de seguridad no generadas directamente por el sistema de certificación, tales como:

a) Registros de accesos físicos;

b) El mantenimiento y los cambios en la configuración de sus sistemas;

c) Los cambios de personal y los cambios de su rol de confianza;

d) Los informes de discrepancia y de compromiso; y

e) El registro de destrucción de los medios de almacenamiento que contienen las claves criptográficas, de datos de activación de certificados o de la información personal de los usuarios.

Todos los registros de auditoria, electrónicos o manuales, contienen la fecha y hora del evento registrado y la identidad del agente que lo causo.

Para facilitar los procesos de auditoría, toda documentación relacionada a los servicios del PCSC CONFIRMA S.A. es almacenada, electrónicamente y/o manualmente, en un local único, conforme a lo establecido en el ítem 12 "seguridad en la operativa" de la norma ISO 27002.

Las ARs vinculada al PCSC CONFIRMA S.A. registran electrónicamente y/o manualmente archivos de auditorías de todos los eventos relacionados a la validación y aprobación de la solicitud, así como la revocación de los

certificados. Los siguientes eventos están obligatoriamente incluidos en los archivos de auditoría:

a) Los AGR que realizan las operaciones;

b) Fecha y hora de las operaciones;

c) La asociación entre los agentes que realizan la validación, aprobación y el certificado generado; y

d) La firma electrónica cualificada del ejecutante.

El PCSC CONFIRMA S.A. a la que está vinculada la AR establece en un documento que está disponible en las auditorías de cumplimiento, el lugar de archivo de los expedientes de los titulares de certificados.

5.4.2. FRECUENCIA DE PROCESAMIENTO DEL REGISTRO (LOGS)

Los registros se analizan mínimamente una vez al mes, en las auditorias periódicas por el personal operacional, Además de las revisiones oficiales, los registros de auditoría son revisados en respuesta a una alerta, por irregularidades o incidentes dentro de los sistemas de la AC.

Todos los eventos significativos son explicados en un informe de auditoría de registros. Tal análisis involucra una revisión de los registros que incluye la verificación de que éstos no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros. Las acciones realizadas a partir de la revisión de auditoría están documentadas. Todas

las medidas adoptadas como resultado de este análisis deberán ser documentadas.

Se mantiene un sistema que permite garantizar:

- Espacio suficiente para el almacenamiento de logs.
- Que los ficheros de logs no se reescriben.
- Que la información que se guarda incluye como mínimo: tipo de evento, fecha y hora, usuario que ejecuta el evento y resultado de la operación.
- Los ficheros de logs se guardarán en ficheros estructurados susceptibles de incorporar en una BBDD para su posterior exploración.

  Los registros de auditorías deben ser recuperados solamente por personal autorizado, ya sea por razones válidas del negocio o por seguridad.

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

La información generada en los registros de auditoria se conservará localmente por dos meses y, consecuentemente, se almacenarán de la manera descripta en el ítem 5.5.2.

Además de las revisiones oficiales, los registros de auditoría son revisados en respuesta a una alerta, por irregularidades o incidentes dentro de los sistemas del PCSC CONFIRMA S.A.

5.4.4. PROTECCIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

El PCSC CONFIRMA S.A. posee un sistema de registro de eventos mediante el cual protege sus registros de auditoría contra lectura no autorizada, modificación y eliminación, utilizando mecanismos de protección conforme a lo dispuesto al Ítem 12 "seguridad en la operativa" de la norma ISO 27002.

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

El PCSC CONFIRMA S.A. genera copias de seguridad de sus registros de auditorías, como mínimo, 1 (una) vez al mes.

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

La información de la auditoria de eventos es recogida internamente y de forma automatizada por el sistema operativo, las comunicaciones de red y por el software de gestión de certificados, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado. Todo ello compone el sistema de acumulación de registros de auditoría.

5.4.7. NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO

Cuando el sistema de acumulación de registros de auditoría registre un evento, por el conjunto de sistemas de auditoría del PCSC CONFIRMA S.A., no se requerirá notificar a ninguna persona, organización, dispositivo o aplicación que causó el evento, a excepción de que el evento sea de índole accidental y resulta probable que pueda volver a ocurrir.

5.4.8. EVALUACIÓN DE VULNERABILIDADES

Los eventos que indiquen posibles vulnerabilidades, detectados en el análisis periódico de los registros de auditoría del PCSC CONFIRMA S.A., serán analizadas detalladamente y, dependiendo de su gravedad, son registradas por separado. Acciones correctivas que surjan son implementadas y registradas con fines de auditoría.

5.5. ARCHIVOS DE REGISTROS

En los siguientes items se describe la política general de archivos de registros, para su uso futuro a ser implementada por el PCSC CONFIRMA S.A. y por las ARs vinculadas a este.

5.5.1. TIPOS DE REGISTROS ARCHIVADOS

Los tipos de registros archivados, que deberá comprender, entre otros:

a) Solicitudes de certificados;

b) Solicitudes de revocación de certificados;

c) Notificaciones de compromiso de claves privadas;

d) Emisiones y revocaciones de certificados;

e) Emisiones de LCR;

f) Cambio de claves criptográficas del PCSC responsable;

g) Información de auditoría prevista en el ítem 5.4.1.

El PCSC CONFIRMA S.A. y/o las Autoridades de Registro según corresponda, serán responsables del correcto archivo de todo este material.

5.5.2. PERÍODOS DE RETENCIÓN PARA ARCHIVOS

a) Las LCRs y los certificados emitidos de firma digital serán conservados permanentemente para fines de consulta histórica;

b) Los dossiers de los titulares de certificado como mínimo, por 10 (diez) años, a contar desde la fecha de expiración o revocación del certificado; y

c) Las demás informaciones, inclusive los archivos de auditoría serán almacenadas, como mínimo, 10 (diez) años.

5.5.3. PROTECCIÓN DE ARCHIVOS

Se protege el archivo de forma que sólo personas debidamente autorizadas puedan obtener acceso al mismo. El archivo es protegido contra visualización, modificación, borrado o cualquier otra manipulación mediante su almacenamiento en un sistema fiable.
Todos los registros archivados son clasificados y almacenados con los requisitos de seguridad compatibles con esta clasificación, de acuerdo con lo establecido en el ítem 12 "seguridad en la operativa" de la norma ISO 27002.

5.5.4. PROCEDIMIENTO DE RESPALDO (BACKUP) DE ARCHIVO

El PCSC CONFIRMA S.A. mantiene procedimientos adecuados de respaldo de archivos (físicos y electrónicos), tanto en el sitio principal como en el alterno, que aseguren la disponibilidad de estos, de acuerdo con un análisis de riesgos determinado por los factores de operación del PCSC CONFIRMA S.A.

Realiza una segunda copia de todo el material archivado en un local externo al PCSC CONFIRMA S.A., recibiendo el mismo tipo de protección utilizada para el archivo principal.

Establece seguir los mismos periodos de retención definidos para los registros de las cuales son copias.

Verifica la integridad de esas copias de seguridad, como mínimo, cada 6 (seis) meses.

5.5.5. REQUERIMIENTOS PARA SELLADO DE TIEMPO DE REGISTROS

Este ítem no aplica.

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

Todo el material archivado de información se realiza de forma interna al PCSC CONFIRMA S.A.

Se mantiene dos copias de seguridad, una de ellas debe ser almacenada fuera del sitio principal de operaciones.

5.5.7. PROCEDIMIENTOS PARA OBTENER Y VERIFICAR LA INFORMACION ARCHIVADA

Se dispone de un procedimiento donde se describe el procedimiento para verificar la información archivada que se encuentra protegida de forma que solo el personal autorizado cuenta con los accesos a los archivos de soporte y archivos informáticos para llevar a cabo verificaciones de integridad.

Esta verificación debe ser llevada a cabo por el Auditor, que debe tener acceso a las herramientas de verificación y control de integridad de la información archivada.

Se realizan pruebas de restauración de la información archivada al menos 1 (una) vez al año.

5.6. CAMBIO DE CLAVE

El PCSC CONFIRMA S.A. cambia su clave de acuerdo con el *tiempo de uso* y *tiempo operacional* de los certificados emitidos dentro de la ICPP, este cambio técnicamente implica la emisión de un nuevo certificado. *El tiempo operacional* de un certificado coincide con el descripto en los campos de ''Válido desde'' y ''Válido hasta'' del mismo. El *tiempo de uso* refiere al establecido para los certificados emitidos en el marco de la ICPP para determinados usos, como se aprecia a continuación:

Tabla No 6 – Certificados emitidos en el marco de la ICPP

Tipo de Certificado	Tiempo de uso en años	Tiempo operacional en años	Descripción
Certificado cualificado de firma, tributario (F2, F3)	4	4	El certificado emitido al titular o responsable del certificado es otorgado por un tiempo máximo de 4 (cuatro) años, al finalizar ese período pierde su validez.
Certificado cualificado tributario (F1)	1	1	El certificado emitido al titular o responsable del certificado es otorgado por un tiempo máximo

			de 1 (un) año, al finalizar ese período pierde su validez.
Certificado de PCSC	6	10	El Certificado emitido al PCSC tendrá un tiempo operacional de 10 (diez) años, que resulta de la suma del tiempo de uso de su certificado [6 (seis) años] más el tiempo de validez máximo del certificado emitido al usuario final [4 (cuatro) años]. Solamente durante el tiempo de uso de su certificado, el PCSC podrá emitir certificados a usuarios finales. En los años restantes del tiempo

			operacional, sólo podrá firmar o sellar la LCR de usuarios finales.
Certificado AC Raíz-Py	10	20	El certificado emitido a la AC Raíz-Py tendrá un tiempo operacional de 20 años, que resulta de la suma del tiempo de uso de su certificado [10 (diez) años] más el tiempo de validez máximo del certificado de un PCSC [10 (diez) años]. Solamente durante el tiempo de uso de su certificado, la AC Raíz-Py podrá emitir certificados a un PCSC. En los años restantes del tiempo operacional sólo

			podrá firmar o sellar la LCR de los PCSC.

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

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

El PCSC garantiza que el tiempo máximo de uso en años de los certificados de niveles inferiores se ajusta con el tiempo operacional de todos los niveles superiores.

5.7. RECUPERACIÓN DE DESASTRES Y COMPROMISO

Los requisitos relacionados con los procedimientos de notificación y recuperación de desastres, previstos en el Plan de Continuidad del Negocio (PCN) del PCSC CONFIRMA S.A. estan de acuerdo con el ítem 17 "aspectos de seguridad de la información en la gestión de la continuidad del negocio" de la norma ISO 27002, para garantizar la continuidad de sus servicios críticos.

5.7.1. PROCEDIMIENTO PARA EL MANEJO DE INCIDENTE Y COMPROMISO

El PCSC CONFIRMA S.A. cuenta con un Plan de Continuidad del Negocio (PCN), con acceso restringido, probado al menos una vez al año, para garantizar la continuidad de sus servicios críticos. También con un Plan de Respuesta a Incidentes y un Plan de Recuperación ante Desastres.

Los procedimientos previstos en el PCN de las ARs vinculadas para la recuperación total o parcial de las actividades de las AR, conteniendo al menos la siguiente información:

a) Identificación de eventos que pueden causar interrupciones en los procesos del negocio, por ejemplo, fallas de equipos, inundaciones e incendios, si fuera el caso;

b) Identificación y concordancia de todas las responsabilidades y procedimientos de emergencia;

c) Implementación de procedimientos de emergencia que permitan la recuperación y restauración dentro de los plazos necesarios;

d) Documentación de procesos y procedimientos conforme a lo establecido;

e) Capacitación adecuada del personal en procedimientos y procesos de emergencia definidos, incluida la gestión de crisis; y

f) Prueba y actualización de planes.

5.7.2. CORRUPCIÓN DE DATOS, SOFTWARE Y/O RECURSOS COMPUTACIONALES

En caso de sospecha de corrupción de datos, software y/o recursos de cómputo, se comunica el hecho al **responsable de Seguridad** de CONFIRMA0 S.A., quien decreta el inicio de la fase de respuesta.

En esta etapa se realiza una rigurosa inspección para comprobar la veracidad del hecho y las consecuencias que puede generar. Este procedimiento es realizado por un grupo predeterminado de personal debidamente capacitado para esta situación.

De ser necesario, el **responsable de Seguridad** decretará la contingencia respectiva; por lo que se pone en ejecución el Plan de Continuidad de Negocios, el cual contiene acciones a tomar en caso de que se dañen los recursos informáticos, software y/o datos y que se pueden resumir como sigue:

1. Se identifican todos los elementos corruptos;
2. El tiempo de compromiso está determinado y es crítico para invalidar operaciones ejecutadas después de ese tiempo;
3. Serealizaunanálisisdelniveldecompromisoparadeterminarlasaccionesatomar,quepueden ir desde una simple restauración de un respaldo de seguridad hasta la revocación del certificado de CA.

Finalmente, el hecho queda documentado para fines de auditoría

5.7.3. PROCEDIMIENTOS DE COMPROMISO DE LA CLAVE PRIVADA DE LA ENTIDAD

5.7.3.1. CERTIFICADO DE ENTIDAD ES REVOCADO

a) En caso de revocación del certificado del PCSC CONFIRMA S.A..:

- Informar a todos sus titulares de certificados.

- Indicar que los certificados y la información del estado de revocación que han sido entregados usando la clave de la AC de CONFIRMA S.A. ya no son válidos.

b) En caso de revocación del certificado del Titular de Firma electrónica cualificada:

- El PCS CONFIRMA S.A.informara al titular cuyo certificado fue revocado acerca de los motivos y procedimientos realizados.

5.7.3.2. CLAVE DE IDENTIDAD ESTA COMPROMETIDA

a) En caso de compromiso de la clave privada de CONFIRMA S.A.:

- Informar inmediatamente al MIC la situación y solicitar la revocación de su certificado.
- Informar a todos sus suscriptores.
- Indicar que los certificados y la información del estado de revocación que han sido entregados usando la clave de la AC de CONFIRMA S.A. ya no son válidos.

b) En caso de compromiso de la clave privada del Titular de Firma electrónica cualificada, firma cualificada tributaria:

- El titular del Certificado debe informar al PCSC CONFIRMA S.A. en el menor tiempo posible y solicitar la revocación del certificado afectado.

5.7.4. CAPACIDAD DE CONTINUIDAD DEL NEGOCIO DESPUES DE UN DESASTRE

El PCSC CONFIRMA S.A. cuenta y mantiene un "Plan de Contingencia, Recuperación frente a Desastres y Continuidad del Negocio" de manera que, en el evento de una interrupción del negocio, las funciones críticas puedan ser recuperadas. Para ello la AC cuenta con una instalación de recuperación de desastres en un sitio alterno localizado en una instalación separada geográficamente del sitio principal. Este sitio alterno está diseñado bajo las mismas especificaciones de seguridad que el sitio principal.

En el caso de un desastre que requiera el cese permanente de operaciones del sitio Principal del PCSC CONFIRMA S.A., el equipo técnico informado y designado para tal caso evaluará la situación y tomará la decisión de declarar formalmente una situación de desastre y gestionar el incidente.

Una vez que es declarada una situación de desastre será iniciada la restauración de la funcionalidad de los servicios de producción en el sitio alterno.

El tiempo objetivo para recuperar la funcionalidad del servicio de Producción crítico es no mayor que 24 horas.

Los procedimientos de recuperación utilizados por la AC de CONFIRMA S.A.. está conforme a lo establecido en el ítem 17 "aspectos de seguridad de la información en la gestión de la continuidad del negocio" de la norma ISO 27002:2022

5.8. EXTINCIÓN DE UN PCSC O ENTIDADES VINCULADAS

En el caso de la extinción de servicios del PCSC CONFIRMA S.A. o de una AR, AV o PSS a ella vinculada.

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

En caso que, un PCSC de CONFIRMA S.A, deje de operar deberá cumplir, como mínimo, con lo siguiente:

a) Solicitar a la AC Raíz-Py, con al menos un mes de anticipación la cancelación de sus suscripción en el registro público de PCSCs, comunicándole el destino que dará a los datos de los certificados, especificando, en su caso, los que va a transferir y a quién, cuando proceda;

b) Notificar a sus titulares o responsables de certificados por él emitidos, con al menos un mes de anticipación antes de la suspensión efectiva o cese de sus operaciones;

c) Publicar en su sitio principal de Internet la fecha de suspensión de los servicios con al menos un mes de anticipación;

d) Publicar la fecha de suspensión de sus servicios por el plazo de 3 días consecutivos en un diario de gran circulación, 10 días hábiles antes de la suspensión efectiva o cese de las operaciones;

e) Preservar toda la información en concordancia con esta DPC y la normativa aplicable; y

f) Proceder a la eliminación y destrucción de la clave privada mediante un mecanismo que impida su reconstrucción.

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

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

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

6. CONTROLES TÉCNICOS DE SEGURIDAD

En este apartado se definen las medidas de seguridad implementadas por el PCSC CONFIRMA S.A. para proteger sus claves criptográficas y sus datos de activación, así como las claves criptográficas de los titulares de certificado. También serán definidos otros controles técnicos de seguridad utilizados por el PCSC y por las ARs a ella vinculadas para la ejecución de sus funciones operacionales.

Se emplean sistemas y productos fiables, protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

6.1.1. GENERACIÓN DEL PAR DE CLAVES

El par de claves criptográficas del PCSC CONFIRMA S.A. fue generado por el propio personal, de acuerdo al procedimiento establecido en el documento Ceremonia de generación de claves, posterior a la habilitación otorgada por el MIC vía resolución ministerial. El par de claves criptográficas se generan y almacenan en módulos de hardware criptográficos con certificación FIPS 140-2 Nivel 3. Se garantiza que la clave privada de firma nunca permanecerá fuera del módulo donde fue generada, a menos que se almacene en un mecanismo de recuperación de claves.

El par de claves es generado solamente por el titular del certificado correspondiente. Los procedimientos específicos son descritos en su PC implementada.

6.1.2. ENTREGA DE LA CLAVE PRIVADA AL TITULAR

El método de entrega de la clave privada al titular de certificado será establecido de acuerdo a cada tipo de certificado emitido por el PCSC y descripto en la PC correspondiente.

6.1.3. ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

La clave pública generada bajo el control PCSC CONFIRMA S.A. es entregada a la AC Raíz mediante el envío de una solicitud de FIRMA de certificado (CSR) que concuerda con la especificación del PKCS#10, firmado electrónicamente con la clave privada correspondiente a la clave pública que se solicita certificar. Para la generación del CSR mencionado, se adopta el formato definido en el documento DOC-ICPP-06 [5].

La clave pública generada bajo control del usuario final se entrega a través de un intercambio en línea utilizando funciones automáticas del software de certificación de CONFIRMA S.A..

6.1.4. ENTREGA DE LA CLAVE PÚBLICA DEL PCSC A LA PARTE USUARIA

Las formas para la disponibilización del certificado del PCSC CONFIRMA S.A., y de todos los certificados de la cadena de certificación, para los usuarios y las partes que confían de la ICPP, comprenden, entre otras:

a) En el momento de disponibilización de un certificado para su titular, usando el formato definido en el documento, DOC-ICPP-06 [5];

b) Un directorio;

c) Una página WEB del PCSC; y

d) Otros medios seguros aprobados por la AA

6.1.5. TAMAÑO DE LA CLAVE

Cada PC implementada por el PCSC CONFIRMA S.A. definirá el tamaño de las claves criptográficas asociadas a los certificados emitidos, en base a los requerimientos aplicables establecidos en el documento *DOC-ICPP-06 [5]*.

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

Los parámetros de generación de claves asimétricas del PCSC de CONFRIMA S.A. adoptarán el estándar definido en el documento *DOC-ICPP-06 [5]*.

Los parámetros de verificación de calidad, son verificados de acuerdo de acuerdo con las normas establecidas en el documento *DOC-ICPP-06 [5]*.

6.1.7. PROPÓSITOS DE USOS DE LA CLAVE (CAMPO KEY USAGE X.509V3)

Los propósitos para los cuales podrán ser utilizadas las claves criptográficas de los titulares de los certificados emitidos por el PCSC CONFIRMA S.A., así como las posibles restricciones aplicables, de conformidad con los usos definidos para los certificados correspondientes, se especifican en la CP implementada.

La clave privada del PCSC CONFIRMA S.A. es utilizada únicamente para la firma de los certificados emitidos por ella y de sus LCR.

Los propósitos para los cuales podrán ser utilizadas las claves criptográficas de los titulares de los certificados emitidos por el PCSC CONFIRMA S.A. están designadas por el campo Key Usage el certificado.

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

Las claves privadas son cifradas en el envío del módulo que lo generó al medio utilizado para su almacenamiento.

Los requisitos aplicables para el módulo criptográfico utilizado para el almacenamiento de la clave privada de los Titulares de Certificados de CONFIRMA S.A.., se basan en lo definido en el documento DOC- ICPP-06 [5], los cuáles son los siguientes:

•Requisito obligatorio: Certificado por el MIC

• Estándares: FIPS 140-2 nivel 2 o nivel 1 (para certificados tipo F1).

FIPS 140-2 nivel 2 o nivel 3 (para certificados tipo F2). FIPS 140-2 nivel 3 (para certificados tipo F2, F3).

6.2.1. ESTÁNDARES Y CONTROLES DEL MÓDULO CRIPTOGRÁFICO

Los módulos criptográficos de generación de claves asimétricas del PCSC CONFIRMA S.A. adoptará las normas definidas en el documento *DOC-ICPP-06 [5]*.

6.2.2. CONTROL MULTI-PERSONA DE CLAVE PRIVADA

El control multi-persona garantiza que nadie tenga el control de forma individual y completa de las actuaciones críticas. Para la llave privada de CONFIRMA S.A., serán requeridos 2 (dos) de 4 (cuatro) titulares de activación de clave.

Para certificados de usuario final, este ítem no es aplicable.

6.2.3. CUSTODIA (ESCROW) DE LA CLAVE PRIVADA

Para los certificados tipo F1, F2, están bajo custodia del titular de los mismos, y éste será el responsable de mantenerla bajo su exclusivo control.

Para certificados de tipo F3:

No se permite la recuperación de claves privadas, es decir, no se permite que terceros obtengan legalmente una clave privada sin el consentimiento de su titular.

El almacenamiento y posterior uso en el ámbito de firma centralizada, utiliza exclusivamente dispositivos certificados y homologados por la DGCE.

Además, CONFRIMA S.A. pone a disposición de los suscriptores, mecanismos adecuados para garantizar que el firmante tiene el control exclusivo del uso de sus datos de creación de la firma electrónica y que la utilización del dispositivo cumple los requisitos de la firma electrónica cualificada.

6.2.4. RESPALDO/COPIA DE LA CLAVE PRIVADA

Como directriz general de la DPC del PCSC CONFIRMA S.A. cualquier persona física o jurídica, titular de certificado, podrá, a su criterio, mantener una copia de seguridad de su propia clave privada.

El PCSC CONFIRMA S.A. mantiene una copia de seguridad de su propia clave privada.

El PCSC CONFIRMA S.A. responsable de esta DPC no podrá almacenar, ni mantener una copia de seguridad, por sí o a través de un tercero, la clave privada del titular de un certificado emitido, salvo en caso de su gestión en nombre del firmante o del creador del sello. Cada PC deberá definir los requisitos específicos aplicables.

En cualquier caso, la copia de seguridad deberá ser almacenada cifrada por un algoritmo simétrico definido en el documento *DOC-ICPP-06 [5]*y protegida con un nivel de seguridad no inferior a aquel definido para la clave original.

CONFIRMA S.A. realiza copia de seguridad de las claves privadas de las AC que hacen posible su recuperación en caso de desastre, de pérdida o deterioro de estas. Tanto la generación de la copia como la recuperación de ésta necesitan al menos de la participación de dos personas.
Claves generadas en archivo p12 no se puede realizar backups de las claves, ya que no dispone de acceso a las mismas. El firmante sí que puede realizar un backup.
Claves generadas en dispositivo seguro de creación de firma: No es posible realizar backups de las claves, ya que no es posible su

exportación. Si estas se encuentran en un HSM, es posible realizar backups de un bloob cifrado con la clave Security World del HSM utilizado, siendo imposible su descifrado sin el uso de las credenciales que sólo el titular del certificado conoce.

6.2.5. *ARCHIVADO DE LA CLAVE PRIVADA*

Las claves privadas de personas físicas titulares de certificados emitidos por el PCSC CONFIRMA S.A. no podrán ser archivadas.

Las claves privadas del PCSC CONFIRMA S.A. son archivadas por un periodo de 10 años después de la emisión del último certificado. Se almacenarán en archivos ignífugos seguros y en el centro de custodia externo. Al menos será necesaria la colaboración de dos personas para recuperar la clave privada de las AC en el dispositivo criptográfico inicial.

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

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

La transferencia de la clave privada de la AC sólo se puede hacer entre módulos criptográficos y requiere de la intervención de personal con rol de confianza. Solo podra ser transferida, en caso de transporte sujeto a los mismos procedimientos empleados para la generación de la clave original. Para este fin se utilizará la RFC 4210 o 6712.

6.2.7. *ALMACENAMIENTO DE LA CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO*

Conforme al Ítem 6.1.

6.2.8. MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

La clave privada del PCSC CONFIRMA S.A. se activa mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por las personas indicadas en la sección 6.2.2.

Cada PC implementada por el PCSC CONFIRMA S.A. describe los requisitos y los procedimientos necesarios para la activación de la clave privada del titular de certificado

6.2.9. MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

El procedimiento de desactivación de la clave privada del PCSC CONFIRMA S.A. es realizado unicamente por el personal con rol de confianza asignado y con control multipersona mediante la parada de la aplicación de la AC.

Cada PC implementada por el PCSC CONFIRMA S.A. describe los requisitos y procedimientos necesarios para la desactivación de la clave privada de la entidad titular de certificado.

6.2.10. MÉTODO DE DESTRUCCIÓN DE CLAVE PRIVADA

El procedimiento de destrucción de clave privada, en el caso de la AC, debe estar documentado y realizado por personal con rol de confianza con control multi persona. El medio de almacenamiento de clave privada se restablece a los valores predeterminados para que no quede información confidencial.

La destrucción de la clave privada debe constar en los registros de auditoría.

Los procedimientos necesarios para la destrucción de la clave privada de la persona física o jurídica y de sus copias de seguridad si las hubiere, es responsabilidad del titular del certificado.

La destrucción se puede realizar de las siguientes formas:

- Destrucción física.
- Sobreescritura.
- Eliminación de los medios de almacenamiento: mediante el uso de un factor de seguridad (contraseñas).

6.3. OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES

6.3.1. *ARCHIVO DE LA CLAVE PÚBLICA*

Las claves públicas del PCSC CONFIRMA S.A. y de los titulares de los certificados, así como las LCRs emitidas y sistemas de OCSP, serán almacenadas y gestionadas por el PCSC emisor, después de la expiración de los certificados correspondientes por un periodo de 10 (diez) años desde su última emisión, para la verificación de firmas generados durante su periodo de validez.

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

La clave privada del PCSC CONFIRMA S.A. responsable de la presente DPC y de los titulares de certificados de firma, tendrán un periodo operacional y periodo de uso conforme a la tabla N° 6 – Certificados emitidos en el marco de la ICPP del ítem 5.6 de este documento. Las correspondientes claves públicas podrán ser utilizadas durante todo el

periodo de tiempo determinado por la normativa vigente, para la verificación de firmas generados durante el plazo de validez de los respectivos certificados.

Cada PC implementada por el PCSC de CONFRIMA S.A. debe definir el periodo máximo de validez del certificado que define, con base a los requisitos aplicables establecidos en esta DPC y en el documento *DOC-ICPP-04 [1]*.

6.4. DATOS DE ACTIVACIÓN

En los siguientes ítems se describen los requerimientos generales de seguridad referentes a los datos de activación. Los datos de activación, son distintos al par de claves criptográficas y se definen como aquellas claves requeridas para la operación de algunos módulos criptográficos y necesitan estar protegidos. Cada PC implementada debe describir los requisitos específicos aplicables.

6.4.1. GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

El PCSC CONFIRMA S.A. mantiene estrictos controles de sus datos de activación para operar los módulos criptográficos conforme a lo establecido en el ítem 6.2.2.del presente documento. Además, se garantiza que los datos de activación de la clave privada del PCSC son únicos.

Cada PC implementada por el PCSC CONFIRMA S.A. garantiza que los datos de activación de la clave privada del titular del certificado serán únicos.

6.4.2. PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

Solo el personal autorizado posee las tarjetas criptográficas con capacidad de activación de las claves privadas del PCSC CONFIRMA S.A., asimismo, conoce los PIN necesarios para su utilización. El número de identificación personal (PIN) es confidencial, personal e intransferible y es el parámetro que protege las claves privadas.

Los datos de activación de clave privada del PCSC CONFIRMA S.A.. están protegidos contra el uso no autorizado a través de encriptación y mecanismos de control de acceso físico

6.4.3. OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

Sin estipulaciones.

6.5. CONTROLES DE SEGURIDAD DEL COMPUTADOR

El PCSC CONFIRMA S.A. emplea sistemas fiables para ofrecer sus servicios de certificación. Realiza controles y auditorias informáticas a fin de establecer una gestión de sus activos informáticos adecuados con el nivel de seguridad requerido en la gestión de sistemas de certificación electrónica.

Respecto a la seguridad de la información, el PCSC CONFIRMA S.A. aplica los controles del esquema de certificación sobre sistemas de gestión de la información ISO 27001.

6.5.1. REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS

La generación del par de claves del PCSC CONFIRMA S.A. será realizada offline para impedir el acceso remoto no autorizado.

Cada computador del PCSC CONFIRMA S.A. y AR vinculada, relacionado directamente con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados, implemetará, entre otras, las siguientes características:

a) Control de acceso a los servicios y perfiles del PCSC;

b) Clara segregación de tareas y atribuciones relacionadas con cada rol de confianza del PCSC;

c) Uso de criptografía para seguridad de base de datos, cuando sea requerido por la clasificación de su información;

d) Generación y almacenamiento de registros de auditoría del PCSC;

e) Mecanismos internos de seguridad para garantizar la integridad de datos y procesos críticos; y

f) Mecanismos para copias de seguridad (*backup*).

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

Cualquier equipo o parte del mismo, para ser sometidos a mantenimiento deberán haber borrado la información confidencial que contenga y

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

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

6.5.2. CLASIFICACIÓN DE LA SEGURIDAD DEL COMPUTADOR

En este apartado de la DPC del PCSC CONFIRMA S.A., debe ser informado, cuando esté disponible, la calificación atribuida a la seguridad computacional del PCSC responsable, de acuerdo con criterios tales como: *Trusted System Evaluation Criteria* (TCSEC), *Canadian Trusted Products Evaluation Criteria*, *European Information Technology Security Evaluation Criteria* (ITSEC) o *Common Criteria*.

6.5.3. CONTROLES DE SEGURIDAD PARA LAS AUTORIDADES DE REGISTRO

Las estaciones de trabajo y de las computadoras portátiles utilizados en los procesos de validación y verificación de certificados en una AR vinculada al PCSC CONFIRMA S.A. cumple con los requisitos de seguridad computacional especificados en el documento. *DOC-ICPP-05 [4]*.

6.6. CONTROLES TÉCNICOS DEL CICLO DE VIDA

En los ítems son descriptos, cuando sea aplicable, los controles implementados por el PCSC de CONFIRMA S.A y por las ARs a ella vinculada en el desarrollo de sistemas y en la gestión de la 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. desarrolla las actividades precisas para la formación y concienciación de los empleados en materia de seguridad. Los materiales empleados para la formación y los documentos descriptivos de los procesos son actualizados después de su aprobación por un grupo para la gestión de la seguridad. En la realización de esta función dispone de un plan de formación anual.

El PCSC CONFIRMA S.A. exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de servicios electrónicos de certificación.

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

6.6.3. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

DPC del PCSC CONFIRMA S.A. debe informar, cuando esté disponible, el nivel de madurez asignado al ciclo de vida de cada sistema, basado en criterios tales como: *Trusted Software Development Methodology* (TSDM)

o el *Capability Maturity Model* do *Software Engineering Institute* (CMM-SEI).

6.6.4. CONTROLES EN LA GENERACION DE LA LCR

Antes de su publicación, todas las LCR generadas por el PCSC CONFIRMA S.A., deben ser comprobadas en cuanto a la consistencia de su contenido, comparándolo con el contenido esperado en relación al número de LCR, la fecha/hora de emisión y otras informaciones relevantes.

6.7. CONTROLES DE SEGURIDAD DE RED

El PCSC CONFIRMA S.A. protege el acceso físico a los dispositivos de gestión de red, y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad, creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos.

La información confidencial que se trasfiere por redes no seguras se realiza de forma cifrada mediante uso de protocolos SSL o del sistema VPN con autenticación por doble factor.

6.7.1. DIRECTRICES GENERALES

A continuación se decriben las directrices generales correspondientes a la seguridad de red de la AC de CONFIRMA S.A. S.A., incluidos firewalls y recursos similares.

En los servidores del sistema de certificación del PCSC CONFIRMA S.A. sólo los servicios estrictamente necesarios para el funcionamiento de la aplicación está habilitados.

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

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

El acceso lógico a los elementos de la infraestructura y protección de la reed están restringidos por medio de un sistema de autenticación y autorización de acceso. Los ruteadores (routers) conectados a redes externas implementan filtros de paquetes de datos, que sólo permitan conexiones a los servicios y servidores previamente definidos como objeto de acceso externo.

6.7.2. FIREWALL

Los Mecanismos de firewall se implementan en equipos de uso específico, configurados exclusivamente para esa función. Un firewall promueve el aislamiento, en subredes específicas, de los equipos servidores con acceso externo - la denominada "zona desmilitarizada" (DMZ) - en relación a los equipos con acceso exclusivamente interno al PCSC CONFIRMA S.A.

El software de firewall, entre otras características, implementa registros de auditoría.

6.7.3. SISTEMA DE DETECCIÓN DE INTRUSOS (IDS)

El sistema de detección de intrusos del PCSC CONFIRMA S.A. esta configurado a modo de reconocer ataques en tiempo real y responder automáticamente, con medidas tales como: enviar traps SNMP, ejecutar programas definidos por la administración de la red, enviar e-mail a los administradores, enviar mensajes de alerta al firewall o al terminal de gerenciamiento, promover la desconexión automática de conexiones sospechosas, o incluso la reconfiguración del firewall.

El IDS es capaz de reconocer diferentes patrones de ataques, incluso contra el propio sistema, con la posibilidad de actualizar su base de reconocimiento.

El IDS provee un registro de los eventos en logs, recuperables en archivos de tipo texto, e implementa una gestión de la configuración.

6.7.4. REGISTRO DE ACCESO NO AUTORIZADO A LA RED

Las tentativas de acceso no autorizado en ruteadores, Firewall o IDS, son registradas en archivos para posterior análisis, que podrá ser automatizada. La frecuencia de examen de los archivos de registro es, como mínimo, diario y todas las acciones tomadas como resultado de este examen son documentadas.

6.8. FUENTES DE TIEMPO

Todos los sistemas del PCSC CONFIRMA S.A. están sincronizados en fecha y hora utilizando una fuente confiable de tiempo ajustados a la fecha y hora oficial paraguaya.

7. PERFILES DE CERTIFICADOS, LCR Y OCSP

7.1. PERFIL DEL CERTIFICADO

Todos los certificados emitidos por el PCSC CONFIRMA S.A. se ajustan al formato definido por la norma ITU X.509 o ISO/IEC 9594-8, según el perfil establecido en RFC 5280.

7.1.1. NÚMERO DE VERSIÓN

Todos los certificados emitidos por el PCSC CONFIRMA S.A. implementan la versión 3 (tres).

7.1.2. EXTENSIONES DEL CERTIFICADO

La ICPP define como obligatorias las siguientes extensiones para los certificados del PCSC:

a)Identificador de la clave de la Autoridad Certificadora "*Authority Key Identifier*", no crítica: el campo *Key Identifier* debe contener el hash SHA-1 de la clave pública de la AC Raíz-Py que emite el certificado;

b) Identificador de la clave del la persona física o jurídica titular del certificado "*Subject Key Identifier*", no crítica: debe contener el hash SHA-1 de la clave pública del PCSC titular del certificado;

c) Uso de Claves "*Key Usage*", crítica: solamente los bits *KeyCertSign* y LC*RSign* deben estar activados;

d) Directivas del Certificado "*Certificate Policies*", no crítica:

d.1.1) el campo ***policyIdentifier*** debe contener los OIDs de las PCs implementadas por el PCSC titular del certificado, para la emisión de

certificados de personas físicas o jurídicas;
d.1.2) el campo **policyQualifiers**

d.1.2.1 el campo ***CPS Pointer*** debe contener la dirección web de la DPC del PCSC que emite el certificado.

d.1.2.2 el campo User Notice debe decir: "Sujeta a las condiciones de uso expuestas en la Declaración de Prácticas de Certificación de CONFIRMA S.A.

e) Restricciones Básicas "*Basic Constraints*", crítica:
e.1 el campo ***Subject Type*** debe contener AC=True
e.2 el campo ***PathLenConstraint*** debe tener valor cero;

f) Puntos de distribución de las LCR "CRL Distribution Points", no crítica:
f.1 el campo ***Distribution Point 1*** debe contener la dirección web donde se obtiene la LCR correspondiente al certificado.

g) Acceso a la Información de la Autoridad Certificadora "Authority Information Access", no crítica:

g.1.1 en el campo ***Access Method 1*** debe contener el identificador de método de acceso a la información de revocación (OCSP)
g.1.2 en el campo ***Access Location 1*** debe contener la dirección Web del servicio del OCSP

g.2.1 en el campo ***Access Method 2*** debe contener el identificador de método de acceso del certificado de la AC Raiz-Py

g.2.2 en el campo ***Access Location 2*** debe contener la dirección web donde se encuentra alojado el certificado de la AC Raiz-Py

7.1.3. IDENTIFICADORES DE OBJETO DE ALGORÍTMOS

Los certificados del PCSC CONFIRMA S.A. son firmados utilizando el algoritmo definido en el documento *DOC-ICPP-06 [5]*.

7.1.4. 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:

a) **OID=2.5.4.6 C= PY**;

b) **OID=2.5.4.10 O= Prestador Cualificado de Servicios de Confianza**;
c) **OID=2.5.4.11 OU= [***CONFIRMA S.A.***]**;

d) **OID: 2.5.4.3 CN= [***siglas* **CA – COMFIRMA S.A.]**; y

e) **OID: 2.5.4.5 Serial Number[** *80113823-0***]**.

7.1.5. RESTRICCIONES DEL NOMBRE

Las restricciones de nombres aplicadas por el PCSC CONFIRMA S.A. estan conforme con las restricciones generales establecidas por la ICPP en el documento *DOC-ICPP-04 [1]*.

7.1.6. OID (OBJECT IDENTIFIER) DE LA DPC

Los OID asignados a las políticas de certificación contenidas en este documento se indican en el apartado 1.2.

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

Este Ítem no aplica.

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

En los certificados del PCSC CONFIRMA S.A. , el campo ***policyQualifiers*** de la extensión "***Certificate Policies***" contienen la dirección web (URL) de la DPC y PC Aplicables.

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

Las extensiones críticas deben interpretarse de acuerdo con RFC 5280.

7.2. PERFIL DE LA LCR

Los Listas de Certificados Revocados LCR son firmados utilizando el algoritmo definido en el documento *DOC-ICPP-06 [5]*.

7.2.1. NÚMERO (S) DE VERSIÓN

Las LCRs generadas por el PCSC CONFIRMA S.A. deberán implementar la versión 2 del estándar ITU X.509, de acuerdo con el perfil establecido en el RFC 5280.

7.2.2. LCR Y EXTENSIONES DE ENTRADAS DE LCR

A continuación se describen todas las extensiones de LCR utilizadas por el PCSC CONFIRMA S.A. y su criticidad.

La AC Raíz-Py define las siguientes extensiones de LCR como obligatorias:

a) **Identificador de la clave de la Autoridad Certificadora *"Authority Key Identifier" no crítico:*** debe contener el hash SHA-1 de la clave pública del PCSC que firma la LCR;

b) ***Número de LCR "CRL Number" no crítico**:* debe contener un número secuencial para cada LCR emitida por el PCSC; y

c) **Puntos de Distribución del Emisor "Issuing Distribution Point" crítico:** debe contener la dirección Web donde se obtiene la LCR correspondiente al certificado.

7.3. PERFIL DE OCSP

Los servicios de respuestas OCSP deberán implementar la versión 1 de la norma ITU X.509 de acuerdo con el perfil establecido en el RFC 6960. Los mismos deben ser firmados o sellados utilizando el algoritmo definido en el documento *DOC-ICPP-06 [5]*.

7.3.1. NÚMERO (S) DE VERSIÓN

Los servicios de respuesta OCSP deben implementar la versión 1 del estándar ITU X.509, según el perfil establecido en RFC 6960.

7.3.2. EXTENSIONES DE OCSP

De conformidad RFC 6960.

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

8.1. FRECUENCIA O CIRCUNSTANCIAS DE EVALUACIÓN

Se llevará a cabo una auditoría externa sobre sobre el PSC de CONFIRMA S.A. al menos cada veinticuatro (24) meses, corriendo con los gastos que ello genere, por un OEC. La finalidad de la auditoría es confirmar que tanto los PCSC, como los servicios de confianza cualificados que prestan cumplen con los requisitos establecidos en esta DPC y en la normativa vigente. Los PCSC enviarán el informe de evaluación de la conformidad correspondiente a la AC Raíz-Py en el plazo de 3 (tres) días hábiles tras su recepción.

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

Además PCSC CONFIRMA S.A.deberá implementar un programa de auditorías internas conforme a lo estipulado en el ítem 18 "cumplimiento" de la norma ISO 27002 para la verificación de su sistema de gestión.

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

La AC Raíz-Py comunicará al PCSC la retirada de su cualificación o de la cualificación del servicio de que se trate.

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

El PCSC CONFIRMA S.A. 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

El equipo de Auditoría Interna del PCSC CONFIRMA S.A. está conformado por personal calificado con experiencia en tecnología de la información, seguridad, tecnología de PKI y criptografía.
Las auditorías externas son realizadas por una firma de auditoría independiente externa que demuestra competencia técnica y experiencia en seguridad informática, en seguridad de sistemas de información y en auditorías de conformidad de servicios de certificación de clave pública, y los elementos relacionados.

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 *DOC- ICPP-11 [6]* para la recepción del informe de evaluación de la conformidad y respecto a las disposiciones en materia de auditoría con arreglo a las cuales los OEC realizarán la evaluación de la conformidad de los PCSC se regirán conforme al *DOC- ICPP-12 [7]* Criterios y procedimientos para realización de auditorías en las entidades miembros de la ICPP.

Las empresas de auditoría son de reconocido prestigio con departamentos especializados en la realización de auditorías informáticas, por lo que no existe ningún conflicto de intereses que pueda desvirtuar su actuación.

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, PC, PSS y demás normas y procedimientos establecidos por ICPP.

El PCSC CONFIRMA S.A. informa que ha recibido una auditoría previa por parte del OEC para fines de habilitación por parte de la AC Raíz-Py y que es auditado al menos cada veinticuatro (24) meses, con el objetivo de mantener la habilitación con base en lo establecido en los Criterios y procedimientos para realización de auditorías en las entidades miembros de la ICPP *DOC- ICPP-12 [7]*. Este documento aborda el objetivo, la frecuencia y el alcance de las auditorías, la identidad y las calificaciones del auditor y otros temas relacionados.

CONFIRMA S.A. debe informar que las entidades del ICPP directamente vinculados él (AV, AR y PSS), también recibieron una auditoría previa, por parte del OEC para fines de habilitación por parte de la AC Raíz-Py, y que es auditado conforme a lo establecido en el párrafo anterior.

Los aspectos cubiertos por la Auditoría son:

a) Controles de seguridad física y estándares técnicos de seguridad;

b) Confidencialidad y calidad de los sistemas de control;

c) Integridad y disponibilidad de los datos;

d) Cumplimiento de los estándares tecnológicos;

e) Seguridad del personal;

f) Cumplimiento de la política y declaración de prácticas de certificación;

g) Procesos de certificación de clave pública;

h) Política de seguridad y privacidad;

i) Controles administrativos del PCSC;

j) Administración de los servicios del PCSC; y

k) Revisión de contratos.

8.5. ACCIONES TOMADAS COMO RESULTADO DE UNA DEFICIENCIA

De acuerdo con los Criterios y procedimientos para la inspección de los miembros de las entidades de la ICPP *DOC- ICPP-17 [3]*) y con los Criterios y procedimientos para realización de auditorías en las entidades miembros de la ICPP *DOC- ICPP-12 [7]*).

8.6. COMUNICACIÓN DE RESULTADOS

De acuerdo con los Criterios y procedimientos para la inspección de los miembros de las entidades de la ICPP *DOC- ICPP-14 [8]*) y con los Criterios y procedimientos para realización de auditorías en las entidades miembros de la ICPP *DOC- ICPP-12 [7])*.

9. OTROS ASUNTOS LEGALES Y COMERCIALES

9.1. TARIFAS

EL PCSC CONFIRMA S.A. deberá comunicar al interesado en adquirir un certificado, todos los costos que deberá asumir para la obtención del certificado.

En todos los casos de incumplimiento de pago por parte del suscriptor, el PCSC CONFIRMA S.A.., podrá atribuirse el derecho a la revocación del certificado emitido.

9.1.1. *TARIFAS DE EMISIÓN Y ADMINISTRACIÓN DE CERTIFICADOS*

Los certificados emitidos bajo la presente DPC son expedidos a favor de personas físicas y de personas jurídicas, aplicándose aranceles diferenciales asociados conforme a la clase de certificado.

Las tarifas para la emisión y renovación de certificados por la AC Raíz-Py de la ICPP para los PCSC estarán definidas conforme al documento Directrices de la Política Tarifaria de la AC Raíz-Py de la ICPP.

9.1.2. *TARIFAS DE ACCESO A CERTIFICADOS*

Este ítem no aplica.

9.1.3. *TARIFAS DE ACCESO A INFORMACIÓN DEL ESTADO O REVOCACIÓN*

No hay tarifa de revocación ni de acceso a la información del estado del certificado.

9.1.4. *TARIFAS POR OTROS SERVICIOS*

Este ítem no aplica.

9.1.5. *POLÍTICAS DE REEMBOLSO*

En el caso de que alguna Política de Certificación especifique alguna tarifa aplicable a la prestación de servicios de certificación o revocación por parte del PCSC CONFIRMA S.A. para el tipo de certificados que defina, será obligado determinar la política de reembolso correspondiente.

9.2. RESPONSABILIDAD FINANCIERA

9.2.1. *COBERTURA DE SEGURO*

El PCSC CONFIRMA S.A. cuenta con un medio de garantía suficiente para cubrir las actividades inherentes a su gestión de conformidad con lo establecido en la normativa vigente.

9.2.2. *OTROS ACTIVOS*

Este ítem no aplica.

9.2.3. *COBERTURA DE SEGURO O GARANTÍA PARA LAS PERSONAS FÍSICAS TITULARES DE CERTIFICADOS*

El PCSC CONFIRMA S.A cuenta con cobertura de un seguro, según lo exigido Art. 10 inciso 3 b) Ley Nro 6822 /21, para las personas física titulares de certificados.

9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

9.3.1. *ALCANCE DE LA INFORMACIÓN CONFIDENCIAL*

Durante el ciclo de vida del certificado, tanto el PCSC CONFIRMA SA como la AR vinculada establecen, como principio general, que ningún documento, información o registro deberán ser divulgados.

9.3.2. *INFORMACIÓN NO CONTENIDA EN EL ALCANCE DE INFORMACIÓN CONFIDENCIAL*

Los tipos de informaciones consideradas NO confidenciales por el PCSC CONFIRMA S.A. y por las AR y AV a ellas vinculadas, los cuales comprenden:

a) Los certificados y las LCRs/OCSPs emitidos por el PCSC;

b) Las PCs implementadas por el PCSC;

c) La DPC del PCSC;y

d) La conclusión de los informes de auditoría.

e) Versión pública de la Política de Seguridad.

Los Certificados, LCR/OCSP y la información corporativa o personal que necesariamente forme parte de ellos o de directorios públicos se consideran información no confidencial.

El PCSC también podrá divulgar, de forma consolidada o segmentada por tipo de certificado, el número de certificados emitidos en el ámbito de ICPP.

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 del PCSC responsable de la DPC será generada y mantenida por el propio PCSC, quien será responsable de su secreto. La divulgación o el uso indebido de la clave privada por parte del PCSC será de su exclusiva responsabilidad.

Se deberá informar que los titulares de certificados de firma electrónica cualificada, tributario, tendrán la tarea de generar y mantener la confidencialidad de sus respectivas claves privadas. Además, son responsables de la divulgación o uso indebido de estas mismas claves.

CONFIRMA S.A. para brindar servicios **DE GENERACIÓN O GESTIÓN DE DATOS DE CREACIÓN DE FIRMA ELECTRÓNICA**, utiliza sistemas y productos fiables, incluidos canales de comunicación electrónicos seguros, procedimientos y mecanismos técnicos y organizativos adecuados que garantizan un entorno confiable y los datos de creación de firma se utilizan bajo el control exclusivo del titular del certificado. Además, CONFIRMA S.A.. custodia y protege los datos de creación de firma frente a cualquiera alteración, destrucción o acceso no autorizado, así como garantiza su continua disponibilidad.

9.4. PRIVACIDAD DE INFORMACIÓN PERSONAL

9.4.1. PLAN DE PRIVACIDAD

El PCSC CONFIRMA S.A.. implementa políticas de privacidad de información, de acuerdo con la normativa vigente. No se puede divulgar

o vender información de los suscriptores o información de identificación de éstos.

9.4.2. *INFORMACIÓN TRATADA COMO PRIVADA*

Cualquier información acerca de de los titulares o responsables de certificados que no esté públicamente disponible a través del contenido del certificado emitido y servicios de LCR/OCSP debe ser tratada como información privada.

9.4.3. *INFORMACIÓN QUE NO ES CONSIDERADA COMO PRIVADA*

El tratamiento de la información que no es considerada como privada, estará sujeto a lo que dispone la normativa al efecto. Únicamente se considera pública la información contenida en el certificado y LCR/OCSP.

9.4.4. *RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA*

El PCSC CONFIRMA S.A. y AR vinculada son responsables de la divulgación indebida de información privada, por lo que deben asegurar que no pueda ser comprometida o divulgada a terceros.

9.4.5. *NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA*

La información privada obtenida por el PCSC 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 tendrán amplio acceso a cualquiera de sus propios datos e identificaciones, y podrán autorizar la divulgación de sus registros a otras personas.

La autorización formal se podrá formalizar:

a) Por medios electrónicos, conteniendo una firma 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*

Para divulgar información privada se requiere de una orden judicial o autoridad administrativa competente que así lo determine y se divulgará estrictamente la información solicitada.

9.4.7. *OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN*

Este ítem no aplica.

9.4.8. *INFORMACIÓN A TERCEROS*

Aplícase lo dispuesto en el ítem 9.4.5 de la DPC.

9.5. DERECHO DE PROPIEDAD INTELECTUAL

Según legislación vigente.

9.6. REPRESENTACIONES Y GARANTÍAS

9.6.1. REPRESENTACIONES Y GARANTÍAS DEL PCSC

El PCSC CONFIRMA S.A. en el marco de prestación de servicios de creación, verificación y validación de firmas electrónicas cualificadas y/o certificados relativos a estos servicios, responderá por el incumplimiento de lo establecido en las Políticas, Declaración de Prácticas de Certificación y en la normativa vigente. De igual manera asumirá toda la responsabilidad frente a terceros por la actuación de las personas en las que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de dichos servicios.

El PCSC declara y garantiza lo siguiente:

9.6.1.1. AUTORIZACIÓN PARA CERTIFICADO

El PCSC CONFIRMA S.A. Implementa procedimientos para verificar la autorización de emisión de un certificado en el marco de la ICPP, contenido en los ítems 3 y 4 de esta DPC. El PCSC, dentro del alcance de la autorización de emisión de un certificado, analiza, audita e inspecciona los procesos de la AR conforme a sus DPC, PCs y normas complementarias.

9.6.1.2. PRECISIÓN DE LA INFORMACIÓN

El PCSC de CONFIRMA S.A implementa procedimientos para verificar la veracidad de la información en los certificados, contenidos en los ítems 3 y 4 de esta DPC. A su vez, la AC Raíz-Py, la veracidad de la información contenida en los certificados que emite, analiza, audita e inspecciona los procesos del PCSC y AR conforme a sus DPC, PCs y normas complementarias.

9.6.1.3. IDENTIFICACIÓN DEL SOLICITANTE DE CERTIFICADO

El PCSC CONFIRMA S.A. implementa procedimientos para verificar la identificación de los solicitantes de certificados, contenidos en los ítems 3 y 4 de esta DPC. El PCSC, en el ámbito de la identificación del solicitante contenida en los certificados que emite, analiza, audita e inspecciona los procesos de la AR conforme sus DPC, PCs y normas complementarias.

9.6.1.4. CONSENTIMIENTO DE LOS TITULARES DE CERTIFICADO

El PCSC de CONFIRMA S.A implementa un contrato de prestación de servicio de confianza para la expresión del consentimiento del titular de certificado, de conformidad a lo establecido en los puntos 3 y 4 de esta DPC.

9.6.1.5. SERVICIO

El PCSC CONFIRMA S.A. mantiene acceso 24x7 a su repositorio con información sobre sus propios certificados, consulta de certificados emitidos y LCR/OCSP.

9.6.1.6. REVOCACIÓN

El PCSC CONFIRMA S.A. revocará los certificados en el marco de la ICPP por cualquier motivo conforme a lo establecido en el punto 4.9 de este documento.

9.6.1.7. EXISTENCIA LEGAL

El PCSC CONFIRMA S.A. indica que la DPC se ajusta a las disposiciones de la Ley No 6822/2021 sus modificaciones y reglamentaciones.

9.6.2. *REPRESENTACIONES Y GARANTÍAS DE LA RA*

Aplícase conforme al ítem 4 de esta DPC.

9.6.3. *REPRESENTACIONES Y GARANTÍAS DEL TITULAR DEL CERTIFICADO*

Toda la información necesaria para la identificación del titular o responsable del certificado debe proporcionarse de manera completa y precisa. Al aceptar un certificado emitido por el PCSC CONFIRMA S.A. el titular es responsable de toda la información proporcionada por él y contenida en ese certificado.

El PCSC debe informar a la AC Raíz-Py de cualquier compromiso de su clave privada y solicitar la revocación inmediata de su certificado.

9.6.4. *REPRESENTACIONES Y GARANTÍAS DE LAS PARTES USUARIAS*

Constituyen derechos de la parte usuaria

a) Negarse a utilizar el certificado para fines distintos de los previstos en esta DPC; y

b) Verificar, en cualquier momento, la vigencia del certificado.

El certificado del PCSC se considera válido cuando:

a) Ha sido emitido por la AC Raíz-Py;

b) No aparece como revocado por la AC Raíz-Py;

c) No ha expirado; y

d) Puede ser verificado utilizando el certificado válido de la AC Raíz-Py.

El uso o aceptación de certificados sin observar las medidas descriptas es por cuenta y riesgo de la parte usuaria, que usa o acepta la utilización del certificado respectivo.

9.6.5. *REPRESENTACIONES Y GARANTÍAS DE OTROS PARTICIPANTES*

Este ítem no aplica.

9.7. EXENCIÓN DE GARANTÍA

Este ítem no aplica.

9.8. LIMITACIONES DE RESPONSABILIDAD LEGAL

CONFIRMA S.A. como Prestador Cualificado de Servicios de Confianza limita su responsabilidad conforme a las disposiciones de la Ley Nro. 6822/2021, sus modificaciones y reglamentaciones.

9.9. INDEMNIZACIONES

El PCSC CONFIRMA S.A. se encuentra en conformidad a la norma vigente de las condiciones de aplicación y limitaciones considerando las responsabilidades de CONFIRMA S.A.

9.10. PLAZO Y FINALIZACIÓN

9.10.1. PLAZO

Esta DPC entra en vigencia a partir de la fecha establecida en el instrumento que la aprueba y expedido por la AC Raíz-Py.

9.10.2. FINALIZACIÓN

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

9.10.3. EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA

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

9.11. NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON PARTICIPANTES

Las notificaciones, citaciones, solicitudes o cualquier otra comunicación necesaria sujeta a las prácticas descritas en la presente DPC 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

Una vez que el PCSC CONFIRMA S.A. realice alguna enmienda a su DPC, se remite para su revisión y aprobación a 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, deberá ser publicada en el repositorio del PCSC.

9.12.3. CIRCUNSTANCIAS EN QUE LOS OID DEBEN SER CAMBIADOS

Si la estructura del certificado se mantiene entonces no es necesario cambiar los OIDs.

9.13. DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS

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

9.14. NORMATIVA APLICABLE

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

9.15. ADECUACIÓN A LA LEY APLICABLE

La presente DPC del PCSC CONFIRMA S.A. se adecua a la legislación aplicable y que el PCSC se compromete a cumplir y observar las disposiciones previstas en ella.

9.16. DISPOSICIONES VARIAS

9.16.1. ACUERDO COMPLETO

Los titulares y partes que confían en los certificados asumen en su totalidad el contenido de la presente DPC y PC.

La presente DPC representa las obligaciones y deberes aplicables al PCSC CONFIRMA S.A. y autoridades vinculadas.

En caso de conflicto entre esta DPC 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, no pueden ser cedidos ni transferidos a terceros.

9.16.3. DIVISIBILIDAD

La invalidez, nulidad o ineficacia de cualquiera de las disposiciones de esta DPC no perjudicará las demás disposiciones, que seguirán siendo plenamente válidas y efectivas. En este caso, la disposición inválida, nula o ineficaz se tendrá por no escrita, por lo que la presente DPC se interpretará como si no la contuviera y, en la medida de lo posible, manteniendo la intención original de las restantes disposiciones.

9.16.4. APLICACIÓN (HONORARIOS DE ABOGADOS Y RENUNCIA DE DERECHOS)

El PCSC CONFIRMA SA, aplica este item de acuerdo con la legislación vigente.

9.16.5. FUERZA MAYOR

Los contratos con los titulares de certificados emitidos por el PCSC CONFIRMA S.A. y esta DPC incluyen cláusulas de fuerza mayor para proteger al PCSC.

9.17. OTRAS DISPOSICIONES

Éste ítem no aplica.

10. DOCUMENTOS DE REFERENCIA

10.1. REFERENCIAS

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

- RFC 3647: "Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework".

- RFC 4210: "Internet X.509 Public Key Infrastructure. Certificate Management Protocol (CMP)".

- RFC 5280: "Internet X.509 Public Key Infrastructure.Certificate and Certificate Revocation List (LCR) Profile".

- RFC 6712: "Internet X.509 Public Key Infrastructure.HTTP Transfer for the Certificate Management Protocol (CMP)".

- RFC 6960: "X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP".

- ISO 27002:2022:" - Information technology - Security techniques - Code of practice for information security management".

- ITU X.500/ISO 9594: "Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services".

- ITU X.509/ISO/IEC9594-8:"- Information technology - Open Systems Interconnection - The Directory - Part 8: Public-key and attribute certificate frameworks".