DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA VIT S.A.

DOC-DPC-VIT S.A.

Versión 1.0

Documento: DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (DPC) de VIT S.A
Versión: 1.0
Razón Social: VIT S.A
Marca Comercial: eFirma
Referencia de la DPC / OID de la DPC: 1.3.6.1.4.1.44234.1.1.1.1
Estado del Documento: 05 de agosto de 2022
Fecha de emisión: 05 de agosto de 2022
Sitio de internet oficial: https://www.efirma.com.py
URL del documento: https://www.efirma.com.py/repositorio/DOC-DPC-VIT S.A. Vers 1.0.pdf
Clasificación: PÚBLICO
Archivo: DOC-DPC-VIT S.A. Vers 1.0.docx
Nº de páginas: 103
Preparado por: VIT S.A.

CONTROL DOCUMENTAL

Documento	
Título: DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DEL PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA DE VIT S.A.	**Nombre Archivo:** DOC-DPC-VIT S.A. Vers1.0
Código: DOC-DPC-VIT S.A.	**Soporte Lógico:** https://www.efirma.com.py/
Fecha: 05/08/2022	**Versión:** 1.0

Registro de cambios		
Versión	**Fecha**	**Motivo de cambio**
1.0	05/08/2022	Versión inicial

Distribución del documento	
Nombre	**Área**
Ministerio de Industria y Comercio (MIC)	Dirección General de Comercio Electrónico (DGCE)
VIT S.A. (PCSC)	DIRECTORIO GERENCIAL
Documento Público	https://www.efirma.com.py/

Control del documento	
Elaborado por: ***WALTER CORREA***	
Elaborado por: ***ALEJANDRO TORALES***	
Verificado por: ***RAQUEL VILLALBA***	
Aprobado por: ***JOSE LUIS CASTILLO***	

Contenido

1. INTRODUCCIÓN

1.1. DESCRIPCIÓN GENERAL

El presente documento contiene la **Declaración de Prácticas de Certificación (DPC) de VIT S.A.**

VIT S.A. es un Prestador Cualificado de Servicios de Confianza, entidad habilitada ante la Autoridad de Aplicación establecida por Ley en Paraguay y encargada de operar la Autoridad Certificadora VIT S.A. en el marco de la ICP-Paraguay y la legislación correspondiente. La Autoridad Certificadora VIT S.A. está subordinada a la Autoridad Certificadora Raíz del Paraguay y presta servicios de emisión, gestión, revocación y otros servicios inherentes a la certificación electrónica cualificada, asumiendo también las funciones de Autoridad de Registro en el marco de la ICP-Paraguay.

La presente Declaración de Prácticas de Certificación constituye el compendio general de normas aplicables a toda actividad certificadora de VIT S.A. como Prestador Cualificado de Servicios de Confianza.

Sin embargo, las distintas especialidades aplicables a cada uno de los diferentes tipos de certificados que se emitan se establecen en las distintas Políticas de Certificación de cada tipo de certificado que, como normas complementarias y específicas, prevalecerán sobre la presente Declaración de Prácticas de Certificación en lo que se refiera a cada tipo de certificado.

En este documento se detallan las normas y condiciones generales de los servicios de certificación que presta VIT S.A. relacionadas, entre otros, con la gestión de los datos de los certificados, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados, y las medidas de seguridad técnicas y organizativas, y los mecanismos de resguardo y accesibilidad a la información relacionadas con la actividad de prestación de servicios de certificación.

Las presentes Prácticas de Certificación fueron elaboradas conforme a las recomendaciones establecidas en el RFC 3647 ‘’INTERNET X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework’’ propuesto por Network Working Group para este tipo de documentos, y tomando como base para las mismas el marco legal de aplicación en Paraguay y cumpliendo con las definiciones y exigencias de la Autoridad Certificadora Raíz del Paraguay. Esta Declaración de Prácticas de Certificación (DPC) de VIT S.A. junto a lo especificado en las Políticas de Certificación de cada tipo de certificado guarda concordancia con las disposiciones de la POLÍTICA DE CERTIFICACIÓN DE LA INFRAESTRUCTURA DE CLAVE PÚBLICA DEL PARAGUAY (ICPP).

1.2. NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

Documento: Declaración de Prácticas de Certificación (DPC) de VIT S.A.
Versión: 1.0
Estado: APROBADO
Fecha de emisión: 05 de Agosto del 2022
URL del documento: https://www.efirma.com.py/repositorio/
Sitio de internet oficial: https://www.efirma.com.py
Referencia de la DPC/ OID de la DPC: 1.3.6.1.4.1.44234.1.1.1.1

1.3. PARTICIPANTES DE LA ICPP

1.3.1. AUTORIDADES CERTIFICADORAS (AC)

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

- **Ministerio de Industria y Comercio (MIC):** en su carácter de Autoridad Certificadora Raíz del Paraguay (CA Raíz) o Autoridad de Certificación Raíz del Paraguay (CA Raíz), indistintamente; emite certificados a los PCSC bajo la jerarquía del Certificado Raíz, el cual es auto-firmado, y a partir de él se inicia la cadena de confianza.

Subordinados al certificado raíz, se encuentran:

- **Prestador Cualificado de Servicios de Confianza (PCSC) VIT S.A.:** en su carácter de Autoridad Certificadora Intermedia, es la persona jurídica que emite certificados digitales para personas físicas y/o jurídicas que permiten identificar a dichos titulares. El PCSC VIT S.A. se encuentra habilitado y cuenta con un certificado firmado y emitido por la CA Raíz con lo cual pasa a formar parte de la estructura y cadena de confianza de la ICP-Paraguay.

La información del **Certificado del PCSC VIT S.A.** es un certificado X.509 versión 3 firmado por la CA Raíz de Paraguay disponible en https://www.efirma.com.py/repositorio/, con:

- **C = PY**
- **O = ICPP**
- **OU = Prestador Cualificado de Servicios de Confianza**
- **CN = VIT S.A.**
- **SERIALNUMBER = RUC80080099-0**

1.3.2. AUTORIDADES DE REGISTRO (AR)

Entidad responsable de la identificación y autenticación de titulares de certificados digitales; la misma no emite ni firma certificados. Una AR interviene en el proceso de solicitud del certificado, en el proceso de revocación o en ambos. La AR, no necesita ser un organismo separado, sino que puede ser parte de la PCSC.

Las AR delegadas son autoridades de registro vinculadas a un PCSC mediante un contrato de prestación de servicios; el funcionamiento de las mismas deberá estar en conocimiento y autorizadas por la CA raíz.

El PCSC VIT S.A. suministra:
a) La lista de todas las AR del PCSC, con informaciones sobre las PC que implementan;

b) Para cada AR del PCSC, las direcciones de todas las instalaciones técnicas, autorizadas por la CA Raíz del Paraguay para funcionar;
c) Acuerdo operacionales celebrados entre un PCSC y una AR delegada.

La lista de Autoridades de Registro de VIT S.A. que gestionan las solicitudes de certificados definidos en esta política se encuentra disponible en la URL https://efirma.com.py/repositorio-publico-i30

d) La lista de todas las AR cuya habilitación fue revocada, con la indicación de la fecha de revocación.

El PCSC VIT S.A. mantiene las informaciones arriba citadas siempre actualizadas en la página https://efirma.com.py/repositorio-publico-i30

1.3.3. AUTORIDADES DE VALIDACIÓN (AV)

El PCSC VIT S.A. cuenta con una AV propia responsable de suministrar información sobre la vigencia de los certificados que a su vez hayan sido registrados por una AR y certificados por la Autoridad de Certificación.

El PCSC VIT S.A. mantiene las informaciones arriba citadas siempre actualizadas en la página web: https://efirma.com.py/va

1.3.4. TITULARES DEL CERTIFICADO

Podrán ser titulares de certificados cualificados de firma electrónica y certificados cualificados tributarios solo personas físicas. Los certificados citados son emitidos por el PCSC VIT S.A.

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 SERVICIOS DE SOPORTE (PSS)

Los PSS son entidades externas a las que recurre el PCSC VIT S.A 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) disponibilización de infraestructura física y lógica y de recursos humanos especializados.

El PCSC VIT S.A. mantiene las informaciones arriba citadas siempre actualizadas en la página web: www.efirma.com.py/repositorio-publico-i30

El PCSC VIT S.A. además mantiene actualizada y publicada información referente a:

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

1.4. USO DEL CERTIFICADO

1.4.1. USOS APROPIADOS DEL CERTIFICADO

Las *Políticas de Certificación correspondientes a cada tipo de certificado* emitido por VIT S.A. constituyen los documentos en los que se determinan los usos de cada tipo de certificado.

1.4.2. USOS PROHIBIDOS DEL CERTIFICADO

Los certificados emitidos deben ser utilizados conforme el marco de la normativa vigente que rige la materia, de la presente DPC y de la PC correspondientes a cada tipo de certificado.

1.5 ADMINISTRACIÓN DE LA POLÍTICA

1.5.1. ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

Nombre: VIT S.A.
RUC: 80080099-0
Dirección: España N° 2028 c/ Brasilia. 6to piso
Teléfono: 021-229-350
Dirección de correo electrónico: info@efirma.com.py
Página Web: https://www.efirma.com.py

1.5.2. PERSONA DE CONTACTO

Nombre: Raquel Villalba

Teléfono: 021-229-350

Dirección: España N° 2028 c/ Brasilia 6to piso

Fax:

Página web: https://www.efirma.com.py

E-mail: info@efirma.com.py

1.5.3. PERSONA QUE DETERMINA LA ADECUACIÓN DE LA DPC A LA PC

La entidad competente para determinar la adecuación de esta DPC a las diferentes Políticas de Certificación de VIT S.A. es el Directorio y el personal autorizado de VIT S.A. conforme con los Estatutos de la empresa.

Además, según establecido en la normativa vigente, el Director General de Firma Digital y Comercio Electrónico será el encargado de determinar la adecuación de la DPC del PCSC que forme parte de la ICP-Paraguay, en este caso de la DPC de VIT S.A.

1.5.4 PROCEDIMIENTOS DE APROBACIÓN DE LA DPC

El Directorio y el personal autorizado de VIT S.A., conforme con los Estatutos de la empresa, aprobarán el contenido de la DPC y sus posteriores enmiendas o modificaciones, y luego será puesta a consideración de la Dirección General de Firma Digital y Comercio Electrónico y autoridades pertinentes del Ministerio de Industria y Comercio para su aprobación.

1.6 DEFINICIONES, SIGLAS Y ACRÓNIMOS

1.6.1 DEFINICIONES

1. **VIT S.A:** Denominación de la Empresa, encargada del servicio de emisión y comercialización de certificados digitales.
2. **eFirma:** Marca Comercial utilizada para identificar los servicios de la empresa.
3. **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.
4. **Autenticación:** proceso técnico que permite determinar la identidad de la persona física o jurídica.
5. **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.
6. **Autoridad de Aplicación:** Ministerio de Industria y Comercioa través de la Dirección General de Comercio Electrónico, dependiente del Viceministerio de Comercio y Servicios.
7. **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.
8. **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.

9. **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.
10. **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.
11. **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.
12. **Gestión de datos de creación de firma:** El PCSC podrá, en nombre del firmante gestionar los datos de creación de firma a los que hayan prestado sus servicios, este servicio deberá ser provisto por un PCSC siempre y cuando cuente con la debida habilitación.
13. **Cadena de certificación:** lista ordenada de certificados que contiene un certificado del firmante y certificados de la AC, que termina en un certificado raíz. El emisor del certificado del firmante 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 o la parte usuaria debe verificar la validez de los certificados en la cadena de certificación.
14. **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.
15. **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.
16. **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.
17. **Cifrado asimétrico:** tipo de cifrado que utiliza un par de claves criptográficas diferentes (ejemplo: privado y público) y matemáticamente relacionadas.
18. **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.
19. **Claves criptográficas:** valor o código numérico que se utiliza con un algoritmo criptográfico para transformar, validar, autenticar, cifrar y descifrar datos.

20. **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.
21. **Compromiso:** violación de la seguridad de un sistema a raíz de una posible divulgación no autorizada de información sensible.
22. **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.
23. **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.
24. **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.
25. **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.
26. **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.
27. **Emisor del certificado:** persona física o jurídica cuyo nombre aparece en el campo emisor de un certificado.
28. **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.

29. **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.
30. **Firmante:** una persona física que crea una firma electrónica.
31. **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.
32. **Habilitación:** autorizaciónque otorga el MIC, una vez cumplidos los requisitos y condiciones establecidos en la norma.
33. **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.
34. **Identificación del Titular 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.
35. **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.
36. **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.
37. **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.
38. **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.

39. **Módulo criptográfico**: software o hardware criptográfico que genera y almacena claves criptográficas.
40. **Módulo de Seguridad de Hardware:** dispositivo basado en un módulo criptográfico tipo hardware que genera, almacena y protege claves criptográficas.
41. **Normas Internacionales:** requisitos de orden técnico y de uso internacional que deben observarse en la prestación de los servicios mencionados en la presente DPC.
42. **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.
43. **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.
44. **Parte usuaria:** persona física o jurídica que confía en el servicio de confianza.
45. **Perfil del certificado:** especificación del formato requerido para un tipo particular de certificado (incluyendo requisitos para el uso de los campos estándar y extensiones).
46. **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.
47. **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.
48. **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.
49. **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.
50. **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.
51. **Repositorio:** sitio principal de Internet confiable y accesible, mantenido por la AC con el fin de difundir su información pública.
52. **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.

53. **Servicio OCSP:** permite utilizar un protocolo estándar para realizar consultas en línea al servidor de la AC sobre el estado de un certificado.
54. **Solicitante de Certificado:** persona física o jurídica que solicita la emisión de un certificado a una AC.
55. **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.
56. **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.
57. **Solicitud de revocación**: documento que se instrumenta mediante un formato autorizado de solicitud para la revocación de un certificado.
58. **Verificación y validación de firma:** determinación y validación de que la firma electrónica fue creado durante el periodo operacional de un certificado válido, por la clave privada correspondiente a la clave pública que se encuentra en el certificado y que el mensaje no ha sido alterado desde que su creación.
59. **X.500:** estándar desarrollado por la ITU que define las recomendaciones del directorio. Da lugar ala serie de recomendaciones siguientes: X.501, X.509, X.511, X.518, X.519, X.520, X.521, X.525.
60. **X.509:** estándar desarrollado por la ITU, que define el formato electrónico básico para certificados electrónicos.

1.6.2 SIGLAS Y ACRÓNIMOS

Tabla Nº 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, CertificateAuthority)
ACI	Autoridad de Certificación Intermedia (CAI por sus siglas en inglés, CertificateAuthorityIntermediate)

AC Raíz-Py	Autoridad Certificadora Raíz del Paraguay
CI	Cédula de identidad civil
NC	Nombre Común (CN por sus siglas en inglés, CommonName)
PC	Políticas de Certificación (CP por sus siglas en inglés, CertificatePolicy)
DPC	Declaración de Prácticas de Certificación (DPC por sus siglas en inglés, CertificationPracticeStatement)
LCR	Lista de certificados revocados (CRL por sus siglas en inglés, CertificateRevocationList)
CSR	Solicitud de firma de Certificado (CSR por sus siglas en inglés, certificateSigningRequest)
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 OrganizationforStandardization).
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, ObjectIdentifier)
OU	Unidad Organizacional (OU por sus siglas en inglés, OrganizationUnit)
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, RegistrationAuthority).
RFC	Petición de Comentarios (RFC por sus siglas en inglés, RequestForComments)
RUC	Registro único del Contribuyente
UPS	Sistemas de alimentación ininterrumpida (UPS por sus siglas en inglés, uninterruptiblepowersupply)
URL	Localizador uniforme de recursos (URL por sus siglas en inglés, UniformResourceLocator).
AV	Autoridad de validación (VA por sus siglas en inglés, ValidationAuthority)

2. RESPONSABILIDADES DE PUBLICACIÓN Y DEL REPOSITORIO

2.1. REPOSITORIOS

El PCSC VIT S.A. dispone en su sitio principal un **Repositorio** público de información, en la dirección URL con protocolo seguro: https://www.efirma.com.py/repositorio/

El PCSC VIT S.A. es responsable de las funciones de su **Repositorio,** el servicio de **Repositorio** referido no contiene ninguna información de naturaleza confidencial.

La disponibilidad del repositorio se define conforme a lo dispuesto en el punto 2.2 de esta DPC.

El PCSC VIT S.A. cumple con las siguientes obligaciones:

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.

Los requisitos aplicables a los repositorios utilizados por el PCSC VIT S.A. se describen a continuación:

a) Localización física y lógica: El PCSC VIT S.A. cuenta con la localización física y lógica en la República del Paraguay, cito Avda. España 2028 c/ Avda. Brasilia.

b) Disponibilidad: La información se detalla en el punto 2.2. de esta DPC.

c) Protocolos de acceso: Se utiliza el protocolo seguro HTTPS**.**

d) Requisitos de seguridad: Se implementa protocolo de seguridad a nivel físico y lógico de red para el acceso al repositorio de la PCSC VIT S.A**.**

2.2 PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

El PCSC VIT S.A. mantiene un **Repositorio** público de internet que permite a las partes que confían verificar en línea la revocación de un Certificado y cualquier otra información necesaria para validar el estado del mismo. Se mantiene publicada, entre otros aspectos, 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;

Los cambios en las especificaciones o en las condiciones del servicio serán comunicados por VIT S.A. a los usuarios en la URL https://www.efirma.com.py

El servicio de publicación de información de la PCSC VIT S.A. deberá estar disponible durante las veinticuatro horas, los siete días de la semana. En caso de interrupción por causa de fuerza mayor, el

servicio se restablecerá en un plazo no mayor a veinticuatro horas, garantizando la disponibilidad del servicio con un mínimo de 99% anual y un tiempo programado de inactividad máximo de 0.5% anual.
La PCSC VIT S.A. dedicará sus mejores esfuerzos para que el servicio se restablezca y esté disponible rápidamente.

2.3 TIEMPO O FRECUENCIA DE PUBLICACIÓN

La actualización de la ***DPC***, ***Políticas de Certificación*** y del ***Contrato de Prestación de Servicios de Confianza*** serán publicadas cuando sufran modificaciones y sean aprobadas por las autoridades correspondientes.

La información de estados de certificados es publicada de acuerdo con lo dispuesto en el punto 4.9.7 de esta DPC.

Las demás informaciones mencionadas en el punto 2.2, serán actualizadas lo más pronto posible y con un máximo de un día hábil desde que se dispongan o surjan modificaciones.

2.4 CONTROLES DE ACCESO A LOS REPOSITORIOS

La información publicada en el **Repositorio** es accesible únicamente para consulta, siendo el acceso a lectura libre y gratuita. El PCSC VIT S.A. dispone de los mecanismos adecuados para garantizar la integridad de los datos publicados en el **Repositorio** y su fiabilidad.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. NOMBRES

3.1.1. TIPOS DE NOMBRES

Los tipos de nombres admitidos para los titulares de los certificados emitidos por el PCSC VIT S.A. responsable de la DPC. Entre los tipos de nombres considerados podrán estar el "distinguishedname" según lo establecido en la ITU X.500, la dirección de correo y la dirección de página web (URL).

3.1.2. NECESIDAD DE NOMBRES SIGNIFICATIVOS

Las reglas definidas correspondientes a cada tipo de suscriptor garantizan que los nombres distintivos (DN) de los certificados son suficientemente significativos y permiten vincular la clave pública con una identidad o entidad.

3.1.3. ANONIMATO O SEUDÓNIMOS DE LOS TITULARES DE CERTIFICADOS

Se admite el uso de seudónimos en los certificados cualificados firma electrónica emitidos por el PCSC VIT S.A. y autorizados por la AC Raíz. El PCSC VIT S.A. al consignar un seudónimo en un certificado electrónico cualificado constata la verdadera identidad del titular del certificado y conserva la documentación que la acredita, en el dossier de titular del certificado.

El PCSC VIT S.A. está 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

La regla primaria para interpretar el formato de los nombres distintivos de los suscriptores en los certificados que emite VIT S.A. es el estándar ITU X.500 DistinguishedName (DN).

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 Tributario

Tipo de Documento	Prefijo	Formato	Descripción
Cédula de identidad	CI	CI999999	Siglas CI seguido del número de cédula de identidad civil, 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 nombre distintivo del suscriptor -DistinguishedName- es único dentro del PCSC VIT S.A. Las reglas definidas en esta DPC y PC de los certificados de VIT S.A. garantizan que el nombre distintivo del suscriptor en los certificados es suficientemente significativo para vincularlo con una identidad o entidad. 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

La PCSC VIT S.A. se reserva el derecho de tomar todas las decisiones en el caso de que haya conflicto derivado de los nombres iguales entre varios solicitantes de certificados. También contempla que, durante el proceso de confirmación de identidad, corresponderá 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 VIT S.A. no arbitrará, mediará o resolverá ninguna disputa concerniente a la propiedad de nombres, nombres de dominio, nombres de empresas o instituciones y marcas registradas.

Se prohíbe a los solicitantes de certificados que incluyan nombres en las solicitudes que puedan suponer infracción de derechos de terceros.

VIT S.A. no determina si un solicitante de certificados tiene derecho sobre las marcas que puedan aparecer en una solicitud de certificado.

VIT S.A. se reserva el derecho de rechazar una solicitud de certificado a causa de conflicto de nombre.

3.2 VALIDACIÓN INICIAL DE IDENTIDAD

Aquí 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:

   i. 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 y biometría presentada. Queda prohibido cualquier tipo de poder para tal fin.

   ii. 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 (SubjectAlternativeName)*** 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

La generación de la solicitud de certificación se hará en presencia del solicitante utilizando mecanismos que garanticen la posesión inequívoca de la clave privada por parte del solicitante. En otros casos, la posesión de la clave privada correspondiente a la clave pública para la que se solicita que se genere el certificado, quedará probada mediante el envío de la solicitud de certificado en formato PKCS#10 u otras demostraciones criptográficas equivalentes, aprobadas por el PCSC VIT S.A. y el MIC, en la cual se incluirá la clave pública firmada mediante la clave privada asociada pudiendo utilizar las referencias contenidas en el RFC 2510, relativos a POP (Proof of Possession). En el caso que sean requeridos procedimientos específicos para las PC implementadas, los mismos deben ser descriptos en esa PC, en el ítem correspondiente.

3.2.2 AUTENTICACIÓN DE IDENTIDAD DE PERSONA JURÍDICA

3.2.2.1 DISPOSICIONES GENERALES

En este ítem están definidos los procedimientos empleados por las ARs vinculadas para la confirmación de la identidad de una persona jurídica.

Se designará como responsable del certificado al representante autorizado de la persona jurídica que solicita el certificado conforme al numeral 3.2, inciso 'a', inciso (ii), quien tendrá el control de la clave privada.

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

a) presentación de la lista de documentos enumerados en el punto 3.2.2.2;

b) presentación de la lista de documentos del responsable del certificado, enumerados en el ítem 3.2.3.1;

c) firma electrónica cualificada del *contrato de prestación de servicio de confianza* mencionado en el ítem 4.1 por el responsable del certificado. En caso de no ser factible, la AR solicitará que el contrato sea firmado manuscritamente por el responsable del certificado para su comparación con el documento de identidad. En este caso, se adjuntará al dossier de titular del certificado, el documento manuscrito digitalizado y firmado con firma electrónica cualificada por el AGR, debiendo mantenerse el original en papel para fines de auditoría.

Se prescinde lo dispuesto en los ítems "b" y "c" si el responsable del certificado posee un certificado cualificado de firma electrónica de la ICPP vigente, con los datos biométricos debidamente recopilados, o cuando utilice un medio de identificación electrónica expedido en virtud de un sistema de identificación electrónica de nivel alto. En estos casos la verificación de los documentos enumerados en el punto 3.2.2.2 se puede realizar electrónicamente, siempre que se realice a través de fuentes oficiales de organismos competentes.

3.2.2.2 DOCUMENTOS REQUERIDOS PARA IDENTIFICAR UNA PERSONA JURÍDICA.

La confirmación de la identidad de una persona jurídica debe hacerse mediante la presentación de al menos los siguientes documentos:

a) si la entidad es pública:

ii. copia simple de la Ley o Carta Orgánica que crea o autoriza su creación;
iii. documento (original o copia autenticada) que acredite la representación; y
iv. cédula tributaria.

b) si la entidad es privada:

i. copia autenticada del estatuto o documento de creación;
ii. copia autenticada del acta de la última asamblea ordinaria y extraordinaria o del documento equivalente que acredite la representación;
iii. prueba de la inscripción en el registro oficial correspondiente; y
iv. cédula tributaria.

La comprobación de los documentos citados precedentemente podrá realizarse por vía electrónica, siempre que se realice a través de fuentes oficiales de organismos competentes.

Estas validaciones deberán incluirse obligatoriamente en el dossier del titular del certificado.

Los documentos, que no puedan comprobarse conforme a las condiciones del párrafo anterior deberán verificarse:

a) por un AGR que no sea el que realizó el paso de identificación;
b) por la AR delegada o AR propia del PCSC; y
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.

3.2.3 AUTENTICACIÓN DE IDENTIDAD DE PERSONA FÍSICA

En este ítem, se definen los procedimientos utilizados por las ARs vinculadas a un PCSC 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) a distancia, utilizando un medio de identificación electrónica expedido en virtud de un sistema de identificación electrónica de nivel alto, para los cuales se haya garantizado la presencia de la persona física previamente a la expedición del certificado cualificado; o,

c) por medio de un certificado de una firma electrónica cualificada expedido de conformidad con la letra a) o b); o,

d) mediante videoconferencia, de acuerdo con los procedimientos y requisitos técnicos definidos en la normativa de AC Raíz-Py, *DOC-ICPP-08 [5]*, que aporten una seguridad equivalente en términos de fiabilidad a la presencia física, garantizando la validación de la misma identificación y la información biométrica, mediante el uso de tecnologías electrónicas seguras de comunicación, interacción, documentación y tratamiento biométrico. La seguridad equivalente será confirmada por un OEC.

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 de extranjero, si es extranjero domiciliado en Paraguay; o
   iii) pasaporte, si es extranjero no domiciliado en Paraguay.
b) recolección y verificación biométrica del solicitante, de acuerdo con las normas emitidas por la AC Raíz-Py, que definen *el procedimiento para la identificación del solicitante y comunicación*

de irregularidades en el proceso de emisión de un certificado en la ICPP - DOC-ICPP-09 [3], así como *el procedimiento de identificación biométrica en la ICPP - DOC-ICPP-10 [4]*.

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 ser verificados:

a) por un agente de registro distinto del que realizó el paso de identificación;

b) por la AR vinculada o AR propia del PCSC; y

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.

La verificación biométrica del solicitante podrá ser realizada mediante consultas a fuentes oficiales de organismos competentes, conforme regulado por la normativa emitida por la AC Raíz-Py de la ICPP, que deberá prever los procedimientos y fuentes oficiales aceptadas para tal fin.

3.2.3.2 INFORMACIÓN CONTENIDA EN UN CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA

La información obligatoria contenida en los campos del certificado cualificado de firma electrónica 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; y
b) número de cédula de identidad civil o número de pasaporte de la persona física, según documento de identidad.

Cada CP puede definir como obligatorio llenar otros campos. 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.

Cada PC puede definir como obligatorio llenar otros campos. 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 PCSC VIT S.A. valida la capacidad del solicitante de un certificado y que no posea impedimentos legales. En el caso de certificados cualificados para firma electrónica, se valida que el solicitante sea mayor de edad.

3.2.6. CRITERIOS PARA INTEROPERABILIDAD

Los servicios de confianza prestados por los prestadores de servicios de confianza establecidos fuera del país serán reconocidos como legalmente equivalentes a los servicios de confianza cualificados prestados por el PCSC VIT S.A. 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 deben garantizar, 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 VIT 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 VIT S.A. se reserva el derecho, sin responsabilidad ante ningún solicitante, de rechazar solicitudes.

El PCSC VIT S.A. mantendrá políticas y procedimientos internos que deben ser revisados periódicamente 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 ESPECIFICOS.

En 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, a ser definidos y aprobados por la AC Raíz-Py.

3.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE NUEVAS CLAVES

Este proceso puede realizarse de acuerdo con una de las siguientes posibilidades:

a) adopción de los mismos requisitos y procedimientos requeridos en los puntos 3.2.2 o 3.2.3;

b) 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, admitiéndose esta hipótesis únicamente para los certificados cualificados de firma electrónica y a los certificados cualificados tributarios;

c) solicitud, por medio electrónico, utilizando un medio de identificación electrónica expedido en virtud de un sistema de identificación electrónica de nivel alto.

d) mediante videoconferencia, de acuerdo con el procedimiento y requisitos técnicos definidos en la normativa de AC Raíz-Py, DOC-ICPP-17 [3], que aporten una seguridad equivalente en términos de fiabilidad a la presencia física, garantizando la validación de la misma identificación, mediante el uso de tecnologías electrónicas seguras de comunicación, interacción y documentación. La seguridad equivalente será confirmada por un OEC.

3.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN

El solicitante de la revocación de un certificado cualificado de la ICPP debe estar identificado. Únicamente los agentes descriptos en el ítem 4.9.2 pueden solicitar la revocación de dicho certificado.

El procedimiento para solicitar la revocación de un certificado cualificado por parte PCSC se describe en el ítem 4.9.3.

Las solicitudes de revocación de certificados deben registrarse.

4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

4.1 SOLICITUD DEL CERTIFICADO

En este ítem, son descritos todos los requisitos y procedimientos operacionales establecidos por el PCSC VIT S.A. y las ARs, a ella vinculadas, para las solicitudes de emisión de certificados. Estos requisitos y procedimientos deberán comprender, en detalles, todas las acciones necesarias tanto del solicitante como del PCSC y la AR en el proceso de solicitud del certificado electrónico.

La descripción también debe contemplar:

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 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.

En caso de imposibilidad técnica de firmar electrónicamente el contrato de prestación de servicio de confianza será aceptada la firma manuscrita del contrato por parte del titular. En este caso será necesaria la verificación de la firma contra el documento de identificación y se adjuntará al dossier de 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 Raíz-Py.

4.1.1 QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO

La presentación de la solicitud debe ser siempre a través de una AR.

En este apartado se detallan las personas que pueden presentar una solicitud de certificado, que, en el marco de la ICPP, son:

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

Los siguientes ítems describen las obligaciones generales de las entidades involucradas.

4.1.2.1 RESPONSABILIDADES Y OBLIGACIONES DEL PCSC

Responsabilidades:

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

b) El PCSC VIT S.A. debe asumir toda la responsabilidad frente a terceros por la actuación de las personas u otros prestadores en los que deleguen la ejecución de algunas de las funciones necesarias para prestación de servicios de confianza, incluyendo las actuaciones de comprobación de identidad previas a la expedición de un certificado cualificado.

Obligaciones:

a) Publicar información veraz y acorde con las reglamentaciones vigentes, en su sitio principal Internet:
   i) La 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.
   iv) No almacenar ni copiar, por sí o a través de un tercero, los datos de creación de firma de la persona física a la que hayan emitido certificados, salvo en caso de su gestión en nombre del firmante. En este caso, el PCSC tiene la obligación de: Utilizar sistemas y productos fiables, incluidos canales de comunicación electrónica seguros; 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;

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

vi) Garantizar su continua disponibilidad.

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

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

d) 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;

e) 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);

f) 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;

g) 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;

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

i) 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;

j) 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;

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

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

m) 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;

n) 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.

o) 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.

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

q) 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.

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

s) 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.

t) 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.

u) 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.

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

w) 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.

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

y) Garantizar un tratamiento lícito de los datos personales.

z) Mantener actualizada una base de datos de certificados.

aa) 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.

bb) 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.

cc) 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.

dd) 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.

ee) 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.

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

gg) Generar y gestionar sus pares de claves criptográficas;

hh) Asegurar la protección de sus claves privadas;

ii) Distribuir su propio certificado;

jj) Emitir, expedir y distribuir los certificados de los usuarios finales;

kk) Informar la emisión del certificado al respectivo solicitante;

ll) 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);

nn) Utilizar un protocolo de comunicación seguro cuando se preste servicios a través de la web a los solicitantes o usuarios de certificados electrónicos;

oo) Identificar y registrar todas las acciones ejecutadas, conformes a las normas, prácticas y reglas establecidas por AC Raíz-Py;

pp) Adoptar las medidas de seguridad y de control previstas en la DPC, PC y PS que se implementan, con sujeción a las normas, criterios, prácticas y procedimientos establecidos por la AC Raíz-Py.

qq) Mantener el cumplimiento de sus procesos, procedimientos y actividades con las normas, prácticas y reglas establecidos por AC Raíz-Py, y la normativa vigente;

rr) Mantener y garantizar la integridad, confidencialidad y seguridad de la información por él tratado;

ss) Mantener y anualmente realizar prueba de su PCN;

tt) Informar a la AC Raíz-Py, mensualmente, la cantidad de certificados electrónicos emitidos y revocados;

uu) No emitir el certificado con una fecha de caducidad que se extienda más allá de la fecha de vencimiento de su propio certificado.

vv) 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;

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

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

yy) 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 por los daños y perjuicios que ocasione.

Obligaciones

a) Recibir las solicitudes de emisión, suspensión revocación de 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, suspensión 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.; y
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 VIT S.A. y las AR vinculadas realizan las funciones de identificación y autenticación según el ítem 3 de esta DPC.

4.2.2 APROBACIÓN O RECHAZO DE SOLICITUDES DE CERTIFICADO

El PCSC VIT S.A. y las AR vinculadas podrán, con la debida justificación formal, aceptar o rechazar 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

El PCSC VIT S.A. cumple con los procedimientos determinados por la AC Raíz-Py. No habrá tiempo máximo para procesar solicitudes en el marco de la ICPP.

4.3 EMISIÓN DEL CERTIFICADO

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

4.3.1 ACCIONES DEL PCSC DURANTE LA EMISIÓN DE LOS CERTIFICADOS

Una vez ejecutadas las labores previas de identificación y autenticación de los solicitantes, el PCSC VIT S.A. verificará que se hayan cumplido los procedimientos establecidos en esta DPC y en la Política de Certificación correspondiente, de acuerdo con las normas técnicas y legislación vigente que rige la materia.

El PCSC VIT S.A. realizará las siguientes acciones durante la emisión de los certificados:

• Asegurarse que la generación de un par de claves y un certificado se haya realizado de manera segura de acuerdo a la sección 3.2.1

• Asociación del par de claves que corresponde al certificado con un suscriptor, y que el par de claves se encuentre en su posesión

• Emisión del certificado electrónico cualificado de acuerdo con el Nombre Distintivo asociado con el suscriptor y según la Política de Certificación correspondiente, firmado por el PCSC VIT S.A.

En ningún momento el PCSC VIT S.A. accederá a la clave privada del solicitante.

Las acciones que requieran de consideraciones adicionales por tipo de certificado serán Según lo especificado en las Políticas de Certificación de cada tipo de certificado.

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

En el caso que el certificado sea emitido en un dispositivo de seguridad criptográfico en presencia del suscriptor en el PCSC VIT S.A.: esta notificación no será necesaria.

En el caso que la emisión no sea en forma presencial: luego de emitido el certificado, el PCSC VIT S.A. notificará por medios electrónicos al suscriptor que se ha creado el certificado, que se encuentra disponible y la forma de obtenerlo.

4.4 ACEPTACIÓN DEL CERTIFICADO

4.4.1 CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE CERTIFICADO

Una vez emitido el certificado de Persona física o Jurídica por el PCSC VIT S.A., el solicitante debe aceptar el certificado aceptando los términos del *Contrato de Prestación de servicios de Confianza* según lo especificado en las Políticas de Certificación de cada tipo de certificado. En caso de la no

aceptación de los términos de usos del certificado detallados en el *Contrato de Prestación de servicios de Confianza*, se procede a revocar el certificado digital.

En caso de los certificados emitidos para persona jurídica, la declaración expresa deberá ser de la persona física responsable de ese certificado.

4.4.2 PUBLICACIÓN DEL CERTIFICADO POR EL PCSC

El certificado del PCSC VIT S.A. y los certificados emitidos a usuarios finales, deberán ser 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 VIT 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 VIT S.A.

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

El PCSC VIT S.A. utiliza su clave privada y garantiza la protección de esa clave según lo previsto en su propia DPC.

Obligaciones del Titular del Certificado

En este ítem se incluyen las obligaciones de los titulares de certificados emitidos por el PCSC VIT S.A., contenidas en el *Contrato de Prestación de Servicio de Confianza* referidos en el ítem 4.1.

a) proporcionar al PCSC VIT S.A. 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 VIT S.A. 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, 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, en su caso, de los medios que den acceso a ellos.

e) no utilizar los datos de creación de firma cuando haya expirado el período de validez del certificado electrónico o el PCSC VIT S.A. 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 de VIT S.A.;

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 VIT S.A. de cualquier compromiso de su clave privada y solicitar la revocación inmediata del certificado correspondiente.

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 LA 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 UN 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 DEL CERTIFICADO 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 CERTIFICADO A OTRAS ENTIDADES

Este ítem no aplica.

4.9 REVOCACIÓN Y SUSPENSIÓN

4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN

En este ítem de la DPC, son consignadas, las circunstancias en la cual un certificado podrá ser revocado.

Igualmente se establece que PCSC VIT S.A. extinguirá la vigencia de los certificados mediante revocación en los siguientes supuestos:

a) solicitud formulada por el firmante, la persona física titular.
b) 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) fallecimiento del firmante; incapacidad sobrevenida, total o parcial.
e) cese en la actividad del PCSC 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.

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

La AC Raíz-Py podrá determinar la revocación del certificado del PCSC VIT 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 REVOCACIÓN

El PCSC VIT S.A. establece que la revocación de un certificado sólo podrá realizarse:

a) por solicitud formulada 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 VIT S.A.;

e) por una AR vinculada al PCSC VIT S.A.;

4.9.3 PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACIÓN

El procedimiento de revocación de un certificado se inicia con la solicitud de revocación y termina con la emisión de una nueva Lista de Certificados Revocados (LCR).

El procedimiento de solicitud será realizado vía la Autoridad de Registro de conformidad al punto 1.3.2 de esta DPC, y podrán ser presenciales o remotas. Los sujetos habilitados para solicitar la revocación se encuentran establecidos en la sección 4.9.2., y la solicitud de revocación que presenten deberá contener las causales o motivos del pedido de revocación.

El procedimiento de solicitud comprende según sea el caso:

• Si la solicitud se realiza en forma presencial en una Autoridad de Registro, ya sea por el suscriptor o un tercero, se debe proceder:

o según lo especificado en las Políticas de Certificación de cada tipo de certificado.

• Si la solicitud se realiza en forma remota, contactando una Autoridad de Registro vía un mensaje de datos firmado digitalmente por el suscriptor del certificado, utilizando el mismo certificado que se quiere revocar, se debe proceder:

o según lo especificado en las Políticas de Certificación de cada tipo de certificado.

• Cuando el propio PCSC VIT S.A. detecte la existencia de algún motivo de revocación de un certificado, el cual se encuentre establecido en la normativa vigente y esta DPC, puede por sí misma realizar el proceso de revocación.

En los casos que la solicitud de revocación provenga del propio PCSC VIT S.A.:

o Notificará al suscriptor del certificado.

o Dejará constancia escrita de los causales de dicha acción en una Solicitud de REVOCACIÓN de Certificado interna firmada por el personal del PCSC VIT S.A.

o Conservará el material que obra de elemento probatorio de referencia para iniciar la acción de revocación.

• En los casos que la solicitud de revocación provenga de una Autoridad Judicial competente; el PCSC VIT S.A.:

o Evaluará la solicitud de revocación recibida.

o Notificará al suscriptor del certificado (Antes de comenzar con el proceso de revocación).

o El PCSC VIT S.A. se reserva el derecho de aplicar la revocación efectiva inmediata del certificado a partir del análisis de dicha solicitud. En ese caso el procedimiento de revocación se iniciará una Solicitud de REVOCACIÓN de Certificado interna.

o Conservará el material que obra de elemento probatorio de referencia para iniciar la acción de revocación.

El PCSC VIT S.A. tiene la responsabilidad de:

• Ejecutar el proceso de revocación

• Verificar de identidad del solicitante de la revocación.

• Validar la información suministrada en la solicitud de revocación.

• Analizar la solicitud de revocación, verificar que la misma ha sido presentada de acuerdo a las exigencias, y evaluar si procede continuar con la revocación efectiva del certificado.

• Informar al suscriptor de la revocación

• Revocar el certificado de acuerdo con la información suministrada en la solicitud.

4.9.4 PERIODO DE GRACIA PARA SOLICITUD DE REVOCACIÓN

El titular del certificado deberá realizar la solicitud de revocación tan pronto le sea posible una vez se haya producido la causa de la misma.

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 VIT S.A. procesara la revocación inmediatamente después de analizar la solicitud.

4.9.6 REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN PARA LA PARTES USUARIA

Las partes usuarias deben evaluar el estado del certificado y el estado de todos los certificados de las CA en la cadena a la que pertenece el certificado, antes de confiar en él.

Para ello, las partes usuarias pueden verificar el estado del certificado mediante el servicio de:

• Verificación en línea OCSP del PCSC VIT S.A., o

• Verificación por la lista LCR más reciente provista por el PCSC VIT S.A.

El PCSC VIT S.A. suministra información a los verificadores acerca de cómo y dónde encontrar la LCR y/o OCSP correspondiente en el Repositorio web http://www.efirma.com.py

4.9.7 FRECUENCIA DE EMISIÓN DEL LCR

La LCR se actualiza y publica inmediatamente cuando surge una revocación o suspensión o con una frecuencia máxima para certificados de los usuarios finales de doce (12) horas.

La LCR mantiene publicado obligatoriamente:

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

4.9.8 LATENCIA MÁXIMA PARA LCR

La CA publicará la LCR en el Repositorio en un plazo no mayor a una hora posterior a su generación. En general, la CA genera y publica la LCR en un mismo proceso, con un tiempo mínimo de latencia para su publicación en el Repositorio.

4.9.9 DISPONIBILIDAD PARA REVOCACIÓN/VERIFICACIÓN DE ESTADO EN LÍNEA

El PCSC VIT S.A. implementa un sistema OCSP para verificación en línea del estado de los certificados emitidos. El mismo permite a posibles entidades y usuarios "verificadores" disponer de un servicio de verificación en tiempo real del estado de los certificados mediante la implementación del protocolo OCSP (Online Certificate Status Protocol), de forma que sus aplicaciones usuarias verificarán el estado del certificado sin necesidad de descargar LCRs.

4.9.10 REQUISITOS PARA LA VERIFICACIÓN DE REVOCACIÓN EN LÍNEA

La parte que confía debe verificar el estado de un certificado en el cual desea confiar, utilizando los mecanismos de verificación del estado de certificados establecidos en la sección anterior.

4.9.11 OTRAS FORMAS DE ADVERTENCIAS DE REVOCACIÓN DISPONIBLES

El PCSC VIT S.A. implementa servicios adicionales de información automáticos a través de mensajes de correo electrónico:

• Revocación: Notifica al suscriptor que su certificado ha sido revocado.

• Expiración próxima: Notifica al suscriptor que su certificado está próximo a expirar, a efectos que el suscriptor tenga presente que puede realizar la renovación del mismo.

4.9.12 REQUERIMIENTOS ESPECIALES POR COMPROMISO DE CLAVE PRIVADA

El PCSC VIT S.A. notificará en un plazo de veinticuatro (24) horas como máximo a la DGFD&CE respecto a circunstancias que produzcan el compromiso de sus claves o su imposibilidad de uso.

En caso que la clave privada del PCSC VIT S.A. se vea comprometida, se revocarán de inmediato los certificados emitidos de acuerdo a la legislación vigente, comunicando dicha acción a todos los suscriptores y terceros que confían.

4.9.13 CIRCUNSTANCIAS PARA SUSPENSIÓN

El PCSC VIT S.A. procederá a la suspensión del certificado 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 VIT S.A. informará al titular del 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

El PCSC VIT S.A. establece que la suspensión de un certificado sólo podrá realizarse:

- Por solicitud formulada a través del firmante, la persona física o jurídica representada por éste, un tercero autorizado;
- Resolución judicial o administrativa competente que lo ordene.
- 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;
- Por el PCSC VIT S.A.;
- Por una AR vinculada al PCSC VIT S.A.;

4.9.15 PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN

En este apartado, se describen los procedimientos establecidos por el PCSC VIT S.A. para la solicitud de suspensión de certificados. El PCSC VIT 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:

El solicitante de suspensión de un certificado será identificado;

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

Se documentarán las razones de la suspensión de un certificado; y

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 VIT S.A.

El PCSC VIT S.A. al suspender un certificado electrónico cualificado, registrara su suspensión en su base de datos de certificados y publicara 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.

El PCSC responsable 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.

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 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 VIT S.A. establece el tiempo de disponibilidad del servicio de publicación de la LCR, certificados emitidos en el repositorio público y el servicio de consulta en línea por medio del protocolo OCSP. Estos servicios están disponibles durante las veinticuatro horas, los siete días de la semana (24/7). En caso de interrupción por causa de fuerza mayor, el servicio se restablecerá 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

El PCSC VIT S.A. disponibiliza el servicio OCSP, que permite consultar el estado de los certificados en línea.

Para hacer uso del servicio de validación en línea es responsabilidad de las partes usuarias disponer de un cliente OCSP que cumpla el RFC 6960.

4.11 FIN DE ACTIVIDADES

Los requisitos y procedimientos en caso de extinción o cese de los servicios del PCSC VIT S.A. se describen en el documento PLAN DE CONTINGENCIA, RECUPERACIÓN DE DESASTRES Y CONTINUIDAD DEL NEGOCIO, en su última versión disponible.

4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES

4.12.1 POLÍTICA Y PRÁCTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES

El PCSC VIT S.A. no podrá almacenar ni copiar, por sí o a través de un tercero, los datos de creación de firma de la persona física o jurídica a la que hayan prestado sus servicios, salvo en caso de su gestión en nombre del firmante. En este caso, se debe utilizar sistemas y productos fiables, incluidos canales de comunicación electrónica seguros, 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. 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.

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

En los siguientes ítems son descriptos los controles de seguridad implementados por el PCSC VIT S.A. y por las ARs a ella vinculadas, para ejecutar de modo seguro sus funciones de generación de claves, identificación, certificación, auditoría y archivo de los registros.

5.1 CONTROLES FÍSICOS

En las secciones siguientes, se describen los controles físicos referentes a las instalaciones que albergan los sistemas del PCSC VIT S.A. y de las ARs vinculadas.

5.1.1 LOCALIZACIÓN Y CONSTRUCCIÓN DEL SITIO

La localización de las instalaciones donde se albergan los sistemas de certificación del PCSC VIT S.A., no son públicamente identificadas. No existe identificación pública externa de las instalaciones e internamente, no son admitidos ambientes compartidos que permitan la visibilidad de las operaciones de emisión y revocación de los certificados. Esas operaciones son segregadas en compartimientos cerrados y físicamente protegidos.

En el PCSC VIT S.A. se implementan entre otros los siguientes 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;

5.1.2 ACCESO FÍSICO

El PCSC VIT S.A. implementa un sistema de control de acceso físico que garantiza la seguridad de sus instalaciones, conforme al ítem 9 “control de accesos” de la norma ISO 27002:2022 y los siguientes puntos:

5.1.2.1 NIVELES DE ACCESO FÍSICO

El PCSC VIT S.A. define 4 (cuatro) niveles de acceso físico a los diversos ambientes del mismo, más 2 (dos) niveles relativos a la protección de la clave privada.

En el primer nivel se sitúa la primera barrera de acceso a las instalaciones del PCSC VIT S.A. Para acceder al área del nivel 1, cada persona es identificada y registrada por el personal de seguridad, a partir de ese nivel personas extrañas a la operativa del PCSC VIT S.A. transitaran debidamente identificadas y acompañadas. Ningún tipo de proceso operacional o administrativo del PCSC VIT S.A. es ejecutado en ese nivel.

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

El segundo nivel es interno al primero, y requiere de la misma forma que el primero, una identificación individual de las personas que en él accedan. Ese es el nivel mínimo de seguridad requerido

para la ejecución de cualquier proceso operacional o administrativo del PCSC VIT S.A. El paso del primer al segundo nivel exige un factor de autenticación electrónica y tarjeta de identificación visible.

El tercer nivel se sitúa dentro del segundo nivel y será el primer nivel en albergar material y actividades sensibles de la operativa del PCSC VIT S.A. Cualquier actividad relativa al ciclo de vida de los certificados electrónicos es localizada a partir de este nivel. Personas que no están involucradas con esas actividades no tienen permiso para acceder a este nivel. Las personas que no cuentan con permiso de acceso no podrán permanecer en ese nivel salvo que 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 que son 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 VIT S.A., no serán aceptadas desde el nivel 3.

En el cuarto nivel, interno al tercero, donde se despliegan, actividades especialmente sensibles a la operación del PCSC VIT S.A., tales como la emisión y revocación de los certificados y la emisión de la LCR. Todos los sistemas y equipamientos necesarios a estas actividades están localizados a partir de este nivel. El nivel 4 posee 2 (dos) factores de autenticación (uno de ellos biométrico) y tarjeta de identificación visible y, adicionalmente, exige, 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 son realizadas de modo a prevenir las amenazas de acceso no autorizado, agua, vapor, gas y fuego. Las tuberías de refrigeración, de energía o de comunicación no permiten la penetración física en las áreas de cuarto nivel. Adicionalmente, debe tener una protección contra las interferencias electromagnéticas externas.

Este ambiente deberá ser construido según las normas internacionales aplicables.

Podrá existir, en el PCSC, 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 producción off-line y cofre de almacenamiento; y

c) Equipamientos de redes e infraestructura (firewall, ruteadores, switches y servidores).

En el quinto nivel, interno al ambiente del nivel 4, deberá disponerse de un cofre o un gabinete reforzado, donde estarán 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 obedece las siguientes especificaciones mínimas:

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

b) poseer cerraduras antirrobo.

En el sexto nivel, interno al ambiente del nivel 4, comprende un cofre o un gabinete reforzado. Los datos de activación de la clave privada del PCSC VIT S.A. son almacenados en ese ambiente.
Para garantizar la seguridad del material almacenado, el cofre o el gabinete obedece 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, es monitoreada por cámaras de vídeo ligadas a un sistema de grabación 24x7. El posicionamiento y la capacidad de esas cámaras no permiten recuperar las contraseñas digitadas en los controles de acceso.

Las cintas de vídeo resultantes de grabación 24x7 son almacenadas, como mínimo, 4 (cuatro) años. Ellas son 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 son almacenadas en el ambiente del nivel 3.

Todas las puertas de transición entre los ambientes de niveles 3 y 4 son 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, se activan automáticamente los sensores de presencia.

Los sistemas de notificación de alarmas utilizan 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, son permanentemente monitoreados por el personal autorizado y estar localizados en el ambiente de nivel 3. Las instalaciones del sistema de monitoreo, a su vez, son monitoreados por cámaras de vídeo cuyo posicionamiento permite el seguimiento de las acciones del personal autorizado.

5.1.2.3 SISTEMAS DE CONTROL DE ACCESO

El sistema de control de acceso se encuentra en el ambiente de nivel 4.

5.1.2.4 MECANISMOS DE EMERGENCIA

Mecanismos específicos son implementados por el PCSC VIT 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 VIT 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.

5.1.3 ENERGÍA Y AIRE ACONDICIONADO

La infraestructura del ambiente de certificación del PCSC VIT S.A. es dimensionada con sistemas y dispositivos que garantizan el funcionamiento ininterrumpido de energía eléctrica en las instalaciones. Las condiciones de funcionamiento ininterrumpido de energía son mantenidas de forma a atender los requisitos de disponibilidad de los sistemas del PCSC VIT S.A. y de sus respectivos servicios. Un sistema puesta a tierra es implantado en la instalación.

Todos los cables eléctricos están protegidos por tuberías y conductos apropiados.

Son utilizados tuberías, conductos, canaletas, paneles y cajas (de paso, distribución y terminación) diseñadas y construidas de forma a facilitar la inspección y detección de intentos de manipulación. Son utilizados conductos separados para los cables de energía, de telefonía y de datos.

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

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

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

El sistema de climatización cumple con los requisitos de temperatura y humedad exigidos por los equipamientos utilizados en el ambiente y dispone de filtros de polvo. En los ambientes de nivel 4, el sistema de climatización es independiente y tolerable a fallas.

La temperatura de los ambientes atendidos por el sistema 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 realizado apenas por la abertura de la puerta.

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

a) generadores de un tamaño compatible;

b) generadores de reserva;

c) sistemas de UPS redundantes; y

d) sistemas redundantes de aire acondicionado.

5.1.4 EXPOSICIÓN AL AGUA

La estructura interna al ambiente de nivel 4, provee de protección física contra exposición a 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 posibilitan 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 VIT S.A. no está permitido fumar o portar objetos que produzcan fuego o chispa.

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

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

5.1.6 ALMACENAMIENTO DE MEDIOS

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

La información relacionada a la infraestructura del PCSC VIT S.A. se almacena de forma segura en armarios ignífugos y cofres de seguridad, según la clasificación de la información en ellos contenida.

5.1.7 ELIMINACIÓN DE RESIDUOS

Todos los documentos en papel que contienen información clasificada como sensible son triturados antes de ir como residuos.

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

5.1.8 RESPALDO FUERA DE SITIO

Las instalaciones de respaldo cumplen con los requisitos mínimos establecidos por este documento. Su localización es tal que, en caso de siniestro que torne inoperante la instalación principal del PCSC VIT S.A., las instalaciones de respaldo no se vean afectadas y tomen totalmente las operaciones del PCSC VIT S.A. en condiciones idénticas en, un máximo, de 48 (cuarenta y ocho) horas.

5.2 CONTROLES PROCEDIMENTALES

En los siguientes ítems son descriptos los requisitos para la caracterización y el reconocimiento de los Roles de Confianza en el PCSC VIT S.A. y las ARs vinculadas a el, junto con las responsabilidades definidas para cada perfil. Para cada tarea asociada a los perfiles definidos, también se establece el número de personas necesarias para su ejecución.

5.2.1 ROLES DE CONFIANZA

El PCSC VIT S.A. garantiza la segregación de tareas para las funciones críticas, con el fin de evitar que un empleado o funcionario que asume un rol de confianza utilice incorrectamente su sistema de certificación sin ser detectado. Las acciones de cada uno de los empleados o funcionarios se limitan de acuerdo a su perfil.

Los Roles del PCSC VIT S.A., contemplan, al menos las siguientes responsabilidades que a continuación serán descriptos:

a) responsables de seguridad: llevan a cabo la actualización e implementación de las políticas y procedimientos de seguridad que han sido aprobados por el PCSC VIT S.A., controlar la formalización de los convenios entre el personal y el PCSC VIT S.A., comunicar las medidas disciplinarias acordadas, supervisando su cumplimiento. Asimismo, deberá cumplir y hacer cumplir las políticas de seguridad del PCSC VIT S.A. y se encargan 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. Comprueban 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 VIT S.A.;

b) responsables de sistemas: los responsables de este rol no están implicados en tareas de auditoría interna. Son 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. Así mismo, establecen y documentan los procedimientos de monitoreo de los sistemas y de los servicios que prestan. Son responsables de mantener el inventario de servidores y resto de componentes de los sistemas de certificación del PCSC VIT S.A. y asumen la gestión de los servicios de ruteamiento y gestión de reglas de firewall, gestión y mantenimiento de los sistemas de detección de intrusos, etc. Son encargados de la instalación de hardware criptográfico del PCSC VIT S.A. y de la eliminación del hardware criptográfico del PCSC de producción. Son responsables del mantenimiento o reparación de equipos en general así como de dispositivos criptográficos del PCSC VIT S.A. (incluida la instalación de nuevo hardware, firmware o software), Igualmente son responsables de los desmontajes y la eliminación permanente por el uso;

c) responsables de la operación diaria del PCSC VIT S.A.: son encargados de realizar las tareas de ejecución y revisión de las copias de seguridad del sistema. Así mismo, 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. Son 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 auditorías**: son los responsables de las tareas de ejecución y revisión de auditoría de los sistemas que conforman la infraestructura tecnológica del PCSC VIT S.A. Esta auditoría se realiza de acuerdo con las normas y criterios de auditoría establecidos en la presente DPC. Además, tiene 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**: son 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.

Todos los operadores del sistema de certificación del PCSC VIT S.A. reciben entrenamiento específico antes de obtener cualquier tipo de acceso. El tipo o nivel de acceso son determinados, en un documento formal, con base en las necesidades de cada perfil.

Cuando un empleado o funcionario se desvincula del PCSC VIT S.A., sus permisos de acceso son revocados inmediatamente. Cuando hay un cambio en la posición o función que el empleado o funcionario ocupa dentro del PCSC VIT S.A., son 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 VIT S.A. en el momento de su desvinculación.

5.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

El PCSC VIT S.A. dispone de control multi-usuario para la generación y la utilización de la clave privada del PCSC VIT S.A., de la forma definida en el ítem 6.2.2.

Todas las tareas ejecutadas en el ambiente donde está localizado el equipamiento de certificación del PCSC VIT S.A. requiere, como mínimo, de 2 (dos) de sus empleados o funcionarios con rol de confianza. Las demás tareas del PCSC VIT S.A. son ejecutadas por un único empleado o funcionario.

5.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

El PCSC VIT S.A. garantiza que todo empleado o funcionario que asume un rol de confianza en el PCSC VIT S.A. será identificado y su perfil será verificado antes de que:

a) sean incluido en una lista de acceso a las instalaciones del PCSC;

b) sean incluido en una lista para acceso físico al sistema de certificación del PCSC;

c) reciban un certificado cualificado de firma electrónica para ejecutar sus actividades operacionales en el PCSC; y

d) reciban una cuenta de usuario del sistema de certificación del PCSC.

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

a) ser directamente asignados a un único empleado o funcionario;

b) no ser compartidos; y

c) ser restringidas las acciones asociadas con el perfil para los cuales fueron creados.

5.2.4 ROLES QUE 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/suspensión o información del titular o responsable del certificado.

5.3 CONTROLES DE PERSONAL

Se describen los requisitos y procedimientos, implementados por el PCSC VIT S.A., por las ARs y PSSs vinculados 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.

El PCSC VIT S.A. garantiza que todos los empleados o funcionarios del PCSC VIT S.A., de las ARs y de los PSSs vinculados, a cargo de las tareas operativas, se han 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 ICPP; 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 VIT S.A. y de las ARs vinculadas e involucrado en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados deberá ser seleccionado y admitido, conforme a lo establecido en el ítem 7 “seguridad ligada a los recursos humanos” de la norma ISO 27002/2022 y además deberán:

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.

5.3.2 PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES

Con propósito de resguardar la seguridad y credibilidad de las entidades, todo personal del PCSC VIT S.A. y de las ARs vinculadas involucradas en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados están sometidos 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 VIT S.A. puede definir requisitos adicionales para la verificación de antecedentes.

5.3.3 REQUERIMIENTOS DE CAPACITACIÓN

Todo el personal del PCSC VIT 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 recibir 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 VIT S.A. y de las RAs vinculadas, involucrado en actividades directamente relacionadas con los procesos de emisión, expedición, distribución, revocación y gerenciamiento de certificados es mantenido y actualizado sobre eventuales cambios o modificaciones tecnológicas de los sistemas del PCSC VIT S.A. o de las ARs.

5.3.5 FRECUENCIA Y SECUENCIA EN LA ROTACIÓN DE LAS FUNCIONES

En este ítem, la DPC podrá definir una política a ser adoptada por el PCSC VIT S.A. y por las ARs vinculadas, para la rotación del personal en los diversos cargos y perfiles por ellas establecidas. Esa política no deberá contrariar los propósitos establecidos en el ítem 5.2.1.

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

5.3.6 SANCIONES PARA ACCIONES NO AUTORIZADAS

El PCSC VIT S.A. prevé así como en su política de RRHH que, en la eventualidad de una acción no autorizada, real o sospechada, realizada por una persona encargada del proceso operacional del PCSC VIT S.A. o de una AR vinculada, el PCSC VIT S.A. de inmediato, suspenderá el acceso de esa persona a su sistema de certificación, iniciara un procedimiento administrativo para determinar los hechos y, si es necesario, tomara las medidas legales pertinentes.

El proceso administrativo referido en el párrafo anterior deberá contener, 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 VIT S.A. deberá comunicar 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

Todo el personal del PCSC VIT 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 ser contratado conforme a lo establecido en los ítems 7 “seguridad

ligada a los recursos humanos" y 15 "relaciones con suministradores" norma ISO 27002/2022 y 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 PCSC VIT S.A. 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 VIT S.A. pone a disposición de todo el personal del mismo y para todo el personal de las ARs vinculadas a él, al menos:

a) su DPC;

b) las PCs que implementan;

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 está clasificada y es mantenida actualizada.

5.4. PROCEDIMIENTO DE REGISTRO DE AUDITORÍA

En los siguientes ítems de la presente DPC se describen los aspectos de los sistemas de auditoría y registro de eventos implementados por el PCSC VIT S.A. con el fin de mantener un entorno o ambiente seguro.

5.4.1. TIPOS DE EVENTOS REGISTRADOS

El PCSC VIT S.A., registra en archivos de auditoría, todos los eventos relacionados a la seguridad de su sistema de certificación. Entre otros, los siguientes eventos son 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 VIT 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.

En este ítem, se especifican todas las informaciones que son registradas por el PCSC VIT S.A.

El PCSC VIT S.A. prevé que todos los registros de auditoría, electrónicos o manuales, contienen la fecha y hora del evento registrado y la identidad del agente que lo causó.

Para facilitar los procesos de auditoría, toda documentación relacionada a los servicios del PCSC VIT S.A. es almacenada, electrónicamente o manualmente, en un local único, conforme a lo establecido en el ítem 12 “seguridad en la operativa” de la norma ISO 27002/2022.

El PCSC VIT S.A., registra electrónicamente 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 son 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 VIT S.A. a sus ARs, establece, en un documento que esté 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)

El PCSC VIT S.A. establece el periodo, no superior a 1 (un) mes, con que los registros de auditoría del PCSC VIT S.A. serán analizados por el personal operacional. Todos los eventos significativos son explicados en un informe de auditoría de registros. Tal análisis involucra una inspección breve de todos los registros, con la verificación de que no fueron alterados, seguida de una investigación más detallada de cualquier alerta o irregularidades en esos registros. Todas las medidas adoptadas como resultado de este análisis son documentadas.

5.4.3 PERÍODO DE CONSERVACIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

Se establece que el PCSC VIT S.A., mantendrá localmente sus registros de auditoría por los menos 2 (dos) meses y, consecuentemente, lo almacenara de la manera descrita 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.

5.4.4 PROTECCIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

Los registros de auditoría archivados se mantienen en forma de prevenir su revelación, modificación, destrucción no autorizada o cualquier otra intromisión.

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

El PCSC VIT S.A. mantiene copias de respaldo de todos los registros auditados.

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

Los archivos de registro son almacenados en los sistemas internos, mediante una combinación de procesos automáticos y manuales ejecutados por las aplicaciones del PCSC VIT S.A.

5.4.7. NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO

Cuando un evento es registrado por el conjunto de sistemas de auditoría del PCSC VIT S.A., no se requerirá notificar a ninguna persona, organización, dispositivo o aplicación que causó el evento.

5.4.8. EVALUACIÓN DE VULNERABILIDADES

Los eventos que indiquen posibles vulnerabilidades, detectadas en el análisis periódico de los registros de auditoría del PCSC VIT S.A., serán analizados detalladamente y, dependiendo de su gravedad, registrados por separado. Acciones correctivas que surjan seran implementadas por el PCSC VIT S.A. y registradas con fines de auditoría.

5.5. ARCHIVOS DE REGISTROS

En los ítems siguientes se describe la política general de archivo de registros, para uso futuro, implementada por el PCSC VIT S.A. y por las ARs a ella vinculada.

5.5.1. TIPOS DE REGISTROS ARCHIVADOS

Se especifican los tipos de registros archivados, que comprenden, 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 VIT S.A.;

g) Información de auditoría prevista en el ítem 5.4.1.

5.5.2. PERÍODOS DE RETENCIÓN PARA ARCHIVOS

Se establece los periodos de retención para cada registro archivado.

a) las LCR y los certificados emitidos por el PCSC son 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 son almacenadas, como mínimo, 10 (diez) años.

5.5.3 PROTECCIÓN DE ARCHIVOS

Se establece que todos los registros archivados son clasificados y almacenados con los requisitos de seguridad compatibles con esta clasificación, conforme a lo establecido en el ítem 12 “seguridad en la operativa” de la norma ISO 27002/2022.

5.5.4 PROCEDIMIENTOS DE RESPALDO (BACKUP) DE ARCHIVO

Una segunda copia de todo el material archivado es almacenada en un local externo al PCSC VIT S.A., recibiendo el mínimo tipo de protección utilizada para el archivo principal.

Las copias de seguridad siguen los periodos de retención definidos para los registros de las cuales son copias.

El PCSC VIT S.A. 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)

Los archivos del PCSC VIT S.A. son de manejo interno y se mantienen por lo menos dos copias de seguridad, una de las cuales debe ser almacenada fuera del sitio principal de operaciones.

5.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR LA INFORMACIÓN ARCHIVADA

Solamente el personal de confianza autorizado está habilitado para obtener acceso al archivo. El PCSC VIT S.A. realizará pruebas de restauración de la información archivada al menos una vez al año. La integridad de la información debe ser verificada cuando es restaurada.

5.6 CAMBIO DE CLAVE

En este ítem, se describen los procedimientos para el suministro, por el PCSC VIT S.A., de un nuevo certificado, antes de la expiración del certificado a pedido del titular del certificado.

El PCSC VIT 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 y 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 del 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.

5.7. RECUPERACIÓN DE DESASTRES Y COMPROMISO

En los siguientes ítems son descriptos los requisitos relacionados con los procedimientos de notificación y recuperación de desastres, previstos en la PCN del PCSC VIT S.A., establecido de acuerdo con el ítem 17 “aspectos de seguridad de la información en la gestión de la continuidad del negocio” de la norma ISO 27002/2022, para garantizar la continuidad de sus servicios críticos.

5.7.1. PROCEDIMIENTO PARA EL MANEJO DE INCIDENTE Y COMPROMISO

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

A continuación se describen los procedimientos previstos en el PCN de las ARs vinculadas para la recuperación total o parcial de sus actividades

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 este apartado de la DPC, deben ser descriptos los procedimientos de recuperación utilizados por el PCSC VIT S.A. cuando los recursos computacionales, software y/o corrupción de datos estuvieren comprometidos o en sospecha de corrupción.

5.7.3. PROCEDIMIENTOS DE COMPROMISO DE CLAVE PRIVADA DE LA ENTIDAD

5.7.3.1 CERTIFICADO DE ENTIDAD ES REVOCADO

En este ítem de la DPC, deben ser descriptos los procedimientos de recuperación utilizados en caso de revocación del certificado del PCSC VIT S.A.

5.7.3.2 CLAVE DE ENTIDAD ESTÁ COMPROMETIDA

En este ítem de la DPC, deben ser descriptos los procedimientos de recuperación utilizados en caso de compromiso de la clave privada del PCSC VIT S.A.

5.7.4. CAPACIDAD DE CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

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

5.8 EXTINCIÓN DE UN PCSC O ENTIDADES VINCULADAS

En este ítem, se describen los requisitos y los procedimientos que deberán ser adoptados en el caso de la extinción de servicios del PCSC VIT S.A. o de una AR, AV o PSS a ella vinculada.

Son 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 VIT S.A., deje de operar cumplirá, 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 VIT S.A., deje de operar, no emitirá ningún certificado pero continuara 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 VIT S.A.

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 VIT S.A., además publicará el cese de actividades o finalización del servicio del PCSC VIT S.A. en su sitio principal de Internet.

6. CONTROLES TÉCNICOS DE SEGURIDAD

En los ítems siguientes, se definen las medidas de seguridad implementadas por el PCSC VIT S.A. para proteger sus claves criptográficas y sus datos de activación, así como las claves criptográficas de los titulares de certificados. Se definen también otros controles técnicos de seguridad utilizados por el PCSC VIT S.A. y por las ARs a ella vinculadas para la ejecución de sus funciones operacionales.

6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

6.1.1. GENERACIÓN DEL PAR DE CLAVES El PCSC VIT S.A.

Implementa controles para brindar seguridad de que los pares de claves del PCSC VIT S.A. se generan e instalan de acuerdo con el protocolo definido para la generación de claves.

El proceso de generación de claves a ejecutar por el PCSC VIT S.A. previene la pérdida, divulgación, modificación o acceso no autorizado a las claves privadas que son generadas.

Certificado del PCSC VIT S.A.

Las claves del certificado del PCSC VIT S.A. se generan mediante un proceso seguro por medio del módulo criptográfico de hardware (HSM – Hardware Security Module), que cumple con el estándar Fips 140-2 nivel 3 y a un procedimiento establecido de Ceremonia de generación de claves. 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 proceso de generación de claves del PCSC VIT S.A. producirá claves que:

- sean apropiadas para la aplicación o propósito destinado y que sean proporcionales a los riesgos identificados;
- usen un algoritmo establecidos en la sección 7.1.3;
- tengan una longitud de clave que sea apropiada para el algoritmo y para el período de validez del certificado del PCSC VIT S.A., de acuerdo con la sección 6.1.5 de tamaños de clave;
- tomen en cuenta los requisitos del tamaño de clave de la CA Raíz-Py.

Certificados de suscriptores.

Según lo especificado en la PC de cada tipo de certificado.

6.1.2. ENTREGA DE LA CLAVE PRIVADA AL TITULAR

Según lo especificado en las Políticas de Certificación de cada tipo de certificado.

6.1.3. ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

La clave pública es tratada desde su generación mediante mecanismos seguros que aseguran su autenticidad e integridad, impidiendo que sea alterada en su tránsito.

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

La distribución de la clave pública del PCSC VIT S.A. se realiza a través dela distribución de su Certificado Digital del PCSC VIT S.A., el cual se encuentra en el Repositorio Público en http://www.efirma.com.py

6.1.5. TAMAÑO DE LA CLAVE

El tamaño de las claves es suficientemente largo para prevenir que otros puedan determinar la clave privada utilizando cripto-análisis durante el periodo de uso del par de claves.

Certificado de CA

El tamaño de las claves para el PCSC VIT S.A. tendrá mínimo 4096 bits RSA.

Certificados de suscriptores

Según lo especificado en la PC de cada tipo de certificado.

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

La DPC debe prever que los parámetros para la generación de claves asimétricas del PCSC responsable adoptarán el estándar definido en el documento DOC-ICPP-06 [5].

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

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

Certificado del PCSC VIT S.A.

La Clave privada del Certificado Digital del PCSC VIT S.A. podrá ser utilizado con el único propósito de:

Firmar los certificados de sus Suscriptores; y,

Firmar la LCR correspondiente

El valor del campo key usage para este certificado es: KeyCertsign=1; CRLSign=1.

Certificado de suscriptores

Según lo especificado en las Políticas de Certificación de cada tipo de certificado.

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

6.2.1 ESTÁNDARES Y CONTROLES DEL MÓDULO CRIPTOGRÁFICO

El PCSC VIT S.A. mantiene controles y estándares según lo especificado en el documento DOC-ICPP-06 [5], para asegurar que su clave privada permanezca confidencial, mantenga su integridad, y que el acceso al hardware criptográfico esté limitado a personas autorizadas. La copia de respaldo de la clave privada de la CA se realiza conforme se especifica en el punto 6.2.4 de la presente DPC.

Los módulos criptográficos para la CA están certificados FIPS 140-2 nivel 3.

Para los suscriptores es según lo especificado en la PC de cada tipo de certificado.

6.2.2 CONTROL MULTIPERSONA DE LA CLAVE PRIVADA

Para la activación de la clave privada de firma de la CA se debe utilizar controles de acceso de múltiples partes.

Para los suscriptores es según lo especificado en las Políticas de Certificación de cada tipo de certificado.

6.2.3 CUSTODIA (ESCROW) DE LA CLAVE PRIVADA

La clave privada de la CA raíz está custodiada por un dispositivo criptográfico hardware certificado con la norma FIPS 140-2 nivel 3, y se garantiza que la clave privada nunca está fuera del dispositivo criptográfico para su uso. La activación y uso de la clave privada requiere el control multipersona detallado anteriormente.

Para los suscriptores es según lo especificado en las Políticas de Certificación de cada tipo de certificado.

6.2.4. RESPALDO/COPIA DE LA CLAVE PRIVADA

Existe un procedimiento de respaldo y recuperación de claves de los módulos criptográficos de la CA que se puede aplicar en caso de contingencia.

Se mantienen, como mínimo, los mismos controles indicados en el punto 6.2.2.

Los respaldos de clave privada del PCSC VIT S.A. son únicamente para propósitos de recuperación en caso de aplicación del Plan de Contingencia, Plan de recuperación frente a desastres, y Plan de Continuidad del negocio del PCSC VIT S.A.. En ellos se incluyen procesos de recuperación de desastres para todos los componentes críticos del sistema de la CA, incluyendo el hardware, software y claves, en el caso de falla de uno o más de estos componentes.

Los dispositivos criptográficos utilizados para el almacenamiento del respaldo de la clave privada del PCSC VIT S.A. son guardados de forma segura, en un sitio alterno, con los mismos niveles de seguridad que el sitio principal, para que sea recuperado en el caso de un desastre.

Las partes de la clave secreta o los componentes necesarios para usar y gestionar los dispositivos criptográficos de recuperación de desastres, estarán también guardados con seguridad en una ubicación fuera del sitio principal.

Para los suscriptores es según lo especificado en las Políticas de Certificación de cada tipo de certificado.

6.2.5. ARCHIVADO DE LA CLAVE PRIVADA

El PCSC VIT S.A. archiva sus claves privadas por un periodo de 10 (diez) años después de la emisión del último certificado.

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

Para los suscriptores es según lo especificado en las Políticas de Certificación de cada tipo de certificado.

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

La clave privada del PCSC VIT S.A. generada por un módulo criptográfico seguro, sólo será transferida, en caso de transporte, mediante un procedimiento privado de manera cifrada en un dispositivo criptográfico seguro, sujeto a los mismos controles empleados para la generación de la clave original y a la sección 6.2.4.

En los casos en los que se transporten claves privadas fuera de los módulos criptográficos, éstas estarán protegidas de forma que se asegure el mismo nivel de protección que si estuviesen físicamente en el interior de los módulos criptográficos.

Para los suscriptores es según lo especificado en la PC de cada tipo de certificado.

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

Los métodos de activación de clave de la CA se basan en mecanismos de autenticación de múltiples factores. Son de ámbito privado y distribución restringida.

Para los suscriptores es según lo especificado en las Políticas de Certificación de cada tipo de certificado.

6.2.9. MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

Los métodos de desactivación de clave de la CA sonde ámbito privado y distribución restringida .Puede realizarse de varias formas, entre ellas, desde el software de administración de la CA, o por time-

out. La desactivación de la misma no implica su eliminación del dispositivo criptográfico donde se almacenan y utilizan.

Para los suscriptores es según lo especificado en las Políticas de Certificación de cada tipo de certificado.

6.2.10. MÉTODO DE DESTRUCCIÓN DE CLAVE PRIVADA

Existe un procedimiento de destrucción de claves de la CA, el mismo incluye los requerimientos de la autorización necesaria para destruirlas.

La CA elimina sus claves privadas de los módulos criptográficos y el respaldo de las mismas cuando hayan expirado o hayan sido revocadas.

Para los suscriptores es según lo especificado en las Políticas de Certificación de cada tipo de certificado.

6.3. OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES

6.3.1. ARCHIVO DE LA CLAVE PÚBLICA

El PCSC VIT S.A. almacena y gestiona tanto su clave pública como la de los titulares de certificados, las LCRs emitidas y el sistema OCSP correspondientes a su infraestructura, después de la expiración de los certificados correspondientes por un periodo de al menos 10 (diez) años desde su última emisión, para la verificación de firmas generadas durante si periodo de validez.

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

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 por la jerarquía de la ICPP para determinados usos.

En el caso del PCSC VIT S.A., corresponden a:

Certificado de PCSC VIT S.A.

Tiempo de uso: 6 años

Tiempo operacional: 10 años

El Certificado emitido por la CA Raíz de Paraguay al PCSC VIT S.A. tiene un tiempo operacional de 10 años, que resulta de la suma del tiempo de uso de su certificado (6 años) más el tiempo de validez máximo del certificado de su suscriptor (4 años).

Solamente durante el tiempo de uso de su certificado, el PCSC VIT S.A. podrá emitir certificados a sus suscriptores. En los años restantes del tiempo operacional solo podrá firmar la LCR de usuarios o suscriptores.

Certificado de suscriptores

Según lo especificado en las Políticas de Certificación de cada tipo de certificado.

6.4 DATOS DE ACTIVACIÓN

El PCSC VIT S.A. mantiene estrictos controles en los datos de activación para operar los módulos criptográficos y que son protegidos por múltiples factores, con dispositivos criptográficos, PIN, código de acceso.

6.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

Certificado de CA

El PCSC VIT S.A. cuenta con un procedimiento seguro, interno, de uso privado y distribución restringida para generar e instalar los datos de activación, que requieren el uso de múltiples partes y factores con dispositivos criptográficos y códigos de acceso.

Certificados de suscriptores

Según lo especificado en las Políticas de Certificación de cada tipo de certificado.

6.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

Sólo el personal autorizado del PCSC VIT S.A. posee los dispositivos criptográficos y conoce sus claves de acceso propias para acceder a los datos de activación.

6.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

Los datos de activación de los módulos criptográficos del PCSC VIT S.A. son cambiados al menos una vez cada seis meses.

6.5 CONTROLES DE SEGURIDAD DEL COMPUTADOR

6.5.1 REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS

El PCSC VIT S.A. realiza el proceso de generación del par de claves offline para impedir el acceso remoto no autorizado.

Cada computador del PCSC VIT S.A., relacionado directamente con los procesos de emisión, expedición, distribución, suspensión, revocación y gestión de certificados, implementan, 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 VIT S.A.;

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 en combinación 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 VIT S.A., el equipo que fue sometido a mantenimiento debe ser inspeccionado. En cualquier equipo que ya no se utilice de forma permanente, son destruidas de él, de manera definitiva, todas las informaciones sensibles almacenadas, relativas a la actividad del PCSC VIT S.A. Todos estos eventos son registrados con fines de auditoría.

Cualquier equipo incorporado en el PCSC VIT S.A. 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

Los sistemas sensibles del PCSC VIT S.A. están en un ambiente informático dedicado y aislado, son de alta seguridad y confiabilidad, con procesos de auditoría, y utilizan productos para la prestación de servicios de certificación con certificación "CommonCriteria".

6.5.3. CONTROLES DE SEGURIDAD PARA LAS AUTORIDADES DE REGISTRO

Según lo especificado en especificados en el documento DOC-ICPP-05 - CARACTERÍSTICAS MINÍMAS DE SEGURIDAD PARA LAS AR DE LA ICPP PARAGUAY, ítem 4.1, 4.2, 5.

6.6 CONTROLES TÉCNICOS DEL CICLO DE VIDA

En los siguientes ítems, son descritos, cuando sean aplicables, los controles implementados por el PCSC VIT S.A. y por las AR a ella vinculada en el desarrollo de sistemas y en la gestión de la seguridad.

6.6.1 CONTROLES PARA EL DESARROLLO DEL SISTEMA

El PCSC VIT S.A. mantiene controles internos para asegurar las actividades de desarrollo, mantenimiento y gestión del ciclo de vida de los sistemas de la CA.

6.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD

Los Administradores del PCSC VIT S.A. son los responsables de garantizar que se cumplan los procedimientos de seguridad correctamente. Además de ejecutar revisiones periódicas para asegurar el cumplimiento de los estándares de implementación de seguridad.

6.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

El PCSC VIT S.A. incluye controles en la gestión de seguridad por medio de herramientas y procedimientos que verifican la adherencia a la configuración de seguridad de los sistemas operativos y redes.

6.6.4. CONTROLES EN LA GENERACIÓN DE LCR

Antes de su publicación, todas las LCR generadas por el PCSC VIT S.A., son 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

6.7.1. DIRECTRICES GENERALES

El equipo del PCSC VIT S.A. está dentro de los límites de la red interna, operando bajo un nivel de seguridad de red crítico.

La red de la CA está protegida contra ataques. El nivel de seguridad de red incluye:

a) La encriptación de las conexiones involucradas con las operaciones de la CA.

b) Los sitios Web están provistos de certificados SSL.

c) La red está protegida por firewalls y sistemas de detección de intrusos.
d) Los accesos externos a información de bases de datos de la CA están prohibidos.
e) La CA controla la ruta de acceso del usuario desde la terminal hasta los servicios.
f) Los componentes de la red local se mantienen en un ambiente físicamente seguro y sus configuraciones son auditadas periódicamente.
g) Los datos sensibles se encriptan cuando se intercambian sobre redes públicas o no confiables.
h) En los servidores de la CA solo están habilitados los servicios esenciales para el funcionamiento de la aplicación.

6.7.2. FIREWALL

El PCSC VIT S.A. dispone de mecanismos de firewall en equipos de uso específico, configurados exclusivamente para esa función. El 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 VIT S.A.

El software de firewall implementa registros de auditoría.

6.7.3. SISTEMA DE DETECCIÓN DE INTRUSOS (IDS)

El PCSC VIT S.A. implementa un sistema de detección de intrusos que tiene la capacidad de ser configurado para reconocer ataques en tiempo real y responde 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, promueve 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 de un registro de los eventos en logs, recuperables en archivos de tipo texto.

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. La frecuencia de examen de los archivos de registro es como mínimo diario y todas las acciones tomadas como resultado de este examen deben son documentadas.

6.8. FUENTES DE TIEMPO

Todos los sistemas 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 VIT 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 VIT S.A. deberán implementar la versión 3 (tres).

7.1.2. EXTENSIONES DEL CERTIFICADO

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

7.1.2. EXTENSIONES DEL CERTIFICADO

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;
b) Identificador de la clave de 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 VIT S.A.;
c) Uso de Claves "Key Usage", crítica: solamente los bits KeyCertSign y CRLSign 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 VIT S.A., para la emisión de certificados de personas físicas o jurídicas;
    d.1.2) el campo policyQualifiers;
        d.1.2.1) el campo DPC Pointer debe contener la dirección web de la DPC del PCSC VIT S.A.
        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 [nombre del PCSC]"
e) Restricciones Básicas "Basic Constraints", crítica:
    e.1) el campo Subject Type debe contener CA=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 ACRaiz-Py.

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

7.1.3. IDENTIFICADORES DE OBJETO DE ALGORITMOS

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

7.1.4. FORMAS DEL NOMBRE

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

OID=2.5.4.6 C= PY;

OID=2.5.4.10 O= ICPP;

OID=2.5.4.11 OU= Prestador Cualificado de Servicios de Confianza;

OID: 2.5.4.3 CN= VIT S.A.

OID: 2.5.4.5 Serial Number= RUC80080099-0

7.1.4.2. Excepcionalmente, para aquellos Prestadores de Servicios de Certificación habilitados por Leyes anteriores cuyo certificado se encuentre válido y vigente, deberán 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= [denominación o razón social de la persona jurídica habilitada como PCSC en mayúsculas y sin tildes, según documento de identificación];

c) OID: 2.5.4.3 CN= [siglas CA- seguido de la denominación o razón social de la persona jurídica habilitada como PCSC en mayúsculas y sin tildes, según documento de identificación]; y

d) OID: 2.5.4.5 Serial Number[conforme al formato descripto en el ítem 3.1.4.1 de este documento].

En caso de revocación o emisión de un nuevo certificado de PCSC VIT S.A., esta excepción no podrá aplicarse por lo que el Prestador de Servicios de Certificación deberá indefectiblemente adoptar lo dispuesto en el ítem 7.1.4.1.

7.1.5. RESTRICCIONES DEL NOMBRE

Los certificados emitidos bajo esta política cuentan con DN conforme a las recomendaciones X.509 que son únicos y no ambiguos.

Los nombres deberán escribirse tal y como figuran en el documento de identidad presentado.

La ICPP establece las siguientes restricciones de nombres, aplicables a todos los certificados:

a) no se deben utilizar tildes ni diéresis; y

b) además de los caracteres alfanuméricos, sólo se podrán utilizar los siguientes caracteres especiales:

Tabla 4 - Caracteres especiales permitidos en los nombres

Caracteres	Código (hexadecimal)
Blanco	20
!	21
"	22
#	23
$	24
%	25
&	26
'	27
(	28
)	29
*****	2ª
+	2B
,	2C
-	2D
.	2E
/	2F
:	3ª
;	3B
=	3D
?	3F
@	40
\	5C

7.1.6. OID (OBJECT IDENTIFIER) DE LA DPC

El OID asignados a esta DPC se indica en el apartado 1.2. de esta DPC.

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 VIT S.A., el campo ***policyQualifiers*** de la extensión "***Certificate Policies***" contiene la dirección web (URL) de la DPC de la CA Raíz-Py que emite el certificado.

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

Las Listas de Certificados Revocados LCRs deberán son firmadas o selladas utilizando el algoritmo definido en el documento *DOC-ICPP-06 [7]*.

7.2.1 NÚMERO (S) DE VERSIÓN

Las LCRs generadas por el PCSC VIT S.A. implementan 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

En este ítem, se describen todas las extensiones de LCR utilizadas por el PCSC VIT 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 VIT S.A. que firmara o sellara la LCR;
b) Número de LCR "CRL Number" no crítico: debe contener un número secuencial para cada LCR emitida por el PCSC VIT S.A.; 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 son implementados en la versión 1 de la norma ITU X.509 de acuerdo con el perfil establecido en el RFC 6960. Los mismos son firmados o sellados utilizando el algoritmo definido en el documento *DOC-ICPP-06 [7]*.

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

Si se implementa, debe cumplir con el RFC 6960.

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

8.1 FRECUENCIA O CIRCUNSTANCIAS DE EVALUACIÓN

El PCSC VIT S.A. será auditado, al menos cada veinticuatro (24) meses, corriendo con los gastos que ello genere, por un OEC. La finalidad de la auditoría es confirmar que el PCSC VIT S.A., como los servicios de confianza cualificados que presta, cumple con los requisitos establecidos en esta DP y en la normativa vigente. El PCSC VIT S.A. enviará un 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 al PCSC VIT S.A. que correrá con los gastos de la misma., para confirmar que tanto el PCSC como los servicios de confianza cualificados que presta cumplen los requisitos de esta DP y de la normativa vigente.

La PCSC VIT S.A., implementa un programa de auditorías internas conforme a lo estipulado en el ítem correspondiente de la norma ISO 27002/2022 para la verificación de su sistema de gestión.

Cuando la AC Raíz-Py requiera al PCSC VIT S.A. que corrija el incumplimiento de requisitos de esta DP o de la normativa vigente, y el mismo 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 son efectuadas conforme a las disposiciones en materia de auditoría, reglamentadas por la AC Raíz-Py.

El PCSC VIT 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 es recurrible.

8.2 IDENTIDAD / CALIDAD DEL EVALUADOR

El equipo de Auditoría Interna está conformado por personal calificado con experiencia en tecnología de la información, seguridad, tecnología de PKI y criptografía.

8.3 RELACIÓN DEL EVALUADOR CON LA ENTIDAD EVALUADA

En el caso de las auditorías externas, los auditores deberán ser independientes e imparciales y deberán ejecutar las evaluaciones acorde al procedimiento establecido por el MIC.

En el caso de las auditorías internas, los auditores son independientes funcionalmente del área objeto de evaluación.

8.4 ASPECTOS CUBIERTOS POR LA EVALUACIÓN

Los elementos objeto de 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) Cumplimiento de la legislación vigente, entre otros.

8.5 ACCIONES TOMADAS COMO RESULTADO DE UNA DEFICIENCIA

El PCSC VIT S.A. tiene procedimientos para ejecutar acciones correctivas para las observaciones detectadas tanto en las Auditorías externas como en las internas.

8.6 COMUNICACIÓN DE RESULTADOS

El PCSC VIT S.A. publica en el Repositorio web los informes relevantes de las auditorías realizadas.

9. OTROS ASUNTOS LEGALES Y COMERCIALES

9.1 TARIFAS

Según lo especificado en las Políticas de Certificación de cada tipo de certificado.

9.1.1 TARIFAS DE EMISIÓN Y ADMINISTRACIÓN DE CERTIFICADOS

Según lo especificado en las Políticas de Certificación de cada tipo de certificado.

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

La Política de Reembolsos del PCSC VIT S.A. refiere a los Certificados Cualificados que emite bajo cualquiera de sus Políticas de Certificación. El PCSC VIT S.A. podrá otorgar un reembolso de la totalidad del importe abonado por el solicitante para los certificados con fallos u errores, o la re-emisión de su certificado sin costo alguno cuando:

a) El solicitante presenta un reclamo sobre dicho certificado dentro de los 15 días posteriores a su fecha de emisión, y
b) dicho reclamo obedece a una falla en el certificado u error en la emisión del mismo por parte del PCSC VIT S.A.

Pasados los 15 días posteriores a la fecha de emisión del certificado, se entenderá total aceptación del certificado emitido y del servicio brindado por el PCSC VIT S.A., y no se realizarán reembolsos ni devoluciones de ningún tipo.

9.2 RESPONSABILIDAD FINANCIERA

9.2.1 COBERTURA DE SEGURO

El PCSC VIT 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 O JURÍDICAS TITULARES DE CERTIFICADOS

No disponible.

9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

9.3.1 ALCANCE DE LA INFORMACIÓN CONFIDENCIAL

Se declara expresamente como información confidencial y no podrá ser divulgada a terceros, excepto en los casos en que la normativa exija lo contrario:

a) Documentaciones que guardan relación con la Solicitud de suscriptores, incluyendo Información financiera y de negocio de los suscriptores.
b) La información vinculada a la continuidad del negocio, contingencia y emergencias.
c) Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
d) Toda información relativa a los parámetros de seguridad, control y procedimientos de auditoría.
e) Toda información que mantiene la CA y que pudiera perjudicar la normal realización de las operaciones
f) Toda otra Información o documentos que el PCSC VIT S.A. haya determinado como “CONFIDENCIAL”

9.3.2 INFORMACIÓN NO CONTENIDA EN EL ALCANCE DE INFORMACIÓN CONFIDENCIAL

No será considerada información confidencial y se considera información de acceso público:

a) La contenida en la Declaración de Prácticas de Certificación y en las diferentes Políticas de Certificación aprobadas.

b) El estado de los certificados emitidos.

c) La lista de certificados revocados (LCR)

d) Toda aquella información que sea calificada como "PÚBLICA".

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 VIT S.A. será generada y mantenida por el mismo, quien será responsable de su secreto. La divulgación o el uso indebido de la clave privada será de su exclusiva responsabilidad.

Los titulares de certificados de firma electrónica cualificada y 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.

La PCSC VIT S.A. brinda servicios de generación o gestión de datos de creación de firma electrónica en nombre del firmante, utilizando sistemas y productos fiables, incluidos canales de comunicación electrónicos seguros, aplica procedimientos y mecanismos técnicos y organizativos adecuados para garantizar que el entorno es confiable y que los datos de creación de firma se utilizan bajo el control exclusivo del titular del certificado. Además de custodiar y proteger los datos de creación de firma frente a cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad.

Si existen responsabilidades específicas para las PCPs implementadas, las mismas deben ser descriptas en dichas PCs, en el ítem correspondiente.

9.4 PRIVACIDAD DE INFORMACIÓN PERSONAL

9.4.1 PLAN DE PRIVACIDAD

El PCSC VIT S.A. implementa una ***Política de Privacidad*** de información de acuerdo con la normativa vigente. Dicha ***Política de Privacidad*** se encuentra publicada en su **Repositorio** web https://www.efirma.com.py

EL PCSC VIT S.A. respeta las condiciones de confidencialidad y seguridad de acuerdo con las normas vigentes respectivas. Salvo la información contenida en el certificado, la suministrada por los firmantes, suscriptores o signatarios a los Prestadores Cualificados de Servicios de Confianza, se considerará PRIVADA y CONFIDENCIAL, en los términos de la normativa vigente y en esa medida no se podrá utilizar para fines distintos a aquellos para lo que fueron recolectados ni divulgar sin autorización expresa y escrita de los firmantes, suscriptores o signatarios.

9.4.2 INFORMACIÓN TRATADA COMO PRIVADA

Cualquier información acerca de los titulares de certificados cualificados que no esté públicamente disponible a través del contenido del certificado emitido ni a través de los servicios de la LCR, se trata como información PRIVADA.

9.4.3 INFORMACIÓN QUE NO ES CONSIDERADA COMO PRIVADA

En el PCSC VIT S.A. el tratamiento de la información que no es considerada como privada, está 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 VIT S.A. y sus ARs vinculadas aseguran que la información PRIVADA no es comprometida ni divulgada a terceras partes.

9.4.5 NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA

La información privada obtenida por el PCSC VIT 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 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

Aplicase 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 VIT S.A., en el marco de prestación de servicios de creación, verificación y validación de firmas electrónicas cualificadas y certificados relativos a estos servicios, responde por el incumplimiento de lo establecido en las Políticas, Declaración de Prácticas de Certificación y en la normativa vigente. De igual manera asume 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.

9.6.1.1 AUTORIZACIÓN PARA CERTIFICADO

El PCSC VIT 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 VIT S.A., 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 VIT S.A. implementa procedimientos para verificar la veracidad de la información en los certificados, contenidos en los ítems 3 y 4 de esta DPC.

9.6.1.3 IDENTIFICACIÓN DEL SOLICITANTE DE CERTIFICADO

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

9.6.1.6 REVOCACIÓN

El PCSC VIT S.A. revocará los certificados de la ICPP por cualquier motivo especificado en este documento.

9.6.1.7 EXISTENCIA LEGAL

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

9.6.2 REPRESENTACIONES Y GARANTÍAS DE LA AR

Aplicase conforme al ítem 4 de esta DPC.

9.6.3 REPRESENTACIONES Y GARANTÍAS DEL TITULAR DE CERTIFICADO

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

El PCSC VIT S.A. informa 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 VIT S.A. 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

El PCSC VIT S.A. en el marco de su actividad como PCSC, la limitación de su responsabilidad será conforme a las disposiciones de la ley N° 6822/2021, sus modificaciones y reglamentaciones.

9.9 INDEMNIZACIONES

El PCSC VIT S.A. podrá indemnizar a los suscriptores exclusivamente según los requerimientos de la legislación vigente en materia de Prestadores de Servicios de Certificación habilitados bajo subordinación de la CA RAÍZ.

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

El procedimiento para enmiendas y que propuestas de modificación de la DPC deben ser revisadas y aprobadas por la AC Raíz-Py antes de ser implementadas. Las modificaciones deben documentarse y mantenerse actualizadas a través de versiones.

9.12.2. PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN

Toda enmienda o modificación de esta DPC se publicará en el **Repositorio** web https://www.efirma.com.py.

9.12.3. CIRCUNSTANCIAS EN QUE LOS OID DEBEN SER CAMBIADOS

Los cambios en los OIDs corresponden a nuevas políticas que contengan otros objetos con OIDs adicionales. Si la estructura del certificado se mantiene entonces no es necesario cambiar los OIDs.

9.13 DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS

Las controversias derivadas de la presente DPC se resolverán de conformidad con la legislación vigente. Debe también establecerse que la DPC del PCSC VIT S.A. 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 Declaración de Prácticas de Certificación se adecua a legislación vigente aplicable a la materia.

9.16 DISPOSICIONES VARIAS

9.16.1 ACUERDO COMPLETO

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

Esta DPC representa las obligaciones y deberes aplicables al PCSC VIT 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 son públicos e indisponibles, y no pueden ser cedidos o 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)

De acuerdo con la legislación vigente.

9.16.5 FUERZA MAYOR

En este ítem de la DPC se debe indicar la limitación de responsabilidad en caso de fuerza mayor que pueda aplicar al servicio que presta.

9.17 OTRAS DISPOSICIONES

Éste ítem no aplica.

10. DOCUMENTOS DE REFERENCIA

10.1 REFERENCIAS EXTERNAS

- 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. CertificatePolicy and CertificationPractices Framework”.
- RFC 4210: “Internet X.509 Public Key Infrastructure. Certificate Management Protocol (CMP)”.
- RFC 5280: “Internet X.509 Public Key Infrastructure.Certificate and CertificateRevocationList (CRL) Profile”.
- RFC 6712: “Internet X.509 Public Key Infrastructure.HTTP Transfer fortheCertificate Management Protocol (CMP)”.

- RFC 6960: "X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP".
- ISO 27002:2022:" - Informationtechnology - Security techniques - Code of practiceforinformationsecuritymanagement".
- ITU X.500/ISO 9594: "Informationtechnology - Open SystemsInterconnection - TheDirectory: Overview of concepts, models and services".
- ITU X.509/ISO/IEC9594-8:"- Informationtechnology- Open SystemsInterconnection-TheDirectory-Part 8: Public-key and attributecertificateframeworks".

10.2 REFERENCIAS A DOCUMENTOS QUE COMPONEN LA ICPP

Tabla Nº 7– Documentos Referenciados

REF.	NOMBRE DEL DOCUMENTO	CÓDIGO
[1]	Directivas obligatorias para la formulación y elaboración de la política de certificación de los Prestadores Cualificados de Servicios de Confianza de la ICPP	DOC-ICPP-04
[2]	Procedimientos operacionales mínimos para el PCSC que brinde el servicio 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 de sello.	DOC-ICPP-07
[3]	Procedimiento de identificación del solicitante y comunicación de irregularidades en el proceso de emisión de un certificado ICPP	DOC-ICPP-09
[4]	Procedimiento de identificación biométrica en la ICPP	DOC-ICPP-10
[5]	Procedimiento de identificación del solicitante de certificados por videoconferencia en la ICPP	DOC-ICPP-08
[6]	Características mínimas de seguridad para las autoridades de registro de la ICPP.	DOC-ICPP-05

[7]	Normas de algoritmos criptográficos de la ICPP.	DOC-ICPP-06
[8]	Procedimiento de acreditación de los organismos de evaluación de la conformidad	DOC-ICPP-11
[9]	Criterios y procedimientos para realización de auditorías en las entidades miembros de la ICPP	DOC-ICPP-12
[10]	Criterios y procedimientos para la inspección de los miembros de las entidades de la ICPP	DOC-ICPP-14
[11]	Directrices de la Política tarifaria de la AC Raíz-Py	DOC-ICPP-13