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

DOC-PCF3-VITSA

Versión 1.0

Documento: POLÍTICA DE CERTIFICACIÓN DE CERTIFICADOS TIPO F3 VIT S.A.
Versión: 1.0
Razón Social: VIT S.A.
Marca Comercial: eFirma
Estado del Documento: Aprobado
Fecha de emisión: 30 Noviembre 2022
Sitio de internet oficial: https://www.efirma.com.py
URL del documento: https://www.efirma.com.py/repositorio/DOC-PCF3-VITSA Vers 1.pdf
Clasificación: PÚBLICO
Archivo: DOC-PCF3-VITSA Vers 1.docx
Nº de páginas: 75
Preparado por: VIT S.A.

CONTROL DOCUMENTAL

Documento	
Título: POLÍTICA DE CERTIFICACIÓN DE CERTIFICADOS TIPO F3 VIT S.A.	**Nombre Archivo:** DOC-PCF3-VITSA Vers 1
Código: DOC-PCF3-VITSA	**Soporte Lógico:** https://www.efirma.com.py/
Fecha: 30/11/2022	**Ubicación Física:** Avda. España 2028 c/ Brasilia - 6to piso
Versión: 1.0	

Registro de cambios		
Versión	**Fecha**	**Motivo de cambio**
1.0	30/11/2022	Versión inicial

Distribución del documento	
Nombre	**Área**
Ministerio de Industria y Comercio (MIC)	Dirección General de Firma Digital y Comercio Electrónico (DGFDyCE).
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 es la Política de Certificación (PC) asociada a los **certificados cualificados de certificados cualificados de firma electrónica y certificados cualificados tributarios Tipo F3**, que contiene las reglas a las que se sujeta la gestión y el uso de los certificados definidos en esta política. Se describen los papeles, responsabilidades y relaciones entre el usuario final y VIT S.A., y las reglas de solicitud, adquisición gestión y uso de los certificados.

Este documento matiza y complementa a la Declaración de Prácticas de Certificación VIT S.A.

Esta PC es aplicable a los siguientes certificados:

- Certificado cualificado de firma electrónica
  - ➢ F3
- Certificado cualificado tributario
  - ➢ F3

Los tipos de certificados “F” define escalas de seguridad (1, 2 y 3), asociados con requisitos menos o más estrictos atendiendo al tipo de certificado. El nivel de seguridad estará caracterizado por los requisitos mínimos definidos para aspectos como: algoritmo y tamaño de la clave criptográfica, medios de almacenamiento de clave, proceso de generación del par de claves, procedimiento de identificación del titular del certificado, frecuencia de emisión de la lista de certificados revocados (LCR) y el plazo de validez del certificado.

El par de claves criptográficas relacionadas a los tipos de certificado F3 deberá obligatoriamente ser generadas y almacenadas en módulos criptográficos tipo hardware gestionado y custodiado por un PCSC en un:

i) módulo de seguridad hardware (HSM).

1.2. NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

Documento: POLÍTICA DE CERTIFICACIÓN DE CERTIFICADOS TIPO F3 VIT S.A.

Versión: 1.0

DPC relacionada: Declaración de Prácticas de Certificación (DPC) de VIT S.A.

Estado: APROBADO

Fecha de emisión: 30 de noviembre de 2022

URL del documento: https://www.efirma.com.py/repositorio/DOC-PCF3-VITSA Vers 1.pdf

Sitio de internet oficial: https://www.efirma.com.py

Las Políticas de Certificación incluidas en el presente documento son:

Nombre de la Política:

POLÍTICA DE CERTIFICACIÓN de Certificado Cualificado de Firma Electrónica Tipo F3 de VIT S.A. (eFirma)

Versión de la Política	1.0
Estado de la Política	APROBADO
Referencia de la Política / OID de la política	1.3.6.1.4.1.44234.1.1.1.12
Fecha de emisión	30 de noviembre del 2022

Nombre de la Política:

- **POLÍTICA DE CERTIFICACIÓN de Certificado Cualificado Tributario Tipo F3 de VIT S.A. (eFirma)**

Versión de la Política	1.0
Estado de la Política	APROBADO
Referencia de la Política / OID de la política	1.3.6.1.4.1.44234.1.1.1.13
Fecha de emisión	30 de noviembre del 2022

1.3. PARTICIPANTES DE LA ICPP

1.3.1. AUTORIDADES CERTIFICADORAS (AC)

Las entidades y personas que intervienen en la ICPP son:

I. AC Raíz-Py: En la cúspide de la Jerarquía de la Infraestructura de Clave Pública del Paraguay (ICPP), se ubica la AC Raíz-Py, la misma cuenta con un certificado auto emitido y aceptado por los terceros que confían en la ICPP. Emite certificados a los PCSC y a partir de allí, comienza la cadena de confianza. Los certificados digitales emitidos por la AC Raíz-Py se rigen y ajustan a su Declaración de Prácticas de Certificación (DPC), cuyo cumplimiento es de carácter obligatorio.

II. ACI; Es una entidad habilitada por la AA, encargada de operar una AC en el marco de la ICPP, debe contar con un certificado emitido por la AC Raíz-Py y solo podrá emitir certificados a personas físicas o jurídicas que sean usuarios finales. En el ámbito de la ICPP un PCSC es considerada una ACI.

El PCSC VIT S.A. presta servicios de **CREACIÓN, VERIFICACIÓN Y VALIDACIÓN DE FIRMAS ELECTRÓNICAS CUALIFICADAS y CERTIFICADOS RELATIVOS A ESTOS SERVICIOS.**

El PCSC VIT S.A. además está habilitado para prestar servicios de **GENERACIÓN O GESTIÓN DE DATOS DE CREACIÓN DE FIRMA ELECTRÓNICA EN NOMBRE DEL FIRMANTE** en los términos establecidos en el documento DOC-ICPP-07 [2].

El PCSC VIT S.A., habilitado para brindar servicios de **GENERACIÓN O GESTIÓN DE DATOS DE CREACIÓN DE FIRMA ELECTRÓNICA EN NOMBRE DEL FIRMANTE**, utiliza sistemas y productos fiables, incluidos canales de comunicación electrónicos seguros, aplicar procedimientos y mecanismos técnicos y organizativos adecuados para garantizar que el entorno sea confiable y que los datos de creación de firma se utilicen bajo el control exclusivo del titular del certificado. Además, deben custodiar y proteger los datos de creación de firma frente a cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad.

Las claves privadas de los firmantes almacenadas en dispositivos estandarizados conforme lo establecido en el documento DOC-ICPP-06 [1], y las firmas electrónicas cualificadas hechas por la clave privada del firmante en otros sistemas son válidas de conformidad a la Ley N° 6822/2021.

1.3.2. AUTORIDADES DE REGISTRO (AR)

El PCSC VIT S.A. cuenta con la dirección de página web (URL) https://www.efirma.com.py/repositorio-publico-i30, donde se publican los datos referentes a las autoridades de registro (AR) habilitadas por el PCSC VIT S.A. para los procesos de recepción, identificación y remisión de solicitudes de emisión o revocación de certificados electrónicos y de identificación de sus solicitantes:

El PCSC VIT S.A. mantiene las informaciones siempre actualizadas.

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

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

El PCSC deberá igualmente publicar información referente a:

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

1.3.3. AUTORIDADES DE VALIDACIÓN (AV)

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

Las AVs delegadas son autoridades de validación vinculadas al PCSC VIT S.A. mediante un acuerdo operacional.

El PCSC VIT S.A. igualmente publica información referente a:

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

1.3.4. TITULARES DEL CERTIFICADO

En el contexto de esta PC y en relación al PCSC VIT S.A, el titular de certificado es toda persona física o jurídica que confía en un certificado y/o en las firmas digitales generadas a partir de un certificado, emitidos dentro de la jerarquía ICPP.

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 o la AR para desempeñar actividades descritas en esta PC o en su DPC 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 deberá mantener las informaciones arriba, citadas y siempre actualizadas.

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

El PCSC deberá igualmente publicar información referente a:

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

1.3.6.2. PRESTADORES DE SERVICIO DE ALMACENAMIENTO (PSA)

El PSA es una entidad vinculada indefectiblemente a un PCSC mediante un acuerdo operacional que deberá ser autorizada por la AC Raíz-Py con la habilitación correspondiente para prestar servicios de almacenamiento de claves privadas para usuarios finales o servicios de firma digital y de verificación de firmas digitales en documentos y transacciones electrónicas o ambos.

El PCSC VIT SA mantiene las informaciones arriba citadas siempre actualizadas en la página web: www.efirma.com.py.

1.4. USO DEL CERTIFICADO

1.4.1. USOS APROPIADOS DEL CERTIFICADO

Tabla N° 1 – USOS APROPIADOS DEL CERTIFICADO

Tipo de Certificado	Descripción de uso apropiado del Certificado
Certificado Cualificado de Firma Electrónica	**Firma digital** • No repudio (Non-Repudiation) • digitalSignature • keyEncipherment
Certificado Cualificado Tributario	**Firma digital** • No repudio (Non-Repudiation) • digitalSignature • keyEncipherment

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 PC.

Cualquier otro uso de los certificados no especificado en esta DPC, en la correspondiente Política de Certificación y en la normativa vigente, está prohibido y podrá sancionarse llegando a la revocación del mismo.

1.5. ADMINISTRACIÓN DE LA POLÍTICA

1.5.1. ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

Nombre: VIT S.A.

RUC: 80080099-0

Dirección: España c/ Brasilia N° 2028 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

Dirección: España N° 2028 c/ Brasilia

Teléfono: 021-229-350

Dirección de correo electrónico: info@efirma.com.py

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

En primera instancia, la entidad competente para determinar la adecuación de la DPC a esta Política de Certificación es el Directorio y personal autorizado del PCSC VIT S.A. conforme con los Estatutos de la empresa. La aprobación definitiva, según establecido en la normativa vigente, el Ministerio de Industria y Comercio será el encargado final de determinar dicha adecuación.

1.5.4. PROCEDIMIENTOS DE APROBACIÓN DE LA PC

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

1.6. DEFINICIONES, SIGLAS Y ACRÓNIMOS

1.6.1. DEFINICIONES

1. **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.
2. **Autenticación:** proceso técnico que permite determinar la identidad de la persona física o jurídica.
3. **Autoridad de Aplicación:** Ministerio de Industria y Comercio a través de la Dirección General de Comercio Electrónico, dependiente del Viceministerio de Comercio y Servicios.
4. **Autoridad de Certificación:** entidad que presta servicios de emisión, gestión, revocación u otros servicios de confianza basados en certificados cualificados. En el marco de la ICPP, son Autoridades de Certificación, la AC Raíz-Py y el PCSC.
5. **Autoridad de Certificación Raíz del Paraguay:** órgano técnico, cuya función principal es coordinar el funcionamiento de la ICPP. La AC Raíz-Py tiene los certificados de más alto nivel, posee un certificado autofirmado y es a partir de allí, donde comienza la cadena de confianza. Las funciones de la AC Raíz-Py son ejercidas por la AA.

6. **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.
7. **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.
8. **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.
9. **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.
10. **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.
11. **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.
12. **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.
13. **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.
14. **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.
15. **Claves criptográficas:** valor o código numérico que se utiliza con un algoritmo criptográfico para transformar, validar, autenticar, cifrar y descifrar datos.

16. **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.
17. **Compromiso:** violación de la seguridad de un sistema a raíz de una posible divulgación no autorizada de información sensible.
18. **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.
19. **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.
20. **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.
21. **Emisor del certificado:** persona física o jurídica cuyo nombre aparece en el campo emisor de un certificado.
22. **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.
23. **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.
24. **Firmante:** una persona física que crea una firma electrónica.
25. **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.

26. **Habilitación:** autorización que otorga el MIC, una vez cumplidos los requisitos y condiciones establecidos en la norma.
27. **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.
28. **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.
29. **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.
30. **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.
31. **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.
32. **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.
33. **Módulo criptográfico**: software o hardware criptográfico que genera y almacena claves criptográficas.
34. **Módulo de Seguridad de Hardware:** dispositivo basado en un módulo criptográfico tipo hardware que genera, almacena y protege claves criptográficas.
35. **Normas Internacionales:** requisitos de orden técnico y de uso internacional que deben observarse en la prestación de los servicios mencionados en la presente DPC.
36. **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.
37. **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.
38. **Parte usuaria:** persona física o jurídica que confía en el servicio de confianza.
39. **Perfil del certificado:** especificación del formato requerido para un tipo particular de certificado (incluyendo requisitos para el uso de los campos estándar y extensiones).

40. **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.
41. **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.
42. **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.
43. **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.
44. **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.
45. **Repositorio:** sitio principal de Internet confiable y accesible, mantenido por la AC con el fin de difundir su información pública.
46. **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.
47. **Servicio OCSP:** permite utilizar un protocolo estándar para realizar consultas en línea al servidor de la AC sobre el estado de un certificado.
48. **Solicitante de Certificado:** persona física o jurídica que solicita la emisión de un certificado a una AC.
49. **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.
50. **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.
51. **Solicitud de revocación**: documento que se instrumenta mediante un formato autorizado de solicitud para la revocación de un certificado.
52. **Verificación y validación de firm:** determinación y validación de que la firma 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.

53. **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.
54. **X.509:** estándar desarrollado por la ITU, que define el formato electrónico básico para certificados electrónicos.

1.6.2. SIGLAS Y ACRÓNIMOS

Tabla N° 2 –Siglas y Acrónimos

Sigla/Acrónimo	Descripción
AA	Autoridad de Aplicación
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
ICPP	Infraestructura de Clave Pública del Paraguay
PCSC	Prestador cualificado de servicios de confianza
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
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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

2.2. PUBLICACIÓN DE INFORMACIÓN DE CERTIFICACIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

2.3. TIEMPO O FRECUENCIA DE PUBLICACIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

2.4. CONTROLES DE ACCESO A LOS REPOSITORIOS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. NOMBRES

3.1.1. TIPOS DE NOMBRES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

3.1.2. NECESIDAD DE NOMBRES SIGNIFICATIVOS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

3.1.3. ANONIMATO O SEUDÓNIMOS DE LOS TITULARES DE CERTIFICADOS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

3.1.4. REGLAS PARA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

3.1.5. UNICIDAD DE NOMBRES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

3.1.6. PROCEDIMIENTO PARA RESOLVER DISPUTA DE NOMBRE

3.1.7. RECONOCIMIENTO, AUTENTICACIÓN Y ROL DE LAS MARCAS REGISTRADAS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

3.2. VALIDACIÓN INICIAL DE IDENTIDAD

3.2.1. MÉTODO PARA PROBAR POSESIÓN DE LA CLAVE PRIVADA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

3.2.2. AUTENTICACIÓN DE IDENTIDAD DE PERSONA JURÍDICA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

3.2.2.1. DOCUMENTOS REQUERIDOS PARA IDENTIFICAR UNA PERSONA JURÍDICA.

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

3.2.2.2. INFORMACIÓN CONTENIDA EN UN CERTIFICADO EMITIDO PARA UNA PERSONA JURÍDICA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

3.2.3. AUTENTICACIÓN DE IDENTIDAD DE PERSONA FÍSICA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

3.2.3.1. DOCUMENTOS REQUERIDOS PARA IDENTIFICAR UNA PERSONA FÍSICA.

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

3.2.3.2. INFORMACIÓN CONTENIDA EN UN CERTIFICADO EMITIDO PARA UNA PERSONA FÍSICA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

3.2.4. AUTENTICACIÓN DE IDENTIDAD DE UNA MÁQUINA O APLICACIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

3.2.4.1 DOCUMENTOS REQUERIDOS PARA LA IDENTIFICACIÓN DE UNA MÁQUINA O APLICACIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

3.2.4.2 INFORMACIÓN CONTENIDA EN UN CERTIFICADO EMITIDO PARA UNA MÁQUINA O APLICACIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

3.2.4. INFORMACIÓN NO VERIFICADA DEL TITULAR DEL CERTIFICADO

3.2.5. VALIDACIÓN DE LA AUTORIDAD (CAPACIDAD DE HECHO)

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

3.2.6. CRITERIOS PARA INTEROPERABILIDAD

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

3.2.7. PROCEDIMIENTOS COMPLEMENTARIOS

3.2.8. PROCEDIMIENTOS ESPECÍFICOS

3.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE NUEVAS CLAVES

3.3.1. IDENTIFICACIÓN Y AUTENTICACIÓN PARA EMISIÓN DE NUEVAS CLAVES ANTES DE SU EXPIRACIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

3.3.2. IDENTIFICACIÓN Y AUTENTICACIÓN PARA EMISIÓN DE NUEVAS CLAVES DESPUÉS DE LA REVOCACIÓN O EXPIRACIÓN DEL CERTIFICADO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

3.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

3.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE REVOCACIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

4.1. SOLICITUD DEL CERTIFICADO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.1.1. QUIÉN PUEDE PRESENTAR UNA SOLICITUD DE CERTIFICADO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.1.2. PROCESO DE INSCRIPCIÓN Y RESPONSABILIDADES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.1.2.1. RESPONSABILIDADES Y OBLIGACIONES DEL PSC VIT S.A.

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.1.2.2. RESPONSABILIDADES Y OBLIGACIONES DE LA RA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.2. PROCESAMIENTO DE LA SOLICITUD DEL CERTIFICADO

4.2.1. EJECUCIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.2.2. APROBACIÓN O RECHAZO DE SOLICITUDES DE CERTIFICADO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.2.3. TIEMPO PARA PROCESAR SOLICITUDES DE CERTIFICADO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.3. EMISIÓN DEL CERTIFICADO

4.3.1. ACCIONES DEL PCSC DURANTE LA EMISIÓN DE LOS CERTIFICADOS

Según lo especificado en la Declaración de Prácticas de Certificación (CPS) de VIT S.A.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.4. ACEPTACIÓN DEL CERTIFICADO

4.4.1. CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE CERTIFICADO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.4.2. PUBLICACIÓN DEL CERTIFICADO POR EL PCSC

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.5. USO DEL PAR DE CLAVES Y DEL CERTIFICADO

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.6. RENOVACIÓN DEL CERTIFICADO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.6.1. CIRCUNSTANCIAS PARA LA RENOVACIÓN DEL CERTIFICADO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.6.2. QUIÉN PUEDE SOLICITAR RENOVACIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.6.3. PROCESAMIENTO DE SOLICITUDES DE RENOVACIÓN DE CERTIFICADO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.6.5. CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RENOVADO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.6.6. PUBLICACIÓN POR EL PCSC DEL CERTIFICADO RENOVADO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.7. RE-EMISIÓN DE CLAVES DE CERTIFICADO (RE-KEY)

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.7.1. CIRCUNSTANCIAS PARA RE-EMISIÓN DE CLAVES DE CERTIFICADO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.7.2. QUIÉN PUEDE SOLICITAR LA CERTIFICACIÓN DE UNA CLAVE PÚBLICA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.7.3. PROCESAMIENTO DE SOLICITUDES DE RE-EMISIÓN DE CLAVES DE CERTIFICADO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.7.5. CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DE UN CERTIFICADO RE-EMITIDO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.7.6. PUBLICACIÓN POR EL PCSC DE LOS CERTIFICADOS RE-EMITIDOS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.8. MODIFICACIÓN DE CERTIFICADOS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.8.1. CIRCUNSTANCIAS PARA MODIFICACIÓN DEL CERTIFICADO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.8.2. QUIÉN PUEDE SOLICITAR MODIFICACIÓN DEL CERTIFICADO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.8.3. PROCESAMIENTO DE SOLICITUDES DE MODIFICACIÓN DEL CERTIFICADO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.8.4. NOTIFICACIÓN AL TITULAR DEL CERTIFICADO DE LA EMISIÓN DE UN NUEVO CERTIFICADO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.8.5. CONDUCTA CONSTITUTIVA DE ACEPTACIÓN DEL CERTIFICADO MODIFICADO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.8.6. PUBLICACIÓN POR EL PCSC DE LOS CERTIFICADOS MODIFICADOS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.8.7. NOTIFICACIÓN POR EL PCSC DE UNA EMISIÓN DE CERTIFICADO A OTRAS ENTIDADES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.9. REVOCACIÓN Y SUSPENSIÓN

4.9.1. CIRCUNSTANCIAS PARA LA REVOCACIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.9.2. QUIÉN PUEDE SOLICITAR REVOCACIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.9.3. PROCEDIMIENTO PARA LA SOLICITUD DE REVOCACIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.9.4. PERIODO DE GRACIA PARA SOLICITUD DE REVOCACIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.9.6. REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN PARA LA PARTE USUARIA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.9.7. FRECUENCIA DE EMISIÓN DEL LCR

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.9.8. LATENCIA MÁXIMA PARA LCR

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.9.9. DISPONIBILIDAD PARA REVOCACIÓN/VERIFICACIÓN DE ESTADO EN LÍNEA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.9.10. REQUISITOS DE VERIFICACIÓN DE REVOCACIÓN EN LÍNEA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.9.11. OTRAS FORMAS DE ADVERTENCIAS DE REVOCACIÓN DISPONIBLES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.9.12. REQUERIMIENTOS ESPECIALES POR COMPROMISO DE CLAVE PRIVADA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.9.13. CIRCUNSTANCIAS PARA SUSPENSIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.9.14. QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.9.15. PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.9.16. LÍMITES DEL PERÍODO DE SUSPENSIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.10. SERVICIOS DE ESTADO DEL CERTIFICADO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.10.1. CARACTERÍSTICAS OPERACIONALES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.10.2. DISPONIBILIDAD DEL SERVICIO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.10.3. CARACTERÍSTICAS OPCIONALES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.11. FIN DE ACTIVIDADES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.12. CUSTODIA Y RECUPERACIÓN DE CLAVES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

4.12.1. POLÍTICA Y PRÁCTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.1. CONTROLES FÍSICOS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.1.1. LOCALIZACIÓN Y CONSTRUCCIÓN DEL SITIO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.1.2. ACCESO FÍSICO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.1.2.1. NIVELES DE ACCESO FÍSICO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.1.2.2. SISTEMAS FÍSICOS DE DETECCIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.1.2.3. SISTEMAS DE CONTROL DE ACCESO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.1.2.4. MECANISMOS DE EMERGENCIA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.1.3. ENERGÍA Y AIRE ACONDICIONADO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.1.4. EXPOSICIÓN AL AGUA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.1.5. PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.1.6. ALMACENAMIENTO DE MEDIOS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.1.7. ELIMINACIÓN DE RESIDUOS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.1.8. RESPALDO FUERA DE SITIO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.2. CONTROLES PROCEDIMENTALES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.2.1. ROLES DE CONFIANZA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.2.2. NÚMERO DE PERSONAS REQUERIDAS POR TAREA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.2.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.2.4. ROLES QUE REQUIEREN SEPARACIÓN DE FUNCIONES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.3. CONTROLES DE PERSONAL

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.3.1. REQUERIMIENTOS DE EXPERIENCIA, CAPACIDADES Y AUTORIZACIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.3.2. PROCEDIMIENTOS DE VERIFICACIÓN DE ANTECEDENTES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.3.3. REQUERIMIENTOS DE CAPACITACIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.3.4. REQUERIMIENTOS Y FRECUENCIA DE CAPACITACIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.3.5. FRECUENCIA Y SECUENCIA EN LA ROTACIÓN DE LAS FUNCIONES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.3.6. SANCIONES PARA ACCIONES NO AUTORIZADAS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.3.7. REQUISITOS DE CONTRATACIÓN A TERCEROS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.3.8. DOCUMENTACIÓN SUMINISTRADA AL PERSONAL

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.4. PROCEDIMIENTO DE REGISTRO DE AUDITORÍA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.4.1. TIPOS DE EVENTOS REGISTRADOS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.4.2. FRECUENCIA DE PROCESAMIENTO DEL REGISTRO (LOGS)

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.4.4. PROTECCIÓN DEL REGISTRO (LOGS) DE AUDITORÍA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.4.7. NOTIFICACIÓN AL SUJETO QUE CAUSA EL EVENTO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.4.8. EVALUACIÓN DE VULNERABILIDADES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.5. ARCHIVOS DE REGISTROS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.5.1. TIPOS DE REGISTROS ARCHIVADOS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.5.2. PERIODOS DE RETENCIÓN PARA ARCHIVOS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.5.3. PROTECCIÓN DE ARCHIVOS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.5.4. PROCEDIMIENTOS DE RESPALDO (BACKUP) DE ARCHIVO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.5.5. REQUERIMIENTOS PARA SELLADO DE TIEMPO DE REGISTROS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.5.7. PROCEDIMIENTOS PARA OBTENER Y VERIFICAR LA INFORMACIÓN ARCHIVADA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.6. CAMBIO DE CLAVE

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.7. RECUPERACIÓN DE DESASTRES Y COMPROMISO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.7.1. PROCEDIMIENTO PARA EL MANEJO DE INCIDENTE Y COMPROMISO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.7.3. PROCEDIMIENTOS DE COMPROMISO DE CLAVE PRIVADA DE LA ENTIDAD

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.7.3.1. CERTIFICADO DE ENTIDAD ES REVOCADO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.7.3.2. CLAVE DE ENTIDAD ESTÁ COMPROMETIDA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.7.4. CAPACIDAD DE CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

5.8. EXTINCIÓN DE UN PCSC O ENTIDADES VINCULADAS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

6. CONTROLES TÉCNICOS DE SEGURIDAD

6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

6.1.1. GENERACIÓN DEL PAR DE CLAVES

Cuando el titular del certificado sea:

- una persona física, éste será el responsable de generar el par de claves criptográficas, salvo en caso de su gestión en nombre del firmante, en donde las claves privadas asociadas a los certificados son generadas y custodiadas por el módulo de activación de firma del PCSC, de forma que el acceso a dichas claves se realiza por medios que garantizan, con un alto nivel de confianza, el control exclusivo por parte del firmante.

En este ítem, la PC debe describir todos los requisitos y procedimientos referentes al proceso de generación de claves aplicables al certificado que define.

La PC debe indicar el algoritmo a ser utilizado para las claves criptográficas de los titulares de certificados definidos conforme al documento DOC-ICPP-06 [1].

Cuando es generada, la clave privada del titular del certificado deberá ser grabada cifrada mediante un algoritmo simétrico conforme al documento DOC-ICPP-06 [1], en un medio de almacenamiento definido para cada tipo de certificado previsto en la ICPP conforme a lo estipulado en la Tabla N° 2 de este ítem.

La clave privada deberá viajar cifrada, utilizando los mismos algoritmos mencionados en el párrafo anterior, entre el dispositivo generador y el medio utilizado para su almacenamiento.

Los medios de almacenamiento de claves privadas cumplirán los siguientes requisitos garantizando como mínimo, por medios técnicos y de procedimiento adecuados, que:

a) la confidencialidad de las claves privadas utilizadas para la creación de firmas electrónicas, esté garantizada razonablemente.

b) las claves privadas utilizadas para la creación de firma electrónica sólo puedan aparecer una vez en la práctica.

c) exista la seguridad razonable de que claves privadas utilizadas para la creación de firma electrónica no pueden ser hallados por deducción y de que la firma está protegido con seguridad contra la falsificación mediante las tecnologías disponibles en el momento.

d) las claves privadas utilizadas para la creación de firma electrónica puedan ser protegidas por el firmante legítimo de forma fiable frente a su utilización por otros.

Estos medios de almacenamiento de claves privadas no alterarán los datos que deben firmarse o sellarse ni impedirán que dichos datos se muestre al firmante antes de firmar.

La generación o la gestión de las claves privadas de firma electrónica en nombre del firmante sólo podrán correr a cargo de un PCSC, en los términos establecidos en el documento DOC-ICPP-07 [2]

Tabla N° 3 – Medio de almacenamiento de claves criptográficas.

Tipo de certificado	Medio de almacenamiento
F3	• Hardware criptográfico certificado por el MIC (HSM)

6.1.2. ENTREGA DE LA CLAVE PRIVADA AL TITULAR

La PC indica que para el caso de claves privadas asociadas a certificados de los tipos F3 son generadas en un dispositivo de creación de firma bajo el control exclusivo del titular o responsable del certificado, en el cual quedarán custodiadas por el PCSC emitente del certificado para su gestión, por tanto, no existe entrega alguna de la clave privada al titular o responsable del certificado.

6.1.3. ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

No contamos con el documento para la especificación.

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

La PC define las formas para la disponibilización del certificado del PCSC responsable, y de todos los certificados de la cadena de certificación, para los usuarios y la parte usuaria, la cual podrá comprender, entre otras:

a) en el momento de disponibilización de un certificado a su titular, usando el formato definido en el documento DOC-ICPP-06 [1];
b) un directorio;
c) la página WEB del PCSC VIT S. A. con URL https://www.efirma.com.py/repositorio; y

d) otros medios seguros a ser aprobados por el MIC.

6.1.5. TAMAÑO DE LA CLAVE

El tamaño de las claves para el titular del certificado tipo F3 es de 2048 o 4096 bits RSA conforme al RFC 5639.

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

Los parámetros para la generación de claves asimétricas del PCSC VIT S.A. siguen el FIPS 140-2 nivel 2 o superior, de conformidad con las disposiciones en el documento **DOC-PKI-06 [3] "NORMAS DE ALGORITMOS CRIPTOGRÁFICOS DE LA PKI-Paraguay", versión 2.0.**

El Proceso para Verificación de parámetros de generación de claves asimétricas de la AC raíz se realiza de conformidad al FIPS 140-2 nivel 3

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

Los valores del campo ***keyUsage*** para los certificados Tipo F3 y Tipo S3 son:

- nonRepudiaton=1;
- digitalSignature=1; y
- KeyEncipherment=1.

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

6.2.1. ESTÁNDARES Y CONTROLES DEL MÓDULO CRIPTOGRÁFICO

No contamos con el documento para la especificación.

6.2.2. CONTROL MULTIPERSONA DE CLAVE PRIVADA

Ítem no aplicable

6.2.3. CUSTODIA (ESCROW) DE LA CLAVE PRIVADA

Las claves privadas correspondientes a los certificados de los tipos F3 y S3 expedidos a usuarios finales, deberán estar custodiadas en módulos criptográficos administrados por el PCSC conforme a lo establecido en el documento DOC-ICPP-07 [2], de forma que únicamente el firmante pueda acceder a su clave privada. El acceso deberá quedar garantizado mediante el uso de 2 (dos) factores de autenticación

6.2.4. RESPALDO/COPIA DE LA CLAVE PRIVADA

Cualquier titular de un certificado, a su criterio, puede mantener una copia de su propia clave privada.

Sin perjuicio del inciso d) del ítem 6.1.1, los PCSC podrán duplicar las claves privadas asociadas a los certificados de los tipos F3 y S3 conforme a lo establecido en el documento DOC-ICPP-07 [2], únicamente con el objeto de efectuar una copia de seguridad de las citadas claves siempre que se cumplan los siguientes requisitos:

a) la seguridad de los conjuntos de datos duplicados es del mismo nivel que para los conjuntos de datos originales.

b) el número de conjuntos de datos duplicados no supera el mínimo necesario para garantizar la continuidad del servicio.

En cualquier caso, la copia de seguridad debe almacenarse cifrada mediante un algoritmo simétrico aprobado por el documento DOC-ICPP-06 [1] y protegida con un nivel de seguridad no inferior al definido para la clave original.

Además de las observaciones anteriores, la PC debe describir todos los requisitos y procedimientos aplicables al proceso de generar una copia de respaldo.

6.2.5. ARCHIVADO DE LA CLAVE PRIVADA

El PSC VIT S.A. no archiva claves privadas de sus suscriptores para certificados de Tipo F3 emitidos bajo esta Política. La clave privada permanece dentro de los límites del dispositivo criptográfico donde fue generada.

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

El PSC VIT S.A. No gestiona claves privadas de sus suscriptores para certificados emitidos bajo esta Política.

6.2.7. ALMACENAMIENTO DE LA CLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO

Los medios de almacenamiento de la clave privada deberán asegurar, por medios técnicos y de procedimiento adecuados, como mínimo, que:

a) la clave privada es única y su confidencialidad es suficientemente asegurada;

b) la clave privada no puede, con una seguridad razonable, ser deducida y debe estar protegida contra falsificaciones realizadas a través de las tecnologías disponibles en la actualidad; y

c) la clave privada puede ser eficazmente protegida por el legítimo titular contra su utilización por parte de terceros.

Esos medios de almacenamiento no deben modificar los datos que serán firmados, ni deben impedir que esos datos sean presentados al firmante antes del proceso de firma.

Respecto al almacenamiento de claves privadas de usuarios finales en el ámbito de la ICPP, éste podrá ser realizado conforme a los siguientes supuestos:

i. por una entidad debidamente habilitada como PSA, en los términos del documento DOC-PKI-07 [2] **"REQUISITOS MÍNIMOS PARA LA DECLARACIONES DE PRÁCTICAS CERTIFICACIÓN DE PRESTADORES DE SERVICIO DE ALMACENAMIENTO DE LA PKI-Paraguay"** y DOC-PKI-08 [3] **"PROCEDIMIENTOS OPERACIONALES MÍNIMOS PARA LOS PRESTADORES DE SERVICIOS DE ALMACENAMIENTO DE LA PKI Paraguay"**; o

ii. por organizaciones que requieran el almacenamiento de claves privadas de sus empleados o funcionarios en los términos del documento DOC-PKI-09 [4] **"PROCEDIMIENTOS OPERACIONALES MÍNIMOS PARA ORGANIZACIONES QUE REQUIERAN EL ALMACENAMIENTO DE CLAVES PRIVADAS DE LA PKI – Paraguay"**;

En los supuestos mencionados en el párrafo anterior, para hacer efectivo el almacenamiento de claves privadas de usuarios finales se deberá cumplir con las siguientes condiciones:

i. se requerirá el conocimiento y consentimiento expreso del titular del certificado en concordancia con las disposiciones establecidas en la DPC del PCSC VIT S.A.; y

ii. se limitará exclusivamente a los certificados del Tipo F3.

TABLA N° 4 – MEDIO DE ALMACENAMIENTO DE CLAVES CRIPTOGRÁFICAS.

Tipo de Certificado	Medio de Almacenamiento
F3	• Hardware criptográfico homologado por el MIC (HSM)

6.2.8. MÉTODO DE ACTIVACIÓN DE CLAVE PRIVADA

El método de activación de la clave privada será definido por el PSA, encargada de generar el par de claves.

6.2.9. MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

Ítem no aplicable.

6.2.10. DESTRUCCIÓN DE CLAVE PRIVADA

Será responsabilidad del suscriptor mantener bajo su exclusivo control la clave privada, y de igual forma la destrucción de la misma. A modo de referencia se indican: el suscriptor podrá destruir el par de claves, mediante procedimientos establecidos por la PSA encargada de almacenar el mismo.

6.3. OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES

6.3.1. ARCHIVO DE LA CLAVE PÚBLICA

Los certificados generados por el PSC VIT S.A. así las CRL emitidas, son almacenados por VIT S.A. durante el periodo de tiempo establecido en la legislación vigente.

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

La PC prevé que las claves privadas de sus titulares deberán ser utilizadas únicamente durante el periodo de validez correspondiente. Las correspondientes claves públicas podrán ser utilizadas durante todo el periodo de tiempo determinado por la normativa vigente, para la verificación de firmas generadas durante el plazo de validez de los respectivos certificados.

La tabla 3 define los períodos máximos de validez admitidos para cada tipo de certificado previsto por la ICPP.

Tabla N° 5 – Período de validez de los certificados

Tipo de certificado	Tiempo de uso en años	Tiempo operacional en años	Periodo máximo de validez del certificado (en años)
F3 y S3	4	4	Emitido por un tiempo máximo de 4 (cuatro) años, al finalizar ese período pierde su validez.

6.4. DATOS DE ACTIVACIÓN

6.4.1. GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

Para los certificados de tipo F3, la generación y almacenamiento del par de claves se realizan en un HSM de una PSA, con capacidad de generación de claves, siendo activados y protegidos por contraseña y / o la identificación biométrica.

6.4.2. PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

Los suscriptores son responsables de proteger sus datos de activación. Se recomienda que las contraseñas se crean al azar, respetando los procedimientos de seguridad básicos, tales como:

a) Nunca proporcionar la contraseña a terceros;

b) Seleccionar 8 o más caracteres en las contraseñas;

c) Establecer contraseñas con caracteres numéricos y alfanuméricos;

d) guardar la contraseña y

e) No escribirla.

6.4.3. OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

No se estipula el tiempo de vida de los datos de activación, pero se recomienda al suscriptor cambiar los datos de activación en forma periódica.

6.5. CONTROLES DE SEGURIDAD DEL COMPUTADOR

6.5.1. REQUERIMIENTOS TÉCNICOS DE SEGURIDAD DE COMPUTADOR ESPECÍFICOS

Se recomienda que el equipo en el que se generan y utilizan las claves privadas estén provistos de mecanismos mínimos de seguridad informática, tales como:

a) la contraseña de la BIOS activada;

b) control de acceso lógico al sistema operativo;

c) Obligación de utilizar contraseñas seguras;

d) las políticas de contraseñas y bloqueo de cuentas;

e) Antivirus, antispyware y anti troyano, instalada, actualizada y habilitada;

f) Firewall personal o corporativo activados, con permisos de acceso mínimos para las actividades;

g) Sistema operativo mantenido actualizado, con la aplicación de las correcciones necesarias (patches, hotfix, etc.);

h) Protector de pantalla accionado como máximo después de cinco minutos de inactividad y solicitando la contraseña de usuario para desbloquear.

6.5.2. CLASIFICACIÓN DE LA SEGURIDAD DEL COMPUTADOR

Ítem no aplicable.

6.5.3. CONTROLES DE SEGURIDAD PARA LAS AUTORIDADES DE REGISTRO

Ítem no aplicable.

6.6. CONTROLES TÉCNICOS DEL CICLO DE VIDA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

6.6.1. CONTROLES PARA EL DESARROLLO DEL SISTEMA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

6.6.2. CONTROLES DE GESTIÓN DE SEGURIDAD

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

6.6.3. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

6.6.4. CONTROLES EN LA GENERACIÓN DE LCR

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

6.7. CONTROLES DE SEGURIDAD DE RED

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

6.7.1. DIRECTRICES GENERALES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

6.7.2. FIREWALL

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

6.7.3. SISTEMA DE DETECCIÓN DE INTRUSOS (IDS)

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

6.7.4. REGISTRO DE ACCESO NO AUTORIZADO A LA RED

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

6.8. FUENTES DE TIEMPO

Todos los sistemas deben estar 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

El certificado digital cumple con:

- ITU-T X.509 V.3 Information technology Open systems interconnection TheDirectory: Public-key and attribute certificate frameworks
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
- RFC 3739 "Internet X.509 Public Key Infrastructure-Qualified Certificates Profile
- ISO 3166-1 "Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países".
- RFC – 3279 '' Internet X.509 Public Key Infrastructure Algorithm Identifier''

Los perfiles de los certificados definidos en este documento se encuentran detallados a continuación.

Tabla N° 6 – **PERFIL DE CERTIFICADO CUALIFICADO DE FIRMA ELECTRONICA TIPO F3**:

Campo X509 V3	Nombre	Ejemplo	Descripción
Version	**Versión de X509**	**V3**	**Los certificados deben ser X.509 versión 3 (V3)**
SerialNumber	**Número de serie**	**18 6f 57 dd 38 6c 47 ad 54 5d 0c 9a 22 f4 96 60**	**Aleatorio asignado por el PSC VIT S.A. Valor único emitido dentro del ámbito de cada PSC.**
SignatureAlgorithm	**Algoritmo de firma digital del certificado**	**sha256RSA**	**El Algoritmo de firma debe ser como mínimo SHA256RSAencryption.**
Issuer	**DN (Nombre distintivo)**	**CN = CA-VIT S.A.** **O = VIT S.A.** **C = PY**	**Este campo indica los datos de identificación del PSC que emitió el certificado.**

		SERIALNUMBER = RUC 80080099-0	
Subject	**C (País)** **OID: 2.5.4.6**	**PY**	**Este campo debe contener el código del país asignado de acuerdo al ISO 3166.**
	O (Organización) **OID: 2.5.4.10**	**CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA**	**En este campo se identifica el tipo de certificado. En este caso se identifica que corresponde a un certificado de persona física y debe ser PERSONA FÍSICA en mayúscula y sin tilde.**
	OU (Organización) **OID: 2.5.4.11**	**F3**	**En este campo se indica el propósito del uso del certificado digital y el módulo hardware en el que fue almacenada la clave privada del titular del certificado es. :** **FIRMA F3**
	CN (Nombre) **OID: 2.5.4.3**	**JUAN FEDERICO ESCAURIZA VILLALBA**	**Este campo debe contener el/los nombre y apellido/s del titular del certificado, según documento de identificación, en mayúsculas y sin tildes, a excepción de la Ñ. Podrán ser incluidos diéresis y apostrofes si corresponde.**
	SerialNumber **OID: 2.5.4.5**	**CI1234567**	**Este campo debe contener las siglas CI, seguidas del número de cédula de Identidad del titular del certificado, según documento de identificación.**
	SN (SurName) **OID: 2.5.4.4**	**ESCAURIZA VILLALBA**	**Este campo debe contener el/los apellido/s del titular del certificado, según documento de identificación, en mayúsculas y sin tildes, a excepción de la Ñ. Podrán ser incluidos diéresis y apostrofes si corresponde.**
	G (GivenName) **OID: 2.5.4.42**	**JUAN FEDERICO**	**Este campo debe contener el/los nombre/s del titular del certificado, según documento de identificación, en mayúsculas y sin tildes, a excepción de la Ñ. Podrán ser incluidos diéresis y apostrofes si corresponde.**

Validity	**Valid from (Válido desde)**	**viernes, 07 de noviembre de 2016 15:16:58**	**El certificado emitido al usuario final es otorgado por un tiempo máximo de dos años, al finalizar ese período pierde su validez.**
	Valid to (Válido hasta)	**lunes, 07 de noviembre de 2018 15:16:58**	
subjectyPublicKeyInfo	**Subject Public Key (Clave pública del sujeto)**	**30 82 01 0a 02 82 01 01 00 b4 46 43 e2 4a 52 1e b4 87 bc 8c f0 a0 f9 df 1f 68 1d 08 e5 00 fe 20 6b fe 3d 2c 5b 48 ad 46 7d 22 65 03 27 10 0c 86 e1 f7 31 dd 23 37 0b ad 08 cc b9 cd 96 03 64 8e 58 c0 fb 8d f9 5e fa 26 df 07 a1 b4 81 f6 ec a5 e7 5e 50 67 61 31 97 bc 76 94 7f 3e be 28 be 0b a8 03 11 57 64 58 f2 70 da 22 b3 f2 ee 28 18 29 57 1c 59 ce 46 ec f9 4c 2d a9 89 89 65 97 b1 19 fb b1 ab 2a e1 09 65 ed 8c c6 6c 46 db 8c 3e a6 50 9d 9f ff ee 51 8c 33 5c 15 aa 6b 88 8e 8e 7c fa af 1d 9d 48 9f 12 2d b1 98 ff b6 88 ac 09 e0 b5 f9 fc 5a b6 32 32 26 d1 00 72 95 7e d9 5b 5a d8 90 84 86 65 49 32 08 b9 a8 3e 2f 0d db bf 2c 4d 48 e0 6f 52 71 19 5f 86 32 ba dc 87 9d 5f 38 66 80 a7 a7 48 3d 9f 10 09 82 28 47 9b 00 00 cb 1c 90 a1 63 af 86 71 9e 75 24 e5 a2 63 a6 d5 e9 8b 0e 96 44 fb fa a3 f1 b5 02 03 01 fa 01**	**Este campo indica la clave pública del titular del certificado. Codificado de acuerdo con el RFC 5280 y con un largo de clave de 2048 bits o 4096 bits y algoritmo RSA Encryption.**
	Extensiones estándar		
subjectKeyIdentifier	**Subject Key Identifier (Identificador de la clave del Sujeto)**	**ac dc d4 d3 cf 0c 20 ce bb 20 29 1b 93 1a 10 bb b2 36 3f a7**	**Este campo debe contener el hash SHA-1 de la clave pública del titular del certificado. Este Campo es usado por el software de validación para ayudar a identificar un certificado que contiene una determinada clave pública.** **No es crítico.**
authorityKeyIdentifier	**Authority Key Identifier (Identificador de la clave**	**Id. de clave=03 7c 7c 9f 6d 5a 72 a5 91 91 b4 db ec 91 fb 03 5f 7c**	**El campo key identifier debe contener el hash SHA-1 de la clave pública del PSC emisor del certificado. Este campo es**

	de la entidad emisora)	**7c 9d**	**usado por los diversos software de validación para ayudar a identificar a la autoridad certificadora que emitió el certificado en la cadena de Confianza.** **No es crítico.**
keyUsage	**Key Usage(Uso de la clave)**	**nonRepudiaton=1;** **digitalSignature=1;** **KeyEncipherment=1.**	**En certificados tipo F3 solamente pueden ser activados los siguientes bits:** **NonRepudiation (renombrado recientemente con el nombre de contentCommitmen);** **digitalSignature;** **keyEncipherment** **Si es crítico.**
extKeyUsage	**Extended Key Usage (uso extendido de la clave)**	**client authentication** **OID = 1.3.6.1.5.5.7.3.2** **E-mail protection** **OID = 1.3.6.1.5.5.7.3.4,**	**Referencia otros propósitos de la clave, adicionales al uso y debe ser consistente con la extensión keyUsage.** **Si es crítico.**
CertificatePolicies	**Policy Identifier**	**1.3.6.1.4.1.44234.1.1.1.13**	**Debe contener el OID de la CP y la CPS correspondiente y la dirección WEB de la CP y CPS del PSC que emite el certificado. No es crítico.**
	PolicyQualifiers	**https://www.efirma.com.py/repositorio**	
	PolicyIdentifier	**1.3.6.1.4.1.44234.1.1.1.1**	
	PolicyQualifiers	**https://www.efirma.com.py/repositorio**	
BasicConstraints	**CA**	**FALSE**	**En este campo debe ir "TRUE" si el certificado corresponde a una CA o "FALSE" si no corresponde.**
Subject Altenative Name	**Subject Altenative Name (nombre alternativo del sujeto)**	**Rfc822Name=jfederico@efirma.com.py** **DirectoryName** **O= TAV S.A.**	**Campos no obligatorios.** • **Rfc822Name= [email del titular del certificado]** • **DirectoryName=2.5.4.10: [nombre de la organización en el**

		OU= AREA TECNICA **SerialNumber= RUC 80080088-0** **T= SOPORTE TECNICO** **OID=2.5.4.1= ABOGADO**	**que presta servicio el titular del certificado]** • **DirectoryName=2.5.4.11: [nombre de la unidad de la organización en el que presta servicio el titular del certificado]** • **DirectoryName =2.5.4.5: RUC [siglas RUC seguido del 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 si no se registran los datos de la organización en la que presta servicio]** • **DirectoryName OID=2.5.4.12: [*posición o función designada al titular del certificado en la organización en el que presta servicio]*** • **DirectoryName OID=2.5.4.1: [*título académico del titular del certificado]*** **Otros campos que componen la extensión "Subject Alternative Name" podrán ser utilizados en la forma y con los propósitos definidos por la RFC 5280, siempre y cuando estén aprobados por el MIC.** **No critico.**
CRLDistributionPoints	**CRL Distribution Points (Puntos de distribución de CRL)**	**[1]Punto de distribución CRL** **Nombre del punto de distribución:** **Nombre completo:** **Dirección URL= https://www.efirma.com.py/repositorio/efirma2.crl** **[2]Punto de distribución CRL** **Nombre del punto de distribución:** **Nombre completo:** **Dirección URL= https://www.efirma.com.py/repositorio/efirma3.crl**	**Este Campo es usado para indicar las direcciones donde puede ser encontrado el CRL correspondientes a la CA que emitió el certificado, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no.** **No es crítico.**

AuthorityInfo Acesss	***Access Method***	**id-ad-ocsp**	**Este Campo es usado para indicar las direcciones donde puede ser encontrado el certificado del PSC.** **Además, para indicar la dirección donde puede accederse al servicio de OCSP, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no.** **La primera entrada debe contener el método de acceso id-ad-caIssuer, utilizando uno de los siguientes protocolos de acceso: HTTPS o LDAP, para la recuperación de la cadena de certificación. La segunda entrada puede contener el método de acceso id-ad-ocsp con el respectivo respondedor OCSP utilizando uno de los siguientes protocolos de acceso HTTPS o LDAP.** **No es crítico.**
	Access Location	**https://www.efirma.com.py/va**	
	Access Method	**id-ad-caIssuer**	
	Access Location	**https://www.efirma.com.py/repositorio/efirma.crt**	

Tabla N° 7 – **PERFIL DE CERTIFICADO CUALIFICADO TRIBUTARIO TIPO F3**

Campo X509 V3	q	Ejemplo	Descripción
Version	**Versión de X509**	**V3**	**Los certificados deben ser X.509 versión 3 (V3)**
SerialNumber	**Número de serie**	**18 6f 57 dd 38 6c 47 ad 54 5d 0c 9a 22 f4 96 60**	**Aleatorio asignado por el PSC VIT S.A. Valor único emitido dentro del ámbito de cada PSC.**
SignatureAlgorithm	**Algoritmo de firma digital del certificado**	**sha256RSA**	**El Algoritmo de firma debe ser como mínimo SHA256RSAencryption.**
Issuer	**DN (Nombre distintivo)**	**CN = CA-VIT S.A.** **O = VIT S.A.** **C = PY** **SERIALNUMBER = RUC**	**Este campo indica los datos de identificación del PSC que emitió el certificado.**

		80080099-0	
Subject	**C (Pais)** **OID: 2.5.4.6**	**PY**	**Este campo debe contener el condigo del país asignado de acuerdo al ISO 3166.**
	O (Organización) **OID: 2.5.4.10**	**CERTIFICADO CUALIFICADO TRIBUTARIO**	**En este campo se identifica el tipo de certificado.** **Si el certificado es de máquina:** **MAQUINA** **Si el certificado es de aplicación:** **APLICACION**
	OU (Organización) **OID: 2.5.4.11**	**F2**	**En este campo se indica el propósito del uso del certificado digital y el módulo (software/hardware) en el que fue almacenada la clave privada del titular del certificado.**
	CN (Nombre) **OID: 2.5.4.3**	**JUAN FEDERICO ESCAURIZA VILLALBA**	**Este campo debe contener el/los nombre y apellido/s del titular del certificado, según documento de identificación, en mayúsculas y sin tildes, a excepción de la Ñ. Podrán ser incluidos diéresis y apostrofes si corresponde.**
	SerialNumber **OID: 2.5.4.5**	**CI1234567**	**Este campo debe contener las siglas CI, seguidas del número de cédula de Identidad del titular del certificado, según documento de identificación.**
	SN (SurName) **OID: 2.5.4.4**	**ESCAURIZA VILLALBA**	**Este campo debe contener el/los apellido/s del titular del certificado, según documento de identificación, en mayúsculas y sin tildes, a excepción de la Ñ. Podrán ser incluidos diéresis y apostrofes si corresponde.**
	G (GivenName) **OID: 2.5.4.42**	**JUAN FEDERICO**	**Este campo debe contener el/los nombre/s del titular del certificado, según documento de identificación, en mayúsculas y sin tildes, a excepción de la Ñ. Podrán ser incluidos diéresis y apostrofes si corresponde.**

Validity	**Valid from (Válido desde)**	**viernes, 07 de noviembre de 2016 15:16:58**	**El certificado emitido al usuario final es otorgado por un tiempo máximo de dos años, al finalizar ese período pierde su validez**
	Valid to (Válido hasta)	**lunes, 07 de noviembre de 2018 15:16:58**	
subjectyPublicKeyInfo	**Subject Public Key (Clave pública del sujeto)**	**30 82 01 0a 02 82 01 01 00 b4 46 43 e2 4a 52 1e b4 87 bc 8c f0 a0 f9 df 1f 68 1d 08 e5 00 fe 20 6b fe 3d 2c 5b 48 ad 46 7d 22 65 03 27 10 0c 86 e1 f7 31 dd 23 37 0b ad 08 cc b9 cd 96 03 64 8e 58 c0 fb 8d f9 5e fa 26 df 07 a1 b4 81 f6 ec a5 e7 5e 50 67 61 31 97 bc 76 94 7f 3e be 28 be 0b a8 03 11 57 64 58 f2 70 da 22 b3 f2 ee 28 18 29 57 1c 59 ce 46 ec f9 4c 2d a9 89 89 65 97 b1 19 fb b1 ab 2a e1 09 65 ed 8c c6 6c 46 db 8c 3e a6 50 9d 9f ff ee 51 8c 33 5c 15 aa 6b 88 8e 8e 7c fa af 1d 9d 48 9f 12 2d b1 98 ff b6 88 ac 09 e0 b5 f9 fc 5a b6 32 32 26 d1 00 72 95 7e d9 5b 5a d8 90 84 86 65 49 32 08 b9 a8 3e 2f 0d db bf 2c 4d 48 e0 6f 52 71 19 5f 86 32 ba dc 87 9d 5f 38 66 80 a7 a7 48 3d 9f 10 09 82 28 47 9b 00 00 cb 1c 90 a1 63 af 86 71 9e 75 24 a2 e5 63 a6 d5 e9 8b 0e 96 44 fb fa a3 f1 b5 02 03 01 01 fa**	**Este campo indica la clave pública del titular del certificado. Codificado de acuerdo con el RFC 5280 y con un largo de clave de 2048 bits o 4096 bits y algoritmo RSA Encryption.**
Extensiones estándar			
subjectKeyIdentifier	**Subject Key Identifier (Identificador de la clave del Sujeto)**	**ac dc d4 d3 cf 0c 20 ce bb 20 29 1b 93 1a 10 bb b2 36 3f a7**	**Este campo debe contener el hash SHA-1 de la clave pública del titular del certificado. Este Campo es usado por el software de validación para ayudar a identificar un certificado que contiene una determinada clave pública.** **No es crítico.**
authorityKeyIdentifier	**Authority Key Identifier (Identificador de la clave de la entidad emisora)**	**Id. de clave=03 7c 7c 9f 6d 5a 72 a5 91 91 b4 db ec 91 fb 03 5f 7c 7c 9d**	**El campo key identifier debe contener el hash SHA-1 de la clave pública del PSC emisor del certificado. Este campo es usado por los diversos software de validación para ayudar a identificar a la**

			autoridad certificadora que emitió el certificado en la cadena de Confianza. **No es crítico.**
keyUsage	**Key Usage(Uso de la clave)**	**nonRepudiation=1;** **digitalSignature=1;** ***keyAgreement*=1;** **KeyEncipherment=1.**	**En certificados tipo F2 solamente pueden ser activados los siguientes bits:** **NonRepudiation (renombrado recientemente con el nombre de contentCommitmen);** **digitalSignature;** **keyEncipherment** **Si es crítico.**
extKeyUsage	**Extended Key Usage (uso extendido de la clave)**	**client authentication** **OID =1.3.6.1.5.5.7.3.2,** **Puede contener el propósito server** **authentication** **OID = 1.3.6.1.5.5.7.3.1.**	**Referencia otros propósitos de la clave, adicionales al uso y debe ser consistente con la extensión keyUsage.** **Si es crítico.**
CertificatePolicies	**Policy Identifier**	**1.3.6.1.4.1.44234.1.1.1.9**	**Debe contener el OID de la CP y la CPS correspondiente y la dirección WEB de la CP y CPS del PSC que emite el certificado.** **No es crítico.**
	PolicyQualifiers	**https://www.efirma.com.py/repositorio**	
	PolicyIdentifier	**1.3.6.1.4.1.44234.1.1.1.1**	
	User Notice (EN)	**https://www.efirma.com.py/repositorio**	
BasicConstraints	**CA**	**FALSE**	**En este campo debe ir "TRUE" si el certificado corresponde a una CA o "FALSE" si no corresponde.**
Subject Altenative	**Subject Altenative Name (nombre alternativo del**	**Rfc822Name=jfederico@efirma.com.py**	**Campo NO obligatorio** • **Rfc822Name= [email del responsable del certificado]**

Name	**sujeto)**	**DirectoryName** **O= TAV S. A.** **SERIALNUMBER= RUC80080088-0** **Desscription: FIRMA ELECTRÓNICA CUALIFICADA** **T= SOPORTE TECNICO** **OID=2.5.4.1= ABOGADO**	**Este campo contiene según sea el titular:** **Persona Física:** **Campo obligatorio** ● **DirectoryName =2.5.4.3: [nombre y apellido del responsable del certificado]** **Persona Jurídica:** **Campos obligatorios** ● **DirectoryName=2.5.4.10:[nombre de la organización titular del certificado]** ● **DirectoryName =2.5.4.3: [nombre y apellido del responsable del certificado]** ● **DirectoryName =2.5.4.5: RUC [siglas RUC seguido del *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 si no se registran los datos de la organización en la que presta servicio*]** **Campos NO obligatorios** ● **DirectoryName=2.5.4.12: [cargo que ocupa en la organización el responsable del certificado]** **Otros campos que componen la extensión "Subject Alternative Name" podrán ser utilizados en la forma y con los propósitos definidos por la RFC 5280 siempre y cuando estén aprobados por el MIC.** **No critico.**
CRLDistributionPoints	**CRL Distribution Points (Puntos de distribución de CRL)**	**[1]Punto de distribución CRL** **Nombre del punto de distribución:** **Nombre completo:** **Dirección URL= https://www.efirma.com.py/repositorio/efirma1.crl**	**Este Campo es usado para indicar las direcciones donde puede ser encontrado el CRL correspondientes a la CA que emitió el certificado, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no.** **No es crítico.**
AuthorityInfo Acesss	***Access Method***	**id-ad-ocsp**	**Este Campo es usado para indicar las direcciones donde puede ser encontrado el certificado del PSC.**
	Access Location	**https://www.efirma.com.py/va**	

	Access Method	**id-ad-caIssuer**	**Además, para indicar la dirección donde puede accederse al servicio de OCSP, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no.** **La primera entrada debe contener el método de acceso id-ad-caIssuer, utilizando uno de los siguientes protocolos de acceso: HTTPS o LDAP, para la recuperación de la cadena de certificación. La segunda entrada puede contener el método de acceso id-ad-ocsp con el respectivo respondedor OCSP utilizando uno de los siguientes protocolos de acceso HTTPS o LDAP.** **No es crítico.**
	Access Location	**https://www.efirma.com.py/repositorio/efirma.crt**	

7.1.1. NÚMERO DE VERSIÓN

Todos los certificados emitidos por el PCSC responsable, según su PC deberán implementar la versión 3 (tres) del certificado definido en la norma ITU X.509 de acuerdo con el perfil establecido en la RFC 5280.

7.1.2. EXTENSIONES DEL CERTIFICADO.

La ICPP define las siguientes extensiones como obligatorias:

a) **Identificador de la clave de la Autoridad Certificadora "Authority Key Identifier", no crítica:** El campo ***key Identifie****r* debe contener el hash SHA-1 de la clave pública del PCSC;

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

c) **Uso de Claves "KeyUsage", crítica:**

c.1.1) **para certificados cualificados de firma electrónica:** debe contener los bits *digitalSignature*, *keyEncipherment* y *nonRepudiation* activados;

c.1.2) **para certificados cualificados tributarios**: debe contener los bits *digitalSignature*, *keyEncipherment* o *keyAgreement* y *nonRepudiation* activados.

d) **Uso extendido de la clave "Extended Key Usage", no crítico:**

d.1) **para certificados cualificados de firma electrónica**: al menos uno de los propósitos *client authentication OID= 1.3.6.1.5.5.7.3.2 o E-mail protection OID = 1.3.6.1.5.5.7.3.4* debe estar activado y pudiendo implementar otros propósitos instituidos, siempre que sean verificables y previstos por el PCSC en su PC de acuerdo con el RFC 5280;

d.2) **para certificados cualificados tributarios**: el propósito *client authentication OID =1.3.6.1.5.5.7.3.2* debe estar activado. Puede contener el propósito *server authentication OID = 1.3.6.1.5.5.7.3.1*.

d.4) **para certificados de firma de respuesta OCSP:** solamente el propósito *OCSPSigning OID = 1.3.6.1.5.5.7.3.9* debe estar presente;

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

e.1) **para certificados cualificados de firma electrónica:**

e.1.1) el campo ***policyIdentifier*** debe contener los OIDs de la PC implementada por el PCSC titular del certificado, para la emisión de certificados de personas físicas;

e.1.2) el campo **policyQualifiers**

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

e.1.2.2) el campo ***User Notice*** debe decir: "**certificado cualificado de firma electrónica tipo** [*siglas:* **F2 (claves en dispositivo cualificado)** o **F3 (clave en dispositivo cualificado centralizado)** *según tipo de certificado*] sujeta a las condiciones de uso expuestas en la DPC del [*nombre del PCSC*]"

e.2) **para certificados cualificados tributarios:**

e.3.1) el campo ***policyIdentifier*** debe contener los OIDs de la PC implementada por el PCSC titular del certificado, para la emisión de certificados de personas físicas;

e.3.2) el campo **policyQualifiers**

e.3.2.1) el campo ***CPS Pointer*** debe contener la dirección web de la DPC del PCSC que emite el certificado.

e.3.2.2) el campo ***User Notice*** debe decir: "**certificado cualificado de firma electrónica tipo** [*siglas:* **F1 (claves en módulo software), F2 (claves en dispositivo cualificado) o F3 (claves en dispositivo cualificado centralizado)** *según tipo de certificado*] sujeta a las condiciones de uso expuestas en la DPC del [*nombre del PCSC*]"

f) **Restricciones Básicas** "***Basic Constraints*****", crítica:**

f.1) el campo ***Subject Type*** debe contener CA=True

f.2) el campo ***PathLenConstraint*** debe tener valor cero;

g) **Puntos de distribución de las LCR "CRL Distribution Points", no crítica:**

g.1) el campo ***Distribution Point 1*** debe contener la primera dirección web donde se obtiene la LCR correspondiente al certificado; y

g.2) el campo ***Distribution Point 2*** debe contener la segunda dirección web donde se obtiene la LCR correspondiente al certificado.

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

h.1) Primer acceso

h.1.1) en el campo ***Access Method 1*** debe contener el identificador de método de acceso a la información de revocación (OCSP); y

h.1.2) en el campo ***Access Location 1*** debe contener la dirección Web del servicio del OCSP, utilizando uno de los siguientes protocolos de acceso: HTTP, HTTPS o LDAP.

h.2) Segundo acceso

h.2.1) en el campo ***Access Method 2*** debe contener el identificador de método de acceso del certificado del PCSC; y

h.2.2) en el campo ***Access Location 2*** debe contener la dirección web donde se encuentra alojado el certificado del PCSC, utilizando uno de los siguientes protocolos de acceso: HTTP, HTTPS o LDAP.

i) **Nombre Alternativo del Sujeto "Subject Alternative Name", no crítica**, en los siguientes formatos:

i.1) Para CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA:

i.1.1) Campo NO obligatorio: Rfc822Name= [*email del titular del certificado***];**

i.1.2) 1 (un) campo otherName, obligatorio, que contiene:

1. **DirectoryName OID=2.5.4.13:** *debe contener el siguiente mensaje***:**

1.1) para certificado del tipo F2: [‘‘FIRMA ELECTRÓNICA CUALIFICADA’’*]*

1.2) para certificado del tipo F3: [‘‘FIRMA ELECTRÓNICA CUALIFICADA CENTRALIZADA’’*]*

i.1.2) 4 (cuatro) campos otherName, NO obligatorios, que contienen:

1. **DirectoryName OID= 2.5.4.10: [***nombre de la organización en el que presta servicio el titular del certificado***]**;
2. **DirectoryName OID= 2.5.4.11: [***nombre de la unidad de la organización en el que presta servicio el titular del certificado***]**;
3. **DirectoryName OID=2.5.4.5: RUC [**siglas **RUC** seguido del *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 si no se registran los datos de la organización en la que presta servicio***]**;
4. **DirectoryName OID=2.5.4.12: [***posición o función designada al titular del certificado en la organización en el que presta servicio o título académico del titular del certificado****]***;

i.2) Para CERTIFICADO CUALIFICADO TRIBUTARIO:

i.2.1) Campo NO obligatorio: Rfc822Name= [*email del titular del certificado***]**;

i.2.2) 3 (tres) campos otherName, obligatorios, que contienen:

1. **DirectoryName OID= 2.5.4.10: [***nombre de la organización en la que presta servicio el titular del certificado o razón social del titular del certificado en caso de tratarse de una organización unipersonal* **]**;
2. **DirectoryName OID=2.5.4.5: RUC [**siglas **RUC** seguido del *número de RUC correspondiente a la organización en la que presta servicio el titular del certificado o el número de RUC del titular del certificado en caso de tratarse de una organización unipersonal***]**;
3. **DirectoryName OID=2.5.4.13:** *debe contener el siguiente mensaje***:**

3.1) para certificado del tipo F1: [''FIRMA ELECTRÓNICA de nivel medio''] *o;*
3.2) para certificado del tipo F2: [''FIRMA ELECTRÓNICA CUALIFICADA''] *o;*
3.3) para certificado del tipo F3: [''FIRMA ELECTRÓNICA CUALIFICADA CENTRALIZADA'']

i.3.3) 2 **(dos) campos otherName, NO obligatorios, que contienen:**

1. **DirectoryName OID= 2.5.4.11: [***nombre de la unidad de la organización en el que presta servicio el titular del certificado***]**; y
2. **DirectoryName OID=2.5.4.12: [***posición o función designada al titular del certificado en la organización en el que presta servicio* ***]***;

Los campos otherName definidos por la ICPP deben cumplir con las siguientes especificaciones:

a) El conjunto de información definido en cada campo otherName debe almacenarse como una cadena de tipo **ASN.1 OCTET STRING o PRINTABLE STRING**; y

b) Solo se pueden utilizar los caracteres de la A a la Z, del 0 al 9, observando lo establecido en el ítem 7.1.5 del presente documento.

Otros campos que componen la extensión "**Subject Alternative Name"** podrán ser utilizados en la forma y con los propósitos definidos por la RFC 5280 siempre y cuando estén aprobados por la AC Raíz-Py.

7.1.3. IDENTIFICADORES DE OBJETO DE ALGORITMOS

El Identificador de objeto (OID) de algoritmo criptográfico podrá ser:

- sha256WithRSAEncryption(1.2.840.113549.1.1.11)

Identificador de objeto (OID) de clave pública

- RSAEncryption(1.2.840.113549.1.1.1)

7.1.4. FORMAS DEL NOMBRE

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

a) **Certificado cualificado de firma electrónica**:

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

ii) **OID=2.5.4.10** **O=CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA**;

iii) **OID=2.5.4.11** **OU= [***podrá ser:* **F2 o F3,** *conforme lo estipulado en el punto 1.1 y 1.4.1 de este documento***]**;

iv) **OID: 2.5.4.3** **CN= [***nombre/s y apellido/s del titular del certificado en mayúsculas y sin tilde, conforme documento de identidad presentado***]**; y

v) **OID: 2.5.4.5** **Serial Number= [**conforme *al formato descripto en el ítem 3.1.4.2 del documento DOC-ICPP-03 [3]***]**;

vi) **OID: 2.5.4.4** **SN= [** *apellido/s del titular del certificado en mayúsculas y sin tilde, conforme documento de identidad presentado***]**; y

vii) **OID:2.5.4.42** **G= [** *nombre/s del titular del certificado en mayúsculas y sin tilde, conforme documento de identidad presentado***]**;

b) **Certificado cualificado tributario**:

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

ix) **OID=2.5.4.10** **O=CERTIFICADO CUALIFICADO TRIBUTARIO**

x) **OID=2.5.4.11** **OU= [***podrá ser:* **F1, F2 o F3,** *conforme lo estipulado en el punto 1.1 y 1.4.1 de este documento***]**;

xi) **OID: 2.5.4.3** **CN= [***nombre/s y apellido/s del titular del certificado en mayúsculas y sin tilde, conforme documento de identidad presentado***]**; y

xii) **OID: 2.5.4.5** **Serial Number= [**conforme *al formato descripto en el ítem 3.1.4.2 del documento DOC-ICPP-03 [3]***]**;

xiii) **OID: 2.5.4.4** **SN= [** *apellido/s del titular del certificado en mayúsculas y sin tilde, conforme documento de identidad presentado***]**; y

xiv) **OID:2.5.4.42** **G= [** *nombre/s del titular del certificado en mayúsculas y sin tilde, conforme documento de identidad presentado***]**;

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 9 - 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. IDENTIFICADOR DE OBJETO DE POLÍTICA DE CERTIFICADO.

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

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 emitidos según la PC, el campo ***policyQualifiers*** de la extensión Políticas de certificado “CertificatePolicies”, debe contener la dirección web (URL) de la DPC del PCSC responsable.

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

Las extensiones críticas deben ser interpretadas conforme a la RFC 5280.

7.2. PERFIL DE LA LCR

No contamos con el documento para la especificación.

7.2.1. NÚMERO (S) DE VERSIÓN

Las LCRs generadas por el PCSC responsable según la PC deberán implementar la versión 2 de la LCRs definida en el estándar ITU X.509, de acuerdo con el perfil establecido en el RFC 5280.

7.2.2. LCR Y EXTENSIONES DE ENTRADAS DE LCR

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

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

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

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

7.3. PERFIL DE OCSP

No contamos con el documento para la especificación.

7.3.1. NÚMERO (S) DE VERSIÓN

Los servicios de respuesta de OCSP deberán implementar la revisión 1 del estándar ITU X.509, de acuerdo con el perfil establecido en el RFC 6960.

7.3.2. EXTENSIONES DE OCSP

Si se implementa, debe cumplir con RFC 6960.

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

8.1. FRECUENCIA O CIRCUNSTANCIAS DE EVALUACIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

8.2. IDENTIFICACIÓN/CALIDAD DEL EVALUADOR

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

8.3. RELACIÓN DEL EVALUADOR CON LA ENTIDAD EVALUADA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

8.4. ASPECTOS CUBIERTOS POR LA EVALUACIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

8.5. ACCIONES TOMADAS COMO RESULTADO DE UNA DEFICIENCIA.

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

8.6. COMUNICACIÓN DE RESULTADOS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9. OTROS ASUNTOS LEGALES Y COMERCIALES

9.1. TARIFAS

9.1.1. TARIFAS DE EMISIÓN Y ADMINISTRACIÓN DE CERTIFICADOS

Las tarifas por la emisión de los certificados tienen un costo de 10 (diez) jornales mínimos como máximo.

La lista de Tarifas del PSC VIT S.A. actualizada se publica en el**Repositorio**webhttps://www.efirma.com.py

9.1.2. TARIFAS DE ACCESO A CERTIFICADOS

No aplica.

9.1.3. TARIFAS DE ACCESO A INFORMACIÓN DEL ESTADO O REVOCACIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.1.4. TARIFAS POR OTROS SERVICIOS

El acceso a información de las Políticas y a la Declaración de Prácticas de Certificaciones libre y gratuito. Las tarifas aplicables a otros servicios adicionales se acordarán directamente entre el PCSC VIT S.A. y los clientes de otros servicios ofrecidos.

9.1.5. POLÍTICAS DE REEMBOLSO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.2. RESPONSABILIDAD FINANCIERA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.2.1. COBERTURA DE SEGURO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.2.2. OTROS ACTIVOS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.3.1. ALCANCE DE LA INFORMACIÓN CONFIDENCIAL

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.3.2. INFORMACIÓN NO CONTENIDA EN EL ALCANCE DE INFORMACIÓN CONFIDENCIAL

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.3.3. RESPONSABILIDAD DE PROTEGER LA INFORMACIÓN CONFIDENCIAL

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.4. PRIVACIDAD DE INFORMACIÓN PERSONAL

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.4.1. PLAN DE PRIVACIDAD

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.4.2. INFORMACIÓN TRATADA COMO PRIVADA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.4.3. INFORMACIÓN QUE NO ES CONSIDERADA COMO PRIVADA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.4.4. RESPONSABILIDAD PARA PROTEGER INFORMACIÓN PRIVADA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.4.5. NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR INFORMACIÓN PRIVADA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.4.6. DIVULGACIÓN DE ACUERDO CON UN PROCESO JUDICIAL O ADMINISTRATIVO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.4.7. OTRAS CIRCUNSTANCIAS DE DIVULGACIÓN DE INFORMACIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.4.8. INFORMACIÓN A TERCEROS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.5. DERECHO DE PROPIEDAD INTELECTUAL

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.6. REPRESENTACIONES Y GARANTÍAS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.6.1. REPRESENTACIONES Y GARANTÍAS DEL PCSC

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.6.1.1. AUTORIZACIÓN PARA CERTIFICADO

9.6.1.2. PRECISIÓN DE LA INFORMACIÓN

9.6.1.3. IDENTIFICACIÓN DEL SOLICITANTE DE CERTIFICADO

9.6.1.4. CONSENTIMIENTO DE LOS TITULARES DE CERTIFICADO

9.6.1.5. SERVICIO

9.6.1.6. REVOCACIÓN

9.6.1.7. EXISTENCIA LEGAL

9.6.2. REPRESENTACIONES Y GARANTÍAS DE LA AR

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.6.3. REPRESENTACIONES Y GARANTÍAS DEL TITULAR DE CERTIFICADO

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.6.4. REPRESENTACIONES Y GARANTÍAS DE LAS PARTES USUARIAS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.6.5. REPRESENTACIONES Y GARANTÍAS DE OTROS PARTICIPANTES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.7. EXENCIÓN DE GARANTÍA

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.8. LIMITACIONES DE RESPONSABILIDAD LEGAL

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.9. INDEMNIZACIONES

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.10. PLAZO Y FINALIZACIÓN

9.10.1. PLAZO

Esta Política de Certificación empieza a ser efectiva una vez publicada en el **Repositorio** web https://www.efirma.com.py previa aprobación del MIC.

9.10.2. FINALIZACIÓN

La Política de Certificación estará en vigor mientras no se derogue expresamente por la emisión de una nueva versión.

9.10.3. EFECTOS DE LA FINALIZACIÓN Y SUPERVIVENCIA

La finalización de la vigencia de la Política de Certificación, puede ser por derogación expresa, enmiendas o modificaciones; todos los certificados emitidos bajo esa política seguirán vigentes hasta que expiren o sean revocados, salvo que la nueva versión de la Política de Certificación contemple aspectos críticos, en cuyo caso todos los certificados deberán ser revocados inmediatamente.

9.11. NOTIFICACIÓN INDIVIDUAL Y COMUNICACIONES CON PARTICIPANTES

Toda comunicación entre el PCSC VIT S.A. y el suscriptor, se realizará mediante mensajes de datos firmado digitalmente o documento escrito dirigido a cualquiera de las direcciones establecidas como contacto. Las comunicaciones electrónicas se harán efectivas una vez que la reciba el destinatario al que van dirigidas, de igual manera en el caso de las escritas.

9.12. ENMIENDAS

9.12.1. PROCEDIMIENTOS PARA ENMIENDAS

Los cambios efectuados en Política de Certificación deben ser revisados y aprobados por la DGFDyCE del MIC antes de que éstos sean implementados. La documentación puede requerir una revisión.

9.12.2. PROCEDIMIENTO DE PUBLICACIÓN Y NOTIFICACIÓN

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

9.12.3. CIRCUNSTANCIAS EN QUE LOS OID DEBEN SER CAMBIADOS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.13. DISPOSICIONES PARA RESOLUCIÓN DE DISPUTAS

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.14. NORMATIVA APLICABLE

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.15. ADECUACIÓN A LA LEY APLICABLE

La presente Política de Certificación se adecua a legislación vigente aplicable a la materia.

9.16. DISPOSICIONES VARIAS

9.16.1. ACUERDO COMPLETO

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

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

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

9.16.2. ASIGNACIÓN

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.16.3. DIVISIBILIDAD

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

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

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.16.5. FUERZA MAYOR

Según lo especificado en la Declaración de Prácticas de Certificación (DPC) de VIT S.A.

9.17. OTRAS DISPOSICIONES

Esta Política de Certificación en conjunto con la *Declaración de Prácticas de Certificación (DPC) de VIT S.A.* guarda concordancia con las disposiciones de la POLÍTICA DE CERTIFICACIÓN DE LA INFRAESTRUCTURADE CLAVE PÚBLICA DEL PARAGUAY.

10. DOCUMENTOS DE REFERENCIA

10.1. REFERENCIAS EXTERNAS

- RFC 5280: "Internet X.509 Public Key Infrastructure.Certificate and CertificateRevocationList (CRL) Profile".
- RFC 6960: "X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP".
- TU 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".
- Principles and CriteriaforCertificationAuthorities.
- WebTrustSM/TM Principles and CriteriaforRegistrationAuthorities.
- LEY Nº 6822/2021 "DE LOS SERVICIOS DE CONFIANZA PARA LAS TRANSACCIONES ELECTRÓNICAS, DEL DOCUMENTO ELECTRÓNICO Y LOS DOCUMENTOS TRANSMISIBLES ELECTRÓNICOS."

10.2. REFERENCIAS A DOCUMENTOS QUE COMPONEN LA ICPP

Tabla Nº 10 – Documentos Referenciados

REF.	NOMBRE DEL DOCUMENTO	CÓDIGO
[1]	Normas de algoritmos criptográficos de la ICPP.	DOC-ICPP-06

[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]	Directivas obligatorias para la formulación y elaboración de la declaración de prácticas de certificación de los prestadores cualificados de servicios de confianza de la ICPP.	DOC-ICPP-03

10.3. ÍNDICE DE TABLAS