



Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC)

Fecha	Abril 2026
Edición	28
Versión	1
Elaborado por	Gerencia General abril 2026
Aprobado	Alta Dirección abril 2026
Descripción	Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC)
Vigente	Si

Declaración de Copyright y Derecho de Autor.

Proveedor de Certificados PROCERT, C.A. ®. Todos los derechos reservados; el logo de Proveedor de Certificados PROCERT, C.A. ® y los nombres de los productos son marcas comerciales de Proveedor de Certificados PROCERT, C.A. ®, sus desarrollo, aplicaciones, publicaciones y software especializado. La presente Declaración de Practicas de Certificación (DPC) es desarrollada por Proveedor de Certificados PROCERT, C.A. ® a los fines de ajustar la operación de su una infraestructura de clave pública de recursos (RPKI) abierta, a las normas técnicas internacionales y mejores prácticas aplicables a la operación y servicios de una infraestructura de clave pública de recursos (RPKI). En virtud de lo anterior, todo uso, copia, reproducción, manejo o disposición no autorizado por Proveedor de Certificados PROCERT, C.A. ®, expresamente y por escrito, generará responsabilidad, de conformidad con la legislación que regula el Copyright y el derecho de autor. Cualquier solicitud de autorización de uso deberá ser enviada a la siguiente dirección electrónica contacto@procert.net.ve y contar con su debida autorización por escrito por parte de Proveedor de Certificados PROCERT, C.A. ®.

Índice

	Página
1. Control de Versiones	6
2. Título	7
3. Código.	7
4. Introducción.	7
5. Definiciones	7
6. Objetivo	11
7. Alcance.....	12
8. Limitaciones.....	12
9. Comunidad de usuarios y aplicabilidad.....	12
9.1. Aprobación de políticas	12
9.2. Actualización de la documentación.....	12
9.3. Autoridad de certificación (AC).	13
9.4. Autoridad de registro (AR)	17
9.5. Modelo de Confianza.....	21
9.6. Registro de Acceso Público	23
9.7. Certificados electrónicos.....	24
9.8. Terceros de buena fe.....	24
10. Usos de los certificados.....	49
10.1. Usos permitidos.....	49
10.2. Usos no permitidos	49
11. Política de administración de la AC.	49
11.1. Especificaciones de la organización administrativa.....	49
11.2. Persona contacto.....	62
11.3. Competencia para determinar la adecuación de la DPC a las políticas	62
12. Publicación de información del PSC y repositorios de los certificados.	62
12.1. Repositorios.....	62
12.2. Publicación	62
12.3. Frecuencia de publicación.	63
13. Controles de acceso al repositorio de certificados.	63
14. Identificación y autenticación.	63
14.1. Tipos de nombres.....	63
14.2. Necesidad de nombres significativos.....	64
14.3. Interpretación de formatos de nombre	64
14.4. Unicidad de los nombres	64
14.5. Resolución de conflictos relativos a nombres	64
15. Validación inicial de la identidad.	65
15.1. Método de prueba de posesión de la clave privada.....	65
15.2. Autenticación de la identidad de una organización	65
15.3. Comprobación de las facultades de representación	65
15.4. Criterios para operar con AC externas	66
16. Identificación y autenticación de las solicitudes.	66
16.1. De la suspensión o revocación de clave.....	66
16.2. De la renovación de la clave.....	69
17. Ciclo de vida de los certificados del PSC	69
17.1. Solicitud de certificados	70
18. Tramitación de solicitud de un certificado.	71
18.1. Realización de las funciones de identificación y autenticación.....	71
18.2. Aprobación o denegación de un certificado	71

18.3.	Plazo para la tramitación de un certificado.	72
19.	Emisión de certificado.	72
19.1.	Acciones de la AC durante la emisión de un certificado.	72
19.2.	Notificación al solicitante por parte de la AC acerca de la emisión de su certificado.	72
20.	Uso del par de claves y del certificado.	72
20.1.	Uso de la clave privada del certificado.	72
20.2.	Uso de la clave pública y del certificado por los terceros de buena fe	72
21.	Renovación del certificado con cambio de clave.	73
21.1.	Causas para la renovación de un certificado	73
21.2.	Entidad que puede solicitar la renovación de un certificado	73
21.3.	Procedimiento de solicitud para renovación de un certificado	73
21.4.	Notificación de la emisión de un nuevo certificado a la AR	73
21.5.	Publicación del certificado renovado por la AC	73
21.6.	Notificación de la emisión del certificado por la AC a otras entidades	74
22.	Modificación de certificados.	74
23.	Revocación y suspensión de un certificado.	74
23.1.	Circunstancias para la revocación del certificado	74
23.2.	Entidad que puede solicitar la revocación	74
23.3.	Procedimiento de solicitud de la renovación.	74
23.4.	Período de gracia de la solicitud de la revocación	74
23.5.	Circunstancias para la suspensión.	74
23.6.	Procedimiento para la solicitud de suspensión	74
23.7.	Límites del período de suspensión	74
23.8.	Frecuencia de emisión de LCR.	74
23.9.	Disponibilidad de compromiso on-line de revocación y estado de los certificados	75
23.10.	Requisitos de comprobación on-line de revocación	75
23.11.	Otras formas de divulgación de información de revocación disponibles	75
24.	Servicio de comprobación de estado de certificados.	75
24.1.	Características operativas	75
24.2.	Disponibilidad del servicio.	75
24.3.	Características adicionales	75
25.	Finalización de la suscripción.	75
26.	Custodia y recuperación de la clave.	75
26.1.	Prácticas y políticas de custodia y recuperación de la clave:	75
27.	Controles de seguridad física, de gestión y de operaciones.	76
27.1.	Controles de seguridad física.	76
27.2.	Controles funcionales.	78
27.3.	Controles de seguridad personal.	79
27.4.	Procedimientos de control de seguridad.	80
27.5.	Archivo de informaciones y registros	81
28.	Cambio de claves.	82
29.	Recuperación en caso de desastre.	82
29.1.	Procedimiento de gestión de incidentes y vulnerabilidades:	82
29.2.	Alteración de los recursos, hardware, software y/o datos	83
29.3.	Procedimiento de actuación ante la vulnerabilidad de la clave privada de una autoridad	83
29.4.	Seguridad de las instalaciones tras un desastre natural o de otro tipo.	83

30.	Cese de actividad	83
31.	Controles de seguridad técnica.....	84
	31.1. Generación e instalación del par de claves.....	84
	31.2. Protección de la clave privada.	87
	31.3. Otros aspectos de la gestión del par de claves.....	88
	31.4. Datos de activación.	89
	31.5. Controles de seguridad del computador.	90
	31.6. Controles de seguridad del ciclo de vida.....	90
	31.7. Controles de seguridad de la red	90
	31.8. Controles de ingeniería de los módulos criptográficos.	90
32.	Perfiles de certificados LCR / OCSP.....	90
	32.1. Perfil del certificado	90
	32.2. Número de versión.	91
	32.3. Extensiones del certificado.....	91
	32.4. Identificadores de objeto (OID) de los algoritmos	91
	32.5. Formatos de nombres	91
	32.6. Identificador de objeto (OID) de la PC	91
	32.7. Perfil de LCR / OCSP	91
	32.8. Auditoría de conformidad	93
	32.9. Requisitos comerciales y legales.....	94
	32.10. Protección de la información privada/secreta.	96
	32.11. Derechos de propiedad intelectual.	97
	32.12. Representaciones y garantías	98
	32.13. Obligaciones y responsabilidad civil.	98
	32.14. Limitación de responsabilidades.....	103
	32.15. Indemnizaciones	105
	32.16. Plazo y finalización.....	105
	32.17. Notificaciones.....	105
	32.18. Modificaciones.	106
	32.19. Resolución de conflictos.....	106
	32.20. Legislación aplicable	107
	32.21. Conformidad con ley aplicable.....	107
	32.22. De los ajustes al documento.....	107
33.	Marco legal y normativo.....	108
34.	Funciones y responsabilidades dentro de la autoridad de certificación (AC).....	108
35.	Actores sujetos al cumplimiento del presente documento	108
36.	Revisión, aprobación y modificación	108

1. Control de Versiones

Versión	Motivo de Cambio	Publicación	Vigencia
Edición 01	Control y Corrección Semestral (Actualización)	01/01/2008	No
Edición 02	Control y Corrección Semestral (Actualización)	08/07/2009	No
Edición 03	Control y Corrección Semestral (Actualización)	05/01/2010	No
Edición 04	Control y Corrección Semestral (Actualización)	29/07/2010	No
Edición 05	Control y Corrección Semestral (Actualización)	13/01/2011	No
Edición 06	Control y Corrección Semestral (Actualización)	16/06/2011	No
Edición 07	Control y Corrección Semestral (Actualización)	03/01/2012	No
Edición 08	Control y Corrección Semestral (Actualización)	16/07/2012	No
Edición 09	Control y Corrección Semestral (Actualización)	26/02/2013	No
Edición 10	Control y Corrección Semestral (Actualización)	22/08/2013	No
Edición 11	Control y Corrección Semestral (Actualización)	15/01/2014	No
Edición 12	Control y Corrección Semestral (Actualización)	10/07/2014	No
Edición 13	Control y Corrección Semestral (Actualización)	17/11/2014	No
Edición 14	Control y Corrección Semestral (Actualización)	07/04/2015	No
Edición 15	Control y Corrección Semestral (Actualización)	06/10/2015	No
Edición 16	Control y Corrección Semestral (Actualización)	01/02/2016	No
Edición 17	Control y Corrección Semestral (Actualización)	16/03/2016	No
Edición 18	Control y Corrección Semestral (Actualización)	09/05/2016	No
Edición 19	Control y Corrección Semestral (Actualización)	05/06/2017	No
Edición 20	Control y Corrección Semestral (Actualización)	11/07/2017	No
Edición 21	Control y Corrección (Actualización Técnica)	22/09/2017	No
Edición 22	Control y Corrección (Actualización Técnica)	06/01/2018	No
Edición 22	Control y Corrección (Actualización Técnica)	06/06/2018	No
Edición 22	Control, Revisión y Ajuste Semestral (Actualización)	05/01/2019	No
Edición 22	Control, Revisión y Ajuste Semestral (Actualización)	07/06/2019	No
Edición 23	Control, Revisión y Ajuste por Remediación de Acreditación 2019.	06/11/2019	No
Edición 23	Control, Revisión y Ajuste Semestral (Actualización)	02/08/2020	No
Edición 23	Control, Revisión y Ajuste Semestral (Actualización)	07/06/2021	No
Edición 23	Control, Revisión y Ajuste Semestral (Actualización)	07/12/2021	No
Edición 23	Control y Ajuste (Actualización) Migración Daycohost.	08/06/2022	No
Edición 23	Control y Ajuste Auditoria SUSCERTE.	06/12/2022	No
Edición 23	Control, Revisión y Ajuste Semestral (Actualización)	10/01/2023	No
Edición 23	Control, Revisión y Ajuste Semestral (Actualización)	17/07/2023	No
Edición 23	Control, Revisión y Ajuste Semestral (Auditoria Técnica 2023)	14/12/2023	No
Edición 23	Control, Revisión y Ajuste Semestral (Observación de informe de Auditoría SUSCERTE 2023 APARTADO C1)	24/02/2024	No

Edición 24	Control, Revisión y Ajuste Semestral (Actualización – CURVA ELIPTICA)	13/09/2024	No
Edición 24	Ajuste informe Autoría SUSCERTE	19/12/2024	No
Edición 24	Ajuste informe Autoría SUSCERTE	17/08/2025	No
Edición 25	Inclusión certificada TSA Ajuste de Plantillas a la Norma 32 SUSCERTE	19/11/2025	No
Edición 26	Ajuste a observaciones proceso de acreditación	2/12/2025	No
Edición 27	Ajuste por cumplimiento de Procedo de remediación 2025-2026	25/02/2026	No
Edición 28	Inclusión del Certificado de Comercio Electrónico	9/04/2026	Si

2. Título: Documento de la Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC).
3. Código: AC-D-0003.
4. Introducción: El presente documento se constituye en la declaración por parte de Proveedor de Certificados PROCERT ITFB, C.A., a los fines de informar y documentar sus procesos de certificación, para una mejor comprensión y entendimiento por parte de su la Alta Dirección, personal, Clientes, Proveedores y Parte Interesada PSC PROCERT. La declaración de prácticas de certificación permite a la Alta Dirección, personal, Clientes, Proveedores y Parte Interesada del PSC, conocer cada uno de los procesos y subprocesos involucrados en ciclo de vida de los certificados electrónicos; documentar los procesos de recuperación ante desastres, manejo de claves criptográficas y dar una visión general de los equipos e infraestructura que soporta el esquema de confianza del PSC PROCERT. Las políticas de los certificados permiten a la Alta Dirección, personal, Clientes, Proveedores y Parte Interesada del PSC PROCERT, conocer el uso autorizado de cada tipo de certificado que emite el PSC PROCERT, su estructura y sus funciones. La Alta Dirección, personal, Clientes, Proveedores y Parte Interesada del PSC PROCERT que utilicen los certificados electrónicos emitidos por el PSC PROCERT, deberán dar cumplimiento al presente documento de la Declaración de Prácticas de Certificación (DPC) y a la Política de Certificados (PC) y serán responsables por las consecuencias derivadas del uso no ajustado de un certificado electrónico o del incumplimiento de las instrucciones contenidas en el presente documento.
5. Definiciones: Con el objeto de ofrecer una interpretación adecuada al sentido y alcance del presente documento, a continuación, se enunciarán una serie de conceptos, cuyas denominaciones en plural o singular atenderán al significado que se asigna a continuación:
 - 5.1. Archivo de Clave: Significa el proceso de almacenar claves usadas o su ID y/o certificados como un registro en almacenamientos de largo plazo para futuras recuperaciones.
 - 5.2. Auditoria: Significa la revisión y examen del sistema de récords y actividades para evaluar la adecuación y la efectividad de los controles de sistemas para garantizar el cumplimiento con las políticas y procedimientos operacionales establecidos y recomendados para la operación de un PSC y detectar los cambios necesarios en los controles, políticas y procedimientos y asegurar la implantación de dichos cambios en el tiempo.

- 5.3. Auditoria de Cumplimiento: Significa la revisión y examen de los registros y actividades del sistema para probar la adecuación de los controles del sistema para garantizar el cumplimiento de la política establecida y de los procedimientos operacionales, detectar brechas en seguridad y recomendar cambios en los controles, políticas y procedimientos.
- 5.4. Autoridad de Certificación (AC): Significa una autoridad en la cual confían los clientes para crear, emitir y manejar el ciclo de vida de los certificados, la cual a los efectos del decreto ley de mensajes de datos y firmas electrónicas debe contar con la acreditación otorgada por la SUSCERTE.
- 5.5. Autoridad de Registro: Significa la entidad cuyo propósito es suministrar apoyo local a la infraestructura de clave pública (ICP) de una AC. La Autoridad de Registro desempeña un conjunto de funciones orientadas a la validación, comprobación y conformación de la documentación suministrada, así como la identidad física de un cliente que opte a la compra de una firma o certificado electrónicos generado por el PSC PROCERT.
- 5.6. Autoridad de tiempo: Una Autoridad de Tiempo (Time-Stamp Authority, TSA) es una entidad confiable que emite marcas de tiempo digitales para garantizar que ciertos datos existían antes de un momento específico. Según el estándar RFC 3161.
- 5.7. Cadena de Certificado: Significa una cadena de múltiples certificados necesarios para validar un certificado. Las cadenas de certificado se construyen mediante la vinculación y verificación de la firma electrónica en un certificado con una clave pública que se encuentra en un certificado emitido por el PSC PROCERT, la cual se encuentra subordinada y firmada por el certificado raíz generado por la SUSCERTE.
- 5.8. Certificado: Significa una estructura de datos que utiliza el estándar CCITT ITU X.509, que contiene la clave pública de una entidad junto a información asociada y presentada como "un-forgettable" (inolvidable), mediante una firma electrónica de la autoridad de certificación que la generó.
- 5.9. Certificado de Clave Pública: Significa el certificado electrónico que une a la Clave Pública de una entidad con el identificador distintivo de la entidad y que indica un período de validez específico.
- 5.10. Cifrado: Significa el proceso mediante el cual los datos simples de un texto son transformados para ocultar su significado. El cifrado es un proceso reversible que se efectúa mediante el uso de un algoritmo criptográfico y una clave.
- 5.11. Clave: Significa la secuencia de símbolos que controla la operación de una transformación criptográfica (Ej. cifrado, descifrado, verificación criptográfica, función de computación, generación o verificación de firma).
- 5.12. Clave Criptográfica: Significa el parámetro utilizado conjuntamente con un algoritmo con fines de validación, autenticación, cifrado y descifrado.
- 5.13. Clave Privada: Significa la clave asimétrica de una entidad, la cual con normalidad será conocida solamente por esa entidad.
- 5.14. Clave Pública: Significa la clave de un par clave asimétrico de una entidad que puede hacerse pública, aunque no necesariamente esté disponible al público en general ya que puede ser restringida a un grupo predeterminado.
- 5.15. Cliente: Significa la entidad que ha solicitado la emisión de un certificado dentro de la ICP de PROCERT. A los fines del decreto ley de mensajes de datos y firmas electrónicas y su reglamento el cliente será entendido como el signatario y viceversa.

- 5.16. Confidencialidad: Significa la propiedad de no revelar o hacer disponible a terceras personas y sin autorización del propietario, la información y datos correspondientes a personas, entidades y/o procesos.
- 5.17. Control de Acceso: Significa la prevención del uso no autorizado de un recurso, incluyendo la prevención del uso de un recurso de manera no autorizada.
- 5.18. Criptografía: Significa la disciplina que abarca principios, medios y métodos para la transformación de información y datos para contenidos ocultos de información o datos, con el fin de evitar modificaciones no autorizadas y/o evitar el uso no autorizado de la información o los datos, según corresponda.
- 5.19. Declaración de Práctica de Certificación (DPC): Significa la declaración de las prácticas que utiliza la autoridad certificadora para emitir certificados y manejar su ciclo de vida.
- 5.20. Destinatario: Significa la entidad que obtiene (recibe o recupera) un mensaje.
- 5.21. Destrucción de Clave: Significa el proceso de eliminación de todas las copias de una clave mediante el sistema de manejo de claves.
- 5.22. Disponibilidad: Significa la propiedad de la información de ser accesible y utilizable al ser solicitada por una entidad o proceso autorizado.
- 5.23. Entidad: Significa toda persona (natural o jurídica) o sistema (mecánico o electrónico).
- 5.24. Entidad infraestructura de clave pública (ICP) Subordinada: Significa toda entidad que tenga la autoridad para operar y suministrar Servicios de Certificación bajo la ICP de la SUSCERTE.
- 5.25. Estampado de Tiempo: Un Servicio de Estampado de Tiempo (Time-Stamping Service, TSP) es un mecanismo criptográfico que permite demostrar que ciertos datos existían antes de un momento específico. Este servicio se implementa mediante una Autoridad de Estampado de Tiempo (Time-Stamp Authority, TSA), que actúa como tercero confiable y genera un Token de Estampado de Tiempo (Time-Stamp Token, TST) firmado digitalmente.
- 5.26. Evaluación: Significa la valoración contra criterios definidos para dar una medida de confianza en el sentido de que se cumple con los requerimientos correspondientes.
- 5.27. Evento de Auditoría: Significa una acción detectada internamente por el sistema que puede generar un registro de auditoría. Si un evento ocasiona que se genere un registro de auditoría [para grabar en rastro de auditoría]. Éste es un “evento registrado”. De otra manera es un “evento no registrado”. El sistema decide, en la medida que cada evento es detectado, si debe generar un registro de auditoría mediante la preselección del algoritmo de auditoría. El conjunto de eventos de auditoría se fundamenta en la política de seguridad del sistema.
- 5.28. Firma Electrónica: Significa el dato añadido o una transformación criptográfica de una unidad de dato que permite al receptor de la unidad de dato probar la fuente y la integridad del dato y protegerse contra falsificaciones, por ejemplo, del destinatario.
- 5.29. Ficha Criptográfica: Significa el medio en el cual se almacena una clave (Ej. tarjeta inteligente, clave criptográfica).
- 5.30. Generación de Certificado: Significa proceso de crear un certificado a partir de datos de entrada que son específicos a la aplicación y al cliente.
- 5.31. Generación de Clave: Significa el proceso mediante el cual se crean las claves criptográficas. Es la función de generar las variables requeridas para cumplir con los atributos particulares de la clave.

- 5.32. Información de Identificación: Significa la información que se obtiene para identificar positivamente a una entidad y suministrarle los servicios de certificación que solicite.
- 5.33. Infraestructura de clave pública (ICP): Significa la infraestructura necesaria para generar, distribuir, manejar y archivar claves, certificados y listas de revocación de certificado y respondedores de protocolo de estatus de certificado en-línea (PECL).
- 5.34. Infraestructura Operacional: Significa la infraestructura tecnológica mediante la cual se suministran los servicios de certificación. Esta infraestructura necesariamente no coincide con la infraestructura legal o las relaciones existentes o que se desarrollan entre las entidades que forman parte de la ICP de PROCERT o que utilizan los servicios de certificación de la ICP de PROCERT en cualquier forma.
- 5.35. Integridad de Datos: Significa la cualidad o condición de ser preciso, completo y válido y no ser alterado o destruido de manera no autorizada.
- 5.36. Interoperabilidad: la interoperabilidad implica que los equipos y procedimientos usados por dos o más entidades sean compatibles y, por lo tanto, es posible que asuman actividades en común o relacionadas.
- 5.37. Investigación Post-Suspensión: Significa la investigación hecha por la gerencia general y el consultor de tecnología del PSC PROCERT luego de suspender un certificado para determinar si dicho certificado debe ser revocado o reinstaurado como válido.
- 5.38. Lista de Certificados Revocados (LCR): Significa la lista de certificados que han sido revocados o suspendidos por el PSC PROCERT.
- 5.39. Manejo de Clave: Significa la administración y uso de la generación, inscripción, certificación, desincorporación, distribución, instalación, almacenamiento, archivo, revocación, derivación y destrucción de material clave de acuerdo con la política de seguridad.
- 5.40. Nivel de Auditoria: Significa una serie de requerimientos y regulaciones asociadas con los Tipos de certificados como se muestran en esta DPC y PC y contra los cuales se auditan a PSC acreditados ante la SUSCERTE.
- 5.41. Par Clave: Significan las claves en un sistema criptográfico asimétrico que tienen como función la de que uno de los pares de claves descifrará lo que el otro par de clave cifra.
- 5.42. Par Clave Asimétrico: Significa el par de claves relacionadas donde la clave privada define la transformación privada y la clave pública define la transformación pública.
- 5.43. Parte Interesada: Significa la organización o persona que tiene interés en el desempeño o éxito del PSC PROCERT.
- 5.44. Proceso de Verificación: Significa el proceso que toma como entrada de datos el mensaje firmado, la clave de verificación y los parámetros de dominio y que arroja como salida el resultado de la verificación de la firma: válida o inválida.
- 5.45. Protocolo de Estatus de Certificado En-línea (PECL): Es un protocolo utilizado para validar el estatus de un certificado en tiempo real. La respuesta de las solicitudes incluye tres (3) estatus: valido, revocado o desconocido. Su definición en Idioma Inglés es OCSP (Online Certificate Status Protocol).
- 5.46. Proveedor: Significa la organización o persona que suministra un producto o servicio para el PSC PROCERT.
- 5.47. PSC: Significa Proveedor de Servicios de Certificación
- 5.48. Registro de Auditoria: Significa la unidad de dato discreta registrada en el rastro de auditoría cuando ocurre un evento que es registrado. Un registro de auditoría

- consiste de un conjunto de descripciones de auditoría, cada uno de los cuales tiene un conjunto de atributos de auditoría asociados a éste. Cada registro de auditoría tiene una descripción de auditoría para el encabezamiento del registro y usualmente tiene descripciones de auditoría adicionales que describen la entidad(es) y objeto(s) involucrados en el evento.
- 5.49. Resumen de Información: Significa la información básica requerida para la producción de un certificado de clave pública para la verificación de una firma electrónica, la validación del estatus del certificado, así como la información producida como resultado de esta verificación.
 - 5.50. Revocación: Significa el cambio de estatus de un certificado válido o suspendido a “revocado” a partir de una fecha específica en adelante.
 - 5.51. Revocación de Certificado: Significa el proceso que consiste en cambiar el estatus de un certificado de válido o suspendido o revocado. Cuando un certificado tiene estatus revocado, esto significa que una entidad ya no se debe confiar en él para ningún fin.
 - 5.52. Seguridad Física: Significan las medidas utilizadas para proveer protección física a los recursos contra amenazas deliberadas y accidentales.
 - 5.53. Servicios de Certificación: Significa los servicios que se pueden suministrar con relación al manejo del ciclo de vida de los certificados a cualquier nivel de la jerarquía de la ICP, incluyendo servicios auxiliares tales como servicios OCSP, servicios de tiempo compartido, servicios de verificación de identidad, hospedaje de LCR, etc.
 - 5.54. Solicitante: Significa la entidad que ha solicitado la emisión de un certificado dentro de la ICP de PROCERT. El proceso de verificación varía de acuerdo con la naturaleza y, donde aplique, el rol operacional dentro de la ICP correspondiente al certificado que la entidad está solicitando.
 - 5.55. Solicitud de Certificado: Significa la solicitud autenticada por una entidad por su autoridad matriz para emitir un certificado que une la identidad de esa entidad a una clave pública.
 - 5.56. Token de tiempo: Un token de tiempo es un objeto criptográfico emitido por una Autoridad de Estampado de Tiempo (TSA) que vincula de manera segura un conjunto de datos con una marca temporal verificable.
 - 5.57. Uso del Certificado: Significa el conjunto de reglas que indican la aplicabilidad del certificado de una comunidad en particular y/o la clase de aplicación con requerimientos de seguridad comunes. Por ejemplo, un certificado de póliza en particular puede indicar la aplicabilidad de un tipo de certificado para la autenticación de comunicaciones móviles para el mercadeo de productos dentro de un determinado rango de precios.
 - 5.58. Validación: Significa el proceso de verificación de la validez de un Certificado en términos de su estatus (Ej. suspendido o revocado).
6. Objetivo: La DPC y la política de certificados, se constituyen en la guía de mejores principios de gestión y operación del PSC PROCERT, los cuales deben ser documentados e informados a la Alta Dirección, personal, Clientes, Proveedores y Parte Interesada del PSC PROCERT. Los certificados electrónicos emitidos por el PSC PROCERT bajo la clase de “Firma Electrónica”, a los efectos de la aplicación del decreto ley de mensajes de datos y firmas electrónicas y su reglamento, brindarán al propietario de la “firma electrónica”, la oportunidad de contar con un instrumento electrónico que será considerado como plena prueba a los efectos de la legislación venezolana y que adicionalmente brindará las condiciones de reconocimiento de identidad, autenticación informativa dentro de un sistema de claves públicas y

privadas, la posibilidad del establecimiento del no repudio de la "Firma Electrónica" y ofrecerá posibilidad de garantizar la integridad del mensaje y del dato contenido en la "firma electrónica", ampliando sensiblemente el universo de actividades y transacciones que podrán contar con plena validez legal dentro del espectro de la Internet y en diferentes campos, dentro de los cuales pueden ser mencionados, gobierno en línea, comercio en línea, educación en línea, entre otros. La autoridad de registro (AR) del PSC PROCERT establecerá y dará fe, acerca de la identidad y datos suministrados por el cliente al cual se le asigne un certificado electrónico. Dicha información será transmitida a la AC del PSC PROCERT, a los efectos de autorizar la activación del certificado electrónico. Las AR a nivel mundial operan de forma conjunta o separada de las AC. El PSC PROCERT mantiene dentro de su organización interna a la AR.

7. Alcance: El presente documento de la DPC y PC del PSC PROCERT, aplica a la Alta Dirección, personal, Clientes, Proveedores y Parte Interesada del PSC PROCERT, para el proceso de emisión, revocación o renovación de certificados y funcionamiento de la plataforma tecnológica de certificación del PSC PROCERT.
8. Limitaciones: El numeral 32.14 del presente documento establece el límite de responsabilidad que puede ser exigido por fallas en la gestión y operación del PSC PROCERT.
9. Comunidad de usuarios y aplicabilidad.
 - 9.1. Aprobación de políticas: Toda la documentación del PSC PROCERT relacionada con el proceso de generación o revocación de certificados, operación del PSC PROCERT bajo los principios del decreto ley de mensajes de datos y firmas electrónicas (LSMDFE) y su reglamento, será elaborada por el personal y alta dirección del PSC PROCERT y sometido a la aprobación de la SUSCERTE.
 - 9.2. Actualización de la documentación: La Alta Dirección del PSC PROCERT establece las condiciones que aplican para que proceda la revisión o modificación de la documentación. Dichos elementos son los siguientes:
 - Cambios organizacionales.
 - Cambios de la normativa de acreditación como PSC por parte de la SUSCERTE o ente que regule la actividad de certificación electrónica dentro de la República Bolivariana de Venezuela.
 - Cambios en la normativa Internacional que regula la actividad de los PSC.
 - Cambios en la legislación que regula la actividad de los PSC dentro de la República Bolivariana de Venezuela.
 - Cambios en los procesos y/o subprocesos que deban ser documentados.
 - Documentación con más de seis (6) meses, sin modificación o actualización, deberá imprimirse como una nueva versión.

- 9.3. Autoridad de certificación (AC): El PSC PROCERT es una sociedad mercantil, de estricta iniciativa privada, constituida y diseñada a los efectos de constituirse como el primer PSC en cumplimiento de lo establecido en el decreto ley de mensaje de datos y firmas electrónicas, su reglamento o los cuerpos normativos que sustituyan a estos; ofrecer firmas y certificados electrónicos a personas públicas y privadas, naturales o jurídicas, públicas y privadas, prestar el servicio técnico y de soporte a las aplicaciones para firmas y certificados electrónicos; realizar acciones de adiestramiento en materia de firmas y certificados electrónicos, comercio electrónico, demás aplicaciones y usos que involucren su uso; desarrollo, mantenimiento, así como ofrecer aplicaciones para tramites en línea con entes de la administración pública centralizada y descentralizada, gobernaciones y municipios de la República Bolivariana de Venezuela. El PSC PROCERT ha ubicado sus oficinas administrativas en la ciudad de Caracas, Distrito Capital de la República Bolivariana de Venezuela.

- 9.3.1. Certificado raíz del PSC PROCERT: El PSC PROCERT es una autoridad de certificación de primer nivel que se encuentra subordinada a la autoridad de certificación raíz del estado venezolano y únicamente estará en funcionamiento durante la realización de las operaciones para las que se establece. La estructura del certificado raíz del PSC PROCERT es la siguiente:

Certificado de la AC Subordinada del PSC	
Nombre (X.509)	<V3>
Datos del Certificado	
Versión (versión)	V3 (Número de versión del certificado).
Serial (Serial Number)	(Identificador único menor de 32 caracteres hexadecimales.)
Algoritmo de Firma (signatureAlgorithm)	Sha-384ECDSA
Datos de Emisor (issuer)	
Nombre Común (commonName)	Autoridad de Certificación Raíz del Estado Venezolano
Organización (organizationName)	Sistema Nacional de Certificación Electrónica
País (countryName)	VE
Datos de Validez	
No Antes (notBefore)	Fecha en que el periodo de validez del certificado comienza (UTC)
No Después (notAfter)	Fecha en que el periodo de validez del certificado culmina (UTC)
Datos de Titular (subject)	
Nombre Común (commonName)	PROCERT SMIME ECC CA
Organización (organizationName)	Proveedor de Certificados PROCERT ITFB
País (countryName)	VE
Información de Clave Pública del Titular	
Algoritmo de clave pública (algorithm)	ECDSA (384 Bits)

Parámetros de Clave Publica	ECDSA_P384
Extensiones	
Identificador de la clave del titular (Subject Key Identifier)	
Clave de Autoridad emisora (keyIdentifier)	KeyIdentifier <clave pública del propio certificado de la AC Subordinada>
Uso de la llave (keyUsage)	
Firma digital, Firma de certificados, Firma CRL sin conexión, Firma de lista de revocación de certificados (CRL) (86)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier) (Requerido)	
Identificador de la clave del titular (keyIdentifier)	KeyIdentifier <Contiene una copia del Subject Key Identifier (SKI) del certificado de la CA Superior que firmó la AC Subordinada>
Puntos de Distribución de las LCR (cRLDistributionPoints)	
Punto de distribución LCR (distributionPoint)	http://acraiz.suscerte.gob.ve/lcr-ecdsa
AIA (authorityInfoAccess)	
id-ad-ocsp	1.3.6.1.5.5.7.48.1 http://ocsp-ecdsa.suscerte.gob.ve/
PolicyIdentifier (PC/CP)	
PolicyQualifiers (DPC/CPS)	
cPSuri	http://acraiz.suscerte.gob.ve/dpc
Firma	
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha384WithECDSAEncryption)
Firma(signature)	<Contenido de la Firma>

9.3.2. Raíz de certificación del PSC PROCERT: El PSC PROCERT posee una plataforma de certificación auditada y autorizada por la SUSCERTE la cual cumple con los estándares internacionales para operación de una infraestructura de clave pública bajo estándar X-509 V3. El PSC PROCERT se encuentra en capacidad de emitir certificados electrónicos para distintos usos. Las claves criptográficas son generadas por el usuario a través de los CSP contenidos en los browsers. La SUSCERTE previa evaluación de cumplimiento de los requisitos de Ley, firma una petición de certificado con la plataforma del certificado raíz del estado venezolano. Una vez firmado el certificado, el PSC PROCERT se constituye en una autoridad de certificación de segundo nivel y se encuentra subordinada a la SUSCERTE. El certificado raíz generado por la SUSCERTE, debe ser integrado por el PSC PROCERT, dentro de su plataforma de certificación a los efectos de poder a su vez generar y asignar los certificados electrónicos bajo los parámetros del decreto ley sobre mensajes de datos y firmas electrónicas (LSMDFE) y su reglamento (RLSMDFE). El PSC PROCERT debe generar cada veinticuatro (24) horas una lista de certificados revocados (LCR), la cual se constituye en un mecanismo de validación y comprobación del estado de los certificados electrónicos y verificar cuales se encuentran revocados. Todo proceso de revocación de certificado es informado por el PSC PROCERT, vía correo electrónico al Cliente propietario del certificado electrónico. Dicha notificación se

informa mensualmente a la SUSCERTE y se incluye en el depósito digitalizado mantenido por el PSCPROCERT.

9.3.3. Modelo de operación del PSC PROCERT.

9.3.3.1. Sede Administrativa: La sede administrativa gestiona los procesos administrativos, financieros, fiscales y de recursos humanos requeridos para la operación del PSC PROCERT; igualmente, desde la oficina administrativa opera la AR, la cual es la encargada de gestionar la comprobación de la documentación e identidad de los clientes contratantes y dar fe pública de la revisión y conformación de los datos aportados por cada uno de los clientes contratantes de certificados electrónicos. La dirección física de la sede administrativa es la siguiente: Multicentro Empresarial del Este, Núcleo B, Torre Libertador, Piso 13, Oficina B-132, Municipio Chacao de la Ciudad de Caracas, República Bolivariana de Venezuela. El horario de atención al público en general desde la sede administrativa del PSC PROCERT es el siguiente: de 8:00 a.m. a 12:00 m y de 1:00 p.m. a 5:00 p.m.), de lunes a viernes de cada semana, de cada mes calendario, de cada año calendario. El PSC PROCERT proveerá certificados electrónicos de firma a todas las personas naturales y/o jurídicas que cumplan con los requisitos contemplados en el decreto ley de mensaje de datos y firmas electrónicas y reglamento y que finalicen de forma exitosa el proceso de contratación y aceptación de términos contractuales; fijándose un plazo de vigencia para los certificados que sean emitidos, de un (1) año. El PSC PROCERT, contempla que en el supuesto de la ocurrencia de un evento que afecte de forma permanente la integridad de su sede administrativa, se proceda a iniciar operaciones desde una nueva sede que cumpla los requisitos impuestos por la SUSCERTE. No obstante, en caso de desastre que inhabilite o destruya la sede administrativa de PROCERT, se mantiene una previsión contractual con la Universidad Simón Bolívar a los fines de poder operar desde la sede de su centro de datos, por el período de contingencia.

9.3.3.2. Relación con proveedores de tecnología y empresas asociadas: El PSC PROCERT mantiene relaciones comerciales y alianzas estratégicas con las empresas que se indican a continuación: i) Microsoft; ii) Thales; y iii) Daycohost.

9.3.3.3. Página web: El PSC PROCERT mantiene en operación un portal web (www.procert.net.ve) con alta disponibilidad. El portal web del PSC PROCERT en su página de inicio mantiene los vínculos siguientes: i) Sistema AR, donde el usuario podrá obtener información que le facilitara en cuanto a la compra de certificados paso a paso, informarse acerca de los precios de los certificados que provee la PSC PROCERT y sus firmas electrónicas de validez legal ii) Sistema de Certificación, donde el usuario podrá acceder a su casillero de manejo de ciclo de vida del certificado electrónico; iii) EN/ES, donde el usuario al hacer clic cambiara el

lenguaje del portal web de español a inglés y viceversa; iv) LCR donde el usuario podrá descargar la LCR emitida diariamente por el PSC PROCERT; v) Certificado Raíz SUSCERTE, Donde los usuarios podrán descargar la cadena de certificación del estado venezolano. vi) Emitidos, donde el usuario podrá consultar los certificados emitidos por el PSC PROCERT; vii) App y Usos, informarse acerca del uso de los certificados electrónicos, del manejo del certificado durante el ciclo de vida del certificado; viii) Gestión, donde el usuario podrá informarse acerca del uso de los certificados electrónicos, del manejo del certificado durante el ciclo de vida del certificado ix) AC PROCERT, donde el usuario puede acceder a la documentación técnica del PSC PROCERT y las políticas de certificados; x) Firma en línea, donde los usuarios del PSC PROCERT podrán firmar en línea y con certificados emitidos por el PSC PROCERT, documentos electrónicos en formato .PDF; xi) Soporte, donde es posible acceder a la información referida a los sistemas y software soportados por los certificados emitidos por el PSC PROCERT, encontrar a lista de preguntas frecuentes y acceder a videos tutoriales acerca del uso de certificados electrónicos y la firma electrónica; xii) PKI, donde el usuario podrá asesorarse en cuanto a la creación de una infraestructura de clave pública; xiii) SSL, donde el usuario podrá obtener información en cuanto a los certificados de seguridad, precio, uso, y clasificación. xiv) Contáctenos donde el usuario podrá al hacer clic enviar directamente un correo electrónico a la dirección de la PSC PROCERT además de obtener su teléfono de contacto. xv) Twitter, donde el usuario podrá acceder a información técnica publicada en distintos portales o producida por el PSC PROCERT respecto a los certificados electrónicos.

- 9.3.3.4. Centro de datos: El PSC PROCERT mantiene un esquema operacional orientado a garantizar la continuidad operacional y prestación de servicios con altos estándares de calidad, oportunidad y seguridad. El centro de datos se constituye en la sede operacional del PSC PROCERT y desde donde opera la plataforma de emisión de certificados. El centro de datos reúne y mantiene los requisitos de operación que para este tipo de facilidades impone la normativa internacional en materia de seguridad asociada a la tecnología de información, la legislación de la República Bolivariana de Venezuela y las normas impuestas por la SUSCERTE. El mantenimiento y operación de la plataforma tecnológica de certificación del PSC PROCERT es ejecutada por su propio personal. El centro de datos se encuentra en la Ciudad de Caracas y pertenece a la empresa Daycohost. El centro de datos opera las veinticuatro (24) horas del día, los trescientos sesenta y cinco (365) días del año y mantiene una autonomía operacional superior a dos (2) meses. Adicionalmente centro de datos reúne condiciones y características de construcción antisísmica y de prevención de incendio e inundaciones, mantiene un perímetro de seguridad y cuenta con

siete (7) niveles de seguridad de acceso. El centro de datos desde donde opera el PSC PROCERT mantiene las pólizas o instrumentos emitidos por empresas de seguros solventes y reconocidas, a los efectos de mantener un respaldo en caso de ocurrencia de una contingencia que afecta la integridad física de la referida sede administrativa y pueda ofrecer de esa manera una garantía de su continuidad operacional. La AC PROCERT mantiene contrato de operación de centro alerno en caso de daño permanente que imposibilite y restrinja la operación regular del centro de datos.

9.3.3.5. Esquema del modelo operacional del PSC PROCERT



- 9.4. Autoridad de registro (AR): Es la organización interna dentro del PSC PROCERT encargada de validar y comprobar la identificación y los datos suministrados por las personas jurídicas o naturales que compren certificados electrónicos y con el fin de poder dar fe pública que el cliente que detenta y usa un certificado electrónico, es quien efectivamente dice ser o representar en el caso de persona jurídica, garantizando de esa manera la identidad del Cliente de un certificado electrónico y en consecuencia, legalidad de las responsabilidades y obligaciones derivadas del uso de la firma electrónica bajo los supuestos del decreto ley sobre mensajes de datos y firmas electrónicas y su reglamento. Todos los interesados en obtener un certificado electrónico bajo el decreto ley sobre mensajes de datos y firmas electrónicas, su reglamento y la normativa de la SUSCERTE, deberán remitir copia de la documentación soporte de sus datos y acudir a la cita fijada por la AR del PSC PROCERT a los efectos de realizar la verificación, validación presencial y documental de los registros, soportes y demás comprobantes que acreditan su identidad y/o representación de los representantes de personas jurídicas que opten por un certificado electrónico. Si el interesado no atiende la entrevista pautada por la AR del PSC PROCERT quedará anulada su solicitud o petición de registro y se aplicará la retención por penalidad, debiendo en consecuencia el Cliente interesado proceder nuevamente a su registro de solicitud de certificado electrónico ante la página web del PSC PROCERT). La documentación soporte utilizada para validar a los clientes o Clientes que solicitan certificados electrónicos, será almacenada por el PSC PROCERT, durante el período de diez (10) años contados a partir de la vigencia del certificado o de cualquiera de sus renovaciones.

9.4.1. Modelo de Operación de la AR

9.4.1.1. Sede administrativa: La AR del PSC PROCERT mantiene un esquema de gestión orientado a garantizar la continuidad operacional y prestación de servicios con altos estándares de calidad, oportunidad y seguridad. La AR opera desde la sede administrativa del PSC PROCERT y es la encargada de validar y dar conformidad acerca de la identidad de los clientes contratantes de certificados electrónicos, para que, una vez comprobada la información e identidad de los clientes contratantes, se proceda con el registro de los clientes y posterior generación de los certificados electrónicos.

9.4.1.2. Validación de identidad: Recibida la documentación de los clientes la AR del PSC PROCERT a fijar oportunidad para que tenga lugar la entrevista de validación de identidad, la cual podrá ser presencial o vía web con entrevista grabada a tales fines. Durante la entrevista el operador de la AR del PSC PROCERT solicita información del cliente y solicita que el cliente bajo fe de juramento señale que sus datos son verdaderos. Para validar nombres de dominio, la AR del PSC PROCERT hace la debida consulta a <http://www.whois.net/> y <http://www.nic.ve/> El cliente debe suministrar la información que coincida con su registro en Whois.net o Nic.ve. Con la información suministrada por los clientes, se ejecuta la validación de Whois o Nic.ve; con el fin de validar veracidad de la misma. La información proporcionada por el cliente, deben coincidir con los registros de Whois.net o Nic.ve. Sin la documentación correcta y registro, el PSC PROCERT se abstendrá de procesar cualquier solicitud. Para validar la dirección de correo electrónico, la AR del PSC PROCERT envía un correo electrónico solicitando información al cliente. Todos los correos electrónicos enviados por la AR del PSC PROCERT están firmados electrónicamente. Los mensajes de correo electrónico exigirán la autorización del titular de la cuenta de correo electrónico. Cada uno de los correos electrónicos enviados por el PSC PROCERT debe solicitar requisitos diferentes asociados con el proceso de validación en cada caso. Estos mensajes de correo electrónico del PSC PROCERT no son predecibles, ya que se requiere información que sólo el cliente conoce. Además, el personal del PSC PROCERT debe verificar toda la información (declaraciones juradas, estatutos, RIF, la identificación de las empresas, las facturas de servicios públicos). La AR del PSC PROCERT solicitará una declaración acerca de la propiedad de dominio y carta de autorización en los casos de certificados SSL gestionados con proveedores externos. Las solicitudes de certificados (CSR) deben cumplir los requisitos del CA Browser Forum. Los clientes responderán el correo electrónico con toda la información solicitada por la AR PROCERT. Para problemas de soporte técnico, PROCERT utiliza sopORTE@procert.net.ve. En el caso de los certificados SSL gestionados con proveedores externos, solo se procesarán

las solicitudes de certificados (CSR) generadas en cumplimiento del estándar nacional e internacional, atendiendo especialmente las establecidas por el CA Browser Forum, las cuales se indican a continuación:

Según la norma de CA-Browser-Forum-BR-1.5.2 en la sección 7.1.4:

“Name Forms”:

- 1) SAN: Esta extensión DEBE contener al menos una entrada. DEBE ser un dNSName que contenga el nombre de dominio completo o la Dirección IP del servidor
- 2) SAN: Este campo no debe contener dirección IP reservada o Nombre interno
- 3) Common Name: El common name debe encontrarse en el SAN
- 4) Common Name: No colocar en este campo https://
- 5) SAN y Common Name: No debe tener las siguientes características:

El uso del punto(.)

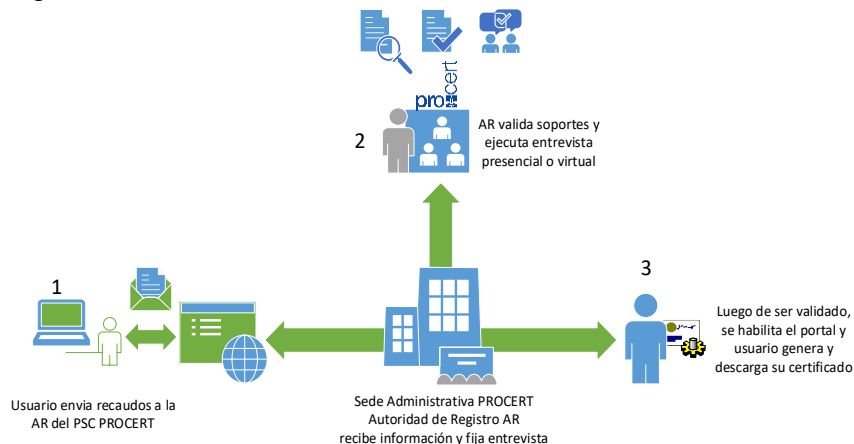
El uso del Espacio en blanco u otro valor que indique un valor ausente o incompleto

El uso del Símbolo de menos (-)

Todos los demás atributos opcionales, cuando están presentes en el campo de la asignatura, DEBEN contener información que ha sido verificada por la CA. Los atributos opcionales NO DEBEN contener metadatos como los caracteres '.', '-' y " (es decir, espacio), y / o cualquier otra indicación de que el valor está ausente, incompleto o no aplicable. Todos los correos electrónicos son firmados por el personal PROCERT. La AR del PSC PROCERT ejecutará las llamadas telefónicas, con el fin de validar toda la información del cliente. La AR del PSC PROCERT utiliza el número de teléfono proporcionado por el cliente en la información entregada al PSC PROCERT. Esta información deberá ser validada con los registros oficiales y públicos de la página Web de la Compañía Telefónica Nacional. Cuando un cliente solicita información para comprar un certificado, recibirá un correo electrónico de la AR del PSC PROCERT con información completa; ofreciendo de esa manera la garantía de proporcionar en cada momento toda la información que el cliente necesita. Los documentos que deben ser presentados por los clientes para la contratación de certificados electrónicos, varían en función del tipo de idos por tipo de certificado y son comunicados a los clientes vía correo electrónico firmado por la AR del PSC PROCERT. Estos documentos pueden variar y los clientes son informados por correo electrónico firmado en cada oportunidad. Esto, con el propósito de prevenir los constantes cambios en el presente documento, derivados de cambios en los requisitos (inclusión o

exclusión de cualquiera de ellos). La integridad del presente documento se protegerá de los cambios innecesarios. Los clientes contratantes de firmas o certificados electrónicos deben ir a la Oficina Administrativa de PROCERT ubicada en Multicentro Empresarial del Este, Núcleo B, Torre Libertador, Piso 13, Oficina B-132, Municipio Chacao en la ciudad de Caracas, República Bolivariana de Venezuela, en la fecha y hora establecidos por el sistema de contratación PROCERT dentro del horario de trabajo de 8:00 am a 12:00 m y de 1:00 pm a 5:00 pm, de lunes a viernes de cada semana de cada mes calendario, de cada año calendario. También es posible validar la identidad del usuario por vía de entrevista electrónica que es grabada y asociada a la información del cliente, todo lo cual se requiere para autorizar la generación del certificado. El cliente contratante deberá notificar las limitaciones o imposibilidad de asistir a la cita fijada por correo electrónico a la dirección de sopORTE@procert.net.ve con no menos de cuarenta y ocho (48) horas antes de la fecha fijada para la cita. La AR del PSC PROCERT reprogramará por una sola ocasión la oportunidad para la validación de identidad y notificará al usuario contratante por correo electrónico. Si el cliente contratante no notifica su imposibilidad de atender la cita reprogramada, y no es posible validar la identidad; entonces la AR del PSC PROCERT procederá a cancelar la solicitud y aplicar la penalidad correspondiente. Respecto a la validación de certificados extranjeros, prevista en el Decreto Ley de Mensajes de Datos y Firmas Electrónicas y su Reglamento, la AR del PSC PROCERT, mantendrá actualizada la data suministrada por los PSC con los cuales mantenga relación de reconocimiento y validación de certificados electrónicos, previniendo en todo momento el uso de certificados revocados. Se programarán anualmente auditorías de control y validación de la documentación e identidad de los clientes contratantes de certificados electrónicos. La documentación se mantendrá en soporte electrónico almacenado en bóveda.

9.4.1.3. Diagrama del modelo de la AR.



9.5. Modelo de Confianza: Se constituye en la guía o referencia técnico-bibliográfica a través de la cual, el cliente conoce el esquema de operación, gestión y validez legal de los certificados electrónicos generados por el PSC PROCERT, permitiendo que el cliente pueda comprobar la validez de los certificados electrónicos y confiar de esa manera en el modelo de operación y gestión del PSC PROCERT. Igualmente, el modelo de confianza permite informar al cliente usuario acerca de la raíz de certificación o autoridad que firma al PSC PROCERT.

9.5.1. Modelo Aplicado para la República Bolivariana de Venezuela: La AC Raíz se encuentra diseñada y opera bajo el principio de “Autoridad de Certificación Auto Firmada”; bajo dicho esquema la AC raíz no se encuentra subordinada a una cadena de certificación o entidad de certificación extranjera, y autofirma un certificado raíz único para la certificación de firmas electrónicas o emisión de certificados electrónicos. En Venezuela el ente rector de la materia es la SUSCERTE. La SUSCERTE cumple con estándares tecnológicos y legales internacionalmente reconocidos y aplicables a la materia de certificación electrónica y es la encargada de realizar la custodia del certificado raíz al cual se encontrarán subordinados todos los PSC públicos o privados, que se encuentren legalmente acreditados para operar en la República Bolivariana de Venezuela. Las actividades de la SUSCERTE y de los proveedores acreditados de servicios de certificación se encuentran normadas por el Decreto Ley de Mensajes de Datos y Firmas Electrónicas y su Reglamento. Todo PSC dentro de la República Bolivariana de Venezuela, acatar y cumplir las resoluciones y normativa técnica emanada de la SUSCERTE y el marco legal aplicable a la materia.

9.5.2. Acreditación como PSC: Dentro del modelo venezolano y la normativa legal contenida en el Decreto Ley de Mensajes de Datos y Firmas Electrónicas, se contempla que todo interesado, ya sea público o privado, cumpla con un proceso de acreditación ante la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), lo cual supone el cumplimiento de los pasos siguientes:

- Auditoria previa a la solicitud de acreditación ante la SUSCERTE, la cual debe ser realizada por un Auditor Informático acreditado por dicho despacho. El auditor acreditado emitirá un informe de auditoría técnica de cumplimiento de la norma y estándares aplicables y exigibles para la operación del PSC. Dicho informe de auditoría técnica se constituye en uno de los requisitos para realizar la solicitud de acreditación o de renovación de acreditación ante la SUSCERTE.
- Presentación de la solicitud de acreditación o de renovación de acreditación ante la SUSCERTE, lo cual supone el cumplimiento a satisfacción de la auditoria previa citada en 9.5.2.1 y el cumplimiento de los requisitos y estándares financieros fijados por la SUSCERTE.
- Una vez cumplidos los puntos 9.5.2.1 y 9.5.2.2, presentar la garantía requerida por el Estado a los efectos de poder operar como PSC.
- Una vez cumplidos todos los requisitos de Ley, la SUSCERTE, emitirá la acreditación y número de operación asignado al PSC en caso de primera solicitud o procederá a la emisión de la providencia administrativa de renovación de acreditación en caso de PSC ya acreditado; posteriormente

en el caso de primera solicitud, la SUSCERTE junto al PSC procederán a la ceremonia de claves e instalarán en la plataforma tecnológica del PSC el certificado raíz emitido y firmado por la SUSCERTE. En los casos de renovación el proceso culmina con la publicación de la providencia administrativa de renovación en la gaceta oficial.

9.5.3. Modelo Aplicado por el PSC PROCERT: El PSC PROCERT es una sociedad mercantil, de estricta iniciativa privada, constituida y diseñada a los efectos de constituirse como el primer proveedor de servicios de certificación electrónica en cumplimiento de lo establecido en el Decreto Ley de Mensaje de Datos y Firmas Electrónicas, su reglamento o los cuerpos normativos que sustituyan a estos; ofrecer firmas y certificados electrónicos a personas naturales o jurídicas, públicas y privadas, prestar el servicio de hospedaje o hosting a entes públicos, gubernamentales o del sector privado; prestar el servicio técnico y de soporte a las aplicaciones para firmas y certificados electrónicos y de hosting; realizar acciones de adiestramiento en materia de firmas y certificados electrónicos, comercio electrónico, subastas electrónicas y demás aplicaciones y usos que involucren su uso; desarrollar, mantener y ofrecer aplicaciones para tramites en línea con entes de la administración pública centralizada y descentralizada, gobernaciones y municipios de la República Bolivariana de Venezuela; compra, venta, distribución, importación y/o exportación de productos, bienes y servicios, software y hardware, así como la realización de toda clase de actividades comerciales, mercantiles e industriales lícitas, representación de empresas nacionales y extranjeras y todos aquellos actos de lícito comercio que permita la Ley, estén o no comprendidos en la enumeración de actividades que antecede. Nuestro mercado principal se constituirá en la Banca Comercial, compañías de seguros, grandes empresas y la pequeña y mediana industria. El PSC PROCERT ha ubicado sus oficinas centrales en la ciudad de Caracas, Distrito Capital de la República Bolivariana de Venezuela y cumple con los requisitos técnicos y económicos financieros exigidos la SUSCERTE, a través de la exhaustiva normativa dictada a tales efectos por dicho ente regulador de la actividad de los PSC. El PSC PROCERT opera bajo estándar tecnológico y claves criptográficas de autoridad subordinada, lo cual facilita la instalación del certificado raíz emitido por la SUSCERTE y la independencia y seguridad de la base de datos de certificados emitidos por el PSC PROCERT. La plataforma de certificación del PSC PROCERT deriva de un hardware y software criptográfico, los cuales se denominan en el caso del hardware "HSM" y en el caso del software criptográfico "Plataforma de Servicios de Certificación", el cual es propiedad de la empresa PROCERT. El PSC PROCERT está en capacidad de emitir certificados electrónicos para distintos usos. Las claves criptográficas se mantienen fuera de línea en el Centro de Datos desde el cual opera el PSC PROCERT. El PSC PROCERT publica la LCR, la cual se constituye en un registro de todos aquellos certificados que, habiendo cumplido su proceso de generación y asignación de Ley, son revocados cuando se encuentra comprometida su clave, por solicitud del usuario, por uso indebido del certificado, por causa imputable al usuario o por cese de operación del PSC PROCERT. La LCR es actualizada cada veinticuatro (24) horas en la página web de

PROCERT (www.procert.net.ve), durante los trescientos sesenta y cinco (365) días de cada año calendario, mientras se encuentre en operación el PSC PROCERT. Adicionalmente el PSC PROCERT cuenta con un enlace OCSP, el cual permite validar en línea el estado de los certificados. Todo proceso de vencimiento o revocación de certificado es notificado de forma automática por correo electrónico al signatario propietario del certificado. El desarrollo de modelo de confianza establecido por el PSC PROCERT, se encuentra contenido en el documento emitido por el PSC PROCERT denominado Modelo de Confianza, distinguido con la nomenclatura AC-D-0001.

9.6. Registro de Acceso Público: El Registro de Acceso Público es un documento de apoyo a la presente DPC y PC, permite suministrar la información referida al acceso al sitio web de la AC, breve descripción de la tecnología utilizada para la generación de certificados, medidas de seguridad aplicables para la protección del sitio web y funcionalidades del mismo, en cumplimiento con los lineamientos impuestos por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) a los efectos de lograr poder operar como PSC. El registro de acceso público permite entre otros puntos los siguientes:

- Asegurar el acceso a información relevante descriptiva del sistema por parte de los Clientes.
- Ofrecer una descripción del sitio web del PSC PROCERT.
- Señalar los servicios y productos ofrecidos por el PSC PROCERT.
- Describir la tecnología (hardware y software) utilizado.
- Descripción de proceso de contratación de certificados electrónicos.
- Información acerca de los mecanismos de seguridad utilizados en el portal web del PSC.

9.6.1. Relativas al Detalle del Sitio Web PROCERT: La plataforma tecnología de PROCERT posee un sitio de acceso electrónico disponible las veinticuatro (24) horas de cada día, durante los trescientos sesenta y cinco (365) días de cada año calendario. La operación de dicho sitio web es monitoreada las veinticuatro (24) horas de cada día, durante los trescientos sesenta y cinco (365) días de cada año calendario. Toda falla del sistema deberá ser atendida de conformidad con lo establecido en el Plan de Recuperación de Negocio y Recuperación ante Desastres (PRD) de PROCERT (AC-P-0001)

9.6.2. Relativas al Contenido de la Página Web PROCERT: El sitio Web de PROCERT contiene la información necesaria para entender el proceso de contratación, uso y aplicaciones de los certificados electrónicos e información relacionada con la actividad de certificación electrónica y la empresa PROCERT; igualmente los clientes usuarios encontrarán la documentación de la AC PROCERT; de la AR PROCERT; y de la información producida y derivada de la SUSCERTE. Las direcciones contenidas en la página web de PROCERT son las siguientes:

- Dirección para petición/activación de certificados.

- Dirección para reporte de eventos ocurridos en la plataforma PROCERT.
- Dirección para la búsqueda de los certificados emitidos.
- Dirección para acceder a la LCR cuya publicación será cada veinticuatro (24) horas de conformidad con lo establecido en el documento de la Política y Estructura de la LCR.
- Dirección para realizar la revocación o suspensión de certificados vigentes.
- Resoluciones de la SUSCERTE.
- Documento de la Política de Certificación y Declaración de Prácticas de Certificación en formato PDF.
- Dirección donde se describen los Productos y Servicios que ofrece PROCERT.
- Documentación Técnica sobre la instalación y usos de los certificados electrónicos.
- Información general acerca de la certificación electrónica (ventajas y tendencias).
- Información de contacto PROCERT.

El desarrollo del Registro de Acceso Público establecido por el PSC PROCERT, se encuentra contenido en el documento emitido por el PSC PROCERT denominado Registro de Acceso Público, distinguido con la nomenclatura AC-R-0002.

9.7. Tipos de certificados.

El PSC PROCERT se encuentra en capacidad de generar certificados de firma electrónica con clave de 384. El estándar aprobado por la SUSCERTE para los certificados nacionales es de 384 bit de longitud de clave. El PSC PROCET actualmente cuenta con autorización de la SUSCERTE para emitir los certificados electrónicos que se indican a continuación:

- Estructura de respuesta para servidor de OCSP
- Estructura de Certificado Electrónico para Persona Natural
- Estructura de Certificado Electrónico para Profesional Titulado
- Estructura de Certificado Electrónico para Empleado de Institución Pública
- Estructura de Certificado Electrónico para Empleado de Empresa Privada
- Estructura de Certificado Electrónico para Banca Electrónica
- Estructura de Certificado Electrónico para Representante de Institución Pública
- Estructura de Certificado Electrónico para Funcionario Público
- Estructura de Certificado Electrónico para Representante de Empresa Privada
- Estructura de Certificado Electrónico para Firma de Transacción
- Estructura de Certificado Electrónico para Factura Electrónica
- Estructura de Certificado Electrónico para Comercio Electrónico

9.7.1. Certificado electrónico para OSCP: Los Certificados para OSCP se utilizan dentro de la Plataforma Tecnológica de Certificación del PSC PROCERT, a los fines de dar cumplimiento al estándar nacional e internacional y nos permiten validar el estado de los certificados emitidos por el PSC PROCERT. Comprobando que es correcto y que no está revocado, permitiendo una mayor seguridad en las transacciones. El uso asignado al certificado para OSCP es el siguiente:

- Determinar el estado de vigencia de un certificado digital X.509 usando otros medios que no sean el uso de CRL.
- Brindar confianza en el usuario de los certificados emitidos por el PSC PROCERT.

Estructura de Certificado Electrónico para OSCP

Certificado para OSCP	
Nombre (X.509)	<V3>
Datos del Certificado	
Versión (versión)	V3 (Número de versión del certificado).
Serial (Serial Number)	(Identificador único menor de 32 caracteres hexadecimales.)
Algoritmo de Firma (signatureAlgorithm)	Sha-384ECDSA
Datos de Emisor (issuer)	
Nombre Común (commonName)	PROCERT SMIME ECC CA
Organización (organizationName)	Proveedor de Certificados PROCERT ITFB
País (countryName)	VE
Datos de Validez	
No Antes (notBefore)	Fecha en que el periodo de validez del certificado comienza (UTC)
No Después (notAfter)	Fecha en que el periodo de validez del certificado culmina (UTC)
Datos de Titular (subject)	
Nombre Común (commonName)	PROCERT SMIME ECC CA
Organización (organizationName)	Proveedor de Certificados PROCERT ITFB
País (countryName)	VE
Información de Clave Pública del Titular (subjectPublicKey)	
Algoritmo de clave pública (algorithm)	ECC (384 Bits)
Parámetros de Clave Publica	ECDSA_P384
Extensiones	
Uso de la llave (keyUsage)	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)	
Clave de Autoridad (keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC>

Usos Extendidos de la Clave (extKeyUsage) (Requerido)	
Firma de OSCP	ocspSigning 1.3.6.1.5.5.7.3.9
AIA (authorityInfoAccess) (Requerido)	
id-ad-ocsp	1.3.6.1.5.5.7.48.1 http://ocspsmime.procert.net.ve/ocsp
Políticas de certificado (certificatePolicies)(Opcional)	
Firma	
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha384WithECDSAEncryption)
Firma(signature)	<Contenido de la Firma>

Usos permitidos: El uso del certificado subordinado del PSC PROCERT estará limitado a la firma de certificados electrónicos para autoridades subordinadas, firma de las listas de certificados revocados y la firma de todos los certificados establecidos en el presente documento. El uso del certificado electrónico para OSCP emitido por el PSC PROCERT es el siguiente:

Tipo de certificado	Uso	Uso mejorado
Certificado electrónico para OSCP	Firma electrónica	Firma OSCP

9.7.2. Certificado electrónico para Persona Natural: El uso asignado para este tipo de certificado es el siguiente:

- Transacciones privadas, distintas a prestación de servicios profesionales.
- Comunicaciones privadas o públicas a título personal.
- Compras electrónicas para personas naturales.
- Declaraciones o trámites en línea ante gobierno para personas naturales.

Estructura del certificado electrónico para Persona Natural.

Certificado Persona Natural	
Nombre (X.509)	<V3>
Datos del Certificado	
Versión (versión)	V3 (Número de versión del certificado).
Serial (Serial Number)	(Identificador único menor de 32 caracteres hexadecimales.)
Algoritmo de Firma (signatureAlgorithm)	Sha-384ECDSA
Datos de Emisor (issuer)	
Nombre Común (commonName)	PROCERT SMIME ECC CA
Organización (organizationName)	Proveedor de Certificados PROCERT ITFB
País (countryName)	VE
Datos de Validez	
No Antes (notBefore)	Fecha en que el periodo de validez del

	certificado comienza (UTC)
No Después (notAfter)	Fecha en que el periodo de validez del certificado culmina (UTC)
Datos de Titular (<i>subject</i>)	
Nombre Común (<i>commonName</i>)	<Nombre Completo>
Nombre (GivenName)	<Nombre del sujeto>
Apellido (Surname)	<Apellido del sujeto>
serialNumber (DN)	<Cedula o Pasaporte>
Dirección de correo(emailAddress)	<La dirección de correo>
Localidad(<i>localityName</i>)	<Ciudad donde se ubica el titular>
Estado (<i>stateOrProvinceName</i>)	<Información del estado o provincia del titular>
País (<i>countryName</i>)	UTF8 [VE] (ISO 3166-1-alpha-2)
Información de Clave Pública del Titular (<i>subjectPublicKey</i>)	
Algoritmo de clave pública (<i>algorithm</i>)	ECC (384 Bits)
Parámetros de Clave Publica	ECDSA_P384
Extensiones	
Uso de la llave (keyUsage)	Firma digital, Sin repudio, Acuerdo de claves
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)	
Clave de Autoridad (<i>keyIdentifier</i>)	KeyIdentifier <Identificador de la clave pública de la AC>
Identificador de la clave del sujeto	
Clave de Autoridad (<i>keyIdentifier</i>)	KeyIdentifier <clave pública del propio certificado de la AC>
Nombre alternativo del sujeto (subjectAlternativeName)	
Formato de correo tradicional	<Dirección de correo electrónico>
Usos Extendidos de la Clave (extKeyUsage) (Requerido)	
Firma de documentos	Firma de documento (1.3.6.1.4.1.311.10.3.12)
Protección de correo	Correo seguro (1.3.6.1.5.5.7.3.4)
Acuerdo clave	KeyAgreement
Puntos de Distribución de las LCR (cRLDistributionPoints)	
Punto de distribución LCR (<i>distributionPoint</i>)	< http://www.procert.net.ve/ecc-crl/smime-ca.crl >
AIA (authorityInfoAccess) (Requerido)	
id-ad-ocsp	1.3.6.1.5.5.7.48.1< http://ocspsmime.procert.net.ve/ocsp >
id-ad-calssuers	1.3.6.1.5.5.7.48.2 < http://www.procert.net.ve/ecc-crt/smime-ca.crt >
Políticas de certificado (certificatePolicies)	
<i>policy identifier(s)</i>	<Indica la política de la CA que confirma el cumplimiento>
PolicyQualifiers (Calificador de política)	

cPSuri	< http://www.procert.net.ve/dpc-pc >
Firma	
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha384WithECDSAEncryption)
Firma(signature)	<Contenido de la Firma>

Uso autorizado del certificado electrónico de firma de firma para Persona Natural.

Uso	Uso mejorado
Firma electrónica, no repudio, cifrado y firma de correo.	Firma de documentos, correo seguro

9.7.3. Certificado electrónico para Profesionales Titulados: El uso asignado para este certificado es el siguiente:

- Transacciones en línea asociadas al ejercicio de profesión u oficio con colegiatura y reconocimiento legal dentro de la República Bolivariana de Venezuela.
- Comunicaciones privadas o públicas asociadas al ejercicio de profesión u oficio con colegiatura y reconocimiento legal dentro de la República Bolivariana de Venezuela.
- Comercio electrónico asociado al ejercicio de profesión u oficio con colegiatura y reconocimiento legal dentro de la República Bolivariana de Venezuela.
- Declaraciones o trámites en línea ante gobierno asociadas al ejercicio de profesión u oficio con colegiatura y reconocimiento legal dentro de la República Bolivariana de Venezuela.

Estructura del certificado electrónico para Profesionales Titulados.

Certificado Profesionales Titulados	
Nombre (X.509)	<V3>
Datos del Certificado	
Versión (versión)	V3 (Número de versión del certificado).
Serial (Serial Number)	(Identificador único menor de 32 caracteres hexadecimales.)
Algoritmo de Firma (signatureAlgorithm)	Sha-384ECDSA
Datos de Emisor (issuer)	
Nombre Común (commonName)	PROCERT SMIME ECC CA
Organización (organizationName)	Proveedor de Certificados PROCERT ITFB
País (countryName)	VE
Datos de Validez	
No Antes (notBefore)	Fecha en que el periodo de validez del certificado comienza (UTC)
No Después (notAfter)	Fecha en que el periodo de validez del certificado culmina (UTC)

Datos de Titular (<i>subject</i>)	
Nombre Común (<i>commonName</i>)	<Nombre Completo>
Nombre (<i>GivenName</i>)	<Nombre del Sujeto>
Apellido (<i>Surname</i>)	<Apellido del Sujeto>
Nombre de la organización (<i>organizationName</i>)	<Contiene el nombre legal verificado del patrocinador>
Dirección de correo (<i>emailAdress</i>)	<La dirección de correo>
Título (<i>title</i>)	<El título o rol profesional>
Serial (<i>serialNumber</i>)	<El Número de Colegiado/Matrícula Profesional>
Identificador de la organización (<i>organizacionIdentifier</i>) O.I.D 2.5.4.97	<Cedula de identidad>
Localidad (<i>localityName</i>)	<Ciudad de ubicación del titular>
Estado (<i>stateOrProvinceName</i>)	<Estado de ubicación del Titular>
País (<i>countryName</i>)	UTF8 [VE] (ISO 3166-1-alpha-2)
Información de Clave Pública del Titular (<i>subjectPublicKey</i>)	
Algoritmo de clave pública (<i>algorithm</i>)	ECC (384 Bits)
Parámetros de Clave Publica	ECDSA_P384
Extensiones	
Uso de la llave (<i>keyUsage</i>)	Firma digital, Sin repudio, Acuerdo de claves
Identificador de clave de Autoridad Certificadora (<i>Authority Key Identifier</i>)	
Clave de Autoridad (<i>keyIdentifier</i>)	KeyIdentifier <Identificador de la clave pública de la AC>
Identificador de la clave del sujeto	
Clave de Autoridad (<i>keyIdentifier</i>)	KeyIdentifier <clave pública del propio certificado de la AC>
Nombre alternativo del sujeto (<i>subjectAlternativeName</i>)	
Formato de correo tradicional	<Dirección de correo electrónico>
Usos Extendidos de la Clave (<i>extKeyUsage</i>) (Requerido)	
Firma de documentos	Firma de documento (1.3.6.1.4.1.311.10.3.12)
Protección de correo	Correo seguro (1.3.6.1.5.5.7.3.4)
Acuerdo clave	KeyAgreement
Puntos de Distribución de las LCR (<i>cRLDistributionPoints</i>)	
Punto de distribución LCR (<i>distributionPoint</i>)	< http://www.procert.net.ve/ecc-crl/smime-ca.crl >
AIA (<i>authorityInfoAccess</i>) (Requerido)	
id-ad-ocsp	1.3.6.1.5.5.7.48.1< http://ocspsmime.procert.net.ve/ocsp >
id-ad-calssuers	1.3.6.1.5.5.7.48.2 < http://www.procert.net.ve/ecc-crt/smime-

	ca.crt
Políticas de certificado (certificatePolicies)	
<i>policy identifier(s)</i>	<Indica la política de la CA que confirma el cumplimiento>
PolicyQualifiers (Calificador de política)	
<i>cPSuri</i>	< http://www.procet.net.ve/dpc-pc >
Firma	
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha384WithECDSAEncryption)
Firma(signature)	<Contenido de la Firma>

Uso autorizado del certificado electrónico de firma para Profesionales Titulados.

Uso	Uso mejorado
Firma electrónica, no repudio, acuerdo de claves y firma de correo.	Firma de documentos, correo seguro

9.7.4. Estructura de Certificado Electrónico para Empleado de Institución Pública: El uso asignado para este tipo de certificado es el siguiente:

- Transacciones en línea.
- Identificar en línea a empleados o trabajadores de empresas públicas.
- Comunicaciones electrónicas sin representación de empresas públicas o privadas.
- No confiere representación legal de empresas públicas.

Estructura del certificado electrónico para Empleado de Institución Pública:

Certificado Empleado de Institución Pública	
Nombre (X.509)	<V3>
Datos del Certificado	
Versión (versión)	V3 (Número de versión del certificado).
Serial (Serial Number)	(Identificador único menor de 32 caracteres hexadecimales.)
Algoritmo de Firma (signatureAlgorithm)	Sha-384ECDSA
Datos de Emisor (issuer)	
Nombre Común (commonName)	PROCERT SMIME ECC CA
Organización (organizationName)	Proveedor de Certificados PROCERT ITFB
País (countryName)	VE
Datos de Validez	
No Antes (notBefore)	Fecha en que el periodo de validez del certificado comienza (UTC)
No Después (notAfter)	Fecha en que el periodo de validez del certificado culmina (UTC)

Datos de Titular (<i>subject</i>)	
Nombre Común (<i>commonName</i>)	<Nombre Completo>
Nombre (<i>GivenName</i>)	<Nombre>
Apellido (<i>Surname</i>)	<Apellido>
Nombre de la organización (<i>organizationName</i>)	<Contiene el nombre legal verificado del patrocinador>
Dirección de correo (<i>emailAddress</i>)	<La dirección de correo>
Título (<i>title</i>)	<Cargo que desempeña el titular del certificado>
Serial (<i>serialNumber</i>)	<El Número de Colegiado/Matrícula Profesional>
Localidad (<i>localityName</i>)	<Ciudad de ubicación del titular>
Identificador de la organización (<i>organizationIdentifier</i>) 2.5.4.97	<Número de identificación fiscal del patrocinador>
Estado (<i>stateOrProvinceName</i>)	<Estado de ubicación del Titular>
País (<i>countryName</i>)	UTF8 [VE] (ISO 3166-1-alpha-2)
Información de Clave Pública del Titular (<i>subjectPublicKey</i>)	
Algoritmo de clave pública (<i>algorithm</i>)	ECC (384 Bits)
Parámetros de Clave Publica	ECDSA_P384
Extensiones	
Uso de la llave (<i>keyUsage</i>)	Firma digital, Sin repudio, Acuerdo de claves
Identificador de clave de Autoridad Certificadora (<i>Authority Key Identifier</i>)	
Clave de Autoridad (<i>keyIdentifier</i>)	KeyIdentifier <Identificador de la clave pública de la AC>
Identificador de la clave del sujeto	
Clave de Autoridad (<i>keyIdentifier</i>)	KeyIdentifier <clave pública del propio certificado de la AC>
Nombre alternativo del sujeto (<i>subjectAlternativeName</i>)	
Formato de correo tradicional	<Dirección de correo electrónico>
Usos Extendidos de la Clave (<i>extKeyUsage</i>) (Requerido)	
Firma de documentos	Firma de documento (1.3.6.1.4.1.311.10.3.12)
Protección de correo	Correo seguro (1.3.6.1.5.5.7.3.4)
Acuerdo clave	KeyAgreement
Puntos de Distribución de las LCR (<i>cRLDistributionPoints</i>)	
Punto de distribución LCR (<i>distributionPoint</i>)	< http://www.procert.net.ve/ecc-crl/smime-ca.crl >
AIA (<i>authorityInfoAccess</i>) (Requerido)	
id-ad-ocsp	1.3.6.1.5.5.7.48.1< http://ocspsmime.procert.net.ve/ocsp >
id-ad-caIssuers	1.3.6.1.5.5.7.48.2 < http://www.procert.net.ve/ecc-crt/smime-

	ca.crt >
Políticas de certificado (certificatePolicies)	
<i>policy identifier(s)</i>	<Indica la política de la CA que confirma el cumplimiento>
PolicyQualifiers (Calificador de política)	
<i>cPSuri</i>	< http://www.procet.net.ve/dpc-pc >
Firma	
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha384WithECDSAEncryption)
Firma(signature)	<Contenido de la Firma>

Uso autorizado del certificado electrónico para Empleado de Institución Pública.

Uso	Uso mejorado
Firma electrónica, no repudio, acuerdo de claves y firma de correo.	Firma de documentos, Correo seguro

9.7.5. Certificado electrónico para Representante Legal de Empresa Privada: El uso asignado para este tipo de certificados es el siguiente:

- Certificar a una persona como representante legal de una entidad jurídica privada.
- Transacciones en línea públicas o privadas, en representación de una sociedad mercantil, civil u otra forma societaria.
- Comunicaciones privadas o públicas en representación de una sociedad mercantil, civil u otra forma societaria.
- Comercio electrónico en representación de una sociedad mercantil, civil u otra forma societaria.
- Declaraciones o trámites en línea ante gobierno en representación de una sociedad mercantil, civil u otra forma societaria.

Estructura del certificado electrónico de firma para Empleado de Empresa Privada.

Certificado Persona Empleado de Empresa privada	
Nombre (X.509)	<V3>
Datos del Certificado	
Versión (versión)	V3 (Número de versión del certificado).
Serial (Serial Number)	(Identificador único menor de 32 caracteres hexadecimales.)
Algoritmo de Firma (signatureAlgorithm)	Sha-384ECDSA
Datos de Emisor (issuer)	
Nombre Común (commonName)	PROCERT SMIME ECC CA
Organización (organizationName)	Proveedor de Certificados PROCERT ITFB
País (countryName)	VE

Datos de Validez	
No Antes (notBefore)	Fecha en que el periodo de validez del certificado comienza (UTC)
No Después (notAfter)	Fecha en que el periodo de validez del certificado culmina (UTC)
Datos de Titular (<i>subject</i>)	
Nombre Común (<i>commonName</i>)	<Nombre Completo>
Nombre (GivenName)	<Nombre>
Apellido (Surname)	<Apellido>
Nombre de la organización (<i>organizationName</i>)	<Contiene el nombre legal verificado del patrocinador>
Dirección de correo (<i>emailAdress</i>)	<La dirección de correo>
Título (title)	<Cargo que desempeña el titular del certificado>
Serial (<i>serialNumber</i>)	<El Número de Colegiado/Matrícula Profesional>
Localidad (<i>localityName</i>)	<Ciudad de ubicación del titular>
Identificador de la organización (<i>organizacionIdentifier</i>) 2.5.4.97	<Número de identificación fiscal del patrocinador>
Estado (<i>stateOrProvinceName</i>)	<Estado de ubicación del Titular>
País (<i>countryName</i>)	UTF8 [VE] (ISO 3166-1-alpha-2)
Información de Clave Pública del Titular (<i>subjectPublicKey</i>)	
Algoritmo de clave pública (<i>algorithm</i>)	ECC (384 Bits)
Parámetros de Clave Publica	ECDSA_P384
Extensiones	
Uso de la llave (<i>keyUsage</i>)	Firma digital, Sin repudio, Acuerdo de claves
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)	
Clave de Autoridad (<i>keyIdentifier</i>)	KeyIdentifier <Identificador de la clave pública de la AC>
Identificador de la clave del sujeto	
Clave de Autoridad (<i>keyIdentifier</i>)	KeyIdentifier <clave pública del propio certificado de la AC>
Nombre alternativo del sujeto (<i>subjectAlternativeName</i>)	
Formato de correo tradicional	<Dirección de correo electrónico>
Usos Extendidos de la Clave (<i>extKeyUsage</i>) (Requerido)	
Firma de documentos	Firma de documento (1.3.6.1.4.1.311.10.3.12)
Protección de correo	Correo seguro (1.3.6.1.5.5.7.3.4)
Acuerdo clave	KeyAgreement
Puntos de Distribución de las LCR (<i>cRLDistributionPoints</i>)	
Punto de distribución LCR (<i>distributionPoint</i>)	< http://www.procert.net.ve/ecc-crl/smime-ca.crl >
AIA (<i>authorityInfoAccess</i>) (Requerido)	

id-ad-ocsp	1.3.6.1.5.5.7.48.1< http://ocspsmime.procet.net.ve/ocsp >
id-ad-calssuers	1.3.6.1.5.5.7.48.2 < http://www.procet.net.ve/ecc-crt/smime-ca.crt >
Políticas de certificado (certificatePolicies)	
<i>policy identifier(s)</i>	<Indica la política de la CA que confirma el cumplimiento>
PolicyQualifiers (Calificador de política)	
<i>cPSuri</i>	< http://www.procet.net.ve/dpc-pc >
Firma	
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha384WithECDSAEncryption)
Firma(signature)	<Contenido de la Firma>

Uso autorizado del certificado electrónico de firma para Empleado de Empresa Privada .

Uso	Uso mejorado
Firma electrónica, no repudio, acuerdo de claves y firma de correo.	Firma de documentos, correo seguro

9.7.6. Certificado Electrónico de Banca Electrónica: El uso asignado al Certificado Electrónico de Banca Electrónica es el siguiente:

- Autenticación.
- Firma Electrónica.
- Protección de transacción en línea.
- Prueba legal del comprobante electrónico.
- Integridad de la Información.
- No repudio.

Estructura del Certificado Electrónico de Banca Electrónica.

Certificado para Banca Electrónica	
Nombre (X.509)	<V3>
Datos del Certificado	
Versión (versión)	V3 (Número de versión del certificado).
Serial (Serial Number)	(Identificador único menor de 32 caracteres hexadecimales.)
Algoritmo de Firma (signatureAlgorithm)	Sha-384ECDSA
Datos de Emisor (issuer)	
Nombre Común (commonName)	PROCERT SMIME ECC CA
Organización (organizationName)	Proveedor de Certificados PROCERT ITFB
País (countryName)	VE
Datos de Validez	
No Antes (notBefore)	Fecha en que el periodo de validez del

	certificado comienza (UTC)
No Después (notAfter)	Fecha en que el periodo de validez del certificado culmina (UTC)
Datos de Titular (<i>subject</i>)	
Nombre Común (<i>commonName</i>)	<Nombre Completo>
Nombre (<i>GivenName</i>)	<Nombre>
Apellido (<i>Surname</i>)	<Apellido>
Nombre de la organización (<i>organizationName</i>)	<Contiene el nombre legal verificado del patrocinador>
Dirección de correo (<i>emailAddress</i>)	<La dirección de correo>
Serial (<i>serialNumber</i>)	<Cedula de identidad o pasaporte>
Localidad (<i>localityName</i>)	<Ciudad de ubicación del patrocinador>
Identificador de la organización (<i>organizationIdentifier</i>) 2.5.4.97	<Número de identificación fiscal del patrocinador>
Estado (<i>stateOrProvinceName</i>)	<Estado de ubicación del Titular>
País (<i>countryName</i>)	UTF8 [VE] (ISO 3166-1-alpha-2)
Información de Clave Pública del Titular (<i>subjectPublicKey</i>)	
Algoritmo de clave pública (<i>algorithm</i>)	ECC (384 Bits)
Parámetros de Clave Publica	ECDSA_P384
Extensiones	
Uso de la llave (<i>keyUsage</i>)	Firma digital, Sin repudio, acuerdo de claves
Identificador de clave de Autoridad Certificadora (<i>Authority Key Identifier</i>)	
Clave de Autoridad (<i>keyIdentifier</i>)	KeyIdentifier <Identificador de la clave pública de la AC>
Identificador de la clave del sujeto	
Clave de Autoridad (<i>keyIdentifier</i>)	KeyIdentifier <clave pública del propio certificado de la AC>
Nombre alternativo del sujeto (<i>subjectAlternativeName</i>)	
Formato de correo tradicional	<Dirección de correo electrónico>
Usos Extendidos de la Clave (<i>extKeyUsage</i>) (Requerido)	
Firma de documentos	Firma de documento (1.3.6.1.4.1.311.10.3.12)
Protección de correo	Correo seguro (1.3.6.1.5.5.7.3.4)
Acuerdo clave	KeyAgreement
Puntos de Distribución de las LCR (<i>cRLDistributionPoints</i>)	
Punto de distribución LCR (<i>distributionPoint</i>)	< http://www.procert.net.ve/ecc-crl/smime-ca.crl >
AIA (<i>authorityInfoAccess</i>) (Requerido)	
id-ad-ocsp	1.3.6.1.5.5.7.48.1< http://ocspsmime.procert.net.ve/ocsp >

id-ad-calssuers	1.3.6.1.5.5.7.48.2 < http://www.procort.net.ve/ecc-crt/smime-ca.crt >
Políticas de certificado (certificatePolicies)	
policy identifier(s)	<Indica la política de la CA que confirma el cumplimiento>
PolicyQualifiers (Calificador de política)	
cPSuri	< http://www.procort.net.ve/dpc-pc >
Firma	
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha384WithECDSAEncryption)
Firma(signature)	<Contenido de la Firma>

Usos Autorizado del Certificado Electrónico de Banca Electrónica.

Uso	Uso mejorado
Firma electrónica, Autenticación, Integridad, acuerdo de claves y No Repudio.	Firma de Documentos y Firma de Correos

9.7.7. Estructura de Certificado Electrónico para Representante de Institución Pública: El uso asignado para este tipo de certificado es el siguiente:

- Transacciones en línea.
- Identificar en línea a empleados o trabajadores de empresas públicas.
- Comunicaciones electrónicas sin representación de empresas públicas o privadas.
- Confiere representación legal de empresas públicas.

Estructura del certificado electrónico para Representante de Institución Pública:

Certificado para Representante de Empresa Pública	
Nombre (X.509)	<V3>
Datos del Certificado	
Versión (versión)	V3 (Número de versión del certificado).
Serial (Serial Number)	(Identificador único menor de 32 caracteres hexadecimales.)
Algoritmo de Firma (signatureAlgorithm)	Sha-384ECDSA
Datos de Emisor (issuer)	
Nombre Común (commonName)	PROCERT SMIME ECC CA
Organización (organizationName)	Proveedor de Certificados PROCERT ITFB
País (countryName)	VE
Datos de Validez	
No Antes (notBefore)	Fecha en que el periodo de validez del certificado comienza (UTC)

No Después (notAfter)	Fecha en que el periodo de validez del certificado culmina (UTC)
Datos de Titular (<i>subject</i>)	
Nombre Común (<i>commonName</i>)	<Nombre Completo>
Nombre (GivenName)	<Nombre>
Apellido (Surname)	<Apellido>
Nombre de la organización (<i>organizationName</i>)	<Contiene el nombre legal verificado del patrocinador>
Dirección de correo (<i>emailAdress</i>)	<La dirección de correo>
Título (title)	<Cargo que desempeña el titular del certificado>
Serial (<i>serialNumber</i>)	<El Número de Colegiado/Matrícula Profesional>
Localidad (<i>localityName</i>)	<Ciudad de ubicación del titular>
Identificador de la organización (<i>organizationIdentifier</i>) 2.5.4.97	<Número de identificación fiscal del patrocinador>
Estado (<i>stateOrProvinceName</i>)	<Estado de ubicación del Titular>
País (<i>countryName</i>)	UTF8 [VE] (ISO 3166-1-alpha-2)
Información de Clave Pública del Titular (<i>subjectPublicKey</i>)	
Algoritmo de clave pública (<i>algorithm</i>)	ECC (384 Bits)
Parámetros de Clave Publica	ECDSA_P384
Extensiones	
Uso de la llave (<i>keyUsage</i>)	Firma digital, Sin repudio, acuerdo de claves
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)	
Clave de Autoridad (<i>keyIdentifier</i>)	KeyIdentifier <Identificador de la clave pública de la AC>
Identificador de la clave del sujeto	
Clave de Autoridad (<i>keyIdentifier</i>)	KeyIdentifier <clave pública del propio certificado de la AC>
Nombre alternativo del sujeto (<i>subjectAlternativeName</i>)	
Formato de correo tradicional	<Dirección de correo electrónico>
Usos Extendidos de la Clave (<i>extKeyUsage</i>) (Requerido)	
Firma de documentos	Firma de documento (1.3.6.1.4.1.311.10.3.12)
Protección de correo	Correo seguro (1.3.6.1.5.5.7.3.4)
Acuerdo clave	KeyAgreement
Puntos de Distribución de las LCR (<i>cRLDistributionPoints</i>)	
Punto de distribución LCR (<i>distributionPoint</i>)	< http://www.procert.net.ve/ecc-crl/smime-ca.crl >
AIA (<i>authorityInfoAccess</i>) (Requerido)	
id-ad-ocsp	1.3.6.1.5.5.7.48.1< http://ocspsmime.procert.net.ve/ocsp >

id-ad-calssuers	1.3.6.1.5.5.7.48.2 < http://www.procert.net.ve/ecc-crt/smime-ca.crt >
Políticas de certificado (certificatePolicies)	
policy identifier(s)	<Indica la política de la CA que confirma el cumplimiento>
PolicyQualifiers (Calificador de política)	
cPSuri	< http://www.procert.net.ve/dpc-pc >
Firma	
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha384WithECDSAEncryption)
Firma(signature)	<Contenido de la Firma>

Usos Autorizado del Estructura de Certificado para Representante de Institución Pública.

Uso	Uso mejorado
Firma electrónica, Autenticación, Integridad, acuerdo de calves y no Repudio.	Firma de documentos, correo seguro

9.7.8. Estructura de Certificado Electrónico para Funcionario Público: El uso asignado para este tipo de certificado es el siguiente:

- Certificar a una persona como funcionario público de carrera, de libre nombramiento o remoción o de elección popular y a que ente de gobierno se encuentra adscrito o pertenece.
- Transacciones en línea públicas o privadas, en representación a Entidades de Gobierno centralizado o descentralizado.
- Comunicaciones privadas o públicas en representación de Entidades de Gobierno centralizado o descentralizado.
- Comercio electrónico en representación de Entidades de Gobierno centralizado o descentralizado.
- Declaraciones o trámites en línea ante gobierno en representación de Entidades de Gobierno centralizado o descentralizado.
- Firma Electrónica de Correos Electrónicos y Documentos Electrónicos.

Estructura de Certificado Electrónico para Funcionario Público: El uso asignado para este tipo de certificado es el siguiente:

Certificado para funcionario público	
Nombre (X.509)	<V3 >
Datos del Certificado	
Versión (versión)	V3 (Número de versión del certificado).
Serial (Serial Number)	(Identificador único menor de 32 caracteres hexadecimales.)
Algoritmo de Firma (signatureAlgorithm)	Sha-384ECDSA
Datos de Emisor (issuer)	

Nombre Común (commonName)	PROCERT SMIME ECC CA
Organización (organizationName)	Proveedor de Certificados PROCERT ITFB
País (countryName)	VE
Datos de Validez	
No Antes (notBefore)	Fecha en que el periodo de validez del certificado comienza (UTC)
No Después (notAfter)	Fecha en que el periodo de validez del certificado culmina (UTC)
Datos de Titular (<i>subject</i>)	
Nombre Común (commonName)	<Nombre Completo>
Nombre (GivenName)	<Nombre del sujeto>
Apellido (Surname)	<Apellido del sujeto>
Nombre de la organización (organizationName)	<Contiene el nombre legal verificado del patrocinador>
Dirección de correo (emailAddress)	<La dirección de correo>
Título (title)	<Cargo que desempeña el titular del certificado>
Serial (<i>serialNumber</i>)	<Número de Cedula o Pasaporte>
Localidad (<i>localityName</i>)	<Ciudad de ubicación del titular>
Identificador de la organización (organizationIdentifier) 2.5.4.97	<Número de identificación fiscal del patrocinador>
Estado (<i>stateOrProvinceName</i>)	<Estado de ubicación del Titular>
País (<i>countryName</i>)	UTF8 [VE] (ISO 3166-1-alpha-2)
Información de Clave Pública del Titular (<i>subjectPublicKey</i>)	
Algoritmo de clave pública (algorithm)	ECC (384 Bits)
Parámetros de Clave Publica	ECDSA_P384
Extensiones	
Uso de la llave (keyUsage)	Firma digital, Sin repudio, acuerdo de claves
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)	
Clave de Autoridad (keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC>
Identificador de la clave del sujeto	
Clave de Autoridad (keyIdentifier)	KeyIdentifier <clave pública del propio certificado de la AC>
Nombre alternativo del sujeto (subjectAlternativeName)	
Formato de correo tradicional	<Dirección de correo electrónico>
Usos Extendidos de la Clave (extKeyUsage) (Requerido)	
Firma de documentos	Firma de documento (1.3.6.1.4.1.311.10.3.12)

Protección de correo	Correo seguro (1.3.6.1.5.5.7.3.4)
Acuerdo clave	KeyAgreement
Puntos de Distribución de las LCR (cRLDistributionPoints)	
Punto de distribución LCR (distributionPoint)	< http://www.procert.net.ve/ecc-crl/smime-ca.crl >
AIA (authorityInfoAccess) (Requerido)	
id-ad-ocsp	1.3.6.1.5.5.7.48.1< http://ocspsmime.procert.net.ve/ocsp >
id-ad-caIssuers	1.3.6.1.5.5.7.48.2 < http://www.procert.net.ve/ecc-crt/smime-ca.crt >
Políticas de certificado (certificatePolicies)	
policy identifier(s)	<Indica la política de la CA que confirma el cumplimiento>
PolicyQualifiers (Calificador de política)	
cPSuri	< http://www.procert.net.ve/dpc-pc >
Firma	
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha384WithECDSAEncryption)
Firma(signature)	<Contenido de la Firma>

Usos Autorizado del Estructura de Certificado para Representante de Institución Pública.

Uso	Uso mejorado
Firma electrónica, Autenticación, Integridad, acuerdo de claves y No Repudio.	Firma de Documentos y Firma de Correos

9.7.9. Certificado electrónico para Representante de Empresa Privada: El uso asignado para este tipo de certificado es el siguiente:

- Transacciones en línea.
- Identificar en línea a empleados o trabajadores de empresas públicas o privadas.
- Comunicaciones electrónicas sin representación de empresas públicas o privadas.
- Confiere representación legal de empresas públicas o privadas.

Estructura del certificado electrónico para Representante de Empresa Privada.

Certificado de Firma de Transacción	
Nombre (X.509)	<V3>
Datos del Certificado	
Versión (versión)	V3 (Número de versión del certificado).
Serial (Serial Number)	(Identificador único menor de 32 caracteres hexadecimales.)

Algoritmo de Firma (signatureAlgorithm)	Sha-384ECDSA
Datos de Emisor (<i>issuer</i>)	
Nombre Común (commonName)	PROCERT SMIME ECC CA
Organización (organizationName)	Proveedor de Certificados PROCERT ITFB
País (countryName)	VE
Datos de Validez	
No Antes (notBefore)	Fecha en que el periodo de validez del certificado comienza (UTC)
No Después (notAfter)	Fecha en que el periodo de validez del certificado culmina (UTC)
Datos de Titular (<i>subject</i>)	
Nombre Común (commonName)	<Nombre Completo>
Nombre (GivenName)	<Nombre del sujeto>
Apellido (Surname)	<Apellido del sujeto>
Nombre de la organización (organizationName)	<Contiene el nombre legal verificado del patrocinador>
Dirección de correo (emailAddress)	<La dirección de correo>
Título (title)	<Cargo que desempeña el titular del certificado>
Serial (<i>serialNumber</i>)	<El Número de Colegiado/Matrícula Profesional>
Localidad (<i>localityName</i>)	<Ciudad de ubicación del titular>
Identificador de la organización (organizationIdentifier) 2.5.4.97	<Número de identificación fiscal del patrocinador>
Estado (stateOrProvinceName)	<Estado de ubicación del Titular>
País (<i>countryName</i>)	UTF8 [VE] (ISO 3166-1-alpha-2)
Información de Clave Pública del Titular (<i>subjectPublicKey</i>)	
Algoritmo de clave pública (algorithm)	ECC (384 Bits)
Parámetros de Clave Pública	ECDSA_P384
Extensiones	
Uso de la llave (keyUsage)	Firma digital, Sin repudio, acuerdo de claves
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)	
Clave de Autoridad (keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC>
Identificador de la clave del sujeto	
Clave de	KeyIdentifier <clave pública del propio

Autoridad (<i>keyIdentifier</i>)	certificado de la AC>
Nombre alternativo del sujeto (subjectAlternativeName)	
Formato de correo tradicional	<Dirección de correo electrónico>
Usos Extendidos de la Clave (extKeyUsage) (Requerido)	
Firma de documentos	Firma de documento (1.3.6.1.4.1.311.10.3.12)
Protección de correo	Correo seguro (1.3.6.1.5.5.7.3.4)
Acuerdo clave	KeyAgreement
Puntos de Distribución de las LCR (cRLDistributionPoints)	
Punto de distribución LCR (<i>distributionPoint</i>)	< http://www.procert.net.ve/ecc-crl/smime-ca.crl >
AIA (authorityInfoAccess) (Requerido)	
id-ad-ocsp	1.3.6.1.5.5.7.48.1< http://ocspsmime.procert.net.ve/ocsp >
id-ad-calssuers	1.3.6.1.5.5.7.48.2 < http://www.procert.net.ve/ecc-crt/smime-ca.crt >
Políticas de certificado (certificatePolicies)	
<i>policy identifier(s)</i>	<Indica la política de la CA que confirma el cumplimiento>
PolicyQualifiers (Calificador de política)	
<i>cPSuri</i>	< http://www.procert.net.ve/dpc-pc >
Firma	
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha384WithECDSAEncryption)
Firma(signature)	<Contenido de la Firma>

Uso autorizado del certificado electrónico para Representante de Empresa Privada.

Uso	Uso mejorado
Firma electrónica, no repudio, acuerdo de claves y firma de correo.	Firma de documentos, Correo seguro

9.7.10. Certificado electrónico para Firma de Transacción: El uso asignado para este tipo de certificado es el siguiente:

- Protección de transacción en línea o fuera de conexión.
 - Prueba legal del registro de transacción.
 - Integridad de la Información.
 - No repudio.
 - Firma electrónica de archivos y documentos electrónicos.
- Estructura del certificado electrónico para firma de transacción.

Certificado de Firma de Transacción	
Nombre (X.509)	<V3>
Datos del Certificado	

Versión (versión)	V3 (Número de versión del certificado).
Serial (Serial Number)	(Identificador único menor de 32 caracteres hexadecimales.)
Algoritmo de Firma (signatureAlgorithm)	Sha-384ECDSA
Datos de Emisor (<i>issuer</i>)	
Nombre Común (commonName)	PROCERT SMIME ECC CA
Organización (organizationName)	Proveedor de Certificados PROCERT ITFB
País (countryName)	VE
Datos de Validez	
No Antes (notBefore)	Fecha en que el periodo de validez del certificado comienza (UTC)
No Después (notAfter)	Fecha en que el periodo de validez del certificado culmina (UTC)
Datos de Titular (<i>subject</i>)	
Nombre Común (commonName)	<Nombre Completo>
Nombre (GivenName)	<Nombre del sujeto>
Apellido (Surname)	<Apellido del sujeto>
Nombre de la organización (organizationName)	<Contiene el nombre legal verificado del patrocinador>
Dirección de correo (emailAddress)	<La dirección de correo>
Título (title)	<Cargo que desempeña el titular del certificado>
Serial (<i>serialNumber</i>)	<El Número de Colegiado/Matrícula Profesional>
Localidad (<i>localityName</i>)	<Ciudad de ubicación del titular>
Identificador de la organización (organizationIdentifier) 2.5.4.97	<Número de identificación fiscal del patrocinador>
Estado (<i>stateOrProvinceName</i>)	<Estado de ubicación del Titular>
País (<i>countryName</i>)	UTF8 [VE] (ISO 3166-1-alpha-2)
Información de Clave Pública del Titular (<i>subjectPublicKey</i>)	
Algoritmo de clave pública (algorithm)	ECC (384 Bits)
Parámetros de Clave Pública	ECDSA_P384
Extensiones	
Uso de la llave (keyUsage)	Firma digital, Sin repudio, acuerdo de claves
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)	
Clave de Autoridad	KeyIdentifier <Identificador de la clave pública de la AC>

(keyIdentifier)	
Identificador de la clave del sujeto	
Clave de Autoridad (keyIdentifier)	KeyIdentifier <clave pública del propio certificado de la AC>
Nombre alternativo del sujeto (subjectAlternativeName)	
Formato de correo tradicional	<Dirección de correo electrónico>
Usos Extendidos de la Clave (extKeyUsage) (Requerido)	
Firma de documentos	Firma de documento (1.3.6.1.4.1.311.10.3.12)
Protección de correo	Correo seguro (1.3.6.1.5.5.7.3.4)
Acuerdo clave	KeyAgreement
Puntos de Distribución de las LCR (cRLDistributionPoints)	
Punto de distribución LCR (distributionPoint)	< http://www.procert.net.ve/ecc-crl/smime-ca.crl >
AIA (authorityInfoAccess) (Requerido)	
id-ad-ocsp	1.3.6.1.5.5.7.48.1< http://ocspsmime.procert.net.ve/ocsp >
id-ad-caIssuers	1.3.6.1.5.5.7.48.2 < http://www.procert.net.ve/ecc-crt/smime-ca.crt >
Políticas de certificado (certificatePolicies)	
policy identifier(s)	<Indica la política de la CA que confirma el cumplimiento>
PolicyQualifiers (Calificador de política)	
cPSuri	< http://www.procert.net.ve/dpc-pc >
Firma	
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha384WithECDSAEncryption)
Firma(signature)	<Contenido de la Firma>

Uso autorizado del certificado para el control de transacción.

Uso	Uso mejorado
Firma electrónica, no repudio y acuerdo de claves	Firma de documentos

9.7.11. Certificado electrónico para firma de Factura Electrónica: El uso asignado al certificado de Certificado Electrónico de Factura Electrónica es el siguiente:

- Protección de transacción en línea.
- Prueba legal del comprobante electrónico.
- Integridad de la Información.
- No repudio
- Firma Electrónica de documentos electrónicos.

Estructura del certificado electrónico de Factura Electrónica.

Certificado de Firma de Factura	
Nombre (X.509)	<V3>
Datos del Certificado	
Versión (versión)	V3 (Número de versión del certificado).
Serial (Serial Number)	(Identificador único menor de 32 caracteres hexadecimales.)
Algoritmo de Firma (signatureAlgorithm)	Sha-384ECDSA
Datos de Emisor (issuer)	
Nombre Común (commonName)	PROCERT SMIME ECC CA
Organización (organizationName)	Proveedor de Certificados PROCERT ITFB
País (countryName)	VE
Datos de Validez	
No Antes (notBefore)	Fecha en que el periodo de validez del certificado comienza (UTC)
No Después (notAfter)	Fecha en que el periodo de validez del certificado culmina (UTC)
Datos de Titular (subject)	
Nombre Común (commonName)	<Nombre Completo>
Nombre (GivenName)	<Nombre del sujeto>
Apellido (Surname)	<Apellido del sujeto>
Nombre de la organización (organizationName)	<Contiene el nombre legal verificado del patrocinador>
Dirección de correo (emailAddress)	<La dirección de correo>
Título (title)	<Cargo que desempeña el titular del certificado>
Serial (serialNumber)	<El Número de Colegiado/Matrícula Profesional>
Localidad (localityName)	<Ciudad de ubicación del titular>
Identificador de la organización (organizationIdentifier) 2.5.4.97	<Número de identificación fiscal del patrocinador>
Estado (stateOrProvinceName)	<Estado de ubicación del Titular>
País (countryName)	UTF8 [VE] (ISO 3166-1-alpha-2)
Información de Clave Pública del Titular (subjectPublicKey)	
Algoritmo de clave pública (algorithm)	ECC (384 Bits)
Parámetros de Clave Pública	ECDSA_P384
Extensiones	
Uso de la llave (keyUsage)	Firma digital, Sin repudio, acuerdo de claves

Identificador de clave de Autoridad Certificadora (Authority Key Identifier)	
Clave de Autoridad (<i>keyIdentifier</i>)	KeyIdentifier <Identificador de la clave pública de la AC>
Identificador de la clave del sujeto	
Clave de Autoridad (<i>keyIdentifier</i>)	KeyIdentifier <clave pública del propio certificado de la AC>
Nombre alternativo del sujeto (subjectAlternativeName)	
Formato de correo tradicional	<Dirección de correo electrónico>
Usos Extendidos de la Clave (extKeyUsage) (Requerido)	
Firma de documentos	Firma de documento (1.3.6.1.4.1.311.10.3.12)
Protección de correo	Correo seguro (1.3.6.1.5.5.7.3.4)
Acuerdo clave	KeyAgreement
Puntos de Distribución de las LCR (cRLDistributionPoints)	
Punto de distribución LCR (<i>distributionPoint</i>)	< http://www.procert.net.ve/ecc-crl/smime-ca.crl >
AIA (authorityInfoAccess) (Requerido)	
id-ad-ocsp	1.3.6.1.5.5.7.48.1< http://ocspsmime.procert.net.ve/ocsp >
id-ad-caIssuers	1.3.6.1.5.5.7.48.2 < http://www.procert.net.ve/ecc-crt/smime-ca.crt >
Políticas de certificado (certificatePolicies)	
<i>policy identifier(s)</i>	<Indica la política de la CA que confirma el cumplimiento>
PolicyQualifiers (Calificador de política)	
<i>cPSuri</i>	< http://www.procert.net.ve/dpc-pc >
Firma	
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha384WithECDSAEncryption)
Firma(signature)	<Contenido de la Firma>

Uso autorizado del certificado electrónico de Factura Electrónica.

Uso	Uso mejorado
Firma electrónica, no repudio, acuerdo de claves	Firma de documentos

9.7.12. Certificado Electrónico para Comercio Electrónico: El uso asignado al Certificado Electrónico para Comercio Electrónico es el siguiente:

- Autenticación.
- Firma Electrónica.
- Protección de transacción en línea.
- Prueba legal del comprobante electrónico.

- Integridad de la Información.
- No repudio.

Estructura del Certificado Electrónico para Comercio Electrónico

Certificado para Comercio Electrónico	
Nombre (X.509)	<V3>
Datos del Certificado	
Versión (versión)	V3 (Número de versión del certificado).
Serial (Serial Number)	(Identificador único menor de 32 caracteres hexadecimales.)
Algoritmo de Firma (signatureAlgorithm)	Sha-384ECDSA
Datos de Emisor (issuer)	
Nombre Común (commonName)	PROCERT SMIME ECC CA
Organización (organizationName)	Proveedor de Certificados PROCERT ITFB
País (countryName)	VE
Datos de Validez	
No Antes (notBefore)	Fecha en que el periodo de validez del certificado comienza (UTC)
No Después (notAfter)	Fecha en que el periodo de validez del certificado culmina (UTC)
Datos de Titular (subject)	
Nombre Común (commonName)	<Nombre Completo>
Nombre (GivenName)	<Nombre>
Apellido (Surname)	<Apellido>
Nombre de la organización (organizationName)	<Contiene el nombre legal verificado del patrocinador>
Identificador de la organización (organizationIdentifier) 2.5.4.97	<Debe contener el identificador legal único del patrocinador ej. Nombre de registro de información fiscal (RIF)>
Nombre de la unidad organizativa (organizationalUnitName)	<Unidad o departamento del patrocinador al que pertenece el individuo>
Dirección de correo (emailAddress)	<La dirección de correo>
Título (title)	<Cargo que desempeña el titular del certificado>
Serial (serialNumber)	<Cedula de identidad o pasaporte>
Estado (stateOrProvinceName)	<Estado de ubicación del Titular>
Localidad (localityName)	<Ciudad de ubicación del patrocinador>
País (countryName)	UTF8 [VE] (ISO 3166-1-alpha-2)
Información de Clave Pública del Titular (subjectPublicKey)	
Algoritmo de clave pública (algorithm)	ECC (384 Bits)

Parámetros de Clave Publica	ECDSA_P384
Extensiones	
Uso de la llave (keyUsage)	Firma digital, Sin repudio
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)	
Clave de Autoridad (keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC>
Identificador de la clave del sujeto	
Clave de Autoridad (keyIdentifier)	KeyIdentifier <clave pública del propio certificado de la AC>
Nombre alternativo del sujeto (subjectAlternativeName)	
Formato de correo tradicional	<Dirección de correo electrónico>
Usos Extendidos de la Clave (extKeyUsage) (Requerido)	
Firma de documentos	Firma de documento (1.3.6.1.4.1.311.10.3.12)
Protección de correo	Correo seguro (1.3.6.1.5.5.7.3.4)
Acuerdo clave	KeyAgreement
Puntos de Distribución de las LCR (cRLDistributionPoints)	
Punto de distribución LCR (distributionPoint)	< http://www.procert.net.ve/ecc-crl/smime-ca.crl >
AIA (authorityInfoAccess) (Requerido)	
id-ad-ocsp	1.3.6.1.5.5.7.48.1< http://ocspsmime.procert.net.ve/ocsp >
id-ad-calssuers	1.3.6.1.5.5.7.48.2 < http://www.procert.net.ve/ecc-crt/smime-ca.crt >
Políticas de certificado (certificatePolicies)	
policy identifier(s)	<Indica la política de la CA que confirma el cumplimiento>
PolicyQualifiers (Calificador de política)	
cPSuri	< http://www.procert.net.ve/dpc-pc >
Firma	
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo sha384WithECDSAEncryption)
Firma(signature)	<Contenido de la Firma>

Uso autorizado del certificado electrónico de Factura Electrónica.

Uso	Uso mejorado
Firma electrónica, no repudio, acuerdo de claves	Firma de documentos

- 9.8. Terceros de buena fe: Los terceros de buena fe, son personas o entidades jurídicas que confían en una firma electrónica, certificado electrónico, lista de certificados revocados o información generada por el PSC PROCERT y sobre las cuales pueden depositar su confianza de acuerdo con el presente documento de la DPC y la PC.

La ICP del PSC PROCERT, está contractualmente obligada, directa o indirectamente (mediante cadena de contratos) con todos los clientes, proveedores y/o parte interesada usuarios de firmas y certificados electrónicos generados por el PSC PROCERT. Para poder pertenecer a una comunidad tan cerrada y depositar su confianza en sus servicios, se requiere del consentimiento de los clientes (terceros de buena Fe), a las condiciones del contrato de adquisición de firmas o certificados electrónicos generados por el PSC PROCERT.

10. Usos de los certificados.

10.1. Usos permitidos: El uso del certificado subordinado del PSC PROCERT estará limitado a la firma de certificados electrónicos para autoridades subordinadas, firma de las listas de certificados revocados y la firma de todos los certificados establecidos en el presente documento. El uso de los certificados electrónicos emitidos por el PSC PROCERT estará limitado según el tipo de certificado y fue descrito de forma precedente.

10.2. Usos no permitidos: El cliente contratante de firmas electrónicas o certificados electrónicos generados por el PSC PROCERT se obliga a utilizarlos conforme a los usos permitidos y señalados en la sección anterior y los establecidos por el decreto con fuerza de ley sobre mensajes de datos y firmas electrónicas, sus reglamentos y otras normas de carácter sublegal vigentes o cualquier texto normativo que los sustituya y regule la actividad de certificación electrónica dentro de la República Bolivariana de Venezuela y para el uso para el cual fue adquirido, quedando expresamente indicado que cualquier violación a las normas, usos y/o leyes de la República Bolivariana de Venezuela queda bajo la responsabilidad del cliente contratante, así como los daños y perjuicios que ocasionare y en un todo le será aplicable las previsiones que al efecto estén contenidas en la ley de ilícitos informáticos y supletoriamente el código penal y procesal penal venezolano. El certificado electrónico cuyo signatario viole el uso autorizado, será revocado. Adicionalmente el cliente contratante asume la responsabilidad de indemnizar al PSC PROCERT por daños y perjuicios ocasionados a terceros derivados de reclamos, acciones, efectos de acción, pérdidas o daños (incluyendo multas legales) que se generaren por el uso indebido del servicio contratado.

11. Política de administración de la AC: Es política y obligación del PSC PROCERT mantener, documentar e informar a los clientes acerca de generación de certificados electrónicos, a los efectos de educar e informar a los clientes de certificados electrónicos acerca de los usos, aplicaciones, responsabilidades y obligaciones del PSC PROCERT, ciclo de vida de certificados e información de interés asociadas a los mismos, la cual permita prevenir potenciales acciones fraudulentas derivadas de certificados falsos emitidos por entes no acreditados y establecer las condiciones requeridas para aplicar el modelo de confianza, respecto a los certificados electrónicos emitidos por el PSC PROCERT.

11.1. Especificaciones de la organización administrativa: El PSC PROCERT se encuentra organizado como administrativa y técnica de la siguiente manera:

- Gerencia General a la cual reportan:
- El consultor de tecnología.

- El Consultor de la PKI
- El consultor de seguridad de la información y cumplimiento.
- El Auditor
- Los operadores de informática.
- La AR.
- El personal de administración.
- Los servicios tercerizados.

11.1.1. Detalle de la organización administrativa: A continuación, se lista el detalle de las funciones de las distintas unidades que conforman la organización administrativa del PSC PROCERT.

11.1.1.1. Gerente general: El PSC PROCERT mantiene dentro de su diseño el cargo de Gerente General, el cual se constituye en una posición gerencial encargada de la gestión, administración y supervisión de las actividades de la AC y de la AR, manteniendo en todo momento el control de la gestión administrativa, operacional y del recurso humano. La posición de gerente general puede ser ocupada por un administrador de empresa, un ingeniero de procesos, un abogado o un economista o un representante de la alta dirección y reporta directamente a la alta dirección del PSC PROCERT.

11.1.1.1.1. Responsabilidades del gerente general.

- Asegurar el cumplimiento de las políticas de empresa en materia de informática, administración y recursos humanos.
- Mantener y actualizar los estándares de tecnología aplicables al área de registro.
- Mantener una balanza de gestión positiva, la cual emita un ejercicio orientado a la economía y cumplimiento del retorno esperado y planeado en el plan de negocios de la AC PROCERT.
- Elaborar y someter a la aprobación de la alta dirección el presupuesto anual de operación de la autoridad de registro.
- Dar cumplimiento a la normativa laboral y demás leyes de corte social que regulen la relación entre la AR de PROCERT y sus trabajadores.
- Mantener las relaciones y comunicaciones institucionales y de operación de la Autoridad de Registro con SUSCERTE.
- Cumplir y hacer cumplir al personal la AR PROCERT, las normas legales aplicables a la materia de certificación electrónica y el marco legal aplicable a la gestión regular de la AC y la AR.

- Garantizar la prestación de servicios bajo cumplimiento de los más altos estándares de calidad, seguridad, oportunidad, rentabilidad, ética y eficacia orientada al logro y satisfacción del cliente, sobre la base de principios de seguridad y tecnología establecidos por el marco legal y la empresa.
- Ejercer la representación de la empresa en todas sus instancias ante entes de gubernamentales y de los distintos niveles de gobierno, órganos judiciales y administrativos, representantes de los sectores productivos público y privados, sociedades regulares con o sin personalidad jurídica y sujetos de derecho particulares que realizan actividades comerciales y lícitas dentro y fuera de la República Bolivariana de Venezuela.
- Ejercer las funciones disciplinarias aplicables al personal de la AR y AC de PROCERT.
- Aprobar la contratación de obras y servicios, personal, bienes de consumo e instrumentos financieros.
- Cumplir y hacer cumplir las obligaciones tributarias que imponga el marco legal aplicable dentro de la República Bolivariana de Venezuela.
- Planificar e implantar la gestión de mercadeo y publicidad de la AR y AC de PROCERT.
- Planificar y establecer el plan de desarrollo y adiestramiento aplicable al personal de la AR y AC de PROCERT.
- Planificar y establecer el plan de remuneración aplicable al personal de la AR y AC de PROCERT.
- Cumplir y hacer cumplir los lineamientos y obligaciones impuesta por la Ley Orgánica de Prevención, Condiciones y Medio Ambiente de Trabajo (LOPCYMAT).
- Mantener actualizados y vigentes los lineamientos y controles de gestión aplicables a la operación regular de AR y AC de PROCERT.
- Fomentar y diseñar iniciativas de nuevos negocios que fomenten y propicien el uso de nuevas tecnologías.
- Fomentar, propiciar y consolidar asociaciones estratégicas con otras AR y AC, a los efectos de establecer el reconocimiento cruzado de los datos que soportan los certificados electrónicos entre distinto entes o AC.

- Aprobar los pagos y solicitudes para proveedores.
- Cumplir las directrices de la Alta Dirección del PSC PROCERT.
- Manejar y Administrar el esquema de servicios en nube.
- Ejecutar las actividades inherentes a AC.

11.1.1.2. Consultor de tecnología: El PSC PROCERT mantiene dentro de su diseño organizacional una posición de consultoría en el área de tecnología, la cual entre sus principales funciones tiene la de gestión, administración y supervisión del grupo de operaciones tecnología de información y recabar información acerca de los últimos avances tecnológicos en materia de certificación electrónica e informática. La posición del consultor de tecnología puede ser ocupada por un ingeniero de sistemas o un ingeniero en computación, y reportará directamente al gerente general. Para desempeñar el cargo de Consultor de Tecnología, el titular deberá contar con experiencia profesional comprobada de al menos tres (3) años, ser venezolano, de comprobada solvencia moral y económica.

11.1.1.2.1. Responsabilidades del consultor de tecnología.

- Planificar, coordinar y administrar la infraestructura tecnológica del personal asignado al departamento de operaciones conforme a los lineamientos estratégicos del PSC PROCERT, a fin de obtener el mayor aprovechamiento de los recursos tecnológicos y proveer soluciones de sistemas de información que la organización requiere, garantizando un servicio oportuno con seguridad, calidad y administración óptima de los recursos.
- Garantizar un óptimo funcionamiento de la plataforma tecnológica que apoya a la AC y a la AR del PSC PROCERT a través del establecimiento de una infraestructura de informática actualizada, eficiente y económicamente sustentable.
- Asegurar la disponibilidad y resguardo de la data, de forma que se pueda cumplir con las exigencias legales y los requerimientos impuestos por la SUSCERTE.
- Proveer información confiable y segura a la alta dirección de la empresa y gerente general,

acerca de las tendencias y mejores prácticas en materia de recursos informáticos y con el fin de facilitar la toma de decisiones de dichos niveles y servir de apoyo para las mismas.

- Identificar y proponer mejoras aplicables a la AC y la AR a través del uso de la tecnología informática disponible en el PSC PROCERT y en el mercado, contribuyendo a la satisfacción de los clientes internos y externos.
- Procurar altos rendimientos de la herramienta informática, garantizando operación confiable y de calidad que redunde en una excelente calidad de servicio y produzca mayores ingresos a la empresa.
- Garantizar al cliente un servicio con los más altos estándares de calidad, seguridad, oportunidad, rentabilidad, ética y eficacia orientada al logro y satisfacción del cliente, sobre la base de principios de seguridad y tecnología establecidos por el marco legal y la empresa.
- Asegurar el cumplimiento de las políticas de empresa en materia de informática, administración y recursos humanos.
- Mantener y actualizar los estándares de tecnología aplicables al área de registro.
- Junto a la Gerencia General, dar cumplimiento a la normativa laboral y demás leyes de corte social que regulen la relación entre la AC y la AR del PSC PROCERT y sus trabajadores.
- Junto a la Gerencia General, cumplir y hacer cumplir al personal de Operaciones de PROCERT, las normas legales aplicables a la materia de certificación electrónica y el marco legal aplicable a la gestión regular de la AC.
- Cumplir y hacer cumplir las obligaciones tributarias que imponga el Marco legal aplicable dentro de la República Bolivariana de Venezuela.
- Cumplir las políticas de empresa en materia de informática, administración y recursos humanos.
- Mantener actualizados y vigentes los lineamientos y controles de gestión aplicables a la operación regular de la AR PROCERT.
- Cumplir los lineamientos y controles de gestión aplicables a la operación regular del PSC PROCERT.
- Cumplir las directrices de la alta dirección y del gerente general del PSC PROCERT.

- Cumplir con las funciones asignadas por el Comité de Seguridad.

•

11.1.1.3. Consultor de la PKI: El PSC PROCERT mantiene dentro de su diseño organizacional una posición de consultoría en el área de la PKI, la cual entre sus principales funciones tiene la de gestión, administración y supervisión de las actividades del grupo de operaciones de la Autoridad de Certificación (AC) y recabar información acerca de los últimos avances tecnológicos en materia de certificación electrónica e informática. La posición del consultor de la PKI puede ser ocupada por un ingeniero de sistemas o un ingeniero en computación, y reportará directamente al gerente general. Para desempeñar el cargo de Consultor de la PKI, el titular deberá contar con experiencia profesional comprobada de al menos tres (3) años, ser venezolano, de comprobada solvencia moral y económica.

11.1.1.3.1. Responsabilidad del Consultor de la PKI:

- Planificar, coordinar y administrar la infraestructura tecnológica del personal asignado al grupo de operaciones de la AC conforme a los lineamientos estratégicos del PSC PROCERT, a fin de obtener el mayor aprovechamiento de los recursos tecnológicos y proveer soluciones de sistemas de información que la organización requiere, garantizando un servicio oportuno con seguridad, calidad y administración óptima de los recursos.
- Garantizar un óptimo funcionamiento de la plataforma tecnológica que apoya a la AC y AR del PSC PROCERT a través del establecimiento de una infraestructura de informática actualizada, eficiente y económicamente sustentable.
- Asegurar la disponibilidad y resguardo de la data, de forma que se pueda cumplir con las exigencias legales y los requerimientos impuestos por la SUSCERTE.
- Proveer información confiable y segura a la alta dirección de la empresa y gerente general, acerca de las tendencias y mejores prácticas en materia de recursos informáticos y con el fin de facilitar la toma de decisiones de dichos niveles y servir de apoyo para las mismas.
- Identificar y proponer mejoras aplicables a la AC y AR a través del uso de la tecnología informática disponible en el PSC PROCERT y

en el mercado, contribuyendo a la satisfacción de los clientes internos y externos.

- Procurar altos rendimientos de la herramienta informática, garantizando operación confiable y de calidad que redunde en una excelente calidad de servicio y produzca mayores ingresos a la empresa.
- Garantizar al cliente un servicio con los más altos estándares de calidad, seguridad, oportunidad, rentabilidad, ética y eficacia orientada al logro y satisfacción del cliente, sobre la base de principios de seguridad y tecnología establecidos por el marco legal y la empresa.
- Asegurar el cumplimiento de las políticas de empresa en materia de informática, administración y recursos humanos.
- Mantener y actualizar los estándares de tecnología aplicables al área de registro.
- Junto a la Gerencia General, dar cumplimiento a la normativa laboral y demás leyes de corte social que regulen la relación entre la AC y AR del PSC PROCERT y sus trabajadores.
- Junto a la Gerencia General, cumplir y hacer cumplir al personal la AC y AR de PROCERT, las normas legales aplicables a la materia de certificación electrónica y el marco legal aplicable a la gestión regular de la AC.
- Cumplir y hacer cumplir las obligaciones tributarias que imponga el Marco legal aplicable dentro de la República Bolivariana de Venezuela.
- Cumplir las políticas de empresa en materia de informática, administración y recursos humanos.
- Mantener actualizados y vigentes los lineamientos y controles de gestión aplicables a la operación regular de la AC y AR PROCERT.
- Cumplir los lineamientos y controles de gestión aplicables a la operación regular del PSC PROCERT.
- Cumplir las directrices de la alta dirección y del gerente general del PSC PROCERT.

11.1.1.4. Consultor de Seguridad de la Información y Cumplimiento: El PSC PROCERT mantiene dentro de su diseño el cargo de Consultor de Seguridad de la Información y Cumplimiento el cual se constituye en una posición encargada de velar por el cumplimiento y establecimiento de las mejores prácticas en materia de seguridad de la información, y cumplimiento del estándar nacional e internacional aplicable a la operación de la AC. La posición de Consultor de Seguridad de la Información y Cumplimiento puede ser ocupada por un Ingeniero de Sistemas, un Ingeniero en Computación o un Técnico Superior en Informática capacitado en la materia, y reportará directamente al Gerente General.

11.1.1.4.1. Responsabilidades del Consultor de Seguridad de la Información y Cumplimiento.

- Planificar, coordinar y establecer el cumplimiento de las mejores prácticas en materia de seguridad de la información, conforme a los lineamientos estratégicos del PSC PROCERT, a fin de obtener el mayor aprovechamiento de los recursos tecnológicos y proveer soluciones de sistemas de información que la organización requiere, garantizando un servicio oportuno con seguridad, calidad y administración óptima de los recursos.
- Asegurar la disponibilidad y resguardo de la data, de forma que se pueda cumplir con las exigencias legales y los requerimientos impuestos por la SUSCERTE.
- Proveer información confiable y segura a la alta dirección de la empresa y gerente general, acerca de las tendencias y mejores prácticas en materia de recursos informáticos y con el fin de facilitar la toma de decisiones de dichos niveles y servir de apoyo para las mismas.
- Identificar y proponer mejoras aplicables en materia de seguridad de información y cumplimiento de normas y estándares aplicables a la AC y AR a través del uso de la tecnología informática disponible en el mercado, contribuyendo a la satisfacción de los clientes internos y externos.
- Procurar altos rendimientos de la herramienta informática, garantizando operación confiable, segura y de calidad que redunde en una excelente calidad de servicio y produzca mayores ingresos a la empresa.
- Garantizar al cliente un servicio con los más altos estándares de calidad, seguridad,

oportunidad, rentabilidad, ética y eficacia orientada al logro y satisfacción del cliente, sobre la base de principios de seguridad y tecnología establecidos por el marco legal y la empresa.

- Asegurar el cumplimiento de las políticas de empresa en materia de seguridad informática, administración de normas y estándares internacionales y cumplimiento de los mismos.
- Mantener y actualizar los estándares de tecnología aplicables a la AC y AR.
- Junto a la gerencia general, dar cumplimiento a la normativa de seguridad de la información y cumplimiento normativo.
- Junto a la gerencia general, cumplir y hacer cumplir al personal del PSC PROCERT las normas legales, estándares y principios de seguridad de la información.
- Junto a la gerencia general planificar la capacitación del personal en materia de seguridad de la información y cumplimiento normativo.
- Cumplir y hacer cumplir los lineamientos y obligaciones impuesta por las normas, estándares y legislación nacional e internacional que regule la operación del PSC PROCERT.
- Mantener actualizados y vigentes los lineamientos y controles de gestión aplicables a la operación regular de la AC.
- Cumplir las directrices de la alta dirección y del gerente general del PSC PROCERT.
- Monitorear el esquema de servicios en nube.
- Ejecutar las actividades inherentes al cargo.

11.1.1.5. Encargado de la AR: El PSC PROCERT mantiene dentro de su diseño organizacional un responsable de la validación de los datos y acreditación de identidad de los signatarios. La posición puede ser ocupada por un Licenciado en administrador, contador público o abogado y reportará directamente al gerente general de la AC del PSC PROCERT.

11.1.1.5.1. Responsabilidades del encargado de la AR.

- Verificar que los signatarios envíen toda la documentación necesaria según el tipo de certificado electrónico que deseen adquirir.
- Validar que la información entregada por el signatario sea correcta.

- Acreditar a todos aquellos signatarios que cumplan con los requisitos establecidos por el PSC PROCERT.
- Identificar y proponer mejoras en el proceso de acreditación, con el fin de facilitar el proceso de acreditación de los signatarios.
- Cumplir las políticas de empresa en materia de informática, administración y recursos humanos.
- Cumplir la normativa laboral y demás leyes de corte social que regulen la relación entre el PSC PROCERT sus trabajadores.
- Cumplir las normas legales aplicables a la materia de certificación electrónica y el marco legal aplicable a la gestión regular del PSC PROCERT.
- Cumplir los lineamientos y obligaciones impuesta por la Ley Orgánica de Prevención, Condiciones y Medio Ambiente de Trabajo (LOPCYMAT). Cumplir los lineamientos y controles de gestión aplicables a la operación regular del PSC PROCERT.
- Cumplir las directrices de la alta dirección y del gerente general del PSC PROCERT.
- Crear en sistema a los usuarios cuya documentación e identidad sean comprobadas.

11.1.1.6. Auditores: El PSC PROCERT contempla el proceso de auditoría interna dentro de sus procesos y a los fines de garantizar el cumplimiento oportuno de los estándares, normas, legislación y políticas internas que regulan la operación del PSC PROCERT. La Posición de Auditor debe ser ocupada por un ingeniero en sistemas o técnico superior en informática y reportará directamente al gerente general.

11.1.1.6.1. Responsabilidades del Auditor.

- Verificar que los procesos internos y resultados de auditorías externas sean cumplidos y ejecutados.
- Identificar y proponer mejoras en los procesos internos del PSC PROCERT.
- Cumplir las políticas de empresa en materia de informática, administración y recursos humanos.
- Cumplir la normativa laboral y demás leyes de corte social que regulen la relación entre el PSC PROCERT sus trabajadores.
- Cumplir las normas legales aplicables a la materia de certificación electrónica y el marco

legal aplicable a la gestión regular del PSC PROCERT.

- Cumplir los lineamientos y obligaciones impuesta por la Ley Orgánica de Prevención, Condiciones y Medio Ambiente de Trabajo (LOPCYMAT). Cumplir los lineamientos y controles de gestión aplicables a la operación regular del PSC PROCERT.
- Cumplir las directrices de la alta dirección y del gerente general del PSC PROCERT.

11.1.1.7. Operadores de informática: El PSC PROCERT mantiene dentro de su diseño organizacional un grupo de trabajo conformado por los operadores de informática los cuales pueden ser asignados a la gestión y operación de la AR y AC del PSC PROCERT. Los operadores de informática mantienen el control y monitoreo de los datos de la autoridad de certificación (AC). La posición de operador de informática debe ser ocupada por un ingeniero en sistemas o técnico superior en informática y reportará directamente al consultor de tecnología y gerente general.

11.1.1.7.1. Responsabilidades de los operadores de informática.

- Operar la infraestructura de la AC. a fin de obtener el mayor aprovechamiento de los recursos tecnológicos y proveer soluciones de sistemas de información que la organización requiere, garantizando un servicio oportuno con seguridad, calidad y administración óptima de los recursos.
- Apoyar al consultor de tecnología con el fin de garantizar un óptimo funcionamiento de la AC. a través del establecimiento de una infraestructura de informática actualizada, eficiente y económicamente sustentable.
- Apoyar al consultor de tecnología con el fin de asegurar la disponibilidad y resguardo de la data, de forma que se pueda cumplir con las exigencias legales y los requerimientos impuestos por la SUSCERTE.
- Proveer información confiable y segura al consultor de tecnología, gerente general y alta gerencia acerca de las tendencias y mejores prácticas en materia de registro de data, recursos informáticos y con el fin de facilitar la toma de decisiones de dichos niveles y servir de apoyo para las mismas.
- Identificar y proponer mejoras aplicables a la AC a través del uso de la tecnología informática

disponible en el mercado, contribuyendo a la satisfacción de los clientes internos y externos.

- Procurar altos rendimientos de la herramienta informática, garantizando operación confiable y de calidad que redunde en una excelente calidad de servicio y produzca mayores ingresos a la empresa.
- Garantizar al cliente un servicio con los más altos estándares de calidad, seguridad, oportunidad, rentabilidad, ética y eficacia orientada al logro y satisfacción del cliente, sobre la base de principios de seguridad y tecnología establecidos por el marco legal y la empresa.
- Cumplir las políticas de empresa en materia de informática, administración y recursos humanos.
- Cumplir y ayudar al consultor de tecnología y gerente general a mantener actualizados los estándares de tecnología aplicables al área de registro de identidad.
- Cumplir la normativa laboral y demás leyes de corte social que regulen la relación entre la AC y sus trabajadores
- Cumplir las normas legales aplicables a la materia de certificación electrónica y el marco legal aplicable a la gestión regular de la AC.
- Cumplir los lineamientos y obligaciones impuesta por la Ley Orgánica de Prevención, Condiciones y Medio Ambiente de Trabajo (LOPCYMAT).
- Cumplir los lineamientos y controles de gestión aplicables a la operación regular de la AR y AC.
- Apoyar al consultor de tecnología y gerente general en el fomento y desarrollo de iniciativas de nuevos negocios que fomenten y propicien el uso de nuevas tecnologías.
- Cumplir las directrices de la alta dirección, del gerente general y del consultor de tecnología.
- Por delegación del consultor de tecnología o gerente general y solo en caso de contingencia, apoyar al encargado de la autoridad de registro en la creación del archivo electrónico correspondiente a la documentación entregada por los clientes.

11.1.1.8. Asistente administrativo: El PSC PROCERT mantiene dentro de su diseño organizacional un cargo de asistente administrativo el cual se encuentra encargado de asistir a la gerencia general en la gestión administrativa regular del PSC PROCERT. El asistente administrativo es el encargado de la gestión de trámites de pagos de productos y servicios requeridos por el PSC PROCERT y mantener actualizada la gestión ante clientes y proveedores. La posición de asistente administrativo debe ser ocupada por un técnico superior en administración o mercadeo y comercialización, y reportará directamente al gerente.

11.1.1.8.1. Descripción de las responsabilidades.

- Cumplir las políticas de empresa en materia de informática, administración y recursos humanos.
- Cumplir la normativa laboral y demás leyes de corte social que regulen la relación entre el PSC PROCERT y sus trabajadores
- Cumplir las normas legales aplicables a la materia de registro de identidad y el marco legal aplicable a la gestión regular del PSC PROCERT.
- Garantizar la prestación de servicios bajo cumplimiento de los más altos estándares de calidad, seguridad, oportunidad, rentabilidad, ética y eficacia orientada al logro y satisfacción del cliente, sobre la base de principios de seguridad y tecnología establecidos por el marco legal y la empresa.
- Tramitar los pagos y solicitudes para proveedores.
- Cumplir y hacer cumplir las obligaciones tributarias que imponga el marco legal aplicable dentro de la República Bolivariana de Venezuela.
- Apoyar a la Gerencia General en la gestión de publicidad del PSC PROCERT.
- Cumplir los lineamientos y obligaciones impuesta por la Ley Orgánica de Prevención, Condiciones y Medio Ambiente de Trabajo (LOPCYMAT).
- Cumplir los lineamientos y controles de gestión aplicables a la operación regular del PSC PROCERT.
- Cumplir las directrices de la alta dirección de la autoridad y del gerente general del PSC PROCERT.

- 11.2. Persona contacto: El presente documento de la DPC y la PC, es administrado por la alta dirección y gerente general del PSC PROCERT. Las preguntas u otras comunicaciones sobre este documento y respecto a la operación y generación de los certificados del PSC PROCERT, deben dirigirse a: Proveedor de Certificados PROCERT ITFB, C.A. Multicentro Empresarial del Este, Núcleo B, Torre Libertador, Pío 13, Oficina B-132, Municipio Chacao, Caracas. E-mail: contacto@procert.net.ve, Código Postal 1063, Teléfono máster: +58-0212-2674880, Fax: +58-0212-2671270.
- 11.3. Competencia para determinar la adecuación de la DPC a las políticas: La Alta Dirección del PSC PROCERT es la encargada de validar y conformar la adecuación de la DPC a las distintas políticas de operación y certificación requeridas para la operación de un PSC. En todo caso, la validación efectuada por la alta dirección del PSC PROCERT, respecto a la adecuación de la DPC a las distintas políticas de operación y generación de certificados será sometida a la revisión y aprobación por parte de la SUSCERTE.
12. Publicación de información del PSC y repositorios de los certificados.
- 12.1. Repositorios: A fin de garantizar la completa disponibilidad de este documento de la DPC y la PC, y demás documentos esenciales, el PSC PROCERT mantiene un repositorio dentro de su Página Web: <http://www.procert.net.ve/>.
- Para el certificado de la AC Subordinada PROCERT, los certificados emitidos por dicha AC y la DPC:
<https://www.procert.net.ve/Internas/AC.aspx>
 - Para la lista de Certificados Revocados
 - <http://www.procert.net.ve/ecc-crl/smime-ca.crl>
 - Para el servicio de validación en línea (OCSP)
 - ocspsmime.procert.net.ve/ocsp El repositorio público del PSC PROCERT, no contiene ninguna información confidencial o privada.
- 12.2. Publicación: Es obligación para el PSC PROCERT publicar la información relativa a sus prácticas, sus certificados y el estado actualizado de dichos certificados. Las publicaciones que realice el PSC PROCERT, de toda la información clasificada como pública, se anunciara en su respectiva página web de la siguiente forma:
- La lista de certificados revocados (LCR), se encuentra disponible en formato CRL V2, en <http://www.procert.net.ve/ecc-crl/smime-ca.crl>
 - El presente documento se encuentra disponible en: <https://www.procert.net.ve/Internas/AC.aspx>
 - El certificado de la AC Subordinada PROCERT se encuentra disponible en: <https://www.procert.net.ve/Internas/AC.aspx>
 - Los certificados emitidos por la AC Subordinada PROCERT se encuentran en: <https://www.procert.net.ve/Internas/AC.aspx>
 - Los datos de contacto del PSC PROCERT en la dirección: <https://www.procert.net.ve/#contacto> [Procert](https://www.procert.net.ve/#contacto)
 - La documentación técnica del PSC PROCERT en la dirección: <https://www.procert.net.ve/Internas/AC.aspx>

12.3. Frecuencia de publicación.

- Certificados del PSC: La publicación del certificado se realizará una vez obtenida la acreditación por parte de la SUSCERTE. El periodo de validez es de diez años.
- Lista de certificados revocados (LCR): La publicación de la lista de certificados revocados se realizará cada 24 horas
- Declaración de prácticas de certificación: A menos que explícitamente se indique lo contrario en este documento de la PC y DPC, se publicarán en el sitio web del PCS PROCERT (www.procert.net.ve), las nuevas versiones de este documento, una vez las mismas sean aprobadas por la alta dirección del PSC PROCERT y la SUSCERTE.

13. Controles de acceso al repositorio de certificados: El acceso a la información publicada por el PSC PROCERT será de consulta y no podrá ser modificada por personas no autorizadas. La información pública solo será actualizada por el personal encargado de esa función que labora en el PSC PROCERT. Además, se garantiza la consulta a la LCR a los certificados emitidos, al servidor OCSP y el presente documento.

14. Identificación y autenticación.

14.1. Tipos de nombres: El PSC PROCERT solo genera y firma certificados de nombres acordes al estándar x 500. Para el PSC PROCERT: El nombre distintivo (DN) del PSC PROCERT está formado por los siguientes atributos:

- CN: PSCPROCERT
- O: Sistema Nacional de Certificación Electrónica.
- OU: Proveedor de Certificados PROCERT
- C: VE.
- E: contacto@procert.net.ve
- L: Chacao
- S: Miranda

El nombre alternativo (AN) del PSC PROCERT está formado por los siguientes atributos:

- DNSName: procert.net.ve.
- otherName:
- OID 2.16.862.2.1. (Código de identificación del PSC PROCERT acreditado)
- OID 2.16.862.2.2.: RIF J- 31635373-7

Para los Signatarios: El nombre distintivo (DN) del signatario está formado por los siguientes atributos:

- CN: (Nombre del Titular)
- O: (Nombre de la Organización).
- C: VE.
- E: (correo electrónico)
- L: Municipio
- S: Estado

El nombre alternativo (AN) del signatario está formado por los siguientes atributos:

- otherName: OID 2.16.862.2.2.: (Numero de Cedula de Identidad o Pasaporte)

- 14.2. Necesidad de nombres significativos: El PSC PROCERT requerirá de los clientes contratantes de firmas o certificados electrónicos sus nombres y apellidos completos y conformen figuran representados en la cédula de identidad laminada que posea el solicitante de la firma o certificado electrónico. No serán admitidos o procesados por la AR los datos correspondientes a diminutivos de nombres, alias o seudónimos con los cuales se pretenda identificar el cliente. En el caso de las poblaciones indígenas serán considerados los nombres que figuran en su cédula de identidad o pasaporte. En todo caso el PSC PROCERT garantiza que los DN contenidos en los campos de los certificados son lo suficientemente distintivos y significativos para poder vincular la identidad de un cliente a su firma o certificado electrónico.
- 14.3. Interpretación de formatos de nombre: Las reglas utilizadas para la interpretación de los nombres distinguidos en los certificados emitidos están descritos en la ISO/IEC 9595 (X.500) DistinguishedName (DN). Adicionalmente todos los certificados emitidos por el PSC PROCERT utilizan codificación UTF8 para todos los atributos, según la RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, January 2013.
- 14.4. Unicidad de los nombres: La Autoridad de Certificación de la SUSCERTE define como campo DN del certificado de autoridad como único y sin ambigüedad. Para ello se incluirá como parte del DN, específicamente en el campo OU, el nombre o razón social del PSC PROCERT, por lo tanto, la unicidad se garantiza mediante la confianza sobre la unicidad de los nombres mercantiles en el registro nacional. Adicionalmente y respecto a los clientes; si existe un cliente que mantenga contrato y haya adquirido más de un tipo de firma o certificado electrónico, la base de datos del PSC PROCERT mantendrá un esquema uniforme e igualitario de datos del cliente contratante y no será permitido o procesado por la AR del PSC, datos personales disimiles y que correspondan a un mismo cliente.
- 14.5. Resolución de conflictos relativos a nombres: En el caso de una ocurrencia de conflicto de nombre entre clientes y que corresponda a nombre y apellidos iguales, la AR del PSC PROCERT procederá a realizar la distinción de identidad y autenticación de la misma a través del uso del número de cédula de identidad y RIF personal de cada cliente del PSC PROCERT con las cuales se haya generado el conflicto de nombre.

15. Validación inicial de la identidad.
 - 15.1. Método de prueba de posesión de la clave privada: El esquema de operación del PSC PROCERT y su plataforma tecnológica de certificación se encuentran configurados para que el cliente genere su par de claves (pública y privada). En virtud de lo anterior, una vez emitido cada certificado, es el cliente quien tiene la custodia y resguardo de su clave privada, presumiendo que el mismo la posee y resguarda obligándose conforme a la ley, salvo denuncia de el mismo cliente de compromiso de su clave privada, caso en el cual se procederá a la revocación de la firma o certificado electrónico que corresponda.
 - 15.2. Autenticación de la identidad de una organización: La AR del PSC PROCERT cuando se trate de firmas electrónicas que acrediten empresas o entes públicos procederá de la manera siguiente:
 - 15.2.1. Ente público: La AR procederá a comprobar la publicación en la gaceta oficial de la república bolivariana de Venezuela de la resolución que crea a la entidad o empresa pública. Todo certificado electrónico de organización deberá estar asociado a un responsable humano por dicho certificado. La AR del PSC PROCERT cumplirá los pasos de verificación y comprobación de identidad y representación. Una vez comprobadas la identidad de la organización y las facultades de representación se procederá a validar el resto de la información solicitada por el sistema de contratación del PSC PROCERT y cumplido el procedimiento exitosamente, la AR comunicará a la AC del PSC PROCERT, su conformidad respecto a los datos para que se proceda a la generación del certificado electrónico contratado por el cliente.
 - 15.2.2. Ente privado: La AR procederá a comprobar la existencia de la empresa privada a través de la revisión de su documento constitutivo-estatutario, debidamente inscrito en la oficina del registro mercantil correspondiente a la circunscripción judicial del domicilio de la empresa Privada, como de la publicación del registro de empresa en un diario mercantil. Todo certificado electrónico de organización deberá estar asociado a un responsable humano por dicho certificado. La AR del PSC PROCERT cumplirá los pasos de verificación y comprobación de identidad y representación. Una vez comprobadas la identidad de la organización y las facultades de representación se procederá a validar el resto de la información solicitada por el sistema de contratación del PSC PROCERT y cumplido el procedimiento exitosamente, la AR comunicará a la AC del PSC PROCERT, su conformidad respecto a los datos para que se proceda a la generación del certificado electrónico contratado por el cliente.
 - 15.3. Comprobación de las facultades de representación: La AR del PSC PROCERT cuando se trate de firmas electrónicas que acrediten la representación de empresas procederá de la manera siguiente:
 - 15.3.1. Ente público: La AR procederá a comprobar la publicación en la gaceta oficial de la república bolivariana de Venezuela de la resolución que crea a la entidad o empresa pública. Posteriormente se validará la publicación

en la gaceta oficial de la república bolivariana de Venezuela del cuerpo normativo o estatutario que señala las funciones y atribuciones del representante del ente público y delimita su ejercicio de función. Seguidamente la AR del PSC PROCERT validará la publicación en la gaceta oficial de la república bolivariana de Venezuela de la designación en cargo del representante de la entidad o empresa pública. Una vez comprobadas las facultades de representación se procederá a validar el resto de la información solicitada por el sistema de contratación del PSC PROCERT y cumplido el procedimiento exitosamente, la AR comunicará a la AC del PSC PROCERT, su conformidad respecto a los datos para que se proceda a la generación del certificado electrónico contratado por el cliente.

15.3.2. Ente privado: La autoridad de registro (AR) procederá a comprobar la existencia de la empresa privada a través de la revisión de su documento Constitutivo-Estatutario, debidamente inscrito en la oficina del registro mercantil correspondiente a la circunscripción judicial del domicilio de la empresa privada, como de la publicación del registro de empresa en un diario mercantil. Posteriormente se validarán con vista al documento constitutivo de la empresa privada o de las asambleas que lo hayan modificado, las funciones y atribuciones del representante de la empresa privada y su duración en cargo. Seguidamente la AR del PSC PROCERT validará la designación en cargo realizada en asamblea ordinaria o extraordinaria de la empresa privada, debidamente inscrita y publicada en la oficina del registro mercantil correspondiente y publicado posteriormente en diario mercantil. Una vez comprobadas las facultades de representación se procederá a validar el resto de la información solicitada por el sistema de contratación del PSC PROCERT y cumplido el procedimiento exitosamente, la AR comunicará a la AC del PSC PROCERT, su conformidad respecto a los datos para que se proceda a la generación del certificado electrónico contratado por el cliente.

15.4. Criterios para operar con AC externas: La operación con AC externas al PSC PROCERT no se encuentra normada o desarrollada por la SUSCERTE. No obstante, el decreto ley sobre mensajes de datos y firmas electrónicas, si contempla dicha posibilidad, quedando abierta la posibilidad de establecer esquemas de operación con autoridades de certificación externas una vez se cuente con la normativa que regule la materia.

16. Identificación y autenticación de las solicitudes.

16.1. De la suspensión o revocación de clave: Bajo el esquema de operación del PSC PROCERT y de su plataforma tecnológica de certificación, el cliente genere su par de claves (pública y privada) y es por ello por lo que el compromiso de la clave privada del cliente producirá obligatoriamente la necesidad de revocar el certificado generado para dicho cliente. La Suspensión de las firmas o certificados electrónicos generados por la AC usualmente precede a la revocación y donde proceda dicha revocación se hará de acuerdo con los procedimientos específicos descritos en aparte.

16.1.1. Circunstancias para la suspensión.

- La Clave Privada del cliente se ha perdido, ha sido revelada sin autorización, ha sido robada o comprometida de cualquier manera.
- La seguridad, confianza o integridad de la ICP está materialmente afectada debido compromiso de la clave privada del PSC PROCERT.
- Se ha producido una emisión indebida o defectuosa de un certificado debido a que:
 - Un pre-requisito material para la emisión del certificado no fue satisfecho;
 - Se conoce un hecho material en el certificado, o razonablemente se cree que es falso.
 - Cualquier otra circunstancia que requiera investigación para garantizar la seguridad, integridad o confianza de la ICP.
 - El resultado de la investigación será la orden de la alta dirección o gerente general para producir una solicitud de suspensión o una decisión para proceder con la suspensión.

16.1.2. ¿Quién puede solicitar una suspensión o revocación?: Una Suspensión o revocación puede ser solicitada por las entidades siguientes:

- El propietario del certificado o un representante con poder expreso para ejecutar suspensiones o solicitudes de revocación.
- Un representante de PROCERT a quién explícitamente se le haya dado la autoridad para realizar suspensiones o solicitudes de revocación.
- La decisión de un tribunal mediante el cual se declare ejecutable una decisión cautelar o ejecutoria solicitando la suspensión o revocación de una firma o certificado electrónico emitido por PROCERT.
- Una solicitud válida de suspensión o revocación recibida de cualquiera de las entidades antes mencionadas tendrá como resultado una suspensión inmediata y el inicio de una investigación post-suspensión para determinar si una revocación seguirá a la suspensión o si la suspensión debe ser levantada.
- La suspensión o revocación de una firma o certificado electrónico también puede ser solicitada por la Gerencia General y la Gerencia de Informática.
- Una solicitud de suspensión de la alta dirección o la gerencia general resultará en la suspensión inmediata de la firma o certificado electrónico y en el inicio de una investigación post-suspensión.

16.1.3. Límites del período de suspensión: Las firmas o certificados electrónicos emitidos por la raíz de certificación de la AC permanecerán suspendidos por un máximo de veinte (20) días. A su terminación o antes de su terminación, PROCERT determinará si el certificado debe ser revocado o restablecido como válido.

16.1.4. Procedimiento para la solicitud de suspensión: Para procesar una solicitud de suspensión la raíz de certificación del PSC PROCERT, hará lo siguiente:

- Suspenderá el certificado, registrará el motivo de la suspensión y conservará la documentación relevante.
- Notificará al Cliente propietario del certificado suspendido, señalando los detalles del certificado y la fecha y hora de la suspensión.
- Continuar salvaguardando la clave pública asociada al certificado suspendido hasta la fecha de expiración del Certificado, en cuyo momento deberá ser destruido.
- Notificar (cuando proceda) oportunamente a sus entidades ICP subordinadas, la suspensión de su certificado.

16.1.5. Circunstancias para la revocación: Una firma o certificado electrónico emitido por la raíz de certificación de la AC en todos los casos, será revocado mediante una solicitud de revocación de certificado emitida por la alta dirección o la gerencia general y solamente en los siguientes casos:

- Cuando luego de pasar por todo el procedimiento de suspensión se determine que se requiere una revocación debido a circunstancias materiales que se están averiguando en la investigación post-suspensión que amerita la revocación del certificado; y
- Cuando la alta dirección del PSC PROCERT solicite la revocación de un certificado sin importar si la investigación post-suspensión se ha llevado a cabo.

16.1.6. Procedimiento para la solicitud de revocación: Para procesar una solicitud de revocación la raíz de certificación del PSC PROCERT, hará lo siguiente:

- Revocar el certificado, registrará el motivo de la revocación y conservará la documentación relevante.
- Generará inmediatamente una LRC (lista de revocación de certificado).
- Notificará al Cliente propietario del certificado revocado, señalando los detalles del certificado y la fecha y hora de la revocación.
- Continuar salvaguardando la clave pública asociada al certificado revocado hasta la fecha de expiración del Certificado, en cuyo momento deberá ser destruido.
- Notificar (cuando proceda) oportunamente a sus entidades ICP subordinadas, la revocación de su certificado.

16.1.7. Solicitud de revocación y/o suspensión: La revocación o suspensión de certificados se realiza cuando la persona (natural o jurídica) ha dejado de existir o cesado en las actividades por las cuales se le otorgo el certificado, también, aplica en caso de que la seguridad de la llave privada se haya visto comprometida. La revocación o suspensión de un certificado electrónico la puede efectuar el propietario del certificado o por solicitud de la alta dirección o gerente general del PSC PROCERT. Para realizar la solicitud de suspensión o revocación debe seguir los siguientes pasos:

Paso 1: Notificación de la suspensión o revocación, indicando claramente los motivos, utilizando alguno de los siguientes medios:

Teléfono Máster: (58-212) 267.48.80

Fax: (58-212) 267.12.70

E-mail para revocación: soporte@procert.net.ve

Paso 2: Ratificación presencial de la solicitud de revocación o suspensión: El signatario deberá identificarse ante la autoridad de registro (AR) y ratificar la revocación o suspensión del certificado.

16.1.8. Período de gracia de la solicitud de revocación: Las solicitudes de revocación deben procesarse dentro de las veinticuatro (24) horas de haber recibido una decisión definitiva de la raíz de certificación de la AC, para revocar un certificado de acuerdo con los procedimientos operacionales del PSC PROCERT.

16.2. De la renovación de la clave

16.2.1. Rutinarias: La identificación y autenticación para la renovación del certificado se debe realizar utilizando las técnicas para la autenticación e identificación inicial.

16.2.2. De la clave después de una renovación – clave no comprometida: El esquema de operación del PSC PROCERT y su plataforma tecnológica de certificación, se encuentran configurados para que el cliente genere su par de claves (pública y privada). Siempre y en todo caso el compromiso de clave derivará del mismo cliente pues el PSC PROCERT no genera el par de claves (pública y privada). La identificación y autenticación para la renovación de un certificado después de una revocación sin compromiso de la clave será la misma que para el registro inicial. Adicionalmente el signatario deberá demostrar satisfactoriamente al PSC PROCERT que las causas de la revocación anterior ya no están presentes.

17. Ciclo de vida de los certificados del PSC: Las firmas y los certificados electrónicos generados por el PSC PROCERT tienen un ciclo de vida de un (1) años contados a partir de la fecha de activación de la firma o certificado electrónico por parte de la AC.

17.1. Solicitud de certificados: Los clientes interesados en adquirir una firma o certificado electrónico generado por el PSC PROCERT, deberán ingresar a la página web del PSC PROCERT (www.procert.net.ve) y acceder al vínculo "Sistema AR", seleccionar el tipo de certificado, aceptar los contratos, asistir a la entrevista con la AR del PSC PROCERT, generar sus claves y por último descargar su firma o certificado electrónico.

17.1.1. Proceso de generación de la solicitud de certificados y responsabilidades: El cliente contratante una vez cumplido y culminado el proceso de contratación del certificado electrónico de su preferencia en la página Web del PSC PROCERT (www.procert.net.ve), deberá remitir al apartado postal del PSC PROCERT la información requerida en cada una de las ventanas del sistema de contratación del PSC PROCERT. Posteriormente deberá concurrir a las oficinas administrativas del PSC PROCERT a los efectos de cumplir con la asistencia a la entrevista pautada por la AR a los efectos de la validación de los datos del cliente solicitante, sea éste persona natural o jurídica. Si el cliente no asiste a la entrevista fijada por la AR se entenderá que desiste de su solicitud y se procederá a imponer el cargo de penalización referido en el sistema de contratación del PSC PROCERT. Si el cliente notifica su imposibilidad de concurrir a la fecha establecida se le fijará una nueva oportunidad. Si el cliente no asiste a la fecha replanteada se entenderá que desiste de su solicitud y se procederá a imponer el cargo de penalización referido en el sistema de contratación de PROCERT. A través de este procedimiento existe una interacción entre la AC y la AR ya que el procedimiento descrito anteriormente se tiene que realizar antes de que la AC pueda aprobar el certificado que el cliente haya solicitado El módulo de la AR del PSC PROCERT permite administrar las peticiones de certificados y enviarlas al módulo de la AC.

17.1.2. Proceso de firma del certificado: El PSC PROCERT, una vez validada la identidad del signatario deberá aprobar desde el sistema de certificación la emisión del certificado para la firma del mismo, el proceso es el siguiente:

- El Encargado de la AR notifica al consultor de tecnología y al gerente general la aprobación de la solicitud y aprueba el certificado utilizando el sistema de certificación de PROCERT.
- El consultor de tecnología y al gerente general activan localmente el HSM y el servidor de certificación, y aprueban de forma simultánea la firma del certificado electrónico.

17.1.3. Proceso para la generación de la solicitud de renovación de las claves del certificado: El proceso para la renovación de un certificado será el mismo que para el registro inicial.

17.1.4. Procedimiento para realizar una solicitud de revocación de un certificado: La revocación o suspensión de certificados se realiza cuando la persona (natural o jurídica) ha dejado de existir o cesado en las actividades por las cuales se le otorgo el certificado, también, aplica en caso de que la seguridad de la llave privada se haya visto comprometida. La revocación o suspensión de un certificado electrónico la puede efectuar el propietario del certificado o La alta dirección o gerente general del PSC PROCERT.

Para realizar la solicitud de suspensión o revocación debe seguir los siguientes pasos:

Paso 1: Notificación de la suspensión o revocación, indicando claramente los motivos, utilizando alguno de los siguientes medios:

Teléfono máster: (58-212) 267.48.80

Fax: (58-212) 267.12.70

E-mail para revocación: sopORTE@PROCERT.NET.VE

E-mail para suspensión: sopORTE@PROCERT.NET.VE

Paso 2: Ratificación presencial de la solicitud de revocación o suspensión: El suscriptor deberá identificarse ante la autoridad de registro (AR) del PSC PROCERT y ratificar la revocación o suspensión del certificado.

18. Tramitación de solicitud de un certificado.

18.1. Realización de las funciones de identificación y autenticación: Las funciones de identificación y autenticación de los clientes que optan a la compra de una firma o certificado, está asignada a la AR del PSC PROCERT. La explicación detallada de las funciones y atribuciones de la AR del PSC PROCERT se encuentran detallados en el aparte 11.1.1.5. y 15 del presente documento de la DPC y PC.

18.2. Aprobación o denegación de un certificado: La aprobación o denegación de una firma o certificado electrónico se encuentra asignada a la AC del PSC PROCERT. Toda solicitud de firma o certificado electrónico que no sea validada por la AR del PSC PROCERT automáticamente será rechazada y en consecuencia denegada. La autoridad de certificación antes de dar inicio al proceso de aprobación de una firma o certificado electrónico validará el cumplimiento de las condiciones siguientes:

- Validar el pago efectuado por el cliente
- Validar el informe emitido por la AR
- Validar el tipo de certificado solicitado y tramitar ante el Sistema AR el cual es el módulo de generación de certificados.

Una vez verificados y cumplidos a satisfacción los pasos señalados, la AC del PSC PROCERT procederá a generar la firma o certificado electrónico y según sea el caso.

- 18.3. Plazo para la tramitación de un certificado: El plazo para la tramitación y proceso de compra de la firma o certificado electrónico seleccionado por el cliente, dependerá en gran medida de la información suministrada por el mismo cliente y de su asistencia a la entrevista de validación con la AR del PSC PROCERT. Si producto de la entrevista la AR determina que el cliente cumple los requisitos establecidos por el PSC PROCERT, informará a la AC para que proceda a la generación y firma de la firma o certificado electrónico, según corresponda. El lapso establecido por el PSC PROCERT para la aprobación y firma de los certificados, es de tres (3) días continuos luego de la entrevista de validación de identidad y datos con la AR del PSC PROCERT. La AC del PSC PROCERT generará y firmará los certificados dentro del referido lapso y notificará al cliente, para que este proceda a la descarga e instalación de la firma o certificado electrónico.
19. Emisión de certificado.
- 19.1. Acciones de la AC durante la emisión de un certificado: El PSC PROCERT es el encargado de generar los certificados adquiridos por los clientes. Posterior a la aprobación por parte de la AR del PSC PROCERT, el administrador del módulo de la AC procede a la aceptación y aprobación de la emisión del certificado; es en este momento donde el aplicativo de certificación se comunica vía https con la AC y le solicita la firma de la clave pública del certificado. La AC firma el certificado y se lo envía al aplicativo de certificación utilizando también la comunicación https. Luego de emitido el certificado el signatario podrá descargarlo y proceder a su instalación.
- 19.2. Notificación al solicitante por parte de la AC acerca de la emisión de su certificado: La AC del PSC PROCERT es la encargada de notificar vía correo electrónico al cliente acerca de la generación de su firma o certificado electrónico y de los pasos que deberá seguir para la instalación de la firma o certificado electrónico, según corresponda. El sistema de la AC emite un correo electrónico automático, que es enviado a la cuenta de correo electrónico suministrado por el cliente.
20. Uso del par de claves y del certificado.
- 20.1. Uso de la clave privada del certificado: La entrega de clave a los clientes no es realizada y en consecuencia no será suministrada, ya que cada cliente generará su propio par de claves (pública y privada). El titular solo puede utilizar la clave privada y el certificado para usos autorizados en esta DPC. El cliente es el único responsable de la custodia y cuidado de su clave privada y deberá reportar al PSC PROCERT acerca del compromiso de la clave privada del cliente, sin menoscabo de responder personalmente por las acciones y consecuencias derivadas del uso indebido de sus firmas o certificados electrónicos por parte de terceras personas.
- 20.2. Uso de la clave pública y del certificado por los terceros de buena fe: El certificado de raíz de AC se hace público a los efectos de la validación de la ruta. La huella del certificado y los certificados de la ICP de la AC PROCERT están disponibles en la Página Web de PROCERT (www.procernet.ve). Los terceros de buena fe deben confirmar la validez de las copias de sus certificados de la ICP de la AC PROCERT usando estas huellas. Los usos asignados a los

certificados se encuentran definidos en el aparte 9 que precede del presente documento de DPC y PC.

21. Renovación del certificado con cambio de clave.

21.1. Causas para la renovación de un certificado: Toda firma o certificado electrónico generado por el PSC PROCERT podrá ser renovado, siempre y cuando sean cumplidas las condiciones siguientes:

- Que se haya cumplido el término de vigencia de la firma o certificado electrónico del cual es propietario.
- Que la firma o certificado electrónico no haya sido revocado por el PSC PROCERT por razones de uso ilícito de la firma o certificado electrónico, según corresponda
- Que el solicitante cumpla con el proceso de contratación del PSC PROCERT y de validación por parte de la AR del PSC PROCERT.

21.2. Entidad que puede solicitar la renovación de un certificado: Todo propietario de firma o certificado electrónico generado por el PSC PROCERT que cumpla con los requisitos solicitados por la PSC PROCERT, podrá solicitar ante el PSC PROCERT la nueva emisión o generación de la firma o certificado electrónica según corresponda, salvo que exista prohibición o mandato expreso contenido en sentencia judicial firme y que señale la prohibición de emitir certificados al solicitante.

21.3. Procedimiento de solicitud para renovación de un certificado: Los clientes interesados en renovar una firma o certificado electrónico generado por el PSC PROCERT, deberán ingresar a la página web de PROCERT (www.procert.net.ve) y acceder al vínculo "Sistema AR", seleccionar el tipo de certificado, aceptar los contratos, ingresar sus datos personales, asistir a la entrevista con la AR del PSC PROCERT, generar sus claves y por último descargar su firma o certificado electrónico.

21.4. Notificación de la emisión de un nuevo certificado a la AR: La AC del PSC PROCERT es la encargada de notificar vía correo electrónico al cliente acerca de la emisión de una nueva firma o certificado electrónico y de los pasos que deberá seguir para la instalación de la firma o certificado electrónico, según corresponda.

21.5. Publicación del certificado renovado por la AC: La AC PROCERT, posee un repositorio de todos los certificados emitidos y renovados tanto en su servidor de certificación como en una base de datos redundante. El acceso al repositorio de los certificados emitidos es público y puede ser realizado por los clientes, proveedores o parte interesada a través de la página Web del PSC PROCERT (www.procert.net.ve), accediendo al vínculo de "Certificados Emitidos" e ingresando los datos correspondientes al tipo de firma o certificado electrónico y el nombre o apellido del cliente propietario de la firma o certificado electrónico.

- 21.6. Notificación de la emisión del certificado por la AC a otras entidades: La operación con AC externas al PSC PROCERT no se encuentra normada o desarrollada por la SUSCERTE. No obstante, el decreto ley sobre mensajes de datos y firmas electrónicas, si contempla dicha posibilidad, quedando abierta la posibilidad de establecer esquemas de operación con autoridades de certificación externas una vez se cuente con la normativa que regule la materia.
22. Modificación de certificados: Las firmas o certificados electrónicos generados por el PSC PROCERT, deben mantener su integridad durante su período de vigencia y no podrá ser objeto de modificación o cambio alguno.
23. Revocación y suspensión de un certificado.
- 23.1. Circunstancias para la revocación del certificado: Las circunstancias para la revocación del certificado son las señaladas en el aparte 16.1.5 del presente documento de DPC y PC.
- 23.2. Entidad que puede solicitar la revocación: La entidad que puede solicitar la revocación de la firma o certificado electrónico según corresponda se encuentra señalada en el aparte 16.1.2 del presente documento de DPC y PC.
- 23.3. Procedimiento de solicitud de la renovación: El procedimiento de solicitud de la renovación de la firma o certificado electrónico según corresponda, es el señalado en el aparte 21.3 del presente Documento de DPC y PC.
- 23.4. Período de gracia de la solicitud de la revocación: El período de gracia de la solicitud de la revocación de la firma o certificado electrónico es de veinte (20) días. A su terminación o antes de su terminación, PROCERT determinará si el certificado debe ser revocado o restablecido como válido.
- 23.5. Circunstancias para la suspensión: Las circunstancias para la suspensión de firma o certificado electrónico según corresponda, es el señalado en el aparte 16.1.1 del presente documento de DPC y PC.
- 23.6. Procedimiento para la solicitud de suspensión: El procedimiento para la suspensión de firma o certificado electrónico según corresponda, es el señalado en el aparte 16.1.4 del presente Documento de DPC y PC.
- 23.7. Límites del período de suspensión: El límite del período de suspensión de firma o certificado electrónico según corresponda, es el señalado en el aparte 16.1.3 del presente documento de DPC y PC.
- 23.8. Frecuencia de emisión de LCR: La LCR se constituye en un registro de todos aquellos certificados que, habiendo cumplido su proceso de generación y asignación de Ley, son revocados cuando se encuentra comprometida su clave, por solicitud del Cliente, por uso indebido del certificado, por causa imputable al Cliente o por cese de operación de la AC. La LCR es publicada cada veinticuatro (24) horas en la página web del PSC PROCERT (www.procort.net.ve).

- 23.9. Disponibilidad de compromiso on-line de revocación y estado de los certificados: La AC tiene la capacidad de entregar la lista de certificados revocados utilizando el OCSP a través del enlace <http://ocspsmime.procert.net.ve/ocsp>
- 23.10. Requisitos de comprobación on-line de revocación: El cliente del PSC PROCERT podrá acceder en línea a la verificación del estado de un certificado a los fines de verificar si se encuentra suspendido o revocado. El cliente deberá ingresar en la Página Web del PSC PROCERT (www.procert.net.ve) y acceder el módulo “AC PROCERT” seguidamente buscar la opción *Publicación de los certificados revocados AC PROCERT* y seleccionar la opción OCSP.
- 23.11. Otras formas de divulgación de información de revocación disponibles: El PSC PROCERT notificará vía correo electrónico al cliente que corresponda, acerca de la suspensión o revocación de su certificado.
24. Servicio de comprobación de estado de certificados.
- 24.1. Características operativas: El PSC PROCERT posee servicios de comprobación de estado de la firma o certificado electrónico. Dichos servicios son la LCR y el acceso OCSP para acceso en línea a la comprobación del estado de las firmas y certificados electrónicos generados por el PSC PROCERT. El funcionamiento de la LCR se encuentra establecido en el apartado 32.7 del presente documento de DPC y PC. El funcionamiento del acceso vía OCSP se encuentra establecido en los apartes 23.9 y 23.10 que preceden.
- 24.2. Disponibilidad del servicio: El PSC PROCERT mantiene disponibles los servicios de la LCR y acceso OCSP a través de su página web (www.procert.net.ve). La AC PROCERT mantiene en operación su portal web, cumpliendo con un alto porcentaje de disponibilidad.
- 24.3. Características adicionales: Características adicionales a los servicios de LCR y acceso OCSP se encuentran señaladas de forma precedente en este documento de DPC y PC.
25. Finalización de la suscripción: El cliente del PSC PROCERT podrá dar el uso permitido de la firma o certificado electrónico y durante su período de vigencia. Llegado a término el período de vigencia del certificado, el cliente podrá optar al proceso de renovación y nueva emisión. Si el cliente no opta por la renovación o nueva emisión, tendrá a su disponibilidad en los archivos del PSC PROCERT y por un lapso de diez (10) años, los registros correspondientes a la generación de su certificado.
26. Custodia y recuperación de la clave.
- 26.1. Prácticas y políticas de custodia y recuperación de la clave: La clave privada del PSC PROCERT se custodia en un dispositivo criptográfico HSM. Para el acceso al repositorio de claves privadas es necesario el uso de tarjetas inteligentes. El esquema de operación del PSC PROCERT y su plataforma tecnológica de certificación se encuentran configurados para que el cliente genere su par de claves (pública y privada). Siempre y en todo caso el compromiso de clave

derivará del mismo cliente pues el PSC PROCERT no genera el par de claves (pública y privada). En virtud de lo anterior, si el cliente extravía su clave privada, se deberá proceder a la emisión de un nuevo certificado y deberá cumplir el proceso de contratación del PSC a tales efectos. La clave pública siempre estará en el repositorio, de conformidad con lo señalado en el aparte 31.1.4 de presente documento de declaración de prácticas de certificación (DPC) y política de certificados (PC).

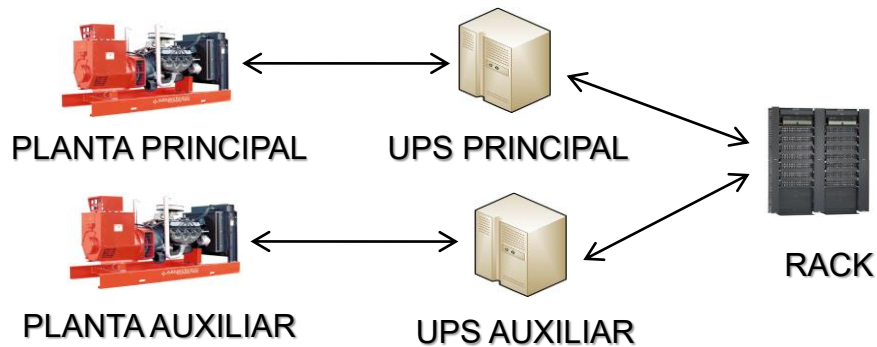
27. Controles de seguridad física, de gestión y de operaciones.

27.1. Controles de seguridad física: Ubicación y construcción del PSC. La AC PROCERT mantiene un esquema operacional orientado a garantizar la continuidad operacional y prestación de sus servicios con altos estándares de calidad, oportunidad y seguridad. El centro de datos se constituye en la sede operacional de la AC PROCERT y desde donde opera la plataforma de emisión de certificados. El centro de datos reúne y mantiene los requisitos de operación que para este tipo de facilidades impone la normativa internacional en materia de seguridad asociada a la tecnología de información, la legislación de la república bolivariana de Venezuela y las normas impuesta por la SUSCERTE. El personal de operaciones del PSC PROCERT es el encargado, en conjunto con el Gerente General y el consultor de tecnología de Informática de gestionar y mantener la operación de la plataforma tecnológica de generación de certificados instalada en el centro de datos situado en la calle 7, Centro de Datos Daycohost, Las Mercedes, Municipio Chacao de la Ciudad de Caracas, República Bolivariana de Venezuela. El centro de datos opera las veinticuatro (24) horas del día, los trescientos sesenta y cinco (365) días del año y mantiene una autonomía operacional superior a dos (2) meses. Adicionalmente el centro de datos reúne condiciones y características de construcción antisísmica y de prevención de incendio e inundaciones, mantiene un perímetro de seguridad y cuenta con siete (7) niveles de seguridad de acceso. El centro de datos desde donde opera la AC PROCERT, mantiene las pólizas o instrumentos emitidos por empresas de seguros solventes y reconocidas, a los efectos de mantener un respaldo en caso de ocurrencia de una contingencia que afecta la integridad física de la referida sede administrativa y pueda ofrecer de esa manera una garantía de su continuidad operacional. La AC PROCERT mantiene contrato de operación de centro alternativo en caso de daño permanente que imposibilite y restrinja la operación regular del centro de datos.

27.1.1. Acceso físico: La AC PROCERT dentro de su plataforma tecnológica de certificación electrónica, mantiene medidas de control de acceso tanto lógicas (aplicativo de certificación) como físicas (equipos) garantizando la integridad y seguridad de los servicios prestados. Para el control de acceso físico existen siete (7) capas de seguridad, desde el exterior hasta los servidores donde está instalado el aplicativo de certificación. Además de procedimientos de seguridad que restringe el acceso solo a personal autorizado con autorización para el acceso a cada una de las siete (7) capas de seguridad física y conocer la información de acceso (login y password) del sistema operativo de los equipos que conforman la plataforma de certificación de la AC PROCERT. El acceso físico para el interior del rack (apertura) debe estar permitido solo al personal del PSC PROCERT. Características del centro de datos:

- La vigilancia con personal armado y cámaras digitales comprende el servicio 7X24X365 días. En este nivel se registran los equipos portátiles de computación.
- La cerca perimetral limita el acceso físico a la sede del centro de datos.
- El control de ingreso a la entrada del área interna del centro de datos se constituye en un mecanismo de doble aseguramiento de ingreso del personal autorizado.
- El control de ingreso al pasillo de acceso al área de servidores se constituye en un triple mecanismo de aseguramiento de acceso al área pública del centro de datos y al área de servidores. En este control se válida la identidad de la persona autorizada por PROCERT para ingresar al área de servidores.
- El dispositivo biométrico sensible al calor e identidad tiene como objetivo bloquear el acceso al área de servidores para el personal no autorizado y acompañado por personal técnico y de operaciones.
- El carnet de magnético de seguridad para puerta de acceso al área interna de control del área de servidores valida que en efecto sólo el personal autorizado y poseedor de la tarjeta cuenta con acceso al área de control de servidores.
- El control de acceso al cuarto de servidores es realizado por los operadores de área de control externa del área de servidores. Los operadores validan la identidad de la persona que ingresará al área de servidores, luego registra sus datos y la hora de ingreso y egreso.
- La llave de acceso al rack de servidores de PROCERT está en posesión del personal de PROCERT para asegurar la seguridad y custodia de los servidores y de la autoridad de certificación.
- El mecanismo de seguridad de acceso a la puerta del rack de servidores de PROCERT se constituye en el sistema de seguridad que permite que sólo los operadores de PROCERT podrán acceder a los servidores de la plataforma de certificación.

27.1.2. Alimentación eléctrica y acondicionador de aire: El rack donde se encuentran instalados los servidores de la plataforma de certificación de la autoridad de certificación AC PROCERT cuenta con dos (2) líneas de tensión distintas, una principal y otra auxiliar, dichas líneas de tensión están conectadas a dos (2) fuentes de energía ininterrumpida (UPS), los cuales a su vez están conectadas a dos (2) plantas generadoras de energía. A continuación, se muestra un gráfico referencial de la conexión del suministro de energía:



Dicha distribución garantiza el suministro de energía eléctrica y por consiguiente de aire acondicionado.

27.1.3. Exposición de agua: El centro de datos reúne y mantiene los requisitos de operación que para este tipo de facilidades impone la normativa internacional en materia de seguridad asociada a la tecnología de información, la legislación de la república bolivariana de Venezuela y las normas impuesta por la SUSCERTE.

27.1.4. Protección y prevención de incendios: El centro de datos reúne y mantiene los requisitos de operación que para este tipo de facilidades impone la normativa internacional en materia de seguridad asociada a la tecnología de información, la legislación de la república bolivariana de Venezuela y las normas impuesta por la SUSCERTE.

27.1.5. Sistemas de almacenamiento: El centro de datos reúne y mantiene los requisitos de operación que para este tipo de facilidades impone la normativa internacional en materia de seguridad asociada a la tecnología de información, la legislación de la república bolivariana de Venezuela y las normas impuesta por la SUSCERTE.

27.1.6. Eliminación de residuos: El centro de datos reúne y mantiene los requisitos de operación que para este tipo de facilidades impone la normativa internacional en materia de seguridad asociada a la tecnología de información, la legislación de la república bolivariana de Venezuela y las normas impuesta por la SUSCERTE.

27.1.7. Almacenamiento de copias de seguridad: El centro de datos reúne y mantiene los requisitos de operación que para este tipo de facilidades impone la normativa internacional en materia de seguridad asociada a la tecnología de información, la legislación de la república bolivariana de Venezuela y las normas impuesta por la SUSCERTE.

27.2. Controles funcionales.

27.2.1. Papeles de confianza: La AC y AR mantendrán un esquema de gestión y operación basado en una estructura plana, sustentada sobre la interacción e interdependencia del personal en sus diversos roles y funciones. La operación regular del PSC PROCERT será dividida en funciones de operación y administración. La alta dirección se

constituye en el nivel con mayor poder de decisión y mando dentro de la organización. Las actividades de operación y administración serán coordinadas por la gerente general y el consultor de tecnología del PSC PROCERT, las cuales reportarán directamente a la alta dirección. La operación, control, monitoreo y seguimiento diario de la gestión de la plataforma tecnológica de certificación será realizada por los operadores de informática. El grupo de operadores de informática contará con un coordinador de operadores, el cual será designado por el gerente general y el consultor de tecnología y deberá contar con la aprobación de la alta dirección. El grupo de operadores de informática estará integrado por un total de hasta cuatro (4) operadores, los cuales estarán en capacidad de atender y resolver todo requerimiento operacional de la plataforma tecnológica de certificación. La gestión regular de la AR será asignada a un encargado de acreditación de identidad y datos. La gestión regular del gerente general será apoyada por un asistente administrativo, quien realizará gestiones de oficinistas y recepcionista, tramitará pagos y coordinará la relación con los servicios tercerizados y mantendrá el inventario de material administrativo y logístico requerido por el personal del PSC PROCERT.

27.2.2. Número de personas requeridas por rol: La estructura interna y medular del PSC PROCERT se encuentra discriminada de la manera siguiente:

- Gerencia General (1)
- El consultor de tecnología (1).
- Consultor PKI (1)
- El consultor de seguridad de la información y cumplimiento (1).
- El Auditor (1).
- Los operadores de informática (4).
- La autoridad de registro (AR) (1).
- El personal de administración (1).
- Los servicios tercerizados (20)

27.2.3. Identificación y autenticación de cada rol: La identificación y autenticación de cada rol, así como el establecimiento de nuevas obligaciones o responsabilidades corresponderá a la Alta Dirección del PSC PROCERT. Las funciones y responsabilidades asociadas a cada cargo se encuentran señaladas dentro de la sección 11.1.1 que precede.

27.3. Controles de seguridad personal.

27.3.1. Requerimientos de antecedentes, calificación, experiencia y acreditación: Todo el personal del PSC involucrado en la operación de la ICP está sujeto a la investigación y verificación de antecedentes. Las referencias son rigurosamente investigadas en el caso del personal operacional. Toda la operación de la ICP del PSC PROCERT está bajo la responsabilidad directa de la alta dirección. El personal involucrado en el control y la operación de la ICP estarán suficientemente entrenados para cumplir con las funciones asignadas a su rol y recibirá entrenamiento continuo para garantizar los niveles de concienciación sobre las políticas de seguridad y los procedimientos. El proceso de

adiestramiento y desarrollo del personal se regulará por el documento de la política de adiestramiento y desarrollo del personal de PROCERT (AC-D-005).

27.3.2. Requerimientos de formación: Ningún miembro del personal del PSC PROCERT puede tener acceso físico u operar cualquier componente de la ICP sin capacitación previa y sin contar con la presencia de otros miembros designados del personal que tengan las destrezas requeridas para confirmar que no se lleven a cabo acciones inapropiadas o sin autorización o sin contar con la debida capacitación y formación. Los procedimientos son definidos y documentados para todas las operaciones relacionadas con la ICP. Los procedimientos operacionales son revisados regularmente al surgir nuevos requerimientos operacionales.

27.3.3. Sanciones por acciones no autorizadas: Todo procedimiento no contemplado en el presente documento de DPC y PC) deberá contar con la aprobación expresa y por escrito de la alta dirección del PSC PROCERT y de SUSCERTE de lo contrario será considerado como acto de sabotaje a los fines internos del PSC PROCERT y será sancionado con despido justificado, por incumplimiento de las obligaciones que impone la relación de trabajo.

27.4. Procedimientos de control de seguridad.

27.4.1. Tipos de eventos registrados: EL PSC PROCERT, almacena registros electrónicos de eventos (logs) relativos a su actividad como PSC. Estos registros son almacenados de forma automática y electrónica y en los casos del acceso físico en formato papel y otros medios. Cada registro de eventos incluye datos relativos a la fecha y hora en que se produjo, número de serie, descripción del evento y el sistema o persona que lo origina. Los récords mínimos de auditoría que deben ser mantenidos incluyen:

- Eventos de los equipos que conforman la plataforma:
 - Instalación y configuración del sistema operativo.
 - Instalación y configuración de cualquier aplicación instalada en el equipo.
 - Instalación y configuración de la autoridad de certificación.
 - Instalación y configuración del módulo criptográfico.
 - Accesos o intentos de acceso al equipo.
 - Actualizaciones.
 - Realización de copias de seguridad
- Eventos del software de certificación:
 - Gestión de usuarios.
 - Gestión de roles.
 - Gestión de plantillas de certificados.
 - Lista de control de acceso (ACLs).
 - Gestión de certificados (todo lo contemplado en el ciclo su vida)
- Eventos relacionados con el acceso físico:
 - Acceso del personal al centro de datos.
 - Acceso del personal a los equipos y sistemas.

- Eventos de acciones correctivas:
 - Errores de hardware.
 - Errores de software.

27.4.2. Frecuencia de procesados de registros de logs: Los registros de auditoría se llevan a cabo en cualquier momento que se realice una operación en la raíz de certificación de la AC del PSC PROCERT, de lo contrario la raíz de certificación de la AC se mantiene fuera de línea. El personal de operaciones notifica a su administrador de seguridad cuando un proceso o acción causa un evento crítico de seguridad o discrepancia. A las entidades infraestructura de clave pública (ICP) subordinadas (cuando aplique) también se les requiere notificar cualquier evento que pueda causar un evento crítico de seguridad o discrepancia. En todo caso, la gerencia general y el consultor de tecnología decidirán los pasos a seguir.

27.4.3. Período de retención para los logs de auditoría: Los registros de Auditoría se retienen por un período de diez (10) años.

27.4.4. Protección de los logs de auditoría: El sistema de recolección de auditoría del PSC PROCERT es una combinación de procesos automáticos y procedimientos manuales desempeñados por la raíz de certificación de la AC del PSC PROCERT, los sistemas operativos y por el personal operacional. Por lo tanto, el sistema es mantenido mediante mecanismos de control de acceso y separación de roles con relación al software y el hardware que manejan la recolección automática y mediante procedimientos operacionales confidencialmente documentados, conocidos y seguidos por el personal de la AC del PSC PROCERT. Adicionalmente, la integridad de los eventos de auditoría se protege mediante la firma de cada evento con la clave privada de la persona que lleva cabo la acción.

27.5. Archivo de informaciones y registros: Todos los records de la ICP de la AC del PSC PROCERT referentes a la operación de sus servicios de certificación son archivados y retenidos por un período mínimo de veinte (20) años. El recurso de tiempo para la raíz de certificación de la AC del PSC PROCERT es verificado periódicamente de manera independiente y todos los records automatizados de la raíz de certificación del PSC PROCERT, están asociados a la hora y fecha de su ocurrencia. Los archivos de records se mantienen bajo estricto control de acceso y están sujetos a la inspección de auditores. Todos los archivos de records e información de identificación serán archivados directamente por la AR del PSC PROCERT requerirá a la AR que archive los records e información por un período de diez (10) años a partir de la fecha de expiración del certificado y hará sus mejores esfuerzos para que dicha cadena cumpla con sus obligaciones en esta materia. En todo caso los records pueden ser archivados en papel o en forma electrónica.

27.5.1. Tipo de informaciones y eventos registrados: El tipo de información y registro de eventos será el mismo contemplado en el aparte 27.4.1., del presente documento de DPC y PC.

- 27.5.2. Período de retención para el archivo: El período de retención para archivo será el mismo contemplado en el aparte 27.4.3., del presente documento de DPC y PC.
- 27.5.3. Protección del archivo: El método de protección de archivo será el mismo contemplado en el aparte 27.4.4., del presente documento de DPC y PC.
- 27.5.4. Requerimiento para el estampado de tiempo para el registro: Los procesos y pasos que deberán ser cumplidos por el PSC PROCERT para prestar el servicio de estampado de tiempo no se encuentran normados o desarrollados por la Superintendencia de SUSCERTE.
- 27.5.5. Sistema de repositorio de archivos de auditoría (interno vs externo): Cada uno de los equipos presentes en la plataforma de certificación posee un módulo para almacenar los logs de eventos, específicamente eventos de las aplicaciones, de los sistemas y de seguridad, incluyendo el aplicativo de certificación. Este registro de eventos permite auditar y verificar los intentos de accesos, los accesos y las operaciones dañinas, sean estas intencionales o no. El registro de eventos también es almacenado en dispositivos físicos de memoria en los cuales se hace el respaldo completo al inicio de operaciones
28. Cambio de claves: El esquema de operación del PSC PROCERT y su plataforma tecnológica de certificación se encuentran configurados para que el cliente genere su par de claves (pública y privada). Siempre y en todo caso el compromiso de clave derivará del mismo cliente pues el PSC PROCERT no genera el par de claves (pública y privada). En virtud de lo anterior, si el cliente extravía su clave privada, se deberá proceder a la emisión de un nuevo certificado y deberá cumplir el proceso de contratación del PSC a tales efectos. La clave pública siempre estará en el repositorio, de conformidad con lo señalado en el aparte 32.14 de presente documento de DPC y PC.
29. Recuperación en caso de desastre.
- 29.1. Procedimiento de gestión de incidentes y vulnerabilidades: El PSC PROCERT ha establecido un plan de continuidad de negocio y recuperación ante desastres (PRD) (AC-P-001), ante el evento de un eventual compromiso parcial o total de la ICP de la AC PROCERT. El plan de recuperación ante desastre es revisado periódicamente a la luz de los cambios riesgos en el ambiente. El plan de recuperación ante desastre está orientado a:
- Fallas/corrupción de recursos de computación;
 - Compromiso de la Integridad de la clave; y
 - Desastres naturales y terminación.

La alta dirección, representada por un director, el gerente general, el consultor de tecnología y los operadores de informática, deben tomar los correctivos y emprender las actividades necesarias para restablecer la plataforma tecnológica de certificación en el momento de presentarse un escenario de desastre. En el plan de continuidad de negocio y recuperación ante desastre (PRD) (AC-P-001), se especifica el procedimiento a realizar en cada uno de los

escenarios considerados como desastre y a continuación se mencionan las principales responsabilidades de cada uno de los cargos a la hora de ejecutarse el plan de recuperación: i) un director junto al gerente general declaran el escenario de desastre y aprueban la activación del plan de contingencia; ii) el consultor de tecnología gestiona, supervisa y apoya la ejecución de todas las actividades de recuperación del desastre; iii) Los operadores ejecutan las actividades de restauración del servicio.

29.2. Alteración de los recursos, hardware, software y/o datos: El PSC PROCERT ha establecido un plan de continuidad de negocio y recuperación ante desastres (PRD) (AC-P-001), ante el evento de un eventual compromiso parcial o total de la ICP. El plan de recuperación ante desastre es revisado periódicamente a la luz de los cambios riesgos en el ambiente.

29.3. Procedimiento de actuación ante la vulnerabilidad de la clave privada de una autoridad: El PSC PROCERT, aunque tiene previsto activar el HSM (para la firma de certificados) de forma local y solo en presencia del consultor de tecnología y el gerente general, considera como uno de sus escenarios de desastre el compromiso de su clave privada, y las acciones que serán puestas en marcha luego de detectar el mencionado compromiso son las siguientes:

- Cese inmediato del servicio de venta y generación de certificados electrónicos.
- Declaración el PSC PROCERT del escenario de desastre.
- Notificación a la SUSCERTE del compromiso de la clave, para la inmediata revocación del certificado del PSC PROCERT.
- Publicación del evento en la Página Web del PSC PROCERT.
- Notificación a los clientes del PSC PROCERT vía e-mail.
- Notificar a la compañía aseguradora que mantiene la fianza de operación del PSC.
- Analizar el motivo del compromiso y realizar un informe técnico detallando las razones por las que se vio comprometida la clave privada del PSC PROCERT.
- Acordar junto con la SUSCERTE las acciones a tomar para la reactivación del servicio de emisión de certificados.

29.4. Seguridad de las instalaciones tras un desastre natural o de otro tipo: El centro de datos desde donde opera la AC mantiene las pólizas o instrumentos emitidos por empresas de seguros solventes y reconocidas, a los efectos de mantener un respaldo en caso de ocurrencia de una contingencia que afecta la integridad física de la referida sede administrativa y pueda ofrecer de esa manera una garantía de su continuidad operacional.

30. Cese de actividad: El PSC PROCERT tiene contemplado en el supuesto que ocurra una cesación de operaciones, los siguientes supuestos:

- 30.1. Extinción por vencimiento de acreditación.
- Extinción por cese de operaciones.

- Extinción por revocación de acreditación. En este caso, y solo por razones comprobadas de incumplimiento, procederá la ejecución de la garantía solicitada por la SUSCERTE al momento de la acreditación
- Extinción derivada de aspectos tecnológicos.

En el caso de ocurrencia de cualquier de los supuestos antes indicados el PCS PROCERT, estará en la obligación de colocar a disposición de la SUSCERTE el repositorio de todos los certificados emitidos durante su gestión, incluyendo el estatus de cada uno de ellos.

31. Controles de seguridad técnica.

31.1. Generación e instalación del par de claves.

31.1.1. Generación del par de claves: El PSC PROCERT, genera su par de claves (pública y privada) utilizando un dispositivo de hardware criptográfico (HSM) que cumple con el FIPS 140-1 Nivel 3. El esquema de operación del PSC PROCERT y su plataforma Tecnológica de Certificación, se encuentran configurados para que el cliente genere su par de claves (pública y privada). Siempre y en todo caso el compromiso de clave derivará del mismo cliente pues el PSC PROCERT no genera el par de claves (pública y privada). En virtud de lo anterior, si el cliente extravía su clave privada, se deberá proceder a la emisión de un nuevo certificado y deberá cumplir el proceso de contratación del PSC a tales efectos. La clave pública siempre estará en el repositorio, de conformidad con en el presente documento de DPC y (PC).

31.1.2. Entrega de la clave privada: El esquema de operación del PSC PROCERT y su plataforma tecnológica de certificación, se encuentran configurados para que el cliente genere su par de claves (pública y privada) siempre y en todo caso el compromiso de clave derivará del mismo cliente pues el PSC PROCERT no genera el par de claves (pública y privada). En virtud de lo anterior, si el cliente extravía su clave privada o la misma se ve comprometida, se deberá proceder a la emisión de un nuevo certificado y deberá cumplir el proceso de contratación del PSC a tales efectos.

31.1.3. Entrega de la clave pública: El esquema de operación del PSC PROCERT se encuentra configurado para que el cliente genere su par de claves (pública y privada). Siempre y en todo caso el compromiso de clave derivará del mismo cliente pues el PSC PROCERT no genera el par de claves (pública y privada). Si el cliente extravía su clave privada se revoca el certificado anterior y debe proceder a la generación de un nuevo certificado. La clave pública siempre estará en el repositorio, de conformidad con lo señalado en el presente documento de declaración de prácticas de certificación (DPC) y política de certificados (PC).

31.1.4. Disponibilidad de la clave pública: El PSC PROCERT se encuentra en la obligación de mantener en su repositorio y disponible su clave pública, la cual cualquier cliente o parte interesada puede acceder a través de la página Web de PROCERT (<https://ura.procercert.net.ve/pscprocercert/cadena.p7b>).

31.1.5. Tamaño de las claves: Los módulos de la raíz de certificación de la AC y las claves tienen una longitud de al menos 4096 bits y utilizan el algoritmo ECDSA.

31.1.6. Parámetros de generación de la clave pública y verificación de la calidad: Los parámetros utilizados para la generación de las claves públicas cumplen con los requerimientos FIPS 140-2 Nivel 3. La generación del par de claves (pública y privada) que utiliza la plataforma de certificación del PSC PROCERT es un proceso sencillo, pero que requiere de precauciones especiales. A continuación, se describen los pasos a seguir para la generación del par de claves y cuáles son las precauciones que deben tomarse a fin de garantizar la protección de la clave privada:

- El usuario final debe ingresar a la página web del PSC PROCERT (<http://www.procert.net.ve>) presionar click sobre el enlace sistema de certificación (<https://www.procert.net.ve/sistemaAR/login.aspx>) y de esta forma ingresar al sistema de certificación.
- Allí debe de verificar que los datos contenidos están correctos, dicha solicitud está compuesta en cuatro (02) partes:

David Coronado

08-10-2024

Inicio

Crear Proceso

Firmar Documentos

Documentos Pendientes

Ver Mis Documentos

Imagen de Firma

Renovacion de Datos

Peticiones

Certificados

Cambiar Contraseña

Procert INT J-3883279-7

Copyright © 2023

Todos los Derechos Reservados

Solicitud de Certificado Online

Nombre

David

Apellidos

Coronado

Cédula

V-75737364

Correo electrónico

jose.tovar1205@gmail.com

Datos de Domicilio

Estado o Provincia

Distrito Capital

País

Venezuela

Dirección Fiscal

Caracas Quinta Crespor av sur4 ressiena piso 5 apto 5b

Generar

Información del Usuario: Esta sección contiene el nombre y apellido del usuario que fue suministrado al PSC PROCERT. Subject: Información general del usuario que, dependiendo del tipo de certificado, algunos campos serán obligatorios, a continuación, se enlista los campos y cuales son obligatorios por certificados

Tipo de Certificado	Nombre	Organización	Departamento	Título	Email	País	Estado	Dirección
Representante legal de empresa privada	✓	✓	✓	✓	✓	✓	✓	✓
Representante de empresa publica	✓	✓	✓	✓	✓	✓	✓	✓

Empleados de Empresas	✓	✓	✓	✓	✓	✓	✓	✓
Banca Electrónica	✓	✓	✓	✓	✓	✓	✓	✓
Funcionario Publico	✓	✓	✓	✓	✓	✓	✓	✓
Profesional Titulado	✓			✓	✓	✓	✓	✓
Persona Natural	✓				✓	✓	✓	✓
ocsp	✓	✓			✓	✓	✓	✓
Factura Electrónica	✓	✓			✓	✓	✓	✓
Firma de Transacción	✓	✓			✓	✓	✓	✓
Comercio Electrónico	✓	✓	✓	✓	✓	✓	✓	✓

Información del nombre alternativo: En esta sección debe de contener el número de RIF o C.I. del signatario. Opciones de clave: En esta sección se debe escoger el Proveedor de Servicios Criptográfico (CSP), es importante tomar en cuenta que, si el certificado se va a instalar en un Etoken criptográfico, los drivers de dicho dispositivo deben de estar instalados previamente en el equipo que se va a utilizar para generar el par de claves (pública y privada) del usuario. Posteriormente el usuario debe aceptar los términos y condiciones para habilitar el botón generar. Luego de presionar el botón generar el usuario tendrá la opción de proteger su clave privada con un nivel de seguridad alto utilizando una contraseña. Posterior a la aprobación de la solicitud por la autoridad de certificación del PSC PROCERT enviará al correo del usuario un link donde podrá descargar el certificado. El procedimiento de generación de par de claves mencionado garantiza la privacidad de la clave privada del usuario, ya que el usuario es quien la genera, el PSC PROCERT solo garantiza la vinculación del individuo con la clave pública, dicha clave pública está asociada a su vez a la clave privada.

31.1.7. Hardware/software de generación de claves: El software utilizado por el PSC PROCERT para la generación del par de claves y certificados es una combinación de la autoridad de certificación de Microsoft y software especializado de certificación electrónica. La AC utiliza un módulo criptográfico para almacenar de forma segura su clave privada. Dicho modulo criptográfico o HSM Luna marca Thales, posee certificaciones FIPS 140-1 y FIPS 140-2, y todas las especificaciones técnicas de este dispositivo de seguridad se indican a continuación:

- Algoritmos Criptográficos soportados.
 - Cifrado simétrico.
 - AES – Rijndael.
 - ArcFour (compatible con RC4).
 - CAST.
 - DES.
 - Triple-DES.
- Cifrado de Clave Pública.
 - DSA.
 - El Gamal.

- ECDSA.
- Mecanismos de Intercambio de Claves.
 - DH.
 - DES / DES3 XOR.
 - Funciones HASH y HMAC.
 - MD2.
 - MD5.
 - RIPEMD 160.
 - SHA-2.

Referencias: A los efectos de documentar y proveer información del hardware criptográfico utilizado por la AC, se señala la dirección web que se indica a continuación: <https://www.thales-esecurity.com/knowledge-base>. Adicionalmente, el módulo criptográfico utilizado por la AC soporta la generación de claves de 4096 bits y tiene la capacidad de firmar y cifrar.

31.1.8. Propósitos de utilización de claves: La Clave de privada del PSC PROCERT puede ser usada para:

- Firma de Certificados a las autoridades de certificación de pólizas.
- Firma de certificados establecidos en la presente DPC.
- Firma de listas de revocación de certificado.
- Firma de certificados para la certificación cruzada, aprobada por la SUSCERTE y la gerencia general y el consultor de tecnología de PROCERT.

31.2. Protección de la clave privada.

31.2.1. Estándares para los módulos criptográficos: El módulo criptográfico usado por la ICP del PSC PROCERT, está certificado para cumplir con los requerimientos de FIPS nivel 3. En el caso de la raíz de certificación de PROCERT, dicho modulo se mantiene fuera de línea.

31.2.2. Control “N” de “M” de la clave privada: La Clave privada del PSC PROCERT, se encuentra bajo control multipersona. Esta se activa mediante la inicialización del software de la AC por medio de una combinación de operadores de la AC, Administradores del HSM y usuarios del sistema operativo. Este es el único método de activación de dicha clave.

31.2.3. Custodia de la clave privada: La clave privada de la AC está protegida por un HSM. La AC ha establecido los pasos a seguir para la instalación del HSM, los mismos se detallan a continuación:

- Instalación de los drivers: Se deberá instalar los drivers correspondientes al HSM en el servidor de certificación.
- Instalación física
- Creación del Mundo de Seguridad.: Se creará el Mundo de Seguridad bajo los comandos establecidos y siguiendo los siguientes parámetros:

- Se crearán los perfiles y toles dentro del mundo de seguridad.
- 31.2.4. Copia de seguridad de la clave privada: El respaldo de la clave privada se realiza en dos (2) unidades de CD/DVD (principal y respaldo) selladas con un precinto y almacenadas en una caja de seguridad. La clave de cifrado de la raíz de certificación del PSC PROCERT solamente se respalda a los fines de recuperación ante Desastres.
- 31.2.5. Archivo de la clave privada: La clave privada de la AC se encuentra almacenada en un componente de hardware denominado HSM, el cual es el encargado de respaldarla y cifrarla. Tanto el respaldo como el cifrado son almacenados en una unidad de almacenamiento de datos, la cual el administrador de la AC se asegurará de mantener a resguardo en un lugar seguro y fuera del centro de datos.
- 31.2.6. Inserción de la clave privada en el módulo criptográfico: La AC ha establecido los parámetros y lineamientos bajo los cuales se hará la generación de claves, las mismas se detallan a continuación:
- Se generará el nuevo mundo de seguridad.
 - Se instalará la autoridad de certificación bajo la modalidad de Subordinada y se generará la petición de certificado.
 - La SUSCERTE firmará la solicitud del certificado del PSC PROCERT.
 - Se instalará y activará el certificado del PSC PROCERT.
- 31.2.7. Método de activación de la clave privada: Para la activación de la clave privada es necesario utilizar tarjetas inteligentes, requiere dos de cuatro tarjetas de administrador y una de dos tarjetas de operador, adicionalmente, es necesario el acceso al sistema operativo del servidor de certificación.
- 31.2.8. Método de destrucción de la clave privada: La clave privada de origen de la AC puede ser destruida retornando al HSM a su estado original de fábrica y borrando todos los símbolos de respaldo.
- 31.2.9. Ranking del módulo criptográfico: La AC utiliza un módulo criptográfico para almacenar de forma segura su clave privada. Dicho modulo criptográfico o HSM marca NCIPHER, modelo nShield PCI 500 TPS, F3 SEE Ready y posee certificaciones FIPS 140-1 y FIPS 140-2. Estos dispositivos se encuentran dentro de la categoría de hardware de alta seguridad, los cuales son utilizados por entidades bancarias y de seguridad de estado en todo el mundo, gozando de experiencia y seguridad comprobada.
- 31.3. Otros aspectos de la gestión del par de claves.
- 31.3.1. Archivo de la clave pública: La clave pública del PSC PROCERT es archivada según el formato PKCS#7, por un periodo de 10 años.
- 31.3.2. Períodos operativos de los certificados y período de uso del par de claves: El certificado del PSC PROCERT tendrá una validez de 10 años. Las firmas y los certificados electrónicos generados por el PSC

PROCERT tienen un ciclo de un (1) años contados a partir de la fecha de activación de la firma o certificado electrónico por parte de la AC de PROCERT. El par de claves asociado a cada firma o certificado electrónico tiene igualmente el mismo lapso de vigencia que la firma o certificado del que se trate.

31.4. Datos de activación.

31.4.1. Generación e instalación de datos de activación: La generación del par de claves (pública y privada) que utiliza la plataforma de certificación de la AC PROCERT es un proceso sencillo, pero que requiere de precauciones especiales. A continuación, se describen los pasos a seguir para la generación del par de claves y cuáles son las precauciones que deben tomarse a fin de garantizar la protección de la clave privada:

- La validación de la identidad del individuo se ejecuta por parte de la AR la cual le envía a la AC la información necesaria para que la creación del usuario dentro del sistema de y de esta forma garantizar la vinculación de identidad de la persona con su clave pública. El usuario final debe ingresar a la página web de PROCERT (<http://www.procert.net.ve>) y presionar click sobre el enlace Certificados Electrónicos, luego pulsar sobre el cuadro que señala el Sistema de certificación (<https://www.procert.net.ve/sistemaAR/login.aspx>), acceder y registrarse en el sistema de certificación.
- Luego de registrarse, debe ingresar al aplicativo de solicitud de certificados colocando su información de acceso (login y password) y validar su dirección de correo electrónico.
- Luego de validada su dirección de correo electrónico, el usuario deberá acceder al enlace certificados y realizar una petición de certificado, seleccionando el tipo de certificado (firma electrónica), ingresando la información personal solicitada, seleccionando el proveedor de servicios de cifrado (CSP) y presionando el botón Generar. Nota: Hay que tener mucha precaución con el CSP y el equipo y/o dispositivo donde se está generando la petición de certificado, ya que es allí donde va a quedar instalado el certificado.
- Al presionar el botón Generar se crean el par de claves (pública y privada), y automáticamente es enviada la petición de certificado a la autoridad de registro para que sea validada presencialmente la identidad del usuario que está realizando la solicitud.
- El procedimiento de generación de par de claves mencionado garantiza la privacidad de la clave privada del usuario, ya que el usuario es quien la genera, PSC PROCERT solo garantiza la vinculación del individuo con la clave pública, dicha clave pública está asociada a su vez a la clave privada.
- Una vez validada la identidad por la AR y generado el certificado por la AC, el cliente procede a descargar las firma o certificado electrónico en el repositorio de su computadora, aceptando la fuente de emisión del certificado.

- 31.4.2. Protección de datos de activación: La activación del certificado emitido es realizada utilizando el sistema de certificación del PSC PROCERT, limitándose en el equipo o dispositivo donde se hayan generado el par de claves.
- 31.5. Controles de seguridad del computador.
- 31.5.1. Requisitos técnicos específicos: El PSC PROCERT, ha definido una serie de controles de seguridad aplicables a los equipos informáticos, tales como el uso de los equipos, controles de acceso físico y lógico, planes de auditorías, autenticación y pruebas de seguridad.
- 31.5.2. Calificaciones de seguridad computacional: El PSC PROCERT, utiliza productos certificados, al menos, por el Nivel E3 de las normas ITSEC.
- 31.6. Controles de seguridad del ciclo de vida.
- 31.6.1. Controles de desarrollo de sistemas: El software AC usado por la ICP de PROCERT para la emisión de certificado y el manejo del ciclo de vida ha sido desarrollado de acuerdo con los requerimientos de la Criterios de Evaluación de Seguridad de tecnología de Información (ITSEC por sus siglas en inglés) Nivel E3. El HSM utilizado por la infraestructura de clave pública (ICP) y las AC que cumple con los requerimientos FIPS 140-2.
- 31.6.2. Controles de administración de seguridad: Los controles para el manejo de la seguridad se cumplen mediante una separación rígida de los roles del operador para cumplir los requerimientos de la política de seguridad establecida.
- 31.6.3. Calificaciones de seguridad del ciclo de vida: Durante todo el ciclo de vida de las claves se deben implementar controles de seguridad que permitan instrumentar y auditar cada fase de los sistemas de la AC del PSC PROCERT.
- 31.7. Controles de seguridad de la red: El hardware y software para la ICP de la AC son mantenidos “off-line” en una instalación de alta seguridad dentro de un exhaustivo control de seguridad y rigurosos controles de acceso interno. Se mantiene sofisticados sistemas de detección contra intrusos para notificar al personal de seguridad sobre cualquier violación a los controles de acceso. Adicionalmente, la raíz de certificación de la AC se mantiene fuera de línea y no se relaciona con ningún componente externo.
- 31.8. Controles de ingeniería de los módulos criptográficos: El PSC PROCERT utiliza módulos criptográficos (hardware y software) disponibles comercialmente y desarrollados por terceros. El PSC PROCERT únicamente utiliza módulos criptográficos con certificación FIPS 140-2, Level 3 (nShield F3) y Level 2 (nShield F2).
32. Perfiles de certificados LCR / OCSP.
- 32.1. Perfil del certificado: Los certificados del PSC PROCERT son emitidos conforme a las siguientes normas:

- RFC 6818: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, January 2013
- ITU-T Recommendation X.509 (2016): Information Technology – Open System Interconnection - The Directory: Authentication Framework
- ETSI TS 101 862 V1.3.3 (2006-01): Qualified Certificate Profile, 2006
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile, March 2004 (prevaleciendo en caso de conflicto la TS 101 862).

32.2. Número de versión: Como se indicó en el aparte 32.1., que precede, el número de versión del certificado es V3.

32.3. Extensiones del certificado: Las extensiones de los certificados del PSC PROCERT permiten codificar información adicional en los certificados. Las extensiones estándar X.509 definen los siguientes campos: i) SubjectKeyIdentifier; ii) AuthorityKeyIdentifier; iii) BasicConstraints; iv) Certificate Policies; v) KeyUsage; vi) LCRDistribucionPoint; vii) SubjectAlternativeName; y viii) AuthorityInformationAccess.

32.4. Identificadores de objeto (OID) de los algoritmos: El OID del algoritmo criptográfico utilizado por el PSC PROCERT es: SHA384 with ECDSA Encryption (1.3.132.0.34)

32.5. Formatos de nombres: El formato y significado asignado a los nombres en cada uno de las firmas y certificados electrónicos generados por el PSC PROCERT se encuentran detallados en el apartado 14 del presente documento de la DPC y PC.

32.6. Identificador de objeto (OID) de la PC: PSC PROCERT, utilizará la definición de política de asignación de OID's según el árbol privado de numeración asignado por la SUSCERTE.

32.7. Perfil de LCR / OCSP: La LCR es una lista de firmas y certificados electrónicos, en la cual concretamente, se muestran los números de serie de las firmas o certificados electrónicos revocados por una AC, los números de serie que han sido revocados ya no son válidos, y por ende el usuario no debe confiar en ningún certificado incluido en la LCR del sistema. Una LCR es un archivo que contiene: i) Nombre del emisor de la LCR; ii) Números de serie de la firma o certificado; iii) Fecha de revocación de las firmas o certificados, iv) La fecha efectiva y la fecha de la próxima actualización y v) la razón de la revocación. Dicha lista está firmada electrónicamente por la propia AC que la emitió.

Lista de revocación de certificados

General Lista de revocaciones

Certificados revocados:

Número de serie	Fecha de revocación
550000005838df4c2e6fcd300000...	miércoles, 2 de octubre ...

Entrada de revocación

Campo	Valor

Valor:

Aceptar

Cuando un usuario desea comprobar la validez de un certificado debe descargar e instalar la LCR actualizada desde los servidores de la misma autoridad de certificación (AC) que emitió la firma o certificado, al realizar esto, las firmas o certificados que se encuentren instalados en el computador en donde se halla instalado la LCR, automáticamente se validan, si los mismos se encuentran revocados, se invalidan; también se puede comprobar a través del número de serie ubicado en la LCR el status de algún otro certificado. Se comprueba la autenticidad de la lista gracias a la firma electrónica de la autoridad de certificación.

Nombre del campo	Valor
Versión	V2 (Número de versión del certificado).
Algoritmo de Firma:	Sha-384ECDSA (Algoritmo de Firma)
Datos del emisor	
CN	PROCERT SMIME ECC CA
O	Proveedor de Certificados PROCERT ITFB
C	VE (VENEZUELA)
Período de validez	
Última Actualización:	Fecha y hora emisión LCR.
Próxima Actualización:	Fecha próxima LCR.
Lista de certificados revocados	
Certificados Revocados	Contiene la lista de certificados revocados (número de serie y fecha de revocación).
Extensiones	
Identificación clave autoridad certificadora	Proporciona un medio para identificar la clave pública que corresponde a la clave privada utilizada para firmar una LCR (ID DE CLAVE)
Nombre alternativo del emisor	

Punto distribución LCR	http://www.procert.net.ve/ecc-crl/smime-ca.crl
Información del emisor	http://ocspsmime.procert.net.ve/ocsp
Política de certificados	http://www.procert.net.ve/dpc-pc/

El perfil correspondiente al OCSP se encuentra detallado en el aparte 23.9 y 23.10 del presente documento de la DPC y PC.

32.8. Auditoría de conformidad: En el caso de la raíz de certificación de la AC es supervisada y auditada anualmente por la SUSCERTE, la cual en cualquier momento y con la frecuencia que considere apropiada puede realizar auditorías exhaustivas o parciales para determinar si el manejo de la clave criptográfica de la AC cumple con las directrices de Ley para operar como PSC.

32.8.1. Frecuencia de los controles de conformidad para cada entidad: Las auditorías de control y seguimiento ordenadas por ley e impuestas por mandato de la SUSCERTE serán efectuadas anualmente; y mediante dichas auditorías se establecerá el nivel de cumplimiento del PSC PROCERT acerca de la normativa de Ley y técnica, nacional e internacional aplicable a todo PSC en operación. Todo PSC acreditado ante SUSCERTE debe realizar la auditoría anual de seguimiento si opta a la renovación de su acreditación para operación durante el año siguiente al proceso de auditoría.

32.8.2. Auditores: Las auditorías anuales serán efectuadas por el auditor seleccionado por el PSC PROCERT. El auditor seleccionado deberá estar acreditado ante el registro de auditores que mantiene la SUSCERTE.

32.8.3. Relación entre el auditor y la autoridad auditada: Entre el PSC PROCERT y el auditor seleccionado, solamente existe una relación comercial que no causa dependencia. El PSC PROCERT contratará la auditoría de seguimiento ordenada por la SUSCERTE y el auditor prestará el servicio con la obligación de generar un informe de cumplimiento, el cual entregará al PSC PROCERT y a la SUSCERTE, y de mantener en todo momento la confidencialidad de la información a la cual tuvo acceso durante el proceso de auditoría.

32.8.4. Tópicos cubiertos por el control de conformidad: Los tópicos cubiertos por la Auditoría de Cumplimiento incluyen:

- Seguridad física.
- Evaluación de tecnología.
- Administración de servicios CA.
- Investigación de personal.
- Documento de la de la DPC y la PC y otras políticas y documentos aplicables.
- Contratos.
- Protección de datos y consideraciones sobre privacidad.
- Planificación de recuperación ante desastres.

32.8.5. Acciones para tomar como resultado de una deficiencia: Todo punto u observación generado por el auditor acreditado ante la SUSCERTE respecto a la operación y generación de certificados del PSC PROCERT y que sea considerado como “disconformidad”, será sometido a plan de remediación y cumplimiento, el cual deberá establecer el cronograma y tiempo fijado para superar la “disconformidad”, en el supuesto que la misma sea declarada. Si el PSC PROCERT no supera o cumple con el proceso de remediación de la “disconformidad”, no podrá optar a la renovación de su acreditación como PSC y cesará operación.

32.8.6. Comunicación del resultado: Los resultados de las auditorias se consideran información comercial sensitiva. A menos que esté estipulado en el contrato, serán protegidos como información confidencial de acuerdo con la sección 32.9.2 de este documento de la DPC y la PC.

32.9. Requisitos comerciales y legales.

32.9.1. Aranceles: El decreto ley de mensajes de datos y firmas electrónicas establece la obligación del PSC PROCERT, de constituir garantías para su operación como organismo acreditado por ante la SUSCERTE. La normativa de la SUSCERTE fija un pago de tasa de ley a los fines de optar a la acreditación como PSC, el monto de la referida tasa es de MIL UNIDADES TRIBUTARIAS (1000 U.T.). Igualmente se solicita una fianza a favor de la SUSCERTE) cuyo monto es de CUARENTA Y UN MIL UNIDADES TRIBUTARIAS (41,000 U.T.). Dicha fianza se constituye a los fines de garantizar la continuidad de operación del PSC PROCERT y en el supuesto de cese de operación; situación en la cual la SUSCERTE asumirá el control y operación de la plataforma tecnológica del PSC PROCERT. Adicionalmente, la SUSCERTE establece la obligación para el PSC PROCERT de mantener garantía constituida en forma de póliza de seguro y a favor de los clientes usuarios de firmas o certificados electrónicos generados por el PSC PROCERT.

32.9.2. Responsabilidad financiera: Los límites de la responsabilidad del PSC PROCERT hacia sus clientes, está regulada mediante acuerdos contractuales con dichas clientes. La responsabilidad del PSC PROCERT para con los clientes, partes dependientes y cualquier otra entidad usuaria de firmas o certificados electrónicos generados por el PSC, está limitada contra reclamos de cualquier tipo, incluyendo los contractuales, ilegales, extra contractual y de naturaleza delictiva, en cada certificado en particular sin importar el número de transacciones, firmas electrónicas es o causas de acción que surjan o estén relacionadas con dicho certificado o cualquier servicio prestado con respecto a dicho certificado y en forma acumulativa. Todos y cada uno de los reclamos que surjan de la ICP con relación a un certificado (sin reparar en la entidad causante de los daños), estarán sujetos a los límites de responsabilidad aplicables a éstos de acuerdo con este documento de la DPC y PC. Sujeto a las limitaciones anteriores, el

límite de responsabilidad agregada de la AC PROCERT hacia todos los clientes, partes dependientes y cualquier otra entidad, ni por todo el período de validez de un certificado emitido por la AC (a menos que sea revocado o suspendido antes de su expiración), hacia todas las personas con relación a dicho certificado es de quince mil unidades tributarias (15.000 U.T.). En ningún caso la responsabilidad de la AC excederá el límite antes mencionado.

32.9.3. Política de confidencialidad.

32.9.3.1. Información confidencial: Toda la recopilación y uso de la información compilada por la AC PROCERT es realizada cumpliendo con la legislación de la venezolana y basándose en las distinciones suministradas en este documento de la política de certificación y DPC entre “Resumen de Información” e “Información de Identificación”. La información personal recopilada y usada por los proveedores de servicios de certificación operados por terceros deberá cumplir con la legislación sobre protección de datos aplicable. En ausencia de alguna legislación local, los PSC cumplirán con el estándar mínimo contemplado en este documento de la DPC y PC. En los casos cese de operaciones, se procederá a transferir a la SUSCERTE los datos personales y demás datos correspondientes en su condición de ente rector de los servicios de certificación electrónica. En todo caso, se debe buscar el almacenamiento y disponibilidad de dichos datos a los fines de mantener la condición de servicios de certificación a los clientes correspondientes. Los detalles sobre cómo PROCERT recopila, procesa y almacena datos personales se encuentran en la política de modelo de operación de la autoridad de registro (AR) de la autoridad de certificación (AC) del PSC PROCERT. En adición a lo antes expuesto, se señala que la información de identificación es la información obtenida para identificar positivamente una entidad y suministrar los servicios de certificación que ésta solicita. La información de identificación será tratada como información confidencial a menos que la entidad a la cual se refiere la información dé su consentimiento de manera explícita.

32.9.3.2. Información no confidencial: Tipos de información no considerados confidenciales.

- Resumen de información.
- Todos los certificados emitidos por la ICP del PSC PROCERT, para uso público pueden ser divulgados públicamente.
- Todos los Certificados emitidos por la AC PROCERT en su condición servicios de certificación a terceros también pueden ser divulgados públicamente.

32.9.3.3. Publicación de información sobre revocación o suspensión de un certificado: La LCR se constituye en un registro de

todos aquellos certificados que, habiendo cumplido su proceso de generación y asignación de Ley, son revocados cuando se encuentra comprometida su clave, por solicitud del cliente, por uso indebido del certificado, por causa imputable al cliente o por cese de operación de la AC. La LCR es publicada cada veinticuatro (24) horas en (www.procercert.net.ve). Todo proceso de revocación de certificado es informado por el PSC PROCERT vía correo electrónico al Cliente propietario del certificado electrónico. Dicha notificación es elaborada con copia a la SUSCERTE y se incluye en el depósito digitalizado mantenido por el PSC PROCERT.

32.9.3.4. Divulgación de información como parte de un proceso judicial o administrativo: La(s) razón(es) para la suspensión o revocación de un certificado pueden hacerse públicas de acuerdo con la ley aplicable o bajo la responsabilidad única y absoluta del PSC PROCERT. La información sobre suspensión de certificados será revelada solo al cliente propietario del certificado o a la SUSCERTE bajo requerimiento derivado de proceso judicial y bajo mandato de cumplimiento. Ningún documento o registro en poder de la AC o la AR del PSC PROCERT será entregado a las agencias oficiales salvo que ocurran algunos de los hechos señalados a continuación: i) se produzca debidamente una orden o solicitud judicial; ii) el representante oficial de la ley esté debidamente identificado; y iii) se cumpla con los demás procedimientos legales. Como principio general, ningún documento confidencial o registro almacenado por la AC y AR del PSC PROCERT es entregado a ninguna persona excepto donde: i) Se produzca una solicitud de información debidamente documentada (Ej. que haya cumplido con todos los procedimientos legales); y ii) La persona que requiere la información es una persona autorizada para hacerlo y está debidamente identificada. Los servicios de certificación prestados bajo la autoridad de terceros pueden ser objeto de este tipo de solicitudes de información, como evidencia civil o para propósitos de descubrimiento, relacionados con la AC del PSC PROCERT en cualquier jurisdicción donde los procedimientos legales apropiados se hayan cumplido.

32.10. Protección de la información privada/secreta.

32.10.1. Información considerada privada: El PSC PROCERT considerará información privada, a tenor de lo dispuesto en la Constitución de la República Bolivariana de Venezuela, la siguiente: i) nombres y apellidos; ii) número de cédula de identidad y RIF; iii) Direcciones y datos telefónicos del cliente; y iv) datos suministrados en el proceso de contratación de firma o certificado electrónico.

- 32.10.2. Información considerada no privada: Tipos de información no considerados confidenciales: i) resumen de información; ii) todos los certificados emitidos por la ICP para uso público pueden ser divulgados públicamente; y iii) todos los certificados emitidos por la AC en su condición servicios de certificación a terceros también pueden ser divulgados públicamente.
- 32.10.3. Responsabilidades de proteger la información privada/secreta: El PSC PROCERT tiene la obligación de mantener a resguardo la información suministrada por los clientes contratantes de firmas o certificados electrónicos generados por el PSC PROCERT. A tales fines, se mantendrán los datos bajo archivo electrónico con certificados de seguridad asociados al acceso de la misma. El acceso a la información de los clientes estará limitado al representante de la AR y al Gerente General del PSC PROCERT.
- 32.10.4. Prestación del consentimiento en el uso de la información privada/secreta: La información dispuesta en archivos por el PSC PROCERT será manejada como información confidencial y la misma no será suministrada a terceros distintos al cliente propietario de la firma o certificado electrónico, salvo que medie aprobación expresa y autenticada en notaría pública por parte del cliente cuya información se trate, autorización realizada por escrito vía correo electrónico firmado o certificado por el cliente propietario de la firma o certificado electrónico o derivado de mandato judicial impuesto por Tribunal y derivado de causa en proceso.
- 32.10.5. Comunicación de la información a autoridades administrativas y/o judiciales: Respecto a la comunicación de la información, serán seguidos y aplicables los principios y requerimientos señalados en el aparte 32.9.2.4 que precede y forma parte del presente Documento de la DPC y la PC.
- 32.11. Derechos de propiedad intelectual.
- 32.11.1. Condición general: Excepto por los componentes que pueden ser propiedad intelectual de Terceros, todos los derechos de propiedad intelectual, incluyendo los derechos de autor en todos los directorios de certificados, LCR y certificados; a menos que explícitamente se indique lo contrario, todas las prácticas, política, los documentos operacionales y de seguridad referentes a la ICP del PSC PROCERT (electrónicos o no) así como los contratos, le pertenecen y seguirán siendo propiedad de PROCERT. Mediante los contratos correspondientes para la prestación de servicios de certificación, PSC PROCERT podrá otorgar una licencia a terceros para el uso de certificados, LCR y otras prácticas autorizadas y documentos de política en la medida que lo requieran para la prestación de servicios de certificación de acuerdo con el presente documento de la DPC y la PC.
- 32.11.2. Claves pública y privada: Todos los derechos de propiedad intelectual de las claves pública y privada generadas estarán

amparados por la entidad por la cual dichas claves fueron generadas o por la entidad designada por esta. Los servicios de certificación operados bajo la autoridad de clientes finales no obtendrán ningún derecho en lo absoluto en relación con los certificados, su contenido, formato o estructura.

32.11.3. Certificado: En todo momento PSC PROCERT se reserva el derecho de suspender o revocar cualquier certificado de acuerdo con los procedimientos y las políticas establecidas en el presente documento de la DPC y PC.

32.11.4. Nombres distinguidos: Los derechos de propiedad intelectual en nombres distinguidos y números de identificación de clientes no son responsabilidad del PSC PROCERT a menos que se especifique lo contrario en un contrato o acuerdo.

32.11.5. Propiedad intelectual: La propiedad intelectual del presente documento de la DPC y PC, así como de toda la información, publicaciones y documentos generados por el PSC PROCERT y contenidos o no dentro de su página web (www.procert.net.ve), son propiedad exclusiva del PSC PROCERT.

32.12. Representaciones y garantías: El PSC PROCERT mantiene un ejercicio autónomo como sociedad mercantil, respecto a sus marcas registradas y derechos de autor tutelados. Adicionalmente el PSC PROCERT mantiene acuerdos de representación con distintas empresas de tecnología de la información, seguridad informática y certificación electrónica, así como proveedores de hardware criptográfico. Las garantías asociadas a los productos que mercadea y vende el PSC PROCERT distinto a firmas o certificados electrónicos, será tramitada por el PSC PROCERT y cumplida ante sus clientes nacionales.

32.13. Obligaciones y responsabilidad civil.

32.13.1. Obligaciones de la autoridad de registro (AR): La AR del PSC PROCERT asume bajo el presente documento, el cumplimiento de una serie de requerimientos técnicos, legales y procedimentales, los cuales se señalan a continuación:

- Acatar y cumplir los mandatos de la Constitución de la República Bolivariana de Venezuela, del decreto ley sobre mensajes de datos y firmas electrónicas (LSMDFE), su reglamento (RLSMDFE) y de los demás cuerpos normativos, leyes, decretos, reglamentos o resoluciones gubernamentales que sean sancionados y publicados en gaceta oficial y que regulen la materia de certificación electrónica o de autoridad de certificación electrónica y que sean de obligatorio cumplimiento. Acatar las directrices y normativas técnicas emanadas de la SUSCERTE.
- Cumplir y mantener vigente los recaudos y requisitos requeridos para la acreditación como proveedor de servicios de certificación electrónica bajo los mandatos del decreto ley sobre mensajes de datos y firmas electrónicas (LSMDFE), su reglamento (RLSMDFE)

o los cuerpos normativos que los sustituyan y regulen la actividad de las autoridades de certificación.

- Presentar, mantener y cumplir con la vigencia de la póliza de seguro requerida por la SUSCERTE para operar una autoridad de certificación electrónica.
- Cumplir los contratos de prestación de servicios de certificación mantenidos con los clientes de la autoridad de certificación.
- Mantener y actualizar la documentación del PSC PROCERT.
- Publicar en la página web (www.procert.net.ve) el documento de la (DPC y PC, la información sobre LCR y la política de vida de certificados del PSC PROCERT, así como toda la documentación que sea de obligatorio cumplimiento a tenor de lo dispuesto en el decreto ley sobre mensajes de datos y firmas electrónicas o la normativa emanada de la SUSCERTE.
- Mantener y asegurar la confidencialidad de la información suministrada por los clientes usuarios del servicio de certificación electrónica. La única excepción de confidencialidad será derivada de requerimiento judicial o legal de información de los clientes por parte de una autoridad judicial legítima y competente para realizar el requerimiento de información y siempre derivado de procedimiento legal que garantice la debida notificación del cliente propietario de la información, con el fin de mantener la protección a la intimidad prevista en la Constitución de la República Bolivariana de Venezuela.
- Mantener un registro y archivo de las contrataciones de servicios del PSC PROCERT por un lapso de diez (10) años contados a partir de la fecha de suscripción de cada uno de los contratos para la adquisición de certificados de certificación electrónica.
- Mantener y actualizar la documentación que sea de obligatorio cumplimiento a tenor de lo dispuesto en el decreto ley sobre mensajes de datos y firmas electrónicas o la normativa SUSCERTE.
- Verificar que los signatarios clientes de PROCERT envíen toda la documentación necesaria según el tipo de certificado electrónico que deseen adquirir.
- Validar que la información entregada por el signatario sea correcta.
- Acreditar a todos aquellos signatarios que cumplan con los requisitos establecidos por el PSC PROCERT.
- Identificar y proponer mejoras en el proceso de acreditación, con el fin de facilitar el proceso de acreditación de los signatarios.
- Cumplir las políticas de empresa en materia de informática, administración y recursos humanos.
- Cumplir la normativa laboral y demás leyes de corte social que regulen la relación entre el PSC PROCERT y sus trabajadores.
- Cumplir las normas legales aplicables a la materia de certificación electrónica y el marco legal aplicable a la gestión regular del PSC PROCERT.

32.13.2. Obligaciones de la autoridad de certificación (AC): El PSC PROCERT asume bajo el presente documento el cumplimiento de una serie de

requerimientos técnicos, legales y procedimentales, los cuales se señalan a continuación:

- Acatar y cumplir los mandatos de la Constitución de la República Bolivariana de Venezuela, del decreto ley sobre mensajes de datos y firmas electrónicas (LSMDFE), su reglamento (RLSMDFE) y de los demás cuerpos normativos, leyes, decretos, reglamentos o resoluciones gubernamentales que sean sancionados y publicados en gaceta oficial y que regulen la materia de certificación electrónica o de autoridad de certificación electrónica y que sean de obligatorio cumplimiento. Acatar las directrices y normativas técnicas emanadas de la SUSCERTE.
- Cumplir y mantener vigente los recaudos y requisitos requeridos para la acreditación como proveedor de servicios de certificación electrónica bajo los mandatos del decreto ley sobre mensajes de datos y firmas electrónicas (LSMDFE), su reglamento (RLSMDFE) o los cuerpos normativos que los sustituyan y regulen la actividad de las autoridades de certificación.
- Presentar, mantener y cumplir con la vigencia de la póliza de seguro requerida por la SUSCERTE para operar una autoridad de certificación electrónica.
- Cumplir los contratos de prestación de servicios de certificación mantenidos con los clientes de la autoridad de certificación.
- Mantener y actualizar la documentación del PSC PROCERT, en especial el documento de la DPC y la PC, la LCR.
- Publicar en la página web (www.procort.net.ve) el documento de la DPC y la PC, la información acerca de la LCR, así como toda la documentación que sea de obligatorio cumplimiento a tenor de lo dispuesto en el decreto ley sobre mensajes de datos y firmas electrónicas o la normativa emanada de la SUSCERTE.
- Cumplir y asegurar la ejecución de auditorías de cumplimiento anuales por parte de auditores acreditados ante la SUSCERTE.
- Mantener y asegurar la confidencialidad de la información suministrada por los clientes usuarios del servicio de certificación electrónica. La única excepción de confidencialidad será derivada de requerimiento judicial o legal de información de los clientes por parte de una autoridad judicial legítima y competente para realizar el requerimiento de información y siempre derivado de procedimiento legal que garantice la debida notificación del cliente propietario de la información, con el fin de mantener la protección a la intimidad prevista en la Constitución de la República Bolivariana de Venezuela.
- Mantener un registro y archivo de las contrataciones de servicios de certificación electrónica por un lapso de diez (10) años contados a partir de la fecha de suscripción de cada uno de los contratos para la adquisición de certificados de certificación electrónica.
- Mantener y renovar el contrato de prestación de servicios con el centro de datos desde donde opera la plataforma de certificación de la AC PROCERT.

- Mantener y actualizar la documentación que sea de obligatorio cumplimiento a tenor de lo dispuesto en el decreto ley sobre mensajes de datos y firmas electrónicas o la normativa emanada de la SUSCERTE.

32.13.3. Obligaciones de los terceros de buena fe: Los clientes usuarios finales de certificados electrónicos emitidos por la AC, así como los terceros de buena fe, deben cumplir las condiciones siguientes:

- Acceder la página web del PSC PROCERT (www.procert.net.ve) y activar los botones de compra de certificados electrónicos.
- Seleccionar el tipo de certificado que desea el cliente.
- Leer y aceptar el contenido del contrato de prestación de servicios de certificación.
- Leer y aceptar las prácticas de certificación del PSC PROCERT.
- Cumplir y completar bajo fe de juramento el ingreso de datos y contactos de personas jurídicas o naturales, según sea el caso.
- Cancelar electrónicamente el importe de costo del certificado electrónico.
- Generar sus claves criptográficas.
- Cumplir con la remisión de información soporte de sus datos y contactos, en original o copia certificada al casillero postal señalado en la página web del PSC PROCERT (www.procert.net.ve).
- Asistir a la entrevista fijada por la AR de para la validación de datos y contactos del cliente.
- Cumplir con el uso contratado y aceptado del certificado electrónico adquirido por el cliente.
- Asistir a las oficinas administrativas del PSC PROCERT dentro de las cuarenta y ocho (48) horas siguientes a la revocación y publicación del certificado del cliente en la LCR de la AC PROCERT.
- Verificar los costos asociados al registro, renovación de los certificados en la Página Web (www.procert.net.ve).
- En todos los casos, al aceptar o recibir el certificado emitido a éste, el cliente garantiza lo siguiente:
 - Que los datos contenidos en el certificado son exactos.
 - Confiar en el contenido y uso del certificado electrónico.
 - Que la clave criptográfica privada asociada con la clave pública contenida en el certificado no ha sido comprometida.
 - Que sólo usará el par de clave criptográfica y los certificados electrónicos de acuerdo con los usos autorizados para el tipo y/o clase correspondiente;
 - Que ejercerá el cuidado razonable para evitar el uso sin autorización de la clave criptográfica privada asociada a la clave pública contenida en el certificado;
 - Que el cliente cumplirá con las obligaciones tributarias asociadas a la venta del certificado electrónico, fijada por la legislación que regula la materia de impuestos, tasas

o contribuciones dentro de la República Bolivariana de Venezuela.

- Notificará a otros clientes usuarios del certificado, a la AC y a otros Proveedores de Servicios de Certificación que procesaron su emisión (Ej. Autoridad de Registro autorizada), previo a la expiración del Certificado, lo siguiente:
 - Que la clave privada ha sido extraviada, robada, o está potencialmente comprometida;
 - Que ha perdido el control de su clave privada debido a que su contraseña ha sido comprometida o por otra razón;
 - Inexactitud o cambios al contenido del certificado; y/o
 - Que el cliente final desea suspender o revocar un certificado por cualquier razón que considere apropiada.
- Todas los clientes que deseen confiar en la ICP del PSC PROCERT, las LCR, las cadenas de certificados, el presente documento de la DPC y la PC, pólizas de certificado u otros servicios de certificación o cualquier otra información publicada por el PSC PROCERT se les exige estar de acuerdo con los contratos de adquisición de firmas electrónicas y certificados electrónicos que a tales efectos hayan suscrito en la página web (www.procort.net.ve) y en adición asumir las obligaciones siguientes:
 - Verificar la validez, suspensión o revocación del certificado, utilizando información actualizada sobre el estado del certificado en la LCR.
 - Tomar en cuenta cualquier limitación sobre el uso y límites de responsabilidad del certificado;
 - Confiar en las Firmas Electrónicas y Certificados solamente cuando dicha confianza sea razonable. Al considerar la viabilidad de la dependencia, los aspectos a tomar en cuenta incluirán si:
 - La Firma Electrónica fue creada durante el período de validez del certificado
 - La Firma Electrónica puede verificarse exitosamente
 - Todas las huellas digitales de la clave pública de los certificados dentro de las cadenas de certificados correspondientes son verificadas exitosamente
 - Los certificados en la cadena de certificados son validados exitosamente
 - No existen circunstancias adicionales que puedan afectar la confiabilidad de la firma electrónica, certificado, cadena de certificado o LCR.

32.13.4. Obligaciones del repositorio: El PSC PROCERT se encuentra en la obligación de mantener en su repositorio y disponible su clave pública, la cual cualquier cliente o parte interesada puede acceder a través de la página Web (<https://www.procort.net.ve/>). Adicionalmente, el PSC PROCERT, mantendrá accesible todos sus certificados emitidos, incluyendo la información de su estatus.

32.13.5. Renuncia de garantías: El PSC PROCERT cuenta con garantías constituidas a favor de la SUSCERTE y de los clientes propietarios de firmas o certificados electrónicos generados por el PSC PROCERT. La renuncia de garantía no será aplicable en la mejor salvaguarda de los clientes y de la SUSCERTE.

32.14. Limitación de responsabilidades.

32.14.1. Límites de responsabilidad y garantía limitada: El enfoque de la AC en cuanto al uso de las Infraestructuras clave pública, certificados y firmas electrónicas es permitir a organizaciones grandes y pequeñas, así como a las personas, que se beneficien de estas tecnologías de la manera menos agobiante y más eficiente. Para lograr esto, la AC suministra los servicios de certificación descritos en este documento de la DPC y PC. El presente documento de la DPC y PC contempla las garantías suministradas por PROCERT, las cuales cubren la seguridad y regulaciones procedimentales que proveen varios niveles de seguridad y manejo del riesgo (de bajo a alto). La AC sigue los procedimientos establecidos en las referidas garantías y al hacerlo no pretende suministrar un cien por ciento de seguridad, lo que resulta imposible, con las condiciones de operación de los servicios de certificación. Al hacerlo, la AC simplemente busca incrementar el nivel general de seguridad. Por lo tanto, PSC PROCERT asume la responsabilidad del cumplimiento de los procedimientos y las medidas de seguridad descritas en las garantías.

32.14.2. Deslinde de responsabilidades: El PSC PROCERT declara que no asumirá la responsabilidad de datos y procedimientos que no se encuentren contemplados y señalados en la norma legal aplicable decreto ley sobre mensajes de datos y firmas electrónicas (LSMDFE), el reglamento (RLSMDFE) y la normativa de la SUSCERTE, dentro de esos procedimientos, garantías y procesos se enuncian los siguientes:

- La de alcanzar resultados específicos.
- De comerciabilidad o idoneidad para un propósito específico,
- Con relación a la exactitud o confiabilidad de la información contenida en los Certificados que no sean suministrados y/o verificados por la AR.
- Que no están relacionadas con los temas cubiertos por este Documento de la DPC y PC.
- Sobre la responsabilidad o estabilidad comercial o financiera de terceros que suministren los servicios de certificación bajo su propia autoridad o usando o dependiendo de los servicios de certificación, en los casos de doble certificación;
- Sobre la validez jurídica, la capacidad de satisfacer requerimientos formales o el estatus de prueba de las firmas electrónicas, certificados o claves criptográficas y
- Con relación a los asuntos fuera del control razonable de la AC.
- Si la AC es responsable de su incumplimiento con las garantías o por cualquier otra razón, se procederá la indemnización contemplada en la fianza establecida por la SUSCERTE, no

obstante se observará en todo momento que el pago de daños excesivos que se pretendan fijar no aplicarán para aquellas actividades que no están directamente relacionadas con las condiciones de los servicios de certificación (de la misma manera que una autoridad pública no puede ser responsable por lo que una persona haga con una “Firma Electrónica”). La AC por lo tanto requiere que los miembros de la comunidad de la infraestructura de clave pública de PROCERT consientan con el hecho que PROCERT no asume responsabilidad por ningún tipo de daños que surjan de las circunstancias descritas más abajo (incluyendo daños especiales, consecuentes, incidentales, indirectos o punitivos), sin importar que haya sido notificada de ellos (o de su potencialidad) o no, o si éstos son razonablemente previsibles o no.

- Transacciones subyacentes entre los clientes y terceros, incluyendo las partes dependientes;
- Los servicios y/o productos de Terceros (incluyendo el hardware y software) que interactúan o usan los servicios de certificación, certificados, firmas electrónicas, etc.;
- Si existe un retraso, mutilación, o pérdida u otros errores en relación con los datos o documentos mientras son creados, almacenados o comunicados;
- Dependencia inaceptable de un Certificado, una firma electrónica, una clave criptográfica o par clave, o los servicios de certificación a los cuales se refiere esta política de certificación;
- Incumplimiento de terceros (incluyendo miembros de la comunidad de ICP de PROCERT) con protección de datos local o legislación sobre privacidad, legislación sobre protección al consumidor o cualquier otro cumplimiento legislativo o regulatorio requerido por la jurisdicción local; o
- Cualquier daño indirecto o consecuente, pérdida de utilidades, pérdida plusvalía, pérdida de ahorros estimados, pérdida de ganancias, pérdida de negocios, interrupción de negocios; o pérdida de información.
- Para mayor protección de los riesgos relacionados con la condición de servicios de certificación y para garantizar la estabilidad a largo plazo de la ICP, el monto de cualquier daño reconocido también está limitado bajo las condiciones fijadas en la póliza de seguro requerida por la SUSCERTE para la operación del PSC PROCERT.

32.14.3. Limitaciones de pérdidas: Los límites de la responsabilidad del PSC PROCERT hacia los clientes, está regulada mediante acuerdos contractuales con dichas clientes. Como referencia a estos contratos se incorporan este documento de la DPC y PC y las demás políticas de acreditación elaboradas por el PSC PROCERT y referidas en la Política de Seguridad de la Información de ésta. A menos que se haya acordado explícitamente o se haya incorporado explícitamente en una firma electrónica o certificado, la responsabilidad de PROCERT para con los clientes, proveedores o parte interesada, está limitada contra reclamos de cualquier tipo, incluyendo los contractuales, ilegales, extra contractual y de naturaleza delictiva, en cada certificado en particular sin importar el número de transacciones, firmas electrónicas o causas

de acción que surjan o estén relacionadas con dicho certificado o cualquier servicio prestado con respecto a dicho certificado y en forma acumulativa. Todos y cada uno de los reclamos que surjan de la ICP con relación a una firma electrónica o certificado (sin reparar en la entidad causante de los daños o en la entidad que emitió el certificado o suministró los servicios de certificación), estarán sujetos a los límites de responsabilidad aplicables a éstos de acuerdo con este documento de la DPC y PC. La responsabilidad máxima por certificado de la ICP del PSC PROCERT, se establecerá en el certificado correspondiente. Este límite de responsabilidad por certificado aplicará sin reparar en el número de transacciones, firmas electrónicas o causas de acción que surjan o estén relacionadas a dicho certificado o cualquier servicio suministrado con respecto a dicho certificado y sobre una base acumulativa. sujeto a las limitaciones anteriores, el límite de responsabilidad agregada de la AC del PSC PROCERT hacia todos los clientes, partes dependientes y cualquier otra entidad que no sean entidades ICP subordinadas, ni por todo el período de validez de un certificado emitido por la AC del PSC PROCERT (a menos que sea revocado o suspendido antes de su expiración), hacia todas las personas con relación a dicho Certificado es de quince mil unidades tributarias (15.000 U.T.). En ningún caso la responsabilidad del PSC PROCERT excederá el límite antes mencionado.

- 32.15. Indemnizaciones: Toda indemnización será producto de un proceso de investigación y análisis o de resolución de conflictos conforme al aparte 32.20 del presente documento y donde de forma comprobada se determine la responsabilidad del PSC PROCERT derivada de negligencia o impericia.
- 32.16. Plazo y finalización.
- 32.16.1. Plazo: Todo cliente que guarde o mantenga reclamo en contra del PSC PROCERT, deberá notificarlo en el más corto plazo y dentro de las dos (2) semanas siguientes a la ocurrencia del hecho considerado como fundamento o base de reclamo. Todo reclamo será tramitado y guardará relación directa con el período de vigencia de la firma o certificado electrónico generado por el PSC PROCERT. No serán tramitados reclamos luego de vencido el período de vigencia de una firma o certificado electrónico.
- 32.16.2. Finalización: Todo reclamo generado por cliente propietario de firma o certificado electrónico deberá ser tramitado y sustanciado por el PSC PROCERT, manteniendo evidencia escrita de cada proceso. El acuerdo o finalización de cada reclamo producirá un documento de acuerdo entre el PSC PROCERT y el cliente que corresponda, dejando sentado la solución al reclamo, la fecha y la conformidad y finiquito de Ley otorgado por el cliente del cual se trate.
- 32.17. Notificaciones: A menos que explícitamente se indique lo contrario en este documento de la DPC y la PC, las notificaciones deben hacerse ya sea mediante un mensaje electrónicamente firmado que pueda ser verificado con un certificado capaz de ser validado dentro de la iICP del PSC PROCERT o enviado a través de correo registrado o servicios de correo similares que

suministren un recibo indicando la entrega. En ambos casos, la notificación será efectiva a partir del momento en que se reciba un acuse de recibo digitalizado o un recibo de correo regular indicando la entrega firmada por la persona o entidad que envía la notificación. Si no es recibido dentro de las cuarenta y ocho (48) horas laborables a partir del momento en que supuestamente debía ser recibido por la AC del PSC PROCERT, se considerará que la notificación no ha sido recibida por la AC del PSC PROCERT. Las notificaciones, de acuerdo con el párrafo anterior deben ser enviadas a la siguiente dirección de correo electrónico o postal:

Proveedor de Certificados PROCERT ITFB, C.A.
Multicentro Empresarial del Este, Núcleo B, Torre Libertador,
Piso 13, Oficina B-132, Municipio Chacao, Caracas
E-mail: contacto@procert.net.ve
Código Postal 1063
Teléfono máster: +58-0212-2674880
Fax: +58-0212-2671270.

32.18. Modificaciones.

32.18.1. Procedimiento de especificación de cambios: El proceso de especificación de cambios de la DPC será efectuado de conformidad con lo señalado en numeral 36 del presente documento de la DPC y PC.

32.18.2. Procedimientos de publicación y notificación: El proceso de publicación y notificación de los cambios efectuados la documentación del PSC PROCERT que requiera una publicación en su sitio web (www.procert.net.ve) de conformidad con los lineamientos impuestos por la SUSCERTE deberá cumplir previamente los pasos contemplados en el aparte 32.22 del presente documento, contar con la aprobación de la SUSCERTE para proceder a su publicación y notificación a los clientes de la actualización vía correo electrónico. Internamente el PSC PROCERT dejará constancia acerca de cada modificación realizada a su documentación a través del uso del formato para ajuste de documentos (AC-F-0001).

32.18.3. Procedimiento de aprobación de la DPC: El proceso de ajuste de la DPC será efectuado de conformidad con lo señalado en el aparte 32.22 del presente documento de la DPC y PC.

32.19. Resolución de conflictos.

32.19.1. Resolución extrajudicial de conflictos: El PSC PROCERT y el cliente contratante reconocen que la solución pronta y equitativa de las controversias que puedan producirse en relación con la operación, generación o venta de la firma y certificados electrónicos, redundará tanto en sus propios intereses como en la ejecución del servicio contratado. A este fin, manifiestan su decisión de realizar todos los esfuerzos posibles para resolver todas las controversias que puedan plantearse mediante negociación a los niveles pertinentes. Si la controversia no se ha resuelto a través de la negociación antes referida, dentro de los quince (15) días hábiles después de iniciada la

misma, entonces, a solicitud del usuario contratante se someterá la controversia a la SUSCERTE), en virtud de lo establecido en el numeral 13 del artículo 22 el Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas. La solución alcanzada con la mediación de la SUSCERTE y aceptada por las partes, será vinculante y de obligatorio cumplimiento. El Usuario estará igualmente en libertad de acudir al organismo encargado de la protección, educación y defensa del usuario conforme a la Ley que regula la materia. En caso de no llegar a ningún acuerdo quedará libre la vía de reclamo por proceso ordinario.

32.19.2. Jurisdicción competente.

En el supuesto de no haber sido resueltos los posibles conflictos existentes de conformidad con lo establecido en el aparte 32.19.1. que precede, el cliente contratante quedará en libertad de acudir a la vía ordinaria de juicio, siendo la Jurisdicción competente la de los tribunales del área metropolitana de Caracas.

32.20. Legislación aplicable: Lo no previsto en el presente documento de la DPC y la PC, será regulado de conformidad con lo establecido en la normativa legal vigente y aplicable a la materia dentro de la República Bolivariana de Venezuela.

32.21. Conformidad con ley aplicable: Todos los procesos, procedimientos, información técnica y legal contenida en el presente documento de la DPC y la PC, se encuentra en un todo elaborada y de conformidad con lo establecido en el decreto ley sobre mensajes de datos y firmas electrónicas y las normas de rango sublegal emanadas de la SUSCERTE.

32.22. De los ajustes al documento: En todo caso los ajustes a la documentación requerida por la SUSCERTE para la operación de un PSC serán realizados en cada oportunidad que ocurra un cambio en el marco normativo y legal aplicable a los PSC, cuando ocurra un cambio técnico que justifique el ajuste o cambio, cuando sea requerido por la SUSCERTE o cada seis (6) meses.

32.22.1. Mecanismo de desarrollo del documento: El presente documento de la DPC y la PC se encuentra desarrollado sobre la base de la normativa de acreditación aplicable a los interesados a convertirse en PSC. Dicha normativa de acreditación es dictada y emitida por la SUSCERTE. Adicionalmente el presente documento de la DPC y la PC cumple con los requerimientos de la normativa internacional aplicable al área de certificación electrónica.

32.22.2. Mecanismo para ajuste del documento: Los cambios en el decreto ley de mensajes de datos y firmas electrónicas, su reglamento, la normativa de la SUSCERTE o de la normativa internacional vinculante y exigida para la operación de los PSC, que contemplen cambios sustanciales en los procesos de seguridad y operación, los cuales incluyan variación de los procedimientos y actividades de los PSC producirán una revisión del presente Documento, con el fin de ajustar los procesos y procedimientos a los estándares y normativa

aplicable y aprobada por SUSCERTE para la operación de los PSC. Todo ajuste al presente documento de la DPC y la PC será producto del trabajo del equipo técnico y legal del PSC PROCERT y requerirá contar para su implantación, con la aprobación de alta dirección, conforme a lo señalado en el aparte 32.22.3. del presente aparte. El proceso de ajuste será documentado y realizado conforme al documento de la política de documentación y gestión documental (AC-PO-0002).

32.22.3. Mecanismo para aprobación de los ajustes al documento: Todo ajuste o modificación del documento de la DPC y la PC, deberá contar con la aprobación de la alta dirección del PSC PROCERT, ser documentada y constar por escrito, señalando el número de edición y revisión, fecha de elaboración, fecha de aprobación y la firma del representante de la alta dirección que aprueba el ajuste o modificación. Se documentará el ajuste o modificación y su aprobación conforme al documento de la política de documentación y gestión documental (AC-PO-0002).

33. Marco legal y normativo.

- Decreto ley de mensaje de datos y firmas electrónicas y su reglamento.
- Normativa de la superintendencia de servicios de certificación electrónica (SUSCERTE).
- Normativa PROCERT.
- Estándar internacional ITU- T X.509 V3.
- Estándar Internacional ITU-T X.609.
- Norma ISO 9001:2015.
- Norma ISO/IEC 9594-8:2020.
- Norma ISO/TR 10013:2021.
- Norma ISO/IEC 27001:2022.

34. Funciones y responsabilidades dentro de la autoridad de certificación (AC): Las funciones y responsabilidades de los distintos niveles de la AC respecto al manejo, control y resguardo del presente documento, se encuentran definidos dentro del documento para el establecimiento de funciones y responsabilidades (AC-PO-0003).

35. Actores sujetos al cumplimiento del presente documento: El presente documento de la DPC y PC, emitido por el PSC PROCERT conforme a los lineamientos de la SUSCERTE, se constituye en norma de obligatorio cumplimiento y sujeción por parte de los actores que se indican a continuación:

- Alta Dirección del PSC PROCERT.
- Empleados del PSC PROCERT.
- Clientes usuarios de certificados electrónicos emitidos por el PSC PROCERT.
- Parte Interesada usuaria de los certificados electrónicos por el PSC PROCERT.

36. Revisión, aprobación y modificación: Los procesos asociados a la revisión, aprobación, modificación o ajuste de la documentación del PSC PROCERT serán regulados por la política de documentación y gestión documental (AC-PO-0002).