Proveedor de Certificados PROCERT ITFB, C. A.
Política de Certificado Electrónico para Servidor Seguro (SSL)

Índice

1. Control De Versiones

Versión	Motivo de Cambio	Publicación	Vigencia
Edición 01	Control y Corrección Semestral (Actualización)	12/08/2011	No
Edición 02	Control y Corrección Semestral (Actualización)	08/02/2012	No
Edición 03	Control y Corrección Semestral (Actualización)	22/09/2012	No
Edición 04	Control y Corrección Semestral (Actualización)	05/02/2013	No
Edición 05	Control y Corrección Semestral (Actualización)	13/08/2013	No
Edición 06	Control y Corrección Semestral (Actualización)	16/01/2014	No
Edición 07	Control y Corrección Semestral (Actualización)	24/02/2015	No
Edición 08	Control y Corrección Semestral (Actualización)	18/01/2016	No
Edición 09	Control y Corrección Semestral (Actualización)	18/01/2016	No
Edición 10	Control y Corrección Semestral (Actualización)	06/06/2017	No
Edición 11	Control y Corrección Semestral (Actualización)	27/07/2017	No
Edición 11	Control y Corrección Semestral (Actualización)	06/01/2018	No
Edición 11	Control y Corrección Semestral (Actualización)	06/06/2018	No
Edición 11	Control, Revisión y Ajuste Semestral (Actualización)	05/01/2019	No
Edición 11	Control, Revisión y Ajuste Semestral (Actualización)	07/06/2019	No
Edición 11	Control, Revisión y Ajuste por Remediación de Acreditación 2019.	18/11/2019	No
Edición 11	Control, Revisión y Ajuste Semestral (Actualización)	04/09/2020	No
Edición 11	Control, Revisión y Ajuste Semestral (Actualización)	07/06/2021	No

Edición 11	**Control, Revisión y Ajuste Semestral (Actualización)**	**07/12/2021**	**No**
Edición 11	**Control y Ajuste (Actualización) Migración Daycohost.**	**08/06/2022**	**No**
Edición 11	**Control y ajuste Auditoria SUSCERTE**	**21/12/2022**	**No**
Edición 11	**Control, Revisión y Ajuste Semestral (Actualización)**	**10/01/2023**	**No**
Edición 11	**Control, Revisión y Ajuste Semestral (Actualización)**	**17/07/2023**	**Si**

2. **Título:** Política de certificado electrónico para servidor de seguro (SSL).

3. **Código:** AC-D-0011.

4. **Introducción:** El PSC PROCERT procede a la emisión y publicación de presente documento de la política de certificado electrónico para servidor seguro (SSL) (PC-6), el cual tiene como fin, documentar, informar a la alta dirección, personal, proveedores, clientes y parte interesada del PSC PROCERT, cerca del uso autorizado y soporte técnico del certificado de firma electrónica para servidor de seguro (SSL). Los clientes, proveedores o parte interesada que utilicen los certificados electrónicos emitidos por el PSC PROCERT deberán dar cumplimiento la presente política de certificado, a los fines de conocer las responsabilidades y obligaciones del PSC PROCERT, respecto al ciclo de vida de los certificados, el proceso de gestión de certificados electrónicos. La presente política se encuentre ajustada a los mandatos impuestos por el Decreto Ley de Mensajes de Datos y Firmas Electrónicas (LSMDFE), su Reglamento y marco normativo que regula la materia dentro de la República Bolivariana de Venezuela

5. **Definiciones.**
   - **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 records 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 Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).
   - **5.5. Autoridad de registro:** Significa la entidad cuyo propósito es suministrar apoyo local a la infraestructura de clave pública (ICP) de una autoridad de certificación (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 electrónica o certificado electrónico generado por la autoridad de certificación (AC) PROCERT.

5.6. 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 la autoridad de certificación (AC) de PROCERT, la cual se encuentra subordinada y firmada por el certificado raíz generado por la SUSCERTE.

5.7. 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.

5.8. 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.

5.9. 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.

5.10. 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).

5.11. Clave criptográfica: Significa el parámetro utilizado conjuntamente con un algoritmo con fines de validación, autenticación, cifrado y descifrado.

5.12. Clave privada: Significa la clave asimétrica de una entidad, la cual normalmente será conocida solamente por esa entidad.

5.13. 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.

5.14. Cliente: Significa la entidad que ha solicitado la emisión de un certificado dentro de la infraestructura de clave pública (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.

5.15. 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.

5.16. 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.

5.17. 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.

5.18. 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.

5.19. Destinatario: Significa la entidad que obtiene (recibe o recupera) un mensaje.

5.20. **Destrucción de clave:** Significa el proceso de eliminación de todas las copias de una clave mediante el sistema de manejo de claves.

5.21. Disponibilidad: Significa la propiedad de la información de ser accesible y utilizable al ser solicitada por una entidad o proceso autorizado.

5.22. **Entidad:** Significa toda persona (natural o jurídica) o sistema (mecánico o electrónico).

5.23. Entidad infraestructura de clave pública (ICP) subordinada: Significa toda entidad que tenga la autoridad para operar y suministrar servicios de certificación bajo la infraestructura de clave pública (ICP) de la SUSCERTE.

5.24. **Evaluación:** Significa la valoración contra criterios definidos para dar una medida de confianza en el sentido de que se cumple con los requerimientos correspondientes.

5.25. Evento de auditoria: 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.

5.26. 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.

5.27. **Ficha criptográfica:** Significa el medio en el cual se almacena una clave (Ej. tarjeta inteligente, clave criptográfica).

5.28. Generación de certificado: Significa proceso de crear un certificado a partir de datos de entrada que son específicos a la aplicación y al Cliente.

5.29. **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.

5.30. Información de identificación: Significa la información que se obtiene para identificar positivamente a una entidad y suministrarle los Servicios de Certificación que solicite.

5.31. 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).

5.32. 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 infraestructura de clave pública (ICP) de PROCERT o que utilizan los Servicios de Certificación de la infraestructura de clave pública (ICP) de PROCERT en cualquier forma.

5.33. Integridad de datos: Significa la cualidad o condición de ser preciso, completo y válido y no ser alterado o destruido de manera no autorizada.

5.34. **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.

5.35. Investigación post-suspensión: Significa la investigación hecha por la gerencia general y el consultor de tecnología de PROCERT luego de suspender un certificado para determinar si dicho certificado debe ser revocado o reinstaurado como válido.

5.36. **Lista de certificados revocados (LCR):** Significa la lista de certificados que han sido revocados o suspendidos por el PSC PROCERT.

5.37. **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.

5.38. Nivel de auditoria: Significa una serie de requerimientos y regulaciones asociadas con los Tipos de certificados como se muestran en declaración de prácticas de certificación (DPC) y política de certificado (PC) (AC-D-0003) y contra los cuales se auditan a PSC acreditados ante la SUSCERTE.

5.39. **Par clave:** Significan las claves en un sistema criptográfico asimétrico que tienen como función la de que uno de los pares descifrará lo que el otro par de clave cifra.

5.40. 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.

5.41. Parte interesada: Significa la organización o persona que tiene interés en el desempeño o éxito del PSC PROCERT.

5.42. 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.

5.43. 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).

5.44. Proveedor: Significa la organización o persona que suministra un producto o servicio para Proveedor de Certificados PROCERT ITFB, C.A.

5.45. PSC: Significa Proveedor de Servicios de Certificación

5.46. 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 auditora para el encabezamiento del registro y usualmente tiene descripciones de auditoría adicionales que describen la entidad(es) y objeto(s) involucrados en el evento.

5.47. **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.

5.48. Revocación: Significa el cambio de estatus de un certificado válido o suspendido a "revocado" a partir de una fecha específica en adelante.

5.49. 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.

5.50. Seguridad física: Significan las medidas utilizadas para proveer protección física a los recursos contra amenazas deliberadas y accidentales.

5.51. 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 OCPS, servicios de tiempo compartido, servicios de verificación de identidad, hospedaje de Lista de Certificados Revocados (LCR), etc.

5.52. **Solicitante:** Significa la entidad que ha solicitado la emisión de un certificado dentro de la infraestructura de clave pública (ICP) de PROCERT. El proceso de verificación varía de acuerdo con la naturaleza y, donde aplique, el rol operacional dentro de la infraestructura de clave pública (ICP) correspondiente al certificado que la entidad está solicitando.

5.53. 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.

5.54. 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.

5.55. Validación: Significa el proceso de verificación de la validez de un certificado en términos de su estatus (Ej. suspendido o revocado).

6. **Objetivo:** La presente política de certificado, se constituye en la guía de mejores principios de gestión y operación del PSC PROCERT aplicables a la generación y uso del certificado electrónico para servidor seguro (SSL); los cuales deben ser documentados e informados a todos los clientes, proveedores y parte interesada contratantes de certificados electrónicos. Las actividades desarrolladas por el PSC PROCERT en el área de certificación electrónica, se encuentran reguladas por el Decreto Ley de Mensajes de Datos y Firmas Electrónicas y su Reglamento, como marco normativo y de referencia. La supervisión por parte del Estado Venezolano será ejercida por la SUSCERTE. Los certificados electrónicos emitidos por la AC del 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, 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. Igualmente el cliente contratante de certificados electrónico, a través del conocimiento del sistema y operaciones utilizados por la autoridad de certificación (AC) del PSC PROCERT, así como la rigurosa normativa y lineamientos técnicos que está debe cumplir a los efectos de acreditarse ante la SUSCERTE como PSC, creará la conciencia de los rigurosos pasos cumplidos por el PSC PROCERT y de la supervisión estricta del Estado Venezolano a través de la SUSCERTE, creando de esa manera un vínculo de confianza, el cual se constituye en requisito indispensable para la aceptación, valoración y validez del sistema de certificación electrónica a nivel mundial y se traduce en la masificación y uso de las amplias posibilidades ofrecidas por el certificado electrónico en el campo de las transacciones y operaciones ejecutadas dentro del Internet. La AR 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 entregada por el cliente a la transmitida a la AR, quien cumplidos los pasos creará el expediente electrónico y notificará a la AC del PSC PROCERT, a los efectos de autorizar la activación del certificado electrónico.

7. **Alcance:** La presente política de certificado electrónico para servidor seguro (SSL) del PSC PROCERT, aplica a la alta dirección, clientes, proveedores y parte interesada y para el proceso de emisión de certificados, funcionamiento del certificado, acceso al certificado y funcionamiento de la plataforma tecnológica de certificación de la AC del PSC PROCERT, conforme a los lineamientos impuestos por la SUSCERTE.

8. **Limitaciones:** La presente política de certificado electrónico para servidor seguro (SSL) del PSC PROCERT se constituye en el marco referencial acerca del PSC PROCERT, suministrando la información requerida para la compresión y documentación de los procesos asociados a la generación de certificados para servidor de seguro (SSL). El numeral 32.14 de la declaración de prácticas de certificación (DPC) del PSC PROCERT (AC-D-0003), establece el límite de responsabilidad que puede ser exigido por fallas en la gestión y operación del PSC PROCERT. De igual forma, el numeral 33 del documento de la declaración de prácticas de certificación (DPC) del PSC PROCERT (AC-D-0003), señala el marco legal y normativo aplicable y exigible a los PSC acreditados ante la SUSCERTE.

9. **Usos de los certificados:** La AC tiene la capacidad de generar certificados de firma electrónica con clave desde 2048 hasta 4096, según corresponda el tipo de certificado a emitir. Se describe a continuación el certificado electrónico para servidor seguro (SSL).

9.1. Certificado electrónico para servidor seguro (SSL): Los Certificados de SSL certifican que una persona es propietaria de un dominio en internet y está bajo el control de dicha persona. El uso asignado al certificado SSL es el siguiente:

- Protección de transacciones en línea entre servidores y clientes pertenecientes a un sistema integrado de tecnología de la información.
- Protección de comunicaciones en línea entre servidores y clientes pertenecientes a un sistema integrado de tecnología de la información.
- Identificación del dominio ante terceros.
- Brindar confianza en el usuario del dominio web protegido

9.2. Estructura del certificado electrónico para servidor seguro (SSL)

Campo del certificado	Valor del certificado
Versión:	V3 (Número de versión del certificado)
Número de Serie:	(Identificador único 32 caracteres hexadecimales.)
Algoritmo de Firma:	Sha-256RSA. (Algoritmo de Firma)
Datos del emisor	
CN	PSCPROCERT
O	Sistema Nacional de Certificación Electrónica
OU	PROCERT
C	VE
E	contacto@procert.net.ve
L	Av. Libertador Multicentro Empresarial del Este piso 13 Oficina B-132 Torre Libertador Núcleo B

ST	Miranda
Período de validez	
Válido desde:	(Inicio vigencia del certificado)
Válido hasta:	(Expiración del periodo de validez del certificado).
Datos del titular	
CN	(Dominio o Dirección IP)
O	(Organización Campo)
OU	(Unidad Organizacional) Campo Opcional
OU	(Número de RIF)
C	VE(País)
E	(correo electrónico)
L	(Dirección)
ST	(Estado)
Información de clave publica	
Algoritmo de clave publica	RSA (Algoritmo con el que se generó la clave pública)
Tamaño de clave publica	(2048) / (4096)
Extensiones	
Restricciones básicas	CA: False
Nombre alternativo del emisor	
DNS Name	procert.net.ve
Other Name	
OID 2.16.862.2.1	Código del PSC PROCERT asignado por SUSCERTE)
OID 2.16.862.2.2	RIF-J31635373-7 (RIF de PROCERT)
Identificador de clave del Titular	(Identificador de clave del titular)
Identificador de clave de autoridad certificadora	
Id. de clave	Identificador de la clave
Emisor de certificado	(Datos del emisor)
Número de serie del Certificado	(Número serial)
Uso de clave	No Repudio, Cifrado de Clave, Cifrado de Datos
Uso mejorado de Clave	Autenticación del servidor
Nombre alternativo del titular	
DNS Name	(Nombre de dominio del servidor)
Other name	
OID 2.16.862.2.2	(Número de RIF de la empresa)
Dirección IP	IP del Servidor

DNS Primario	DNS
Punto distribución LCR	http://ura.procert.net.ve/lcr/procertca.crl http://www.procert.net.ve/lcr/procertca.crl
Información del emisor	http://ura.PROCERT.net.ve/ocsp
Política de certificados	http://www.procert.net.ve/dpc-pc/

9.3. 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 servidor seguro (SSL) emitido por el PSC PROCERT estará limitado según el tipo de certificado, y a continuación se menciona el uso del mismo:

Tipo de certificado	Uso	Uso mejorado
Certificado electrónico para servidor seguro (SSL)	No Repudio, cifrado de clave, cifrado de datos	Autenticación del servidor

9.4. 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 sub-legal 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. Adicionalmente le será revocado el certificado electrónico. 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, por parte del usuario contratante del servicio contratado con el PSC PROCERT.

10. Políticas de administración de la AC: Las políticas de administración de la AC son las señaladas en el aparte 11 de la declaración de prácticas de certificación (DPC) (AC-D-0003).

11. Publicación de información del PSC y repositorios de los certificados.

11.1. Repositorios: A fin de garantizar la completa disponibilidad de este documento de la política de certificado de firma electrónica para servidor de seguro (SSL), 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**:** http://www.procert.net.ve/ac.html
- Para la lista de certificados revocados:
  https://ura.procert.net.ve/lcr/procertca.crl
  http://www.procert.net.ve/lcr/procertca.crl
- Para el servicio de validación en línea (OCSP):http://ura.procert.net.ve/ocsp
  El repositorio público del PSC PROCERT, no contiene ninguna información confidencial o privada.

11.2. 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://ura.procert.net.ve/lcr/procertca.crl
  http://www.procert.net.ve/lcr/procertca.crl
- El presente documento se encuentra disponible en:
  http://www.procert.net.ve/ac.html
- El certificado de la AC Subordinada PROCERT se encuentra disponible en:
  http://www.procert.net.ve/ac.html
- Los certificados emitidos por la AC Subordinada PROCERT se encuentran en
  https://ura.procert.net.ve/URA/Public/
- Los datos de contacto del PSC PROCERT en la dirección:
  https://www.procert.net.ve/index.html#contacto
- La documentación técnica del PSC Procert en la dirección:
  http://www.procert.net.ve/ac.html

11.3. Frecuencia de publicación.

11.3.1. **Certificados del PSC:** EL periodo de validez es de diez (10) años.

11.3.2. **Lista de certificados revocados (LCR):** La publicación de la lista de certificados revocados se realizará cada 24 horas.

11.3.3. **Declaración de prácticas de certificación:** A menos que explícitamente se indique lo contrario en este documento de la política de certificado de firma electrónica para servidor de seguro (SSL), se publicarán en la página web del PCS PROCERT (www.procert.net.ve), las nuevas

versiones de este documento, inmediatamente tras la aprobación de las mismas.

12. **Identificación y autenticación:** Las características de la identificación señalados en el numeral 16 y procedimientos para la validación son las señaladas en los apartes 14 y 15 de la declaración de prácticas de certificación (DPC) (AC-D-0003).

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 de la LCR y al OCSP.

14. **Tramitación de solicitud de un certificado.**
    - **14.1. 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 al aparte 11.1.6 y 15 de la declaración de prácticas de certificación (DPC) (AC-D-0003).
    - **14.2. Aceptación 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 del proceso de aprobación de una firma o certificado electrónico validará el cumplimiento de las condiciones siguientes:
      - 14.2.1. Validar el pago efectuado por el cliente.
      - 14.2.2. Validar el informe emitido por la AR.
      - 14.2.3. Validar el tipo de certificado solicitado y tramitar ante la Universal Register Authority (URA), 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. Las circunstancias para la revocación del certificado son las señaladas en el aparte 16.1.5 de la declaración de prácticas de certificación (DPC) (AC-D-0003).
    - **14.3. 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, la AR 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 quince (15) 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.

15. Emisión de Certificado.

15.1. Acciones de la AC durante la emisión de un certificado: La AC del PSC PROCERT es la encargada de generar los certificados adquiridos por los clientes del PSC PROCERT. 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.

15.2. 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.

16. Uso del par de claves y del certificado.

16.1. 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 este documento de la política de certificado de firma electrónica para servidor de seguro (SSL). El cliente es el único responsable de la custodia y cuido 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.

16.2. Uso de la clave pública y del certificado por los terceros de buena fe: El certificado de raíz de certificación de la AC se hace público a los efectos de la validación de la ruta. La huella del certificado y los certificados de la infraestructura de clave pública (ICP) de la AC del PSC PROCERT están disponibles en la página web del PSC PROCERT (www.procert.net.ve). Los terceros de buena fe deben confirmar la validez de las copias de sus certificados de la infraestructura de clave pública (ICP) de la AC del PSC PROCERT usando estas huellas. Los usos asignados a los certificados se encuentran definidos en el aparte 9.7.1 de la declaración de prácticas de certificación (DPC) y política de certificados (PC) de PROCERT.

17. Renovación del certificado con cambio de clave.

17.1. 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:

17.1.1. Que se haya cumplido el término de vigencia de la firma o certificado electrónico del cual es propietario.

17.1.2. 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.

17.1.3. Que el solicitante cumpla con el proceso de contratación del PSC PROCERT y de validación por parte de la AR del PSC PROCERT.

17.2. 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.

17.3. 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 "compra de certificados" (https://www.procert.net.ve/compra.html), seguir los pasos de compra, 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.

17.4. 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.

17.5. 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.

17.6. Notificación de la emisión del certificado por la AC a otras autoridades: 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.

18. **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.

19. **Revocación y suspensión de un certificado**.
    - **19.1. Circunstancias para la revocación del certificado:** Las circunstancias para la revocación del certificado son las señaladas en el aparte 23.1 de la declaración de prácticas de certificación (DPC) (AC-D-0003).
    - **19.2. 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 23.2 de la declaración de prácticas de certificación (DPC) (AC-D-0003).
    - **19.3. Procedimiento de solicitud de la revocación:** El procedimiento de solicitud de la renovación de la firma o certificado electrónico según corresponda, es el señalado en el aparte 23.3 de la declaración de prácticas de certificación (DPC) (AC-D-0003).
    - **19.4. 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.
    - **19.5. Circunstancias para la suspensión:** Las circunstancias para la suspensión de firma o certificado electrónico según corresponda, es el señalado en el aparte 23.5 de la declaración de prácticas de certificación (DPC) (AC-D-0003).
    - **19.6. Procedimiento para la solicitud de suspensión:** El procedimiento para la suspensión de firma o certificado electrónico según corresponda, es el señalado en el aparte 23.6 de la declaración de prácticas de certificación (DPC) (AC-D-0003).
    - **19.7. Límites del período de suspensión:** El límite del período de suspensión de firma o certificado electrónico según corresponda, es el señalado en el aparte 23.7 de la declaración de prácticas de certificación (DPC) (AC-D-0003).
    - **19.8. 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 del PSC PROCERT. La LCR es

publicada cada veinticuatro (24) horas en la página web del PSC PROCERT (www.procert.net.ve) (AC-D-0003).

19.9. 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://ura.procert.net.ve/ocsp.

19.10. 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 de 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.

19.11. Otras formas de divulgación de información de revocación disponibles: El PSC PROCERT noticiará vía correo electrónico al cliente que corresponda, acerca de la suspensión o revocación de su certificado.

20. Servicio de Comprobación de estado de certificados.

20.1. 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 de la declaración de prácticas de certificación (DPC) y política de certificados (PC) (AC-D-0003). El funcionamiento del acceso vía OCSP se encuentra establecido en los apartes 23.9 y 23.10 de la declaración de prácticas de certificación (DPC) (AC-D-0003).

20.2. 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 Autoridad de Certificación (AC) PROCERT mantiene en operación su portal web, cumpliendo con un alto porcentaje de disponibilidad.

20.3. Características adicionales: Características adicionales a los servicios de LCR y acceso OCSP se encuentran señaladas de forma precedente en este documento de la política de certificado electrónico para servidor seguro SSL, en los puntos 18.8 y 18.9.

21. Finalización de la suscripción: El cliente del PSC PROCERT podrá dar el uso permitido a 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.

22. Custodia y recuperación de la clave.

22.1. 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 los apartados 26.1 y 31.1.4 de la declaración de prácticas de certificación (DPC) (AC-D-0003).

23. **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 los apartados 28 y 31.1.4 de la Declaración de Prácticas de Certificación (DPC) (AC-D-0003).

24. **Controles de seguridad física, de gestión y de operaciones:** Los controles de seguridad física de gestión y de operaciones son los señalados en el aparte 27 de la Declaración de Prácticas de Certificación (DPC) (AC-D-0003).

25. **Controles de seguridad técnica:** Los controles de seguridad técnica son los señalados en el aparte 31 de la declaración de prácticas de certificación (DPC) (AC-D-0003).

26. **Requisitos comerciales y legales:** Los requisitos comerciales y legales se encuentran señalados en el aparte 32.9 de la declaración de prácticas de certificación (DPC) (AC-D-0003).

27. **Perfiles de Certificados, LCR / OCSP.**
    - **27.1. Perfil del certificado:** Los certificados del PSC PROCERT son emitidos conforme a las siguientes normas:
      - RFC 6818: Internet X.509 V3 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, 2006 (prevaleciendo en caso de conflicto la TS 101 862).

27.2. Número de Versión: Como se indicó en el aparte 8.1., que precede, el número de versión del certificado es V3.

27.3. 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:

- Subject Key Identifier.
- AuthorityKeyIdentifier
- BasicConstraints.
- Certificate Policies.
- KeyUsage.
- LCRDistribucionPoint.
- SubjectAlternativeName.
- AuthorityInformationAccess.

27.4. Identificadores de Objeto (OID) de los Algoritmos: El OID del algoritmo criptográfico utilizado por el PSC PROCERT es: SHA256withcRSAEncryption (1.2.840.113549.1.1.11).

27.5. 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 los numerales 32.5 y 14 de la declaración de prácticas de certificación (DPC) (AC-D-0003).

27.6. 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.

27.7. 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:

- Nombre del emisor de la LCR
- Números de serie de la firma o certificado
- Fecha de revocación de las firmas o certificados.
- La fecha efectiva y la fecha de la próxima actualización.

Dicha lista está firmada electrónicamente por la propia AC que la emitió. Cuando un usuario desea comprobar la validez de un certificado debe descargar e instalar la LCR actualizada desde los servidores de la misma 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-256RSA (Algoritmo de Firma)
Datos del emisor	
CN	PSCPROCERT.
O	Sistema Nacional de Certificación Electrónica
OU	PROCERT
C	VE (VENEZUELA)
E	contacto@procert.net.ve
L	Av. Libertador Multicentro Empresarial del Este piso 13 Oficina B-132 Torre Libertador Núcleo B
ST	MIRANDA
Período de Validez	
Última Actualización :	Contiene la fecha y hora en que fue emitida la lista de certificados revocados (LCR).
Próxima Actualización :	Fecha en que se emitirá la próxima lista de certificados revocados.
Lista de certificados revocados	
Certificados Revocados	Contiene la lista de certificados revocados indicados por su número de serie y su fecha de revocación.
Extensiones	
Identificación de clave de la 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	
DNSName	**procert.net.ve**
Número de LCR	Número de Identificación de la LCR
Punto de distribución LCR	http://ura.procert.net.ve/LCR/procertca.crl http://procert.net.ve/lcr/procertca.crl

El perfil correspondiente al OCSP se encuentra detallado en el aparte 32 de la Declaración de Prácticas de Certificación (DPC).

27.8. Auditoría de conformidad: En el caso de la raíz de certificación de la AC del PSC PROCERT es supervisada y auditada anualmente por la SUSCERTE. La SUSCERTE 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 PROCERT cumple con las directrices de Ley para operar como PSC.

27.8.1. **Frecuencia de los controles de conformidad para cada entidad:** Las auditorias de control y seguimiento ordenas por Ley e impuestas por mandato de la SUSCERTE serán efectuadas anualmente; y mediante

dichas auditorias 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 auditoria anual de seguimiento si opta a la renovación de su acreditación para operación durante el año siguiente al proceso de auditoría.

27.8.2. **Auditores:** Las auditorias 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.

27.8.3. **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.

27.8.4. **Tópicos cubiertos por el control de conformidad.**

Los tópicos cubiertos por la auditoria de cumplimiento incluyen:

27.8.5. Seguridad física.

27.8.6. Evaluación de tecnología.

27.8.7. Administración de servicios CA.

27.8.8. Investigación de personal.

27.8.9. Documento de la declaración de prácticas de certificación (DPC) y la política de certificados (PC) y otras políticas y documentos aplicables.

27.8.10. Contractos.

27.8.11. Protección de datos y consideraciones sobre privacidad.

27.8.12. Planificación de recuperación ante desastres.

27.8.13. **Acciones a 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.

27.8.14. **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 32.8.6 de la declaración de prácticas de certificación (DPC) (AC-D-0003).

28. Marco legal y normativo.

- Decreto Ley de Mensaje de Datos y Firmas Electrónicas y su Reglamento.
- Normativa de la SUSCERTE.
- Normativa PROCERT.
- Estándar internacional ITU- T X.509 V3.
- Estándar Internacional ITU-T X.609.
- Norma ISO 9000:2005.
- Norma ISO/IEC 9594-8.
- Norma ISO/TR 10013:2001.
- Norma ISO/IEC 27001:2006.

29. Funciones y responsabilidades dentro de la AC: Las funciones y responsabilidades de los distintos niveles de la AC del PSC PROCERT 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).

30. Actores sujetos al cumplimiento del presente documento: El presente documento política de certificado electrónico para servidor seguro SSL, emitido por la AC del 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:

30.1. Alta Dirección de la AC PROCERT.
30.2. Empleados de la AC PROCERT.
30.3. Clientes usuarios de certificados electrónicos emitidos por la AC PROCERT ITFB.
30.4. Parte Interesada usuaria de los certificados electrónicos emitidos por la AC PROCERT ITFB.

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