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

1. CONTROL DE CAMBIOS

Nº	Fecha	Descripción del Cambio	Nº Página	Elaborado por	Revisado por / Aprobado por
0	Agosto 2024	Emisión original	Todas	Gerente Calidad	Gerente General

PSC-PSC-DPC-001

CONTENIDO

2. PRESENTACIÓN

El presente documento conforma la declaración por parte de DOCUMENTOS DIGITALES PSC, C.A. (FirmeDigital) para describir y documentar sus procesos de certificación.

La DPC permite conocer los procesos y subprocesos involucrados en el ciclo de vida de los certificados electrónicos; documentar los procesos de recuperación ante posibles eventualidades, manejo de claves criptográficas y dar una visión amplia de la tecnológica que soporta la estructura de DOCUMENTOS DIGITALES PSC, C.A. Por su parte, las PC permiten conocer el uso autorizado de cada tipo de certificado que emite la compañía, su estructura y sus funciones.

El personal, clientes, proveedores e interesados que utilicen los certificados electrónicos emitidos por la organización, deberán dar cumplimiento al presente documento de DPC y PC y serán responsables por las consecuencias derivadas del uso indebido de un certificado electrónico o del incumplimiento de las normas contenidas en el presente instructivo.

3. DEFINICIONES

Con el objeto de ofrecer una interpretación adecuada de los términos utilizado en el presente documento, a continuación, se detallan una serie de definiciones, cuyas denominaciones en plural o singular atenderán al significado que se le asigna:

- Archivo de Clave: Es el proceso de almacenar claves usadas o su ID y/o certificados como un registro en almacenamientos de largo plazo para futuras recuperaciones.
- Auditoría: Es la revisión del sistema de records y actividades para evaluar 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 en los controles, políticas y procedimientos y asegurar la implantación de dichos cambios en el tiempo.
- Auditoria de Cumplimiento: Es la evaluación 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.
- Autoridad de Certificación (AC): Es la autoridad en la cual confían los clientes para crear, emitir y manejar el ciclo de vida de los certificados, que de conformidad con la legislación venezolana el organismo competente es la SUSCERTE.
- Autoridad de Registro (AR): Entidad cuyo propósito es suministrar apoyo local a la infraestructura de clave pública (ICP) de una AC. La Autoridad de Registro desempeña unas 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.

- Cadena de Certificado: 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 DOCUMENTOS DIGITALES PSC, C.A., la cual se encuentra subordinada por el certificado raíz generado por la SUSCERTE.
- Certificado: Es 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 *unforgettable* (inolvidable), mediante una firma electrónica de la autoridad de certificación que la generó.
- Certificado de Clave Pública: Es 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.
- Cifrado: Es 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.
- Clave: Es la secuencia de símbolos que controla la operación de una transformación criptográfica.
- Clave Criptográfica: Es el parámetro utilizado conjuntamente con un algoritmo con fines de validación, autenticación, cifrado y descifrado.
- Clave Privada: Es la clave asimétrica de una entidad, la cual será conocida únicamente por esa entidad.
- Clave Pública: Es la clave de un par clave asimétrico de una entidad que puede hacerse pública, aunque no necesariamente esté disponible al público en general debido a que puede ser restringida a un grupo predeterminado.
- Cliente: Es la entidad que ha solicitado la emisión de un certificado dentro de la infraestructura de clave pública (ICP) de DOCUMENTOS DIGITALES PSC, C.A. A los efectos de la LSMDFE y su Reglamento el cliente también será entendido como el signatario y viceversa.
- Confidencialidad: Es la acción 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.
- Control de Acceso: Es la prevención del uso no autorizado de un recurso.
- Criptografía: Es 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.
- Declaración de Práctica de Certificación (DPC): Es la declaración de las prácticas que utiliza la autoridad certificadora para emitir certificados y manejar su ciclo de vida.
- Destinatario: Es la entidad que obtiene (recibe o recupera) un mensaje.
- Destrucción de Clave: Es el proceso de eliminación de todas las copias de una clave a través el sistema de manejo de claves.
- Disponibilidad: Es la propiedad de la información de ser accesible y utilizable al ser solicitada por una entidad o proceso autorizado.
- Entidad: Significa toda persona (natural o jurídica) o sistema (mecánico o electrónico).
- Entidad infraestructura de clave pública (ICP) Subordinada: Es toda entidad que tenga la autoridad para operar y suministrar servicios de certificación bajo ICP de la SUSCERTE.
- Evaluación: Es la valoración contra criterios definidos para dar una medida de confianza para que se cumplan con los requerimientos correspondientes.

- Evento de Auditoria: Es 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], este es un “evento registrado”, de otra forma, sería 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.
- Firma Electrónica: Es 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. En la LSMDFE es entendido como la información creada o utilizada por el signatario, asociada al mensaje de datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado.
- Ficha Criptográfica: Es el medio mediante la cual se almacena una clave.
- Generación de Certificado: Es el proceso de crear un certificado a partir de datos de entrada que son específicos a la aplicación y al cliente.
- Generación de Clave: Es 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.
- Información de Identificación: Es la información que se obtiene para identificar positivamente a una entidad y suministrarle los servicios de certificación que solicite.
- Infraestructura de clave pública (ICP): Es la infraestructura 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).
- Infraestructura Operacional: Es la infraestructura para suministrar 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 DOCUMENTOS DIGITALES PSC, C.A. o que utilizan los servicios de certificación de la ICP de DOCUMENTOS DIGITALES PSC, C.A. en cualquier forma.
- Integridad de Datos: Es la cualidad en los datos de ser completos, íntegros y válidos, y no ser alterados o destruidos sin autorización.
- Interoperabilidad: Implica que los equipos y procedimientos usados por dos o más entidades sean compatibles y, por ende, es posible que realicen actividades interconectadas.
- Investigación Post-Suspensión: Es la investigación realizada por la gerencia de DOCUMENTOS DIGITALES PSC, C.A. luego de suspender un certificado para determinar si dicho certificado debe ser revocado o reinstaurado como válido.
- Lista de Certificados Revocados (LCR): Significa la lista de certificados que han sido revocados o suspendidos por DOCUMENTOS DIGITALES PSC, C.A.
- Manejo de Clave: Es 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.
- Nivel de Auditoria: Son una serie de requerimientos asociadas con los tipos de certificados como se muestran en el presente documentos y contra los cuales se auditan a PSC acreditados ante la SUSCERTE.
- Par Clave: Son las claves en un sistema criptográfico asimétrico que tienen como fin que uno de los pares de claves descifrará lo que el otro par de clave cifra.

- Par Clave Asimétrico: Es el par de claves relacionadas donde la clave privada define la transformación privada y la clave pública define la transformación pública.
- Parte Interesada: Es la organización o persona que tiene interés en el desempeño o éxito de DOCUMENTOS DIGITALES PSC, C.A..
- Proceso de Verificación: Es 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.
- 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) posibles estatus: válido, revocado o desconocido.
- Proveedor: Es la organización o persona que suministra un producto o servicio para DOCUMENTOS DIGITALES PSC, C.A..
- PSC: Es el Proveedor de Servicios de Certificación
- Registro de Auditoria: Es la unidad de dato discreta registrada en el rastro de auditoría cuando ocurre un evento que es registrado. 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.
- Resumen de Información: Es la información mínima 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 el resultado de esta verificación.
- Revocación: Es el cambio de estatus de un certificado válido o suspendido a “revocado” con efectos a partir de una fecha precisa.
- Revocación de Certificado: Es 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.
- Seguridad Física: Son las medidas utilizadas para proveer protección física a los recursos contra amenazas deliberadas y accidentales.
- Servicios de Certificación: Son 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 la LCR, entre otros.
- Solicitante: Es la entidad que ha solicitado la emisión de un certificado dentro de la ICP de DOCUMENTOS DIGITALES PSC, C.A. 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.
- Solicitud de Certificado: Es 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.
- Uso del Certificado: Es 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.
- Validación: Es el proceso de verificación de la validez de un Certificado en términos de su estatus.

4. OBJETIVO

Las presentes DPC y PC constituyen una guía de principios de gestión y operación de la organización, los cuales deberán ser instruidos a la gerencia, personal, clientes, proveedores y demás partes interesadas de la compañía.

Los certificados electrónicos emitidos por DOCUMENTOS DIGITALES PSC, C.A. bajo la denominación “firma electrónica” otorgarán a los propietarios de los mismos, un instrumento que tendrá plena validez y eficacia jurídica dentro del ordenamiento jurídico venezolano. Adicionalmente, la firma electrónica otorgará al cliente las máximas condiciones de protección y reconocimiento de su identidad, autenticación, distinción, integridad y protección de los mensajes transmitidos bajo las firmas electrónicas.

La AR establecerá y validará los datos suministrados por el cliente al cual se le asigne un certificado electrónico. Dicha información será transmitida a la AC, con el objetivo de autorizar la activación del certificado electrónico.

5. ALCANCE

Las presentes DPC y PC aplican a la gerencia, personal, clientes, proveedores y partes interesadas de la organización, para el proceso de emisión, revocación o renovación de certificados y funcionamiento de la plataforma tecnológica de la compañía.

6. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

Nombre del Documento	Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC) de DOCUMENTOS DIGITALES PSC, C.A.
Versión del Documento	1.0
Estado del Documento	APROBADO
Referencia de la DPC/OID (Identificador de Objeto)	OID #.##.###.##.#.# (Hash de documento en FirmeDigital)
Fecha de Emisión	Agosto 2024
Fecha de Expiración	10 Años
Localización	Esta DPC y PC se encuentran en www.firmedigital.com

El presente documento conforma la declaración por parte de DOCUMENTOS DIGITALES PSC, C.A. (FirmeDigital) para describir y documentar sus procesos de certificación.

7. COMUNIDAD DE USUARIOS Y APLICABILIDAD.

7.1. Aprobación de políticas (AAP)

Toda la documentación en relación con el funcionamiento de los certificados y operación de la compañía, será elaborada por el personal y dirección de DOCUMENTOS DIGITALES PSC, C.A. y posteriormente, sometida al órgano competente SUSCERTE.

7.2. Actualización de la documentación (AD)

La dirección establece las condiciones que aplican para que proceda la revisión o modificación de la documentación. Dichos elementos son los siguientes: (i) cambios organizacionales, (ii) cambios en la normativa de acreditación por parte del órgano competente o en la legislación correspondiente, (iii) cambios en la normativa internacional, (iv) cambios en los procesos y/o subprocesos que deban ser documentados o, (v) documentación con más de seis (6) meses, sin modificación o actualización, deberá presentarse como una nueva versión.

7.3. Autoridad de Certificación (AC)

Ofrece certificados electrónicos a personas públicas, privadas, naturales o jurídicas; prestará el soporte para la implementación de firmas y certificados electrónicos. Sus servicios serán prestados en todo el territorio de la República Bolivariana de Venezuela.

7.4. Autoridad de Registro (AR)

Conjunto de infraestructura tecnológica y componente humano encargado de validar la identidad; así como, de verificar la veracidad y exactitud de los datos de identificación del solicitante de un CE, y de la gestión operativa de las solicitudes relacionadas al ciclo de vida de un CE.

7.5. Certificado raíz

DOCUMENTOS DIGITALES PSC, C.A. es una autoridad de certificación de segundo nivel y 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 de DOCUMENTOS DIGITALES PSC, C.A. es la siguiente:

Campos del certificado	Valor del certificado
Versión	V1
Número de Serie:	######
Algoritmo de Firma:	ECCP 256 (Curva Eliptica)

Campos del certificado	Valor del certificado
Datos del emisor	
CN	Autoridad de Certificación Raíz del Estado Venezolano
O	Sistema Nacional de Certificación Electrónica
OU	Superintendencia de Servicios de Certificación Electrónica
C	VE
E	acraiz@suscerte.gob.ve
L	Caracas
ST	Distrito Capital
Período de validez	
Válido Desde:	(Inicio vigencia del certificado)
Válido Hasta:	(Expiración del periodo de validez del certificado).
Datos del titular	
CN	DOCUMENTOS DIGITALES PSC, C.A.
O	Sistema Nacional de Certificación Electrónica
OU	FirmeDigital
C	VE
E	soporte@firmedigital.com
L	Maracaibo
ST	Zulia
Información de clave pública	
Algoritmo clave pública	ECCP 256 (Curva Eliptica)
Tamaño clave pública	(4096)
Extensiones	
Restricciones básicas	CA: TRUE Y LOGONITUD DEL PATH = 1
Nombre alternativo del emisor	
Dns name	suscerte.gob.ve
Other name	
OID 2.16.862.2.2	RIF-G-20004036-0 (RIF de SUSCERTE)
Identificador clave 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 serie certificado	(Número de serial)
Uso de la Clave	Firma electrónica del certificado y firma de LCR
Nombre alternativo del titular	
DNSName	firmedigital.com
Other name	

Campos del certificado	Valor del certificado
OID 2.16.862.2.1	88888
OID 2.16.862.2.2	RIF- J505415859
Punto distribución LCR	http://www.suscerte.gob.ve/lcr/CERTIFICADO-RAIZ-.crl
Información del emisor	http://ocsp.suscerte.gob.ve
Política de certificados	http://www.suscerte.gob.ve/dpc

7.6. Raíz de certificación

La organización posee una plataforma de certificación auditada y autorizada por la SUSCERTE la cual cumple con los estándares internacionales para operación de una ICP. La compañía 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, DOCUMENTOS DIGITALES PSC, C.A. 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 DOCUMENTOS DIGITALES PSC, C.A., dentro de su plataforma de certificación a los efectos de poder a su vez generar y asignar los certificados electrónicos bajo los parámetros de la LSMDFE y su RLSMDFE.

DOCUMENTOS DIGITALES PSC, C.A. debe generar cada veinticuatro (24) horas una LCR, la cual se constituye en un mecanismo de validación y comprobación del estado de los certificados electrónicos. Todo proceso de revocación de certificado es informado vía correo electrónico al cliente. Dicha notificación se informa mensualmente a la SUSCERTE y se incluye en el depósito digitalizado mantenido por el DOCUMENTOS DIGITALES PSC, C.A..

7.7. Tercero de Buena Fe:

Los terceros de buena fe, son aquellas personas o entidades jurídicas que confían en una firma electrónica, certificado electrónico, LCR o información generada por DOCUMENTOS DIGITALES PSC, C.A. y sobre las cuales pueden depositar su confianza de acuerdo con el presente documento. La ICP, está obligada, directa o indirectamente con todos los clientes, proveedores y/o parte interesada de firmas electrónicas y certificados electrónicos generados por la compañía.

8. USO DE LOS CERTIFICADOS.

8.1. Usos permitidos:

El uso del certificado estará limitado a la firma de certificados electrónicos para autoridades subordinadas, firma de las listas de certificados revocados y firma de todos los certificados establecidos en el presente documento. El uso de los certificados electrónicos estará limitado según el tipo de certificado emitido.

Los distintos tipos de certificados de firma electrónica emitidos por DOCUMENTOS DIGITALES PSC, C.A. se describen a continuación:

Certificado electrónico de firma para empleados de empresa: El uso asignado para este tipo de certificado es para realizar transacciones en línea, identificar a empleados de empresas públicas o privadas, comunicaciones electrónicas sin representación de empresas públicas o privadas, no confiere representación legal a personas de empresas públicas o privadas.

Estructura del certificado electrónico de firma para empleados de empresa.

Campo del Certificado	Valor del Certificado
Versión	V3 (Número de versión del certificado).
Número de serie	(Identificador único menor de 32 caracteres hexadecimales.)
Algoritmo de firma	ECCP 256 (Curva Eliptica)
Datos del Emisor	
CN	DOCUMENTOS DIGITALES PSC, C.A.
O	Sistema nacional de certificación electrónica
OU	FirmeDigital
C	VE
E	soporte@firmedigital.com
L	Maracaibo
ST	Zulia
Período de Validez	
Válido Desde	(Inicio vigencia del certificado)
Válido Hasta	(Expiración del periodo de validez del certificado).
Datos del Titular	
CN	(Nombre el empleado a certificar)
T	(Cargo del titular)
O	(Nombre de la organización)
OU	(Nombre de la unidad organizativa) opcional
OU	(Número de cédula de identidad o pasaporte)
C	(País)
E	(correo electrónico)

Campo del Certificado	Valor del Certificado
L	(Dirección)
ST	(Estado)
Información de Clave Pública	
Algoritmo de clave pública	ECCP 256 (Curva Eliptica)
Tamaño de clave pública	2048
Extensiones	
Restricciones básicas	CA: False
Nombre alternativo del Emisor	
DNS name	firmedigital.com
Other name	api.firmedigital.com
OID 2.16.862.2.1	(Código asignado por SUSCERTE)
OID 2.16.862.2.2	RIF- J505415859
Identificador clave 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 serie certificado	(Número de serial)
Uso de clave	Firma electrónica, no repudio, cifrado y cifrado de datos
Nombre alternativo del titular	
Other name	
OID 2.16.862.2.2	(Número de cédula de identidad o pasaporte)
Punto de distribución de LCR	http://ura.firmedigital.com/lcr/ca.crl
Información del emisor	http://ura.firmedigital.com/ocsp
Política de certificados	http://www.firmedigital.com/dpc-pc/

Uso autorizado del certificado electrónico de firma para empleados de empresa.

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

Certificado electrónico de firma para representantes de empresas públicas: El uso asignado para este tipo de certificado es certificar a una persona como representante legal de una entidad jurídica publica, transacciones en línea públicas o privadas, en representación de empresas o entidades públicas, comunicaciones privadas o públicas en representación de empresas o entidades públicas, comercio electrónico en representación de empresas o entes públicas o, trámites en línea ante gobierno en representación de empresas o entes públicos.

Estructura del certificado electrónico de firma para representantes de empresas públicas.

Campo del certificado	Valor del certificado
Versión	V3 (Número de versión del certificado).
Número de serie	(Identificador único menor de 32 caracteres hexadecimales.)
Algoritmo de firma	ECCP 256 (Curva Elíptica)
Datos del emisor	
CN	DOCUMENTOS DIGITALES PSC, C.A.
O	Sistema nacional de certificación electrónica
OU	FirmeDigital
C	VE(País)
E	soporte@firmedigital.com
L	Maracaibo
ST	Zulia
Período de validez	
Válido desde	(Inicio vigencia del certificado)
Válido hasta	(Expiración del periodo de validez del certificado).
Datos del titular	
CN	(Nombre del funcionario a certificar)
T	(Cargo del funcionario)
O	(Organización campo opcional)
OU	(Unidad organizacional) campo opcional
C	(País)
E	(correo electrónico)
L	(Dirección)
ST	(Estado)
Información de clave pública	
Algoritmo de clave pública	ECCP 256 (Curva Elíptica)
Tamaño de clave pública	2048
Extensiones	
Restricciones básicas	CA: False
Nombre alternativo del emisor	
DNS name	Firmedigital.com
Other name	
OID 2.16.862.2.1	(Código asignado por la SUSCERTE)
OID 2.16.862.2.2	RIF- J505415859
Identificador clave Titular	(identificador de la clave del titular)
Identificador de la clave de autoridad certificadora	
Id. de clave	(Identificador de la Clave)
Emisor de certificado	(Datos del emisor)
Número serie certificado	(Número Serial)

Uso de clave	Firma electrónica, no repudio, Cifrado
Nombre alternativo del titular	
Other name	
OID 2.16.862.2.2	(Número de Cedula de Identidad o Pasaporte)
Punto distribución LCR	http://ura.firmedigital.com/lcr/ca.crl
Información del emisor	http://ura.firmedigital.com/ocsp
Política de certificados	http://www.firmedigital.com/dpc-pc/

Uso autorizado del certificado electrónico de firma para representantes de empresas públicas.

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

Certificado electrónico de firma para representante legal de empresa privada.
El uso asignado para este tipo de certificados es para 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 o 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 representante legal de empresa privada.

Campo del certificado	Valor del certificado
Versión	V3 (Número de versión del certificado).
Número de serie	(Identificador único menor de 32 caracteres hexadecimales.)
Algoritmo de firma	ECCP 256 (Curva Elíptica)
Datos del emisor	
CN	DOCUMENTOS DIGITALES PSC, C.A.
O	Sistema nacional de certificación electrónica
OU	FirmeDigital
C	VE
E	soporte@firmedigital.com
L	Maracaibo
ST	Zulia
Período de validez	
Válido desde	(Inicio vigencia del certificado)
Válido hasta	(Expiración del período de validez del certificado).
Datos del titular	

Campo del certificado	Valor del certificado
CN	(Nombre del representante legal a certificar)
T	(Cargo del representante legal a certificar)
O	(Nombre de la organización)
OU	(Nombre de la unidad organizativa) opcional
C	(País)
E	(Correo electrónico)
L	(Dirección)
ST	(Estado)
Información de clave publica	
Algoritmo de clave pública	RSA
Tamaño de clave pública	2048
Extensiones	
Restricciones básicas	CA: False
Nombre alternativo del emisor	
DNS name	Firmedigital.com
Other name	
OID 2.16.862.2.1	(Código asignado por SUSCERTE)
OID 2.16.862.2.2	RIF- J505415859
Identificador clave 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 serie Certificado	(Número de Serial)
Uso de la Clave	Firma electrónica, no repudio, cifrado
Nombre alternativo del titular	
Other name	
OID 2.16.862.2.2	(Número de cedula de identidad o pasaporte)
Punto distribución LCR	http://ura.firmedigital.com/lcr/.crl
Información del emisor	http://ura.firmedigital.com/ocsp
Política de certificados	http://www.firmedigital.com/dpc-pc/

Uso autorizado del certificado electrónico de firma para representante legal de empresa privada.

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

Certificado electrónico de firma para profesionales titulados.

El uso asignado para este certificado son las 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 de firma para profesionales titulados.

Campo del certificado	Valor del certificado
Versión	V3(Número de versión del certificado)
Número de serie	Identificador único menor de 32 caracteres hexadecimales.
Algoritmo de firma	Sha-256RSA(Algoritmo de Firma)
Datos del emisor	
CN	DOCUMENTOS DIGITALES PSC, C.A.
O	Sistema nacional de certificación electrónica
OU	ECCP 256 (Curva Elíptica)
C	VE
E	soporte@firmedigital.com
L	Maracaibo
ST	Zulia
Período de validez	
Válido desde	(Inicio vigencia del certificado)
Válido hasta	(Expiración del período de validez del certificado).
Datos del titular	
CN	(Nombre del signatario)
T	(Título profesional)
O	(Organización) campo opcional
OU	(Unidad organizacional) campo opcional
C	VE(País)
E	(correo electrónico)
L	(Dirección)
ST	(Estado)
Información de clave pública	
Algoritmo de clave pública	ECCP 256 (Curva Elíptica)
Tamaño de clave publica	2048
Extensiones	
Restricciones básicas	CA: False
Nombre alternativo del emisor	
DNS name	Firmedigital.com
Other Name	

Campo del certificado	Valor del certificado
OID 2.16.862.2.1	(Código asignado por la SUSCERTE)
OID 2.16.862.2.2	RIF-J501162549
Identificador clave 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 serie certificado	(Número Serial)
Uso de clave	Firma electrónica, no repudio, cifrado.
Nombre alternativo del titular	
Other name	
OID 2.16.862.2.2	(Número de cédula de identidad o pasaporte)
Punto distribución LCR	http://ura.firmedigital.com/lcr/ca.crl http://www.firmedigital.com/lcr/ca.crl
Información emisor	http://ura.firmedigital.com/ocsp
Política de certificados	http://www.firmedigital.com/dpc-pc/

Uso autorizado del certificado electrónico de firma para profesionales titulados.

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

Certificado electrónico de firma para persona natural.

El uso asignado para este tipo de certificado es el de transacciones privadas, distintas a prestación de servicios profesionales, comunicaciones privadas o públicas a título personal, compras electrónicas para personas naturales o, declaraciones o trámites en línea ante gobierno para personas naturales.

Estructura del certificado electrónico de firma para persona natural.

Campo del certificado	Valor del certificado
Versión	V3 (Número de versión del certificado)
Número de serie	Identificador único menor de 32 caracteres hexadecimales.
Algoritmo de firma	ECCP 256 (Curva Elíptica)
Datos del emisor	
CN	DOCUMENTOS DIGITALES PSC, C.A.
O	Sistema nacional de certificación electrónica
OU	FirmeDigital
C	VE
E	soporte@firmedigital.com

Campo del certificado	Valor del certificado
L	Maracaibo
ST	Zulia
Período de validez	
Válido desde	(Inicio vigencia del certificado)
Válido hasta	(Expiración del período de validez del certificado).
Datos del titular	
CN	(Nombre del signatario)
C	VE (País)
E	(correo electrónico)
L	(Dirección)
ST	(Estado)
Información de clave publica	
Algoritmo de clave publica	ECCP 256 (Curva Elíptica)
Tamaño de clave publica	2048
Extensiones	
Restricciones básicas	CA: False
Nombre alternativo del emisor	
DNS Name	Firmedigital.com
Other Name	
OID 2.16.862.2.1	(Código asignado por SUSCERTE)
OID 2.16.862.2.2	RIF- J505415859
Identificador clave 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 serie certificado	(Número Serial)
Uso de clave	Firma electrónica, no repudio, cifrado y firma de correo.
Uso Mejorado	Firma de documentos, correo seguro
Nombre alternativo del titular	
Other name	
OID 2.16.862.2.2	(Número de cedula de identidad o pasaporte)
Punto distribución LCR	http://www.firmedigital.com/lcr/ca.crl
Información del Emisor	http://ura.firmedigital.com/ocsp
Política de certificados	http://www.firmedigital.com/dpc-pc/

Uso autorizado del certificado electrónico de firma para persona natural.

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

Certificado de firma electrónica para funcionario público: El uso asignado para este tipo de certificado es el de certificar a una persona como funcionario público, 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 del público al cual representa, comunicaciones privadas o públicas en representación de del ente público al cual representa, comercio electrónico en representación del ente público al cual representa, declaraciones o trámites en línea ante gobierno en representación del ente público al cual representa, y/o firma electrónica en correos electrónicos o documentos electrónicos.

Estructura del certificado electrónico de firma para funcionario público.

Campo del certificado	Valor del certificado
Versión:	V3 (Número de versión del certificado).
Número de serie:	(Identificador único menor de 32 caracteres hexadecimales.)
Algoritmo de firma:	ECCP 256 (Curva Elíptica)
Datos del emisor	
CN	DOCUMENTOS DIGITALES PSC, C.A.
O	Sistema nacional de certificación electrónica
OU	FirmeDigital
C	VE(País)
E	soporte@firmedigital.com
L	Maracaibo
ST	Zulia
Período de validez	
Válido desde:	(Inicio vigencia del certificado)
Válido hasta:	(Expiración del período de validez del certificado).
Datos del titular	
CN	(Nombre del funcionario a certificar)
T	(Cargo del funcionario)
O	(Organización campo opcional)
OU	(Unidad organizacional) campo opcional
OU	(Número de cédula de identidad o pasaporte)
OU	(Tipo de instrumento utilizado para el nombramiento)
OU	(Número del instrumento de nombramiento)
OU	(Fecha de emisión)
OU	(Fecha efectiva)
OU	(Publicación)
C	(País)
E	(correo electrónico)
L	(Dirección)
ST	(Estado)

Campo del certificado	Valor del certificado
Información de clave publica	
Algoritmo de clave pública	ECCP 256 (Curva Elíptica)
Tamaño de clave publica	(2048)
Extensiones	
Restricciones básicas	CA: False
Nombre alternativo del emisor	
Dns name	Firmedigital.com
Other name	
OID 2.16.862.2.1	(Código asignado por la SUSCERTE)
OID 2.16.862.2.2	RIF- J505415859
Identificador clave titular	(identificador de la clave del titular)
Identificador de la clave de autoridad certificadora	
Id. de clave	(Identificador de la Clave)
Emisor de certificado	(Datos del emisor)
Número serie certificado	(Número Serial)
Uso de clave	Firma electrónica, no repudio, cifrado y firma de correo.
Uso mejorado	Firma de documentos, correo Seguro
Nombre alternativo del titular	
Other name	
OID 2.16.862.2.2	(Número de cédula de identidad o pasaporte)
OID 2.16.862.2.3	(Tipo de Instrumento utilizado para el nombramiento)
OID 2.16.862.2.4	(Número del instrumento de nombramiento)
OID 2.16.862.2.5	(Fecha de emisión)
OID 2.16.862.2.6	(Fecha efectiva)
OID 2.16.862.2.7	(Publicación)
Punto distribución LCR	http://ura.firmedigital.com/lcr/ca.crl http://www.firmedigital.com/lcr/Tca.crl
Información del Emisor	http://ura.firmedigital.com/ocsp
Política de certificados	http://www.firmedigital.com/dpc-pc/

Uso autorizado del certificado electrónico de firma para funcionario público.

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

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.

Campo del certificado	Valor del certificado
Versión	V3 (Número de versión del certificado).
Número de serie:	(Identificador único 32 caracteres hexadecimales.)
Algoritmo de firma:	ECCP 256 (Curva Elíptica)
DATOS DEL EMISOR	
CN	DOCUMENTOS DIGITALES PSC, C.A.
O	Sistema Nacional de Certificación Electrónica
OU	FirmeDigital
C	VE
E	soporte@firmedigital.com
L	Maracaibo
ST	Zulia
Periodo de validez	
Válido Desde:	(Inicio vigencia del certificado)
Válido Hasta:	(Expiración del periodo de validez del certificado).
Datos del titular	
CN	(Identificador del objeto)
T	(Ubicación) opcional
O	(Nombre de la organización)
OU	(Nombre de la unidad organizativa) opcional
OU	(Número de RIF)
C	(País)
E	(correo electrónico)
L	(Dirección)
ST	(Estado)
Información de clave pública	
Algoritmo clave pública	ECCP 256 (Curva Elíptica)
Tamaño clave pública	(2048)
Extensiones	
Restricciones básicas	CA: False
Nombre alternativo del emisor	
Dns name	Firmedigital.com
Other name	
OID 2.16.862.2.1	(Código asignado por la SUSCERTE)
OID 2.16.862.2.2	RIF- J505415859
Identificador de clave del Titular	(Identificador de clave del titular)

Campo del certificado	Valor del certificado
Identificador de clave de autoridad certificadora	
Id. de clave	Identificador de la clave
Emisor de certificado	(Datos del emisor)
Número serie certificado	(Número de serial)
Uso de la clave	Firma electrónica, no repudio
Uso Mejorado de la clave	Firma de Documentos
Nombre alternativo del titular	
Other name	
OID 2.16.862.2.2	(Número de cedula de identidad, pasaporte o RIF)
Punto distribución LCR	http://ura.firmedigital.com/lcrca.crl http://www.firmedigital.com/lcr/ca.crl
Información del emisor	http://ura.firmedigital.com/ocsp
Política de certificados	http://www.firmedigital.com/dpc-pc/

Uso autorizado del certificado para el control de transacción.

Uso	Uso mejorado
Firma electrónica, no repudio	Firma de documentos

Certificado electrónico para firma de Factura Electrónica: El uso asignado para este certificado es el de protección de transacciones en línea, prueba legal del comprobante electrónico, integridad de la información, no repudio y/o, firma de electrónica de documentos electrónicos.

Estructura del certificado electrónico de Factura Electrónica.

Campo del certificado	Valor del certificado
Versión	V3 (Número de versión del certificado).
Número de serie:	(Identificador único 32 caracteres hexadecimales.)
Algoritmo de firma:	ECCP 256 (Curva Elíptica)
Datos del emisor	
CN	DOCUMENTOS DIGITALES PSC, C.A.
O	Sistema Nacional de Certificación Electrónica
OU	FirmeDigital
C	VE
E	soporte@firmedigital.com
L	Maracaibo
ST	Zulia
Periodo de validez	
Válido Desde:	(Inicio vigencia del certificado)
Válido Hasta:	(Expiración del periodo de validez del certificado).

Datos del titular	
CN	(Identificador del objeto)
T	(Ubicación) opcional
O	(Nombre de la organización)
OU	(Nombre de la unidad organizativa) opcional
OU	(Número de RIF)
C	(País)
E	(correo electrónico)
L	(Dirección)
ST	(Estado)
Información de clave pública	
Algoritmo clave pública	ECCP 256 (Curva Elíptica)
Tamaño clave pública	(2048)
Extensiones	
Restricciones básicas	CA: False
Nombre alternativo del emisor	
Dns name	Firmedigital.com
Other name	
OID 2.16.862.2.1	(Código asignado por la SUSCERTE)
OID 2.16.862.2.2	RIF- J505415859
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 serie certificado	(Número de serial)
Uso de la clave	Firma electrónica, No Repudio, Cifrado.
Uso Mejorado de la clave	
Nombre alternativo del titular	
Other name	
OID 2.16.862.2.2	(Número de cedula de identidad, pasaporte o RIF)
Punto distribución LCR	http://ura.firmedigital.com/lcr/Tca.crl http://www.firmedigital.com/lcr/Tca.crl
Información del emisor	http://ura.firmedigital.com/ocsp
Política de certificados	http://www.firmedigital.com/dpc-pc/

Uso autorizado del certificado electrónico de Factura Electrónica.

Uso	Uso mejorado

Firma electrónica, no repudio	N/A

Certificado Electrónico de Banca Electrónica: El uso asignado para este certificado es el de autenticación, firma electrónica, protección de transacción en línea, prueba legal del comprobante electrónico, integridad de la información y/o no repudio.

Estructura del certificado electrónico de Banca Electrónica.

Campo del Certificado	Valor del Certificado
Versión	**V3** (Número de versión del certificado).
Número de Serie	(Identificador único del certificado. Menor de 32 caracteres hexadecimales.)
Algoritmo de Firma	ECCP 256 (Curva Elíptica)
Datos del Emisor	
CN	DOCUMENTOS DIGITALES PSC, C.A.
O	Sistema Nacional de Certificación Electrónico
OU	FirmeDigital
C	VE
E	soporte@firmedigital.com
L	Maracaibo
ST	Zulia
Periodo de Validez	
Valido Desde	(Fecha en que el periodo de validez del certificado comienza).
Válido Hasta	(Fecha en que el periodo de validez del certificado culmina al cumplir 6 meses de vigencia).
Datos del Titular	
CN	(Nombre del Representante Legal a Certificar)
T	(Cargo del Titular) dependiendo del tipo de certificado a instalar en el dispositivo móvil.
O	(Nombre de la Organización)
OU	(Nombre de la Unidad Organizativa) Opcional
C	(País)
E	(Correo Electrónico)
L	(Dirección)
ST	(Estado)
Información de Clave Publica	
Algoritmo de Clave Publica	ECCP 256 (Curva Elíptica)
Tamaño de Clave Publica	2048

Extensiones	
Restricciones básicas	CA: False
Nombre Alternativo Del Emisor	
DNS Name	Firmedigital.com
Other name	
OID 2.16.862.2.1	(Código de identificación de DOCUMENTOS DIGITALES PSC, C.A. acreditado asignado por SUSCERTE)
OID 2.16.862.2.2	RIF- J505415859
Identificador de clave de 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 de Serial)
Uso de la Clave	Firma electrónica, Autenticación, Integridad y No Repudio.
Nombre Alternativo Del Titular	
Other name	
OID 2.16.862.2.2	(Número de Cedula de Identidad o Pasaporte)
Punto de distribución de LCR	http://ura.firmedigital.com/lcr/a.crl
Acceso a la Información de la Entidad Emisora	http://ura.firmedigital.com/ocsp
Política de certificados	http://www.firmedigital.com/dpc-pc/

Usos Autorizado del Certificado Electrónico de Banca Electrónica.

Uso	**Uso mejorado**
Firma electrónica, Autenticación, Integridad y No Repudio.	**N/A**

8.2. Usos no permitidos

El cliente se obliga a utilizarlos conforme a los usos señalados en la sección anterior y de conformidad con la legislación que regula el uso de certificados electrónicos.

El certificado electrónico cuyo signatario viole el uso autorizado, será revocado. Igualmente, dicho uso indebido del certificado acarreara responsabilidades de indemnizar a DOCUMENTOS DIGITALES PSC, C.A. 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.

9. POLÍTICAS DE ADMINISTRACIÓN DE LA AC

Este documento es propiedad de DOCUMENTOS DIGITALES PSC, C.A. (FirmeDigital)

9.1. Persona contacto

El presente documento es administrado por la alta dirección y gerente general. Las dudas u otras comunicaciones sobre este documento y respecto a la operación y generación de los certificados electrónicos, deben comunicarse o dirigirse directamente a:

Calle 78 Dr.Portillo con Avenida 3D, Casa NRO 78-19 (Centro I+D+I), Barrio Valle Frio, Maracaibo, Zulia, Zona Postal 4001, Republica Bolivariana de Venezuela

E-mail soporte@firmedigital.com, Teléfono máster: +58 0424-710-0380

9.2. Competencia para determinar la adecuación de la DPC a las políticas

La dirección 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 adecuación de la DPC a las distintas políticas de operación y generación de certificados será sometida a la revisión y aprobación de la **SUSCERTE.**

10. PUBLICACIÓN DE INFORMACIÓN DEL PSC Y REPOSITORIOS DE LOS CERTIFICADOS.

10.1. Repositorios

A fin de garantizar la completa disponibilidad de este documento (DPC y PC), y demás requerimientos, DOCUMENTOS DIGITALES PSC, C.A. mantiene un repositorio dentro de su Página Web: http://www.firmedigital.com/.
Para el certificado de la AC Subordinada DOCUMENTOS DIGITALES PSC, C.A., los certificados emitidos por dicha AC y la DPC: https://www.firmedigital.com/ac.html
Para la lista de Certificados Revocados https://ura.firmedigital.com/lcr/PSC.crl http://www.firmedigital.com/lcr/.crl
Para el servicio de validación en línea (OCSP) http://ura.firmedigital.com/ocsp El repositorio público de DOCUMENTOS DIGITALES PSC, C.A., no contiene ninguna información confidencial o privada.

10.2. Publicación

Es obligación para la compañía publicar la información relativa a sus prácticas, sus certificados y el estado actualizado de dichos certificados. Dicha información se anunciará a través página

web de la siguiente forma:

La LCR, se encuentra disponible en formato CRL V2, en https://ura.firmedigital.com/lcr/pa.crl
http://www.firmedigital.com/lcr/PSC.crl
El presente documento se encuentra disponible en: https://www.firmedigital.com/dpc
El certificado de la AC se encuentra disponible en: https://www.firmedigital.com/ac
Los certificados emitidos por DOCUMENTOS DIGITALES PSC, C.A. se encuentran en: https://www.firmedigital.com/ac

Los datos de contacto en la dirección:https://www.firmedigital.com/contacto
La documentación técnica en la direcciónhttps://www.firmedigital.com/ac

10.3. Frecuencia de publicación.

10.3.1. Certificados del PSC

La publicación del Certificado del PSC - DOCUMENTOS DIGITALES PSC, C.A. se realizará una vez obtenida la acreditación por parte de la SUSCERTE. El periodo de validez es de diez años.

Los Certificados Electrónicos serán publicados de manera inmediata a su generación o revocación en el publicador del PSC - DOCUMENTOS DIGITALES PSC, C.A.. Los CE emitidos y la LCR son públicos.

10.3.2. LCR

La publicación de la LCR se realizará y actualizará cada 24 horas.

10.3.3. Declaración de prácticas de certificación

A menos que explícitamente se indique lo contrario en este documento, se publicarán en el sitio web de la compañía (www.firmedigital.com), las nuevas versiones de este documento, una vez las mismas sean aprobadas por la SUSCERTE.

10.4. Controles de acceso al repositorio de certificados

El acceso a la información publicada por la compañía será de consulta y no podrá ser modificada sin autorización. La información pública solo será actualizada por DOCUMENTOS DIGITALES PSC, C.A. Además, se garantiza la consulta a la LCR a los certificados emitidos, al servidor OCSP y el presente documento.

11. IDENTIFICACIÓN Y AUTENTICACIÓN.

11.1. Registros de nombres

11.1.1. Tipos de nombres

DOCUMENTOS DIGITALES PSC, C.A. solo genera y firma certificados de nombres acordes al estándar X.509 versión 3.

- **Para el certificado del PSC – DOCUMENTOS DIGITALES PSC, C.A.:** El nombre distintivo (DN) está formado por los siguientes atributos:
- DATOS DEL TITULAR:
  CN: DOCUMENTOS DIGITALES PSC, C.A.
  O: Sistema Nacional de Certificación Electrónica.
  OU: FirmeDigital
  C: VE.
  E: soporte@firmedigital.com
  L: Maracaibo
  S: Zulia

  El nombre alternativo (AN) de DOCUMENTOS DIGITALES PSC, C.A. está formado por los siguientes atributos:
  DNSName: firmedigital.com
  otherName:
  OID 2.16.862.2.1. (Código de identificación DOCUMENTOS DIGITALES PSC, C.A. asignado por SUSCERTE)
  OID 2.16.862.2.2.: RIF-J50116254-9

- **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)

11.1.2. Necesidad de nombres distintivos

Se requerirá a los clientes sus nombres y apellidos completos, tal como aparecen en su cédula de identidad o pasaporte. No serán admitidos o procesados 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 documento de identidad. A todos los efectos se 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.

11.1.3. 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) DintinguishName (DN). Adicionalmente todos los certificados emitidos por la compañía 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, Octubre 2021.

11.1.4. Unicidad de los nombres

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 signatario y la extensión bajo el OID 2.16.862.2.2 la cual corresponde al documento de identificación o RIF.

Por lo tanto, la unicidad se garantiza mediante la confianza sobre la unicidad de los nombres mercantiles en el Registro de Información Fiscal (RIF) emitido por el Servicio Nacional Integrado de Administración Aduanera y Tributario (SENIAT) y el registro de ciudadanos por el Servicio Administrativo de Identificación, Migración y Extranjería (SAIME).

11.1.5. Resolución de conflictos relativos a nombres

En el caso de un conflicto de nombre entre clientes y que corresponda a nombre y apellidos iguales, la AR procederá a realizar la distinción de identidad y autenticación a través del uso del número de cédula de identidad, pasaporte y/o RIF de cada cliente con las cuales se haya generado el conflicto de nombre.

Adicionalmente, si existe un cliente que mantenga contrato y haya adquirido más de un tipo de firma o certificado electrónico, la base de datos mantendrá un esquema igualitario de datos del cliente y no será permitido o procesado por la AR, datos personales disimiles y que correspondan a un mismo cliente.

11.2. Validación inicial de la identidad.

11.2.1. Método de prueba de posesión de la clave privada

El esquema de operación y plataforma tecnológica de certificación se encuentran configurados para que el cliente genere su par de claves (pública y privada).

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 del 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.
DOCUMENTOS DIGITALES PSC, C.A. controla y garantiza de forma automática la emisión del CE firmado al signatario (dueño de la clave privada), correspondiente a la clave pública incluida en la solicitud.
Esta garantía se logra mediante el formato PKCS#12 que incluye en la propia solicitud una firma electrónica de la misma realizada con la clave privada correspondiente a la clave pública del certificado.
DOCUMENTOS DIGITALES PSC, C.A. garantiza la entrega del Contenedor de Clave (Hardware o Software) posterior a la autenticación de identidad del Signatario referenciada en la sección 11.2.2 AUTENTICACIÓN DE LA IDENTIDAD DE LA ORGANIZACIÓN.

11.2.2. Autenticación de la identidad de una organización

La AR cuando se trate de firmas electrónicas que acrediten empresas o entes públicos procederá de la siguiente forma:

11.2.2.1. Ente público

La AR procederá a comprobar la publicación en la gaceta oficial de la República Bolivariana de Venezuela la resolución que acredita a la entidad o empresa pública. Todo certificado electrónico de organización deberá estar asociado a una persona responsable por dicho certificado. La AR 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 y cumplido el procedimiento satisfactoriamente, la AR comunicará a la AC su conformidad respecto a los datos para que se proceda a la generación del certificado electrónico contratado por el cliente.

11.2.2.2. Organización privada

La AR procederá a comprobar la existencia de la empresa privada a través de la revisión de su documento constitutivo-estatutario o su modificación. Todo certificado electrónico de organización deberá estar asociado a un responsable por dicho certificado. La AR 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 de la compañía y cumplido el procedimiento, la AR informará a la AC su conformidad respecto a los datos para que se proceda a la generación del certificado electrónico contratado por el cliente.

11.2.3. Comprobación de las facultades de representación

La AR cuando se trate de firmas electrónicas que acrediten la representación de empresas procederá de la manera siguiente:

11.2.3.1. Ente público

La AR procederá a comprobar la publicación en la gaceta oficial de la resolución que crea a la entidad o empresa pública. Posteriormente se validará en la publicación en la gaceta oficial venezolana el nombramiento, funciones y atribuciones del representante del ente público.

Una vez comprobadas las facultades de representación se procederá a validar el resto de la información solicitada por el sistema de contratación y cumplido el procedimiento, la AR comunicará a la AC, su conformidad respecto a los datos para que se proceda a la generación del certificado electrónico contratado por el cliente.

11.2.3.2. Organización privada

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, así como la publicación del registro de empresa en un diario mercantil.

Seguidamente la AR validará la designación en cargo realizada en asamblea ordinaria o extraordinaria del cliente, debidamente inscrita y publicada en la oficina del registro mercantil correspondiente.

Una vez comprobadas las facultades de representación se procederá a validar el resto de la información solicitada por el sistema de contratación del y cumplido el procedimiento, la AR comunicará a la AC, su conformidad respecto a los datos para que se proceda a la generación del certificado electrónico contratado por el cliente.

11.2.4. Criterios para operar con AC externas

Está sujeto a lo dispuesto por la normativa Legal y Sub-legal emitida por SUSCERTE y los acuerdos suscritos entre el DOCUMENTOS DIGITALES PSC, C.A. y sus usuarios.

11.3. Identificación y autenticación de las solicitudes de renovación de la clave.

11.3.1. Rutinarias

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

11.3.2. De la clave después de una renovación – clave no comprometida

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 que las causas de la revocación anterior ya no están presentes.

11.4. Identificación y autenticación de las solicitudes de revocación de la clave

11.4.1. De la suspensión o revocación de clave

La suspensión de las firmas o certificados electrónicos generados por la AC normalmente precede a la revocación y donde proceda dicha revocación se hará de acuerdo con los procedimientos específicos descritos en aparte.

11.4.2. 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 de DOCUMENTOS DIGITALES PSC, C.A..
- Se ha producido una emisión indebida o defectuosa de un certificado;
- 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 instrucción de la gerencia para producir una solicitud de suspensión o una decisión para proceder con la suspensión.

11.4.3. ¿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 DOCUMENTOS DIGITALES PSC, C.A. a quién 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 la compañía.
- 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 gerencia general resultará en la suspensión inmediata de la firma o certificado electrónico y en el inicio de una investigación post- suspensión.

11.4.4. Límites del período de suspensión

Las firmas o certificados electrónicos emitidos por la AC permanecerán suspendidos por un máximo de veinte (20) días. A su terminación o antes de su terminación, DOCUMENTOS DIGITALES PSC, C.A. determinará si el certificado debe ser revocado o restablecido como válido.

11.4.5. Procedimiento para la solicitud de suspensión

Para procesar una solicitud de suspensión la AC, hará lo siguiente:

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

11.4.6. Circunstancias para la revocación

Una firma o certificado electrónico emitido por la AC podrá ser revocado en los siguientes casos:

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

11.4.7. Procedimiento para la solicitud de revocación

Para procesar una solicitud de revocación la AC hará lo siguiente:

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

11.4.8. 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 del gerente general. Para realizar la solicitud de suspensión o revocación debe seguir los siguientes pasos:

Paso 1: Notificación de la suspensión o revocación, indicando los motivos, utilizando alguno de los siguientes medios: Teléfono Máster: **(58-424) 710-0380 /** e-mail para revocación: soporte@firmedigital.com

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

11.4.9. 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 AC, para revocar un certificado de acuerdo con los procedimientos operacionales de DOCUMENTOS DIGITALES PSC, C.A..

12. CICLO DE VIDA DE LOS CERTIFICADOS DEL PSC

Las firmas y los certificados electrónicos tienen un ciclo de vida de un (1) año contados a partir de la fecha de activación de la firma o certificado electrónico por parte de AC.

12.1. Solicitud de certificados

Los clientes interesados en adquirir una firma o certificado electrónico deberán ingresar en (www.firmedigital.com) y acceder al vínculo “Compra de Bloque(s)”, seleccionar el tipo de certificado, aceptar los contratos, verificar su identidad ante la AR, generar sus claves y descargar su firma o certificado electrónico.

12.1.1. Proceso de generación de la solicitud de certificados y responsabilidades

El cliente una vez cumplido el proceso de contratación del certificado electrónico de su preferencia en (www.firmedigital.com), deberá remitir la información requerida en cada uno de las ventanas del sistema de contratación, el cual ha sido explicado en el presente instructivo.

12.1.2. Proceso de firma del certificado

Una vez validada la identidad del cliente 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 DOCUMENTOS DIGITALES PSC, C.A..
- 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.

12.1.3. 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.

12.1.4. 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 gerencia de DOCUMENTOS DIGITALES PSC, C.A..

12.2. Tramitación de solicitud de un certificado.

12.2.1. 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. La explicación detallada de las funciones y atribuciones de dicha autoridad se encuentran detallados en el presente documento.

12.2.2. Aprobación o denegación de un certificado

La aprobación o denegación de una firma o certificado electrónico se encuentra asignada a la AR. Toda solicitud de firma o certificado electrónico que no sea validada por la AR automáticamente será denegada.

La AC antes de dar inicio al proceso de aprobación de una firma o certificado electrónico validará el cumplimiento del (i) pago efectuado por el cliente, (ii) el informe emanado por la AR y

(iii) confirmar el tipo de certificado requerido por el cliente. Cumplidos con dichos pasos, se procederá a la generación del certificado electrónico correspondiente.

12.2.3. 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 de la información suministrada por el mismo cliente. Si el cliente cumple los requisitos establecidos, informará a la AC para que proceda a la generación de la firma o certificado electrónico, según corresponda.

La AC generará y firmará los certificados dentro de los siguientes tres (3) días de verificada la identidad del cliente. En tal sentido, se notificará al cliente dentro de dicho plazo para que este proceda a la instalación de la firma o certificado electrónico.

12.3. Emisión de certificado.

12.3.1. Acciones de la AC durante la emisión de un certificado

Posterior a la aprobación por parte de la AR, el 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 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. Luego de emitido el certificado el signatario podrá proceder para su utilización.

12.3.2. Notificación al solicitante por parte de la AC acerca de la emisión de su certificado

La AC 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 los mismos, según corresponda. El sistema de la AC genera un correo electrónico automático, que es enviado a la cuenta de correo electrónico suministrado por el cliente.

12.4. Uso del par de claves y del certificado.

12.4.1. 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 de su clave privada y deberá reportar si la misma es comprometida, sin menoscabo de ser responsable por las acciones y consecuencias derivadas del uso indebido de sus firmas o certificados electrónicos por parte de terceras personas.

12.4.2. 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 ICP de la AC están disponibles en (www.firmedigital.com).

12.5. Renovación del certificado con cambio de clave.

12.5.1. Causas para la renovación de un certificado

Toda firma o certificado electrónico podrá ser renovado, siempre y cuando sean se verifique lo siguiente: (i) que se haya vencido el termino de vigencia de la firma o certificado electrónico, (ii) que el certificado no hay sido revocado por ninguna de las causas explicadas en el presente documento y, (iii) que el cliente cumple con el proceso de contratación y renovación requerido por la AR.

12.5.2. Entidad que puede solicitar la renovación de un certificado

Todo propietario de firma o certificado electrónico que cumpla con los requisitos solicitados, podrá solicitar la nueva generación de la firma o certificado electrónica según corresponda, salvo que exista prohibición en sentencia judicial emanada por un Tribunal competente.

12.5.3. Procedimiento de solicitud para renovación de un certificado

Los clientes interesados en renovar una firma o certificado electrónico, deberán ingresar a (www.firmedigital.com/settings/renew) y acceder al vínculo “Configuraciones - renovar”, seleccionar el tipo de certificado, aceptar los contratos, ingresar sus datos personales, validar su identidad con la AR, generar sus claves y por último descargar su firma o certificado electrónico.

12.5.4. Notificación de la emisión de un nuevo certificado a la AR

La AC 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.

12.5.5. Publicación del certificado renovado por la AC

La AC 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 (www.firmedigital.com).

12.5.6. Notificación de la emisión del certificado por la AC a otras entidades

La AC externas a DOCUMENTOS DIGITALES PSC, C.A. no se encuentra normada o desarrollada por la SUSCERTE. Sin embargo, la LSMDFE si contempla dicha posibilidad, quedando abierta la posibilidad de establecer esquemas de operación con AC externas una vez se cuente con la normativa que regule la materia.

12.6. Modificación de certificados

Las firmas o certificados electrónicos deben mantener su integridad durante su período de vigencia y no podrá ser objeto de modificación o cambio alguno.

12.7. Revocación y suspensión de un certificado.

12.7.1. Circunstancias para la revocación del certificado

Las circunstancias para la revocación del certificado son las señaladas en el presente documento.

12.7.2. 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 presente documento.

12.7.3. 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 presente documento.

12.7.4. 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, DOCUMENTOS DIGITALES PSC, C.A. determinará si el certificado debe ser revocado o restablecido como válido.

12.7.5. Circunstancias para la suspensión

Las circunstancias para la suspensión de firma o certificado electrónico según corresponda, es el señalado en el presente documento.

12.7.6. Procedimiento para la solicitud de suspensión

El procedimiento para la suspensión de firma o certificado electrónico según corresponda, es el señalado en el presente documento.

12.7.7. Límites del período de suspensión

El límite del período de suspensión de firma o certificado electrónico según corresponda, es el señalado en el del presente documento.

12.7.8. 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, 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.firmedigital.com).

12.7.9. Disponibilidad de compromiso on-line de revocación y estado de los certificados

La AC tiene la capacidad de entregar la LCR utilizando el OCSP a través del enlace http://ura.firmedigital.com/ocsp

12.7.10. Requisitos de comprobación on-line de revocación

El cliente podrá verificar el estado de un certificado a los fines de verificar si se encuentra suspendido o revocado. El cliente deberá ingresar a (www.firmedigital.com) y acceder el módulo “Autenticar”, y escribir el numero de identificación del certificado en la pagina de verificacion privada.

12.7.11. Otras formas de divulgación de información de revocación disponibles

Se notificará vía correo electrónico al cliente que corresponda, acerca de la suspensión o revocación de su certificado.

12.8. Servicio de comprobación de estado de certificados

12.8.1. Características operativas

DOCUMENTOS DIGITALES PSC, C.A. posee servicios de comprobación de estado de la firma o certificado electrónico. Dichos servicios son la LCR y OCSP para acceso en línea a la comprobación del estado de las firmas y certificados electrónicos.

12.8.2. Disponibilidad del servicio

DOCUMENTOS DIGITALES PSC, C.A. mantiene disponibles los servicios de la LCR y acceso OCSP a través de (www.firmedigital.com). La AC mantiene en operación su portal web, cumpliendo con un alto porcentaje de disponibilidad.

12.8.3. Características adicionales

Características adicionales a los servicios de LCR y acceso OCSP se encuentran señaladas en este documento.

12.9. Finalización de la suscripción

El cliente 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 DOCUMENTOS DIGITALES PSC, C.A. y por un lapso de diez (10) años, los registros correspondientes a la generación de su certificado.

12.10. Custodia y recuperación de la clave.

12.10.1. Prácticas de custodia y recuperación de la clave

La clave privada de la AC DOCUMENTOS DIGITALES PSC, C.A. está protegida por un YUBIHSM . YUBIHSM proporciona módulos de seguridad de hardware (HSM) en un Clúster. Un clúster es una colección de HSM individuales que YUBIHSM CloudHSM mantiene sincronizados. Un clúster se puede considerar un HSM lógico. Al realizar una tarea o una operación en un HSM en un clúster, el resto de los HSM de ese clúster se actualizan automáticamente. La distribución de clústeres en varias zonas de disponibilidad proporciona redundancia y alta disponibilidad. El esquema de certificación se encuentra configurados para que el cliente genere su par de claves (pública y privada). El compromiso de clave derivará del mismo cliente pues el DOCUMENTOS DIGITALES PSC, C.A. no genera el par de claves (pública y privada).

En consecuencia, si el cliente extravía su clave privada, se deberá proceder a la emisión de un nuevo certificado y deberá cumplir el proceso de contratación a tales efectos. La clave pública siempre estará en el repositorio.

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

13.1. Controles de seguridad física

La AC mantiene un esquema operacional orientado a garantizar la continuidad operacional y prestación de sus servicios con altos estándares de calidad, oportunidad y seguridad.

La seguridad es una responsabilidad compartida entre y DOCUMENTOS DIGITALES PSC, C.A.. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

13.1.1. De la Seguridad de la Nube YubiHSM (Tier 3) (FISICO)

YubiHSM (Tier 3) (FISICO) es responsable de proteger la infraestructura que ejecuta los servicios de YubiHSM. YubiHSM también le proporciona servicios que puede utilizar de forma segura. Hay auditores externos que prueban y verifican periódicamente la eficacia de la seguridad en los Programas de conformidad de YubiHSM. La evidencia documentada de que la implementación de los Controles y pautas de seguridad de la información para el Servicio está en consonancia con las afirmaciones realizadas por el proveedor del Servicio en YubiHSM incluye las siguientes certificaciones:

- ISO 9001:2015, certificado 2014-014; (DAYCOHOST)
- ISO 27001:2013, certificado 2013-009;
- ISO 27017:2015, certificado 2015-015;
- ISO 27018:2019, certificado 2015-016; y
- CSA STAR CCM v3.0.1, certificado 2020-026.

13.1.2. De la Seguridad de la Información

DOCUMENTOS DIGITALES PSC, C.A. es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables. Al efecto, DOCUMENTOS DIGITALES PSC, C.A. fundamenta sus procesos de seguridad de la información a través de los siguientes documentos:

- Declaración de Prácticas de Certificación (***PSC-PSC-DPC-001 DOCUMENTOS DIGITALES PSC, C.A.***)
- Política de Seguridad de la Información (***PSC-CCG-POL-002-Política de Seguridad de la Información***)
- Política de Seguridad de la Información para Servicios en la Nube (***PSC-CCG-POL-003 - Política de Seguridad de la Información para Servicios en la Nube***)
- Política de Confidencialidad(***PSC-CCG-POL-004 -Política de Confidencialidad***)
- Política de Control de Acceso(***PSC-CCG-POL-005 -Política de Control de Acceso***)
- Plan de Seguridad de la Información(***PSC-CCG-PLA-001 -Plan de Seguridad de la Información***)
- Plan de Continuidad Organizacional(***PSC-GRI -PLA-001 - Plan de Continuidad Organizacional***)
- Análisis de Impacto Organizacional(***PSC-GRI -PRO-001 - Análisis de Impacto Organizacional***)
- Evaluación de Riesgos de Seguridad de la Información(***PSC-GRI-PRO-002 -Evaluación de Riesgos de Seguridad de la Información***)
- Gestión de Riesgos y Oportunidades(***PSC-GRI-PRO-003 - Gestión de Riesgos y Oportunidades***)
- Plan de Administración de Claves Criptográficas(***PSC-PSC-PLA-001 Plan de Administración de Claves Criptográficas***)
- Manual de Normas y Procesos para la Provisión de Servicios de Certificación Electrónica(***PSC-PSC-PRO-001 Provisión de Servicios de Certificación Electrónica***)

- Manual de Operación de la Autoridad de Certificación(***PSC-PSC-MAN-001 Manual de Operación de la Autoridad de Certificación***)
- Manual de Operación de la Autoridad de Registro(***PSC-PSC-MAN-002 Manual de Operación de la Autoridad de Registro***)

7.1. Controles funcionales.

7.1.1. Papeles de confianza

La AR y AC 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 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, 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 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 inherentes a la operación y trámites de la compañía.

7.1.2. Número de personas requeridas por posición

La estructura interna de DOCUMENTOS DIGITALES PSC, C.A. se encuentra discriminada de la manera siguiente:

- Gerencia General (1)
- El consultor de tecnología (1).
- El consultor de seguridad de la información y cumplimento (1).
- La autoridad de registro (AR) (1).
- El personal de administración (1).
- Los servicios tercerizados

7.1.3. Identificación y autenticación de cada rol

Las funciones y responsabilidades asociadas a cada cargo se encuentran señaladas en el

documento ***PSC-GTH-FOM-005 - Descripción de Cargos***.

7.2. Controles de seguridad personal.

7.2.1. Requerimientos de acreditación

El personal 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. La operación de la ICP 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 DOCUMENTOS DIGITALES PSC, C.A.

7.2.2. Requerimientos de formación

Ningún miembro del personal 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, sin autorización o sin 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.

7.2.3. Sanciones por acciones no autorizadas

Todo procedimiento no contemplado en el presente documento, deberá contar con la aprobación expresa y por escrito de la organización, de lo contrario será considerado como acto de sabotaje y será sancionado conforme a la legislación laboral correspondiente.

7.3. Procedimientos de control de seguridad.

7.3.1. Tipos de eventos registrados

La compañía almacena registros electrónicos de eventos (logs) relativos a su actividad. Estos registros son almacenados de forma automática y electrónica. 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 origino. Los records 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.

7.3.2. Frecuencia de registros de logs

Los registros de auditoria se llevan a cabo en cualquier momento que se realice una operación en la raíz de certificación de la AC, 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 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.

7.3.3. Período de retención para los logs de auditoría

Los registros de Auditoria se retienen por un período de diez (10) años.

7.3.4. Protección de los logs de auditoría

El sistema de recolección de auditoria es una combinación de procesos automáticos y procedimientos manuales desempeñados por la AC, 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.

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.

7.4. Archivo de informaciones y registros

Todos los records de la ICP referentes a la operación de sus servicios de certificación son archivados y retenidos por un período mínimo de siete (7) años.

El recurso de tiempo para la raíz de certificación de la AC es verificado periódicamente de manera independiente y todos los records automatizados de la raíz de certificación 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.

La información de identificación será archivada directamente por la AC y la cual requerirá a la AR que archive los records e información por un período de siete (7) 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.

7.4.1. Tipo de informaciones y eventos registrados

El tipo de información y registro de eventos será el mismo explicado en el presente documento.

7.4.2. Período de retención para el archivo

El período de retención para archivo será el mismo contemplado en el presente documento.

7.4.3. Protección del archivo

El método de protección de archivo será el mismo contemplado en el aparte 27.4.4., del presente documento.

7.4.4. Requerimiento para el estampado de tiempo para el registro

Los procesos y pasos que deberán ser cumplidos para prestar el servicio de estampado de tiempo no se encuentran normados o desarrollados por la SUSCERTE.

7.4.5. 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 log 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 un respaldo en nube y en disco duros externos.
Las unidades de respaldo son almacenadas en bóveda externa al centro de datos.

7.5. Cambio de clave

El esquema de operación de certificación 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 DOCUMENTOS DIGITALES PSC, C.A. no genera el par de claves (pública y privada).
En consecuencia, si el cliente extravía su clave privada, se deberá proceder a la emisión de un nuevo certificado y deberá cumplir el proceso de contratación a tales efectos. La clave pública siempre estará en el repositorio antes explicado.

7.6. Recuperación en caso de desastre.

7.6.1. Procedimiento de gestión de incidentes y vulnerabilidades

DOCUMENTOS DIGITALES PSC, C.A. ha establecido un plan de continuidad de negocio y recuperación ante desastres (PRD), ante un eventual compromiso parcial o total de la ICP de la AC. 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/o, desastres naturales y terminación.

La gerencia debe 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 PRD se especifica el procedimiento a realizar en cada uno de los escenarios considerados como desastre y a continuación se mencionan las principales responsabilidades 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.

7.6.2. Alteración de los recursos, hardware, software y/o datos

Se ha establecido un PDR, ante un eventual compromiso parcial o total de la infraestructura de clave pública (ICP). El plan de recuperación ante desastre es revisado periódicamente.

7.6.3. Procedimiento de actuación ante la vulnerabilidad de la clave privada de una autoridad

Aunque se 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 siguiente:

- Cese inmediato del servicio de venta y generación de certificados electrónicos.
- Declaración del escenario de desastre.
- Notificación a la SUSCERTE del compromiso de la clave.
- Publicación del evento en la página web.
- Notificación a los clientes mediante correo electrónico.
- 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.
- Acordar junto con la SUSCERTE las acciones a tomar para la reactivación del servicio de emisión de certificados.

7.6.4. 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.

7.6.5. Cese de actividad

La organización tiene contemplado en el supuesto que ocurra una cesación de operaciones, los siguientes supuestos:

- 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 la organización 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.

8. CONTROLES DE SEGURIDAD TÉCNICA.

8.1. Generación del par de claves

DOCUMENTOS DIGITALES PSC, C.A., genera su par de claves (pública y privada) utilizando

un módulo de hardware criptográfico YubiHSM que cumple con el FIPS 140-1 Nivel 3.

El esquema de operación de DOCUMENTOS DIGITALES PSC, C.A. y su plataforma Tecnológica de Certificación, se encuentran configurados para que el cliente genere su par de claves (pública y privada). En consecuencia, si el cliente extravía su clave privada, se deberá proceder a la emisión de un nuevo certificado y deberá cumplir el proceso de contratación a tales efectos. La clave pública siempre estará en el repositorio, de conformidad con en el presente documento.

8.1.1. Entrega de la clave privada

El esquema de certificación 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 ya que DOCUMENTOS DIGITALES PSC, C.A. no genera el par de claves (pública y privada).

8.1.2. Entrega de la clave pública

El esquema de operación 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 ya que DOCUMENTOS DIGITALES PSC, C.A. no genera el par de claves (pública y privada).

La clave pública siempre estará en el repositorio, de conformidad con lo señalado en el presente documento.

8.1.3. Disponibilidad de la clave pública

DOCUMENTOS DIGITALES PSC, C.A. 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 (https://ura.firmedigital.com/psc/cadena.p12).

8.1.4. 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 ECCP 256 (Curva Elíptica).

8.1.5. 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 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 con el objeto de garantizar la protección de la clave privada:

El usuario final debe ingresar a la página web (http://www.firmedigital.com) ingresar en el enlace **sistema de certificación** (https://www.firmedigital.com/signature) y de esta forma ingresar al sistema de certificación. Luego debe de verificar que los datos contenidos están correctos**.**

Información del Usuario: Esta sección contiene el nombre y apellido del usuario.

Subject: Información general del usuario que, dependiendo del tipo de certificado, algunos campos serán obligatorios.

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)

8.1.6. Hardware/software de generación de claves

Se utiliza un módulo criptográfico en la nube para almacenar de forma segura la clave privada. Dicho modulo criptográfico en YubiHSM provista por Yubico HSM, 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.
- RSA.
- Mecanismos de Intercambio de Claves.
- DH.
- DES / DES3 XOR.
- Funciones HASH y HMAC.
- MD2.
- MD5.
- RIPEMD 160.
- SHA-2.

- SHA-1.

- **Referencias:** A los efectos de documentar y proveer información del hardware criptográfico en la nube, se señala la dirección web que se indica a continuación: https://www.yubico.com/la-yubikey/yubihsm-2-y-yubihsm-2-fips/?lang=es . Adicionalmente, el módulo criptográfico utilizado por la AC soporta la generación de claves de 4096 bits y tiene la capacidad de firmar y cifrar.

8.1.7. Propósitos de utilización de claves

La clave privada puede ser usada para (i) firma de certificados a las autoridades de certificación de pólizas, firma de certificados establecidos en el presente documento, firma de listas de revocados de certificados, firma de certificados cruzada aprobada por la SUSCERTE y DOCUMENTOS DIGITALES PSC, C.A..

8.2. Protección de la clave privada.

8.2.1. Estándares para los módulos criptográficos

El módulo criptográfico en la nube usado por ICP, está certificado para cumplir con los requerimientos de FIPS nivel 3.

8.2.2. Control “N” de “M” de la clave privada

La clave privada de DOCUMENTOS DIGITALES PSC, C.A., 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.

8.2.3. Custodia de la clave privada

La clave privada de la AC está protegida por el servicio de YubiHSM.

8.2.4. Copia de seguridad de la clave privada

El respaldo de la clave privada se realiza en la nube y físicamente en un disco duro externo almacenado en una caja de seguridad. La clave de cifrado de la raíz de certificación de DOCUMENTOS DIGITALES PSC, C.A. solamente se respalda a los fines de recuperación ante desastres.

8.2.5. Archivo de la clave privada

La clave privada de la AC se encuentra almacenada en un componente lógico Yubi HSM, el cual es el encargado de respaldarla y cifrarla. Tanto el respaldo como el cifrado son

almacenados en la nube y en un disco duro externo, el cual el administrador de la AC se asegurará de mantener a resguardo en un lugar seguro.

8.2.6. 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:

Primero, la verificacion de identidad de la persona (juridica o natural)
Luego, habilitacion para creacion de firma electronica en la plataforma www.firmedigital.com
A continuacion, la persona hace clic en 'Generar Firma' de manera voluntaria
Alli, tiene que aceptar las politicas de privacidad, uso de datos, y contrato de uso

8.2.7. Método de activación de la clave privada

Para poder administrar las claves, debe iniciar sesión en el HSM con el nombre de usuario y la contraseña de un usuario de criptografía (CU). Sólo una CU puede crear una clave. El CU que crea una clave posee y administra esa clave.

8.2.8. Método de destrucción de la clave privada

Normalmente, Yubico no cancela el aprovisionamiento de un dispositivo YubiHSM que contiene material de claves. De este modo, tanto DOCUMENTOS DIGITALES PSC, C.A. como YubiHSM están protegidos frente a los riesgos asociados con la destrucción accidental de material de claves que todavía esté en uso.
Si necesita dejar de utilizar un dispositivo de almacenamiento de credenciales y firmas electrónicas de YubiHSM se realiza una copia de seguridad del contenido del dispositivo HSM en otro HSM controlado por DOCUMENTOS DIGITALES PSC, C.A. o bien se confirma que ya no son necesarias las claves almacenadas en el HSM.
Para dejar de usar un dispositivo HSM:

- Desde la instancia de control, conectarse al HSM a través de SSH.
- Poner a cero el HSM al intentar iniciar sesión en el HSM como el administrador de HSM tres veces con una contraseña no válida.
- Desclasificar el dispositivo HSM ejecutando primero el comando para rotar todos los registros.
- Eliminar todos los registros.
- Utilizar uno de los siguientes métodos para cancelar el aprovisionamiento del HSM:
  - Usar Herramientas de la interfaz de línea de comandos clásicas de YUBIHSM CloudHSM para cancelar el aprovisionamiento del HSM con el comando de delete-hsm.
  - Usar YUBIHSM clásica para cancelar el aprovisionamiento del HSM con el DeleteHsm.

8.2.9. Ranking del módulo criptográfico

La AC utiliza YUBIHSM. Los requisitos de conformidad de YUBIHSM se cumplen a través de la validación FIPS 140-2 de nivel 3 del hardware, en lugar de formar parte de un programa de auditoría independiente.

YUBIHSM administra el firmware en el hardware. Un tercero se encarga de mantener el firmware. Además, NIST evalúa la conformidad con FIPS 140-2 de nivel 3 de todo el firmware, lo que está ampliamente explicado en el sitio oficial del Programa de Validación de Módulos Criptográficos (https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program). Solo se puede instalar el firmware que dispone de una firma criptográfica de la clave FIPS (a la que YUBIHSM no tiene acceso)

8.3. Otros aspectos de la gestión del par de claves.

8.3.1. Archivo de la clave pública

La clave pública de DOCUMENTOS DIGITALES PSC, C.A. es archivada según el formato .pem, por un periodo de 10 años.

8.3.2. Períodos operativos de los certificados y del par de claves

El certificado tendrá una validez de 10 años. Las firmas y los certificados electrónicos generados por DOCUMENTOS DIGITALES PSC, C.A. tienen un ciclo de un (1) año contado a partir de la fecha de activación de la firma o certificado electrónico por parte de la AC. 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.

8.4. Datos de activación.

8.4.1. 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 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 y de esta forma garantizar la vinculación de identidad de la persona con su clave pública.

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.

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 realizado 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.

Una vez validada la identidad por la AR y generado el certificado por la AC, el cliente procede a descargar la firma o certificado electrónico en el repositorio de su computadora, aceptando la fuente de emisión del certificado.

8.4.2. Protección de datos de activación

La activación del certificado emitido es realizada utilizando el sistema de certificación, limitándose en el equipo o dispositivo donde se hayan generado el par de claves.

8.5. Controles de seguridad del computador.

8.6. Requisitos técnicos específicos

Se 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.

8.7. Calificaciones de seguridad computacional

Se utiliza productos certificados, al menos, por el Nivel E3 de las normas ITSEC.

8.8. Controles de seguridad del ciclo de vida.

8.8.1. Controles de desarrollo de sistemas

El software 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 YubiHSM utilizado por la ICP y la AC cumple con los requerimientos FIPS 140-2.

8.8.2. 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.

8.8.3. 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.

8.9. Controles de seguridad de la red

El hardware y software para la ICP y la AC son mantenidos fuera de línea en una instalación de alta seguridad dentro de un control de seguridad y 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.

8.10. Controles de ingeniería de los módulos criptográficos

DOCUMENTOS DIGITALES PSC, C.A. utiliza módulos criptográficos en la nube disponibles comercialmente y desarrollados por terceros. En particular, utiliza módulos criptográficos que cumplen con la certificación FIPS 140-2, Level 3 (nShield F3) y Level 2 (nShield F2).

9. PERFILES DE CERTIFICADOS, LCR y OCSP.

9.1. Perfil del certificado

Los certificados 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, March2004 (prevaleciendo en caso de conflicto la TS 101 862).

Estructura de datos raíz de DOCUMENTOS DIGITALES PSC, C.A.:

1. Campo del Certificado	Valor del Certificado
Versión	V3 (Número de versión del certificado).

Número de serie	(Identificador único menor de 32 caracteres hexadecimales.)
Algoritmo de firma	ECCP 256 (Curva Elíptica)
2. Datos del Emisor	
CN	Autoridad de Certificación Raíz del Estado Venezolano
O	Sistema nacional de certificación electrónica
OU	Superintendencia de Servicios de Certificación Electrónica
C	VE
E	acraiz@suscerte.gob.ve
L	Caracas
ST	Distrito Capital
3. Período de Validez	
Válido Desde	(Inicio vigencia del certificado)
Válido Hasta	(Expiración del periodo de validez del certificado).
4. Datos del Titular	
CN	DOCUMENTOS DIGITALES PSC, C.A.
T	(Cargo del titular)
O	Sistema Nacional de Certificación Electrónica
OU	FirmeDigital
C	VE
E	soporte@firmedigital.com
L	Maracaibo
ST	Zulia
5. Información de Clave Pública	
Algoritmo de clave pública	ECCP 256 (Curva Elíptica)
Tamaño de clave pública	(4096)
6. Extensiones	
Restricciones básicas	CA: TRUE y LONGITUD DEL PATH=1
Uso de la Clave	Firma Electrónica del Certificado y Firma de LCR
Identificador de clave de Titular	(Identificador de clave del titular)
6.1. Nombre alternativo del Emisor	
DNS name	suscerte.gob.ve
Other name 2.1.6.862.2.2	RIF-G-20004036-0
6.2. Identificador de clave de autoridad de certificación	
Id. de clave	(Identificador de la clave de la AC - DOCUMENTOS DIGITALES PSC, C.A.)
Emisor de certificado	(Datos del emisor AC Raíz de SUSCERTE)
Número serie certificado	(Número de Serial de la AC Raíz de SUSCERTE)
6.3. Nombre alternativo del titular	
DNSName	Firmedigital.com
Other name 2.16.862.2.1	###### (Asignado por SUSCERTE)
Other name 2.16.862.2.2	RIF- J505415859
Punto de distribución de LCR	http://ura.firmedigital.com/lcr/ca.crl

Información del emisor	http://ura.firmedigital.com/ocsp
Política de certificados 2.16.862.1.2	http://www.firmedigital.com/dpc-pc/
7. Signature Algorithm	
Signature Algorithm	ECCP 256 (Curva Elíptica)
8. Signature	
Signature Value	[Especifica el contenido de la firma del certificado (valor generado de la función Hash)]

9.1.1. Número de versión

DOCUMENTOS DIGITALES PSC, C.A. emite CE bajo el estándar X.509 de la UIT-T (Unión Internacional de Telecomunicaciones) en su versión 3 de conformidad con el RFC 5280 para perfiles de certificados y LCR's y con el certificado AC Raíz de Venezuela emitido por SUSCERTE.

9.1.2. Extensiones del certificado

Las extensiones utilizadas de forma genérica en los certificados son:

- BasicConstraints: Calificada como crítica.
- KeyUsage: Calificada como crítica.
- CertificatePolicies: Calificada como no crítica
- SubjectAlternativeName: Calificada como no crítica
- LCRDistributionPoint: Calificada como no crítica
- SubjectKeyIdentifier: Calificada como no crítica
- AuthorityKeyIdentifier: Calificada como no crítica
- AuthorityInformationAccess: Calificada como no crítica

En cada PC se establecen las estructuras de datos con el conjunto de extensiones utilizadas por cada tipo de CE.

9.1.3. Identificadores de objeto (OID) de los algoritmos

El OID del algoritmo criptográfico es ECCP 256 (Curva Elíptica) (O.I.D).

9.1.4. Formatos de nombres

Los CE emitidos por DOCUMENTOS DIGITALES PSC, C.A. están restringidos a 'Distinguished names' (DN) X.500 que son únicos y no ambiguos, los CE contienen el DN del emisor y del sujeto del CE en los campos: issuer name y subject name. Para ampliar esta información refiérase a las correspondientes Políticas de Certificación.

9.1.5. Restricciones de los nombres

Los nombres contenidos en los CE de DOCUMENTOS DIGITALES PSC, C.A., están restringidos a 'Distinguished names' (DN) X.500 que son únicos y no ambiguos.

9.1.6. Identificador de objeto (OID) de la PC

DOCUMENTOS DIGITALES PSC, C.A. utiliza la definición de política de asignación de OID's según el árbol privado de numeración asignado por la SUSCERTE.

TIPO DE DOCUMENTO	IDENTIFICADOR DE OBJETO (OID)
DPC PSC - DOCUMENTOS DIGITALES PSC, C.A.	0.00.000.00.0.0
PC Persona Natural	0.00.000.00.0.0
PC Persona Funcionario	0.00.000.00.0.0
PC Profesionales Titulados	0.00.000.00.0.0
PC Representante de Empresa Privada	0.00.000.00.0.0
PC Representante de Empresa Pública	0.00.000.00.0.0
PC de Factura Electrónica	0.00.000.00.0.0.0
PC de Firma de Transacción	0.00.000.00.0.0.0

9.2. Perfil de LCR

La LCR es emitida bajo el estándar X.509 de la UIT-T (Unión Internacional de Telecomunicaciones) versión 2, de conformidad con el CE de la AC Raíz emitido por SUSCERTE y el perfil LCR.

Cuando un usuario desea comprobar la validez de un certificado verificar 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.

A continuación se indica la lista de los campos utilizados:

Campo Estándar X509	Valor del Campo	Ubicación	Descripción del Campo
Versión	V2	CRL	Indica la versión del estándar X509 que soporta los campos indicados en la generación de la lista de revocación de certificados
Signature Algorithm	ECCP 256 (Curva Elíptica)	CRL	Indica el algoritmo de hash que se utilizó para la generación de la

<table>
<tr><td></td><td></td><td></td><td>firma de la LCR</td></tr>
<tr><td>Issuer</td><td><table>
<tr><th>Campo</th><th>Valor</th><th>Descripción</th></tr>
<tr><td>C (Country)</td><td>VE</td><td>Indica el país de procedencia de la CRL. Sigue el estándar ISO para la codificación del país</td></tr>
<tr><td>O (Organization)</td><td>Sistema Nacional de Certificación Electrónica</td><td>Indica la organización a la cual pertenece la CRL</td></tr>
<tr><td>OU (Organization Unit)</td><td>DOCUMENTOS DIGITALES PSC, C.A.</td><td>Indica la unidad organizacional a la cual pertenece la CRL</td></tr>
<tr><td>ST (State)</td><td>Zulia</td><td>Indica el estado en el cual se encuentra ubicado el emisor de la CRL</td></tr>
<tr><td>L (Locality)</td><td>Maracaibo</td><td>Indica la localidad específica donde se encuentra ubicado el PSC</td></tr>
<tr><td>CN (Common Name)</td><td>FirmeDigital</td><td>Indica el nombre que identifica al Proveedor de Servicios de Certificación</td></tr>
<tr><td>E o emailAddress</td><td>soporte@firmedigital.com</td><td>Indica el correo electrónico del PSC</td></tr>
</table></td><td>CRL</td><td>Contiene la información de la entidad emisora de la lista de revocación de certificados, siguiendo el formato DN (Distinguished Name)</td></tr>
<tr><td>Last Update</td><td>Fecha en formato GMT de la última actualización</td><td>CRL</td><td>Indica la fecha en formato GMT de la última actualización de lista de certificados revocados</td></tr>
<tr><td>Next Update</td><td>Fecha en formato GMT de la próxima actualización</td><td>CRL</td><td>Indica la fecha en formato GMT de la próxima actualización de lista de certificados revocados</td></tr>
<tr><td>CRL Extensiones</td><td></td><td></td><td></td></tr>
<tr><td>Authority Key Identifier</td><td><table>
<tr><th>Campo</th><th>Valor</th><th>Descripción</th></tr>
<tr><td>Keyid</td><td>Valor hexadecimal</td><td>Identificador de la clave publica de la AC Raíz</td></tr>
<tr><td>DirNa me</td><td>Contiene el DN (C, O, OU, ST, L, CN, E) de la AC Raíz</td><td>Contiene la información de la AC Raíz con el formato DN</td></tr>
</table></td><td>Extensiones</td><td>Contiene información para identificación de la clave pública de la autoridad de certificación</td></tr>
</table>

			(Distinguished Name)	
	seriall	Numero positivo no negativo	Contiene el numero del certificado del emisor	
Issuer Alternative Name	Campo / OID / Valor /			Extensiones	Contiene información acerca del emisor del certificado. La información almacena es el DNS, RIF del PSC y el identificador del PSC.
	DNS	N/A	www.firmedigital.com	DNS del PSC	
	otherName	2.16.862.2.1	PSC-00000# (Asignado por SUSCERTE)	Identificador único del PSC	
	otherName	2.16.862.2.	RIF-G-20004036-0	Documento de identificación del PSC (RIF)	
CRL Distribution Points	URI: http://ura.firmedigital.com/lcr/ca.crl			Extensiones	Contiene URI donde se encuentra disponible la LCR
Authority Information Access	OCSP – URI: http://ura.firmedigital.com/ocsp			Extensiones	Contiene URI donde se encuentra disponible OCSP
Certificate Policies	Policy: 2.16.862.11.1.1 CPS: http://www.firmedigital.com/dpc-pc/			Extensiones	Contiene los URI donde se encuentra disponible la DPC y el OID de la DPC
CRL Number	Numero positivo no negativo			CRL Number	Numero positivo no negativo
Revoked Certificates	Lista de certificados revocados (serial y fecha de revocacion). Serial en hexadecimal y fecha en formato GMT			CRL	Contiene una lista de todos los certificados revocados identificados por serial y fecha de revocación
Signature Algorithm	ECCP 256 (Curva Elíptica)			CRL	[Especifica el contenido de la firma del certificado (valor generado de la funcion Hash)]
Signature	Especifica el contenido de la firma del certificado			CRL	(valor generado de la función Hash)

9.2.1. Número de versión

La LCR emitida por DOCUMENTOS DIGITALES PSC, C.A. corresponde con el estándar X.509 versión 2

9.2.2. Extensiones de las LCR

Las extensiones de las LCR emitidas por la AC Raíz, son las definidas por el IETF en su RFC 2459, es decir:

- Authority Key Identifier
- LCR Number
- Issuing Distribution Point

9.3. Perfil de OCSP

9.3.1. Número de versión

Los CE de OCSP Responder utilizarán el estándar X.509 versión 3

9.3.2. Extensiones OCSP

Las extensiones X509v3 utilizadas en los certificados de OCSP son:

- Subject Key Identifier
- Authority Key Identifier
- KeyUsage
- extKeyUsage
- Certificate Policies
- Policy Identifier
- URL DPC
- Notice Reference
- Basic Constraints
- Subject Type
- Auth Information Access
- OCSPNoCheck

10. AUDITORÍA DE CONFORMIDAD

10.1. Frecuencia de los controles de conformidad para cada entidad

Las auditorías externas, de control y seguimiento, se efectúan anualmente para la renovación de la acreditación ante SUSCERTE, con el fin de garantizar el correcto desempeño de la relación comercial de DOCUMENTOS DIGITALES PSC, C.A. con los terceros de buena fe, de la Infraestructura Nacional de Certificación Electrónica y las auditorías internas se realizan semestralmente.

10.2. Auditores

Las auditorias anuales serán efectuadas por el auditor seleccionado por DOCUMENTOS DIGITALES PSC, C.A. El auditor seleccionado deberá estar acreditado ante el registro de auditores que mantiene la SUSCERTE.

10.3. Relación entre el auditor y la autoridad auditada

Esta relación se limita estrictamente a los procesos e información requerida para la auditoría. Por lo tanto, la parte auditada de DOCUMENTOS DIGITALES PSC, C.A. no debe tener ninguna relación, actual o planificada, financiera, legal, o de cualquier otra índole que pueda derivar en un conflicto de intereses con el auditor.
Para el auditor externo se debe cumplir lo establecido en la Norma N°047 de SUSCERTE. En el caso de los auditores internos, estos no podrán tener relación funcional con el área objeto de la auditoría.

10.4. Tópicos cubiertos por el control de conformidad

Son objeto de auditoría todos los requisitos técnicos, funcionales y organizativos entre ellos:

- La DPC y PC utilizadas.
- Políticas de Seguridad.
- Administración y gestión de la AC Raíz
- Gestión y distribución de las claves
- Consideraciones de Confidencialidad
- Seguridad Física y lógica
- Sistema de gestión de seguridad de la información del AC Raíz (Plan de Contingencia y Recuperación ante Desastres, Plan de Continuidad de las Actividades, entre otros)
- Personal Operativo.

10.5. 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 y que sea considerado como “No conformidad”, será sometido a plan de remediación y cumplimiento, el cual deberá establecer el cronograma y tiempo fijado para superar la “No conformidad”, en el supuesto que la misma sea declarada.

10.6. 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.

11. REQUISITOS COMERCIALES Y LEGALES.

11.1. Aranceles

El LSMDFE establece la obligación 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 de DOCUMENTOS DIGITALES PSC, C.A. y en el supuesto de cese de operación; situación en la cual la SUSCERTE asumirá el control y operación de la plataforma tecnológica. Adicionalmente, la SUSCERTE establece la obligación para el PSC de mantener garantía constituida en forma de póliza de seguro y a favor de los clientes usuarios de firmas o certificados electrónicos

11.2. Responsabilidad financiera

Los límites de la responsabilidad de DOCUMENTOS DIGITALES PSC, C.A. hacia sus clientes, está regulada mediante acuerdos contractuales con dichos clientes. La responsabilidad para con los clientes, partes dependientes y cualquier otra entidad usuaria de firmas o certificados electrónicos, 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. 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.

Sujeto a las limitaciones anteriores, el límite de responsabilidad agregada de la AC 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 autoridad de certificación (AC) excederá el límite antes mencionado.

11.3. Política de confidencialidad.

11.3.1. Información confidencial

Toda la recopilación y uso de la información compilada es realizada cumpliendo con la legislación de la venezolana y basándose en las distinciones suministradas en este documento. 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. En los casos de 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.

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. DOCUMENTOS DIGITALES PSC, C.A. se compromete a proteger los datos de su actividad como entidad de la Infraestructura Nacional de Certificación Electrónica de Venezuela.

No obstante, DOCUMENTOS DIGITALES PSC, C.A. se reserva el derecho a revelar a los empleados y consultores, externos o internos, los datos confidenciales necesarios para realizar sus actividades como PSC. En este caso los empleados y/o consultores son informados sobre las obligaciones de confidencialidad de forma tal que se comprometen a proteger todos los datos a los que tenga acceso como consecuencia de la relación laboral.

11.3.2. Información no confidencial

Tipos de información no considerados confidenciales:

- Contenido de los CE.
- LCR.
- La clave pública de la AC-DOCUMENTOS DIGITALES PSC, C.A..
- Las versiones de la DPC.
- PC.
- Reglamento y políticas de funcionamiento.
- Toda otra información identificada como “De Uso Público”

11.3.3. Publicación de información sobre revocación o suspensión de un certificado

La AC-DOCUMENTOS DIGITALES PSC, C.A. pública su LCR cada veinticuatro (24) horas y cada vez que se revoque un CE, estando disponibles a través del servicio de publicación del PSC-DOCUMENTOS DIGITALES PSC, C.A. http://ura.firmedigital.com/lcr/ca.crl

11.3.4. Divulgación de información como parte de un proceso judicial o administrativo

La suspensión o revocación de un certificado pueden hacerse públicas de acuerdo con la ley aplicable o bajo la responsabilidad única y absoluta de DOCUMENTOS DIGITALES PSC, C.A.. La información sobre suspensión de certificados será revelada solo al cliente 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 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 es entregado a ninguna persona excepto donde: i) se produzca una solicitud de información debidamente documentada; 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 en cualquier jurisdicción donde los procedimientos legales apropiados se hayan cumplido.

11.4. Protección de la información privada/secreta.

11.4.1. Información considerada privada

De acuerdo a lo dispuesto en la Constitución de la República Bolivariana de Venezuela se considera información privada, la siguiente: i) nombres y apellidos; ii) número de cédula de identidad, pasaporte y RIF; iii) Direcciones y datos telefónicos del cliente; y iv) datos suministrados en el proceso de contratación de firma o certificado electrónico.

11.4.2. Información considerada no privada

Toda información considerada como no privada permanece publica en el Sitio Web de la AR.

11.4.3. Responsabilidades de proteger la información privada/secreta

La organización tiene la obligación de mantener a resguardo la información suministrada por los clientes contratantes de firmas o certificados electrónicos generados. 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 gerencia de DOCUMENTOS DIGITALES PSC, C.A..

11.4.4. Prestación del consentimiento en el uso de la información privada/secreta

La información dispuesta en archivos 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 consentimiento escrito por parte del cliente cuya información se trate, o por mandato judicial impuesto por Tribunal.

11.4.5. 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 presente documento.

11.5. Derechos de propiedad intelectual.

11.5.1. 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 se indique lo contrario, las prácticas, política, los documentos operacionales y de seguridad referentes a la infraestructura de ICP (electrónicos o no) así como los contratos, son de la propiedad de DOCUMENTOS DIGITALES PSC, C.A.. Mediante los contratos correspondientes para la prestación de servicios de certificación,

DOCUMENTOS DIGITALES PSC, C.A. 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.

11.5.2. Claves pública y privada

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.

11.5.3. Certificado

Se reserva el derecho de suspender o revocar cualquier certificado de acuerdo con los procedimientos y las políticas establecidas en el presente documento.

11.5.4. Nombres distinguidos

Los derechos de propiedad intelectual en nombres distinguidos y números de identificación de clientes no son responsabilidad de DOCUMENTOS DIGITALES PSC, C.A. a menos que se especifique lo contrario en un contrato o acuerdo.

11.5.5. Propiedad intelectual

La propiedad intelectual del presente documento, así como de toda la información, publicaciones y documentos generados y contenidos o no dentro de su página web (www.firmedigital.com), son propiedad exclusiva de DOCUMENTOS DIGITALES PSC, C.A..

11.6. Representaciones y garantías

DOCUMENTOS DIGITALES PSC, C.A. mantiene un ejercicio autónomo respecto a sus marcas registradas y derechos de autor tutelados. Adicionalmente mantiene acuerdos de representación con otras empresas en el sector tecnológico, seguridad informática, hardware criptográfico y certificación electrónica.

11.7. Obligaciones y responsabilidad civil.

11.7.1. Obligaciones de la Autoridad de Registro

La AR asume la responsabilidad de una serie de aspectos tal y como se describe a continuación:

- Cumplir con la legislación venezolana que regule la certificación electrónica o de autoridad de certificación electrónica. Asimismo, cumplir con las 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 LSMDFE y su RLSMDFE.
- Cumplir con la vigencia de la póliza de seguro requerida por la SUSCERTE para operar como AC.
- Cumplir los contratos de prestación de servicios de certificación mantenidos con los clientes.
- Mantener y actualizar la documentación de la compañía.
- Publicar en la página web (www.firmedigital.com) el presente documento, la información sobre la LCR y la política de vida de certificados, así como cualquier otra documentación que sea de obligatorio cumplimiento.
- Mantener la confidencialidad de la información suministrada por los clientes, salvo que exista un mandato judicial para develar alguna información protegida por el derecho de confidencialidad.
- Mantener un registro de las contrataciones de servicios del DOCUMENTOS DIGITALES PSC, C.A. 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 la legislación venezolana.
- Verificar que los clientes envíen toda la documentación necesaria según el tipo de certificado electrónico que deseen adquirir. Además, verificar que dicha información sea correcta para su posterior acreditación.
- Establecer acciones de mejoras en el proceso de acreditación.
- Cumplir y hacer las políticas de empresa en materia de informática, administración y recursos humanos.

11.7.2. Obligaciones de la AC

La AC asume la responsabilidad de una serie de aspectos tal y como se describe a continuación:

- Cumplir con la legislación venezolana que regule la certificación electrónica o de autoridad de certificación electrónica. Asimismo, cumplir con las normativas técnicas emanadas de la SUSCERTE.
- Cumplir y mantener vigente los requisitos requeridos para la acreditación como PSC de acuerdo a la normativa vigente.
- 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.
- Actualizar la documentación de la compañía, en especial el DPC, PC y LCR.
- Publicar en (www.firmedigital.com) la DPC, PC, LCR, así como cualquier otro documento exigido por ley.
- Asegurar el cumplimiento de auditorías anuales por parte de auditores acreditados ante la

SUSCERTE.

- Mantener la confidencialidad de la información suministrada por los clientes, salvo que exista un mandato judicial para develar alguna información protegida por el derecho de confidencialidad.
- 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 dichos contratos.
- Monitorear el contrato de prestación de servicios con el centro de datos desde donde opera la plataforma de certificación de la AC.
- Mantener y actualizar la documentación que sea de obligatorio cumplimiento a tenor de lo dispuesto las leyes venezolanas.

11.7.3. Obligaciones del Signatario

- Aportar información cierta y verdadera en la solicitud del certificado y mantenerla actualizada.
- Actuar con diligencia respecto de la custodia y conservación de los datos de generación de firma o cualquier otra información sensible como claves, códigos de activación del certificado, palabras de acceso, números de identificación personal, etc., así como de los soportes del certificado, lo que comprende en todo caso, la no revelación de ninguno de los datos mencionados.
- Conocer y cumplir las condiciones de utilización del certificado previstos en la DPC y en la PC correspondiente de DOCUMENTOS DIGITALES PSC, C.A., y en particular, las limitaciones de uso del certificado.
- Notificar diligentemente a DOCUMENTOS DIGITALES PSC, C.A. las circunstancias o sospecha de pérdida de la confidencialidad, la divulgación, modificación o uso no autorizado de los datos de generación de firma así como cualquier modificación de los datos aportados en la solicitud del certificado, solicitando cuando consecuentemente, la revocación del correspondiente certificado vía electrónica a través del Sitio Web www.firmedigital.com.
- Revisar la información contenida en el certificado, y notificar al PSC- DOCUMENTOS DIGITALES PSC, C.A. cualquier error o inexactitud.
- Eliminar o destruir el certificado del dispositivo criptográfico cuando el certificado caduque, o cuando sea revocado.
- Cualquier otra que se contemple en la DPC y en la PC correspondiente del PSC- DOCUMENTOS DIGITALES PSC, C.A., para el tipo de certificado.

11.7.4. Obligaciones de los terceros de buena fe

Los clientes y terceros de buena fe, deben cumplir las condiciones siguientes:

- Verificar antes de depositar su confianza en un CE, su validez en el momento de efectuar cualquier acción basada en los mismos y asegurarse de que el CE es apropiado para el uso que se pretende.
- Aceptar que los mensajes o documentos firmados con la clave privada del signatario tiene el mismo efecto y validez legal que si se hubiera realizado la firma autógrafa.
- Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los CE en los que confía.
- Notificar cualquier hecho o situación anómala relativa al CE y que pueda ser considerada como

causa de revocación.

11.7.5. Obligaciones del repositorio

DOCUMENTOS DIGITALES PSC, C.A. 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 (https://www.firmedigital.com/). Adicionalmente mantendrá accesible todos sus certificados emitidos, incluyendo la información de su estatus.

11.8. Renuncia de garantías

La organización cuenta con garantías constituidas a favor de la SUSCERTE y de los clientes. Por tal motivo y en mejor derecho de los clientes, la renuncia de dichas garantías no será aplicable a DOCUMENTOS DIGITALES PSC, C.A..

11.9. Limitación de responsabilidades.

11.9.1. Deslinde de responsabilidades

La organización no asumirá la responsabilidad de datos y procedimientos que no se encuentren contemplados en la LSMDFE, el RLSMDFE y normativas de la SUSCERTE, dentro de esos procedimientos y garantías se señalan los siguientes:

- Alcanzar resultados específicos;
- Con relación a la exactitud de la información contenida en los certificados que verificados por la AR;
- Que no están relacionadas con los temas cubiertos por este DPC y PC.
- Sobre la responsabilidad 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;
- Con relación a los asuntos fuera del alcance 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, sin embargo 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.
- 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, entre otros;
- Si existe un retraso, 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 estas DPC;
- Incumplimiento de terceros con protección de datos local o legislación sobre privacidad, legislación sobre protección al consumidor o cualquier otro cumplimiento establecido en la ley; o
- Cualquier daño directo o indirecto, perdida 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 ICP, el monto de cualquier daño reconocido también está limitado bajo las condiciones fijadas en la póliza de seguro requerida por la SUSCERTE antes referida.

11.9.2. Limitaciones de pérdidas

Los límites de la responsabilidad de DOCUMENTOS DIGITALES PSC están estipulados en los acuerdos celebrados con los clientes. Como referencia a estos contratos se incorporan esté documento de la declaración DPC y PC y demás documentos relevantes a la prestación del servicio. La responsabilidad de DOCUMENTOS DIGITALES PSC, C.A. para con los clientes, proveedores o parte interesada, está limitada contra reclamos de cualquier tipo, incluyendo contractuales, 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.

11.10. Indemnizaciones

Toda indemnización será producto de un proceso de investigación y análisis o de resolución de conflictos conforme al presente documento y donde se determine la responsabilidad de la compañía.

11.11. Plazo y finalización.

11.11.1. Plazo

Las PC´s y DPC entran en vigor desde el momento de ser aprobadas por SUSCERTE, para luego ser publicadas en el Sitio Web de la AR a partir de ese momento la versión anterior queda derogada y la nueva versión reemplaza íntegramente a la anterior.

11.11.2. Finalización

Las obligaciones y restricciones que establece este documento, en referencia a información confidencial, auditorías, obligaciones y responsabilidades, nacidas bajo su vigencia, subsistirán

tras su sustitución o derogación por una nueva versión en todo en lo que no se oponga a esta.

11.12. Notificaciones

Las notificaciones deben hacerse mediante un mensaje electrónicamente firmado que pueda ser verificado con un certificado 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 DOCUMENTOS DIGITALES PSC, C.A., se considerará que la notificación no ha sido recibida.

11.13. Modificaciones.

11.13.1. Procedimiento de especificación de cambios

El procedimiento para el cambio de forma unilateral de la DPC, será el siguiente:

- Los cambios solicitados son estudiados y aprobados por la Gerencia de DOCUMENTOS DIGITALES PSC, C.A..
- El personal técnico realiza los cambios requeridos sobre las DPC y las PC, establecidos en el control de Cambio de DOCUMENTOS DIGITALES PSC, C.A..
- El auditor interno procede a validar los cambios aprobados sobre la DPC, las PC, genera un informe de diagnóstico donde se relacionan las conformidades y no conformidades encontradas en la validación.
- Se comunica a los signatarios de los CE los correspondientes cambios a la DPC o PC si los cambios pudieran afectar la aceptabilidad de los CE.
- La DPC y PC actualizada es publicada en el Sitio Web, una vez es aprobada por SUSCERTE.

11.13.2. Procedimientos de publicación y notificación

El proceso de publicación y notificación de los cambios efectuados en la documentación que requiera una publicación en su sitio web, deberá cumplir con lo señalado en el presente documento, contar con la aprobación de la SUSCERTE y notificación a los clientes de la actualización vía correo electrónico.

11.13.3. Procedimiento de aprobación de la DPC

El procedimiento a seguir para la aprobación formal de la DPC/PC:
• La DPC/PC sigue el procedimiento de cambio establecido por el PSC-DOCUMENTOS DIGITALES PSC, C.A..
• El Gerente General de DOCUMENTOS DIGITALES PSC, C.A., es el responsable de aprobar los cambios en la DPC/PC de forma tal que la nueva versión en formato digital es firmada y

enviada a SUSCERTE para su revisión y aprobación formal.
• Una vez revisada y aprobada por SUSCERTE, la DPC/PC de DOCUMENTOS DIGITALES PSC, C.A. es publicada en su Sitio Web.

11.14. Resolución de conflictos.

DOCUMENTOS DIGITALES PSC, C.A. y el cliente reconocen el valor de la solución pronta y equitativa de las controversias que puedan surgir con la operación, generación o venta de la firma electrónica y certificados electrónicos, A tal efecto, fijan un plazo de quince (15) días hábiles para intentar dirimir amistosamente sus diferencias. En el caso que el acuerdo no sea posible, el cliente podrá acudir al órgano competente a la materia SUSCERTE, a fin de que sirva como mediador en el conflicto, cuya resolución será vinculante para las partes de conformidad con lo establecido en la LSMDFE.

11.14.1. Jurisdicción competente

En el supuesto de no lograr resolver los potenciales conflictos amistosamente, las controversias que guarden relación directa o indirecta con este documento se someterán a la jurisdicción, conforme a lo dispuesto en la LSMDFE y su Reglamento Parcial

11.15. Legislación aplicable

Lo no previsto en el presente documento será regulado de conformidad con lo establecido en el ordenamiento jurídico de la República Bolivariana de Venezuela.

11.16. Conformidad con ley aplicable

Todos los procesos, procedimientos, información técnica y legal contenida en el presente documento se encuentra en un todo elaborada y de conformidad con lo establecido en la LSMDFE y normativas de la SUSCERTE.

12. GESTIÓN DE REGISTROS GUARDADOS EN BASE A ESTE DOCUMENTO

12.1. Respaldo y conservación de la política

Esta Declaración de Prácticas de Certificación debe ser respaldada para su protección de acuerdo a los procedimientos del Manual de Normas y Procedimientos de Protección y Conservación de la Información del Servicio (***PSC-CON-PRO-001 - Protección y Conservación de Información del Servicio***)