Soluciones Tecnológicas Apacuana C.A.
Av Leonardo Da Vinci, CC Bello Monte,
Nivel 3, Of D Urb Bello Monte. Caracas
Miranda Zona Postal 1080

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN SOLUCIONES TECNOLÓGICAS APACUANA, C.A.

ABRIL 01, 2024

Por medio de la presente se aprueba el siguiente documento: **"DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (DPC)"** el cual ha sido revisado y certificado por las unidades y responsables que intervienen en el proceso.

Elaborado por:
Consultor externo:
Mercedes Linares Yánez

Aprobado por:		
Director Ejecutivo	**Director de Tecnología**	**Director de Operaciones**
Diego Torrealba	Diego Brito	Jaime Parada

Este Documento fue debidamente aprobado por los miembros de **SOLUCIONES TECNOLÓGICAS APACUANA C.A.**, durante la Reunión Ordinaria N.° 10 de fecha 1 de abril de 2024

CONTENIDO

I. TÍTULO

Documento de Declaración de Prácticas de Certificación (DPC).

II. CÓDIGO

STA-DO-012

III. INTRODUCCIÓN

La práctica de certificación electrónica se ha venido desarrollando en la República Bolivariana de Venezuela, a través de una serie de fundamentos legales y el apoyo de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE). Lo que permite que mediante el presente documento se establezcan las normas y condiciones que regirán los servicios a ser prestados por el Proveedor de Servicios de Certificación de APACUANA, en adelante PSC APACUANA. Este documento está dirigido a los trabajadores de Apacuana y a las instituciones públicas o privadas que por el ejercicio de sus funciones requieran el uso de Certificados Electrónicos a través del PSC APACUANA, para el aseguramiento de las operaciones realizadas en el Sistema de la Empresa. De igual modo, incluye los procesos de solicitud, identificación, activación y revocación de los certificados, así como la gestión y el uso de los dispositivos de generación de firma y verificación. El presente documento se basa en la norma RFC 3647 “Internet X.509V3 Public Key Infrastructure Certificate Policy and Certification Practices Framework” del Internet Engineering Task Force (IETF) (que sustituye a la RFC2527) como guía de asistencia en la redacción de este tipo de documentos. Con la implementación de una Infraestructura de clave pública “ICP”, APACUANA va a proveer seguridad a su información electrónica. Esta “ICP” comprende sistemas y servicios que proveen y administran certificados X.509 v3 para criptografía de llave pública. Es por esto, que la finalidad de este documento es describir las prácticas de certificación que se van a implementar en el PSC APACUANA para asegurar la confiabilidad de llaves públicas a sus usuarios.

IV. REFERENCIAS NORMATIVAS

1. Decreto 1.204 con fuerza de Ley de Mensajes de Datos y Firmas Electrónicas, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N.º 37.148 de fecha 28 de febrero del 2001.

2. Reglamento Parcial del Decreto Ley sobre Mensajes de Datos y Firmas Electrónicas. Gaceta Oficial N.º 38.086 del 14 de diciembre del 2004.

3. Norma SUSCERTE N.º 022. Modelo para la Declaración de Prácticas de Certificación y Políticas de Certificación de los Proveedores de Servicios de Certificación.

4. Norma SUSCERTE N.º 027. Guía para la Acreditación de Proveedores de Servicios de Certificación.

5. Norma SUSCERTE N.º 032. Infraestructura Nacional de Certificación Electrónica: Estructura, Certificados y Listas de Certificados Revocados.

6. Norma SUSCERTE N.º 040. Guía de Estándares Tecnológicos y Lineamientos de Seguridad para la Acreditación como Proveedor de Servicios de Certificación.

V. DEFINICIONES

A los efectos de este documento, se establecen las siguientes definiciones y terminologías:

1. Acreditación: Es el título que otorga la Superintendencia de Servicios de Certificación Electrónica a los Proveedores de Servicios de Certificación para proporcionar certificados electrónicos, una vez cumplidos los requisitos y condiciones establecidas en la Ley Sobre Mensajes de Datos y Firmas Electrónicas (LSMDFE).

2. Archivo de Clave: Proceso de almacenar claves usadas o su ID y/o certificados como un registro en almacenamientos de largo plazo para futuras recuperaciones.

3. Auditoría: Evaluación del sistema de registros y actividades para evaluar la adecuación y la efectividad de los controles de sistemas garantizando el cumplimiento de las políticas y procedimientos operacionales establecidos y recomendados para la operación de un "PSC", detectando los cambios necesarios en los controles, políticas y procedimientos y asegurando los cambios en el tiempo.

4. Auditoría de Cumplimiento: Evaluación de los registros y actividades del sistema para probar la adecuación de los controles y garantizar el cumplimiento de la política establecida de los procedimientos operacionales, detectar debilidades de seguridad y recomendar cambios en los controles, políticas y procedimientos.

5. Autoridad de Certificación (AC): Autoridad que crea, emite y maneja el ciclo de vida de los certificados, la cual a los efectos del Decreto Ley de Mensajes de Datos y Firmas Electrónicas (LSMDFE), debe contar con la acreditación otorgada por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).

6. Autoridad de Registro: Entidad cuyo propósito es suministrar apoyo local a la Infraestructura de Clave Pública “ICP” de una Autoridad de Certificación (AC). La Autoridad de Registro desempeña un conjunto de funciones orientadas a la validación, comprobación y conformación de la documentación suministrada, así como a la identidad física de un usuario.

7. Certificado Electrónico: Mensaje de datos proporcionado por un Proveedor de Servicios de Certificación (PSC) que le atribuye certeza y validez a la firma electrónica.

8. Emisor: Persona que origina un mensaje de datos por sí mismo o a través de terceros autorizados.

9. Firma Electrónica: Información creada o utilizada por el signatario o usuario, asociada al mensaje de datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado.

10. Mensaje de Datos: Toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio electrónico.

11. Nombre significativo: Corresponde al nombre especificado en el documento oficial presentado por el usuario en el momento del registro.

12. Organización: Empresa pública o privada que requiere del uso de un certificado electrónico, para la tramitación de operaciones con Apacuana.

13. Par de Claves: corresponde a la clave pública y privada que componen todo certificado electrónico.

14. Suscriptor: Todo sujeto jurídicamente hábil, susceptible de adquirir derechos y contraer obligaciones.

15. PSC APACUANA: Proveedor de Servicios de Certificación de APACUANA, cuya función es proveer servicios de certificación electrónica de Apacuana, mediante la emisión, revocación y firmar de certificados electrónicos a través de la Autoridad de Certificación (AC) y Autoridad de Registro (AR).

16. Signatario: Persona titular de una firma electrónica o certificado electrónico.

17. Sistema de Información: Herramienta utilizada para generar, procesar o archivar de cualquier forma mensajes de datos.

18. Usuario: Toda persona que utilice un sistema de información.

VI. SÍMBOLOS Y ABREVIATURAS

AC	Autoridad de Certificación.
AR	Autoridad de Registro.
DPC	Declaración de Prácticas de Certificación.
ICP	Infraestructura de Claves Públicas.
LCR	Lista de Certificados Revocados.
OID	Identificador Único de Objeto.
PC	Políticas de Certificados.
PSC APACUANA	Proveedor de Servicios de Certificación de Apacuana.

SUSCERTE	Superintendencia de Servicios de Certificación Electrónica.

VII. IDENTIFICACIÓN DEL DOCUMENTO

Nombre:	Declaración de práctica de certificación
Versión	1.0
Estado	Vigente
Fecha de Emisión	01 de abril de 2024
Fecha de Expiración	En 10 años
Localización Electrónica	/T01-Documentos técnicos/ /T04-Políticas de certificación y administración de los servicios/

VIII. ALCANCE

El presente documento se encuentra dirigido a todos los actores del contexto de firma electrónica, así como para los usuarios de los certificados electrónicos emitidos por el Proveedor de Servicios de Certificación de Apacuana (PSC APACUANA), de acuerdo a lo establecido en las Políticas de Certificados (PC) y a las competencias establecidas en la Ley, donde se requiera establecer la comunicación con las aplicaciones AR y AC de APACUANA, garantizando la integridad y confidencialidad de la información.

Estas aplicaciones, incluyen por los procesos de solicitud, identificación de los certificados, entre otras, sin quedar restringidas a ellas el correo electrónico, la transmisión de información cifrada, accesos a sitios Web seguros y la firma digital. El presente documento se rige por la normativa legal vigente de la

República Bolivariana de Venezuela en materia de mensajes de datos y firma electrónica, contemplando los aspectos de seguridad de la información.

IX. COMUNIDAD DE USUARIOS Y APLICABILIDAD

1. Proveedor de Servicios de Certificación

El PSC que presenta esta Declaración de Prácticas de Certificación es PSC Apacuana, enmarcada dentro de los lineamientos establecidos en la Ley de Mensajes de Datos y Firma Electrónica, su Reglamento Parcial, los cuales pasan por el proceso de aprobación de SUSCERTE antes de ser publicada.

El PSC Apacuana tiene una Autoridad de Certificación (AC), la cual es firmada por SUSCERTE. Esta AC del PSC Apacuana, recibirá solicitudes del signatario y se circunscribe a las operaciones para la emisión certificados electrónicos para firmas electrónicas. En este sentido, la AC, realiza las siguientes operaciones:

- Registro de Solicitud y Firma de Certificado Electrónicos
- Emisión, Renovación de los Certificados Electrónicos
- Revocación y Suspensión de los Certificados Electrónicos
- Emisión, Firma y Procesamiento de la Lista de Certificados Revocados (LCR).
- Emisión, Firma y Procesamiento del certificado electrónico del Servicio de Comprobación de Estado de Certificados en línea (OCSP).

2. Autoridad de Certificación (AC)

El presente documento se encuentra bajo la responsabilidad de la Empresa Apacuana, como PSC APACUANA.

En tal sentido, el PSC APACUANA es responsable de administrar los certificados electrónicos, efectuando todas las actividades relacionadas a la emisión, firma, renovación y revocación de los certificados emitidos de acuerdo a las políticas establecidas en el documento (PC), así como de la publicación de la lista de certificados correspondientes.

Funciones:

1. Aprobar, firmar y revocar las peticiones de certificado.
2. Establecer los perfiles del certificado.
3. Comprobar la identidad del solicitante
4. Aceptar y firmar peticiones de certificado, después de la comprobación de la identidad del solicitante del certificado.
5. Administrar las aplicaciones que utilizan los certificados electrónicos
6. Controlar qué usuarios pueden o no pueden solicitar un tipo de certificado específico.

3. Autoridad de Registro (AR)

La Autoridad de Registro, se regirá de acuerdo a las Políticas de Certificación (PC) definidas acorde a los tipos de certificados, en tal sentido la AC denegará la comprobación de las identidades de acuerdo a las Políticas de Certificación (PC) establecidas.

Funciones:

1. Operar y administrar la autoridad de registro.
2. Realizar la tramitación de solicitudes de certificados electrónicos.
3. Presentar informes sobre las actividades asignadas
4. Provisionar los dispositivos criptográficos de los signatarios y prestar atención de la revocación de los certificados.
5. Realizar soporte de tercer nivel, con relación a problemas reasignados desde el servicio de asistencia al usuario.

4. Modelo de Confianza

Para asegurar la continuidad de las operaciones del PSC APACUANA, se cuenta con un personal altamente calificado por sus responsabilidades, son sometidos a diversos procedimientos de control, a fin de garantizar la estabilidad del servicio prestado a través de los certificados electrónicos. El Ámbito de Aplicación del Modelo de Confianza del PSC APACUANA, se detalla en el apartado “VII AMBITO DE APLICACIÓN”, del documento “STA-DO-Modelo de Confianza”.

5. Registro de Acceso Público

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

1. Asegurar el acceso a información relevante descriptiva del sistema por parte de los Clientes.
2. Ofrecer una descripción del sitio web del Proveedor de Servicios de Certificación (PSC) APACUANA.
3. Señalar los servicios y productos ofrecidos por el Proveedor de Servicios de Certificación (PSC) APACUANA.
4. Describir la tecnología (hardware y software) utilizado.
5. Descripción del proceso de contratación de certificados electrónicos.

6. Información acerca de los mecanismos de seguridad utilizados en el portal web del Proveedor de Servicios de Certificación (PSC

Ver documento “STA-DO-003-Registro de Acceso Público”.

6. Signatario

Persona natural o jurídica, que actúa en nombre propio o en el de una persona jurídica a la que representa y que está autorizada en función de cada una de las Políticas de Certificados establecidas.

7. Terceros de buena fe

Usuarios que decidan aceptar y confiar en los servicios prestados por el PSC APACUANA, para la ejecución de operaciones seguras mediante los sistemas de información de la Empresa Apacuana, que además se encuentren definidos en las Políticas de Certificación.

X. USO DE LOS CERTIFICADOS

1. Usos permitidos.

Los certificados electrónicos emitidos por el PSC APACUANA, serán única y exclusivamente para uso de firma electrónica: Persona Natural, Profesional Titular, Representante de Empresa Pública, Empleado de Institución Pública (Funcionario Público), Representante de Empresa Privada y Empleado de Empresa Privada, que se encuentren relacionados al cargo que cumplan en la empresa y al proceso del prestador del servicio.

2. Usos no permitidos

Los certificados del PSC APACUANA deben utilizarse, conforme a las funciones permitidas y señaladas en la sección anterior, a lo establecido en el Decreto con Fuerza de Ley Sobre Mensaje de Datos y Firmas Electrónicas (LSMDFE). En este sentido los usos no permitidos son todos los que no estén en el apartado anterior.

XI. POLÍTICAS DE ADMINISTRACIÓN DEL PSC APACUANA

1. Especificación del ente organizador

El presente documento, es propiedad de Apacuana, por lo que la Empresa es responsable del registro, mantenimiento y actualización de las (DPC) y (PC), además de mantener las publicaciones actualizadas para sus usuarios. En tal sentido, se detalla toda la información relacionada a la Organización:

Nombre de la AC:	Apacuana.
Correo Electrónico:	contacto@apacuana.com
Dirección de la Organización:	Av. Principal de Bello Monte. C.C. Bello Monte. Piso 3. Oficina 3D. Caracas. Distrito Capital.
Número Teléfonos:	+58 424-2258248
Sitio Web:	https://www.apacuana.com

2. **Persona contacto**

Para cualquier información relacionada a está DPC o a los certificados emitidos por el PSC APACUANA, los usuarios podrán comunicarse a través de los siguientes medios:

Nombre de Contacto:	Diego Torrealba
Número de Contacto:	0412-9986725
Correo Electrónico:	contacto@apacuana.com
Dirección de la Organización:	Av. Principal de Bello Monte. C.C. Bello Monte. Piso 3. Oficina 3D. Caracas. Distrito Capital.
Sitio Web:	https://www.apacuana.com

3. **Competencia para determinar la adecuación de la DPC a las políticas de certificados (PC)**

La adecuación de la Declaración de Prácticas de Certificación y Políticas de Certificación del PSC APACUANA, serán responsabilidad de la Dirección de Operaciones de Soluciones Tecnológicas Apacuana.

XII. PUBLICACIÓN DE INFORMACIÓN DEL PSC APACUANA Y REPOSITORIOS DE LOS CERTIFICADOS

1. **Repositorios**

Los servicios de publicación a los cuales podrán acceder los usuarios, estarán disponibles los (365) trescientos sesenta y cinco días del año, durante las (24) veinticuatro horas del día, en caso de interrupción, el mismo se restablecerá en un plazo no mayor a (48) cuarenta y ocho horas. Los repositorios de los certificados se encontrarán disponibles en las siguientes direcciones electrónicas:

1.1 Para los certificados de la AC Raíz web: https://pub.apacuana.com/ac-raiz Sección: Certificados.

1.2 Para la lista de certificados revocados (LCR):

web: https://pub.apacuana.com/lcr/ Sección: Lista de Certificados Revocados.

1.3 Para la DPC y PC:

web: https://pub.apacuana.com/docs/dpc-pc/

Sección: Declaración de Prácticas de Certificación y Política de Certificación.

2. Validez de la Publicación

El presente documento y sus anexos son públicos y se encuentran disponibles en el sitio web de APACUANA: https://pub.apacuana.com/docs/dpc-pc/

El certificado raíz es público y se encuentra disponible en el sitio: https://pub.apacuana.com/ac-raiz

Los certificados emitidos por el PSC APACUANA se encuentran disponible en el sitio Web: https://portal.apacuana.com/ce

La lista de certificados revocados es pública y se encuentra disponible en el sitio Web del PSC APACUANA: https://pub.apacuana.com/lcr/ACAPACUANA.crl, así mismo estas deben permanecer disponibles al público en todo momento y sólo se procederá a su borrado una vez transcurridos (05) cinco años, no obstante, se mantendrá archivo histórico respaldado en cinta por diez (10) años, transcurrido este tiempo se podrá borrar o destruir permanentemente.

Tal como lo indica la Ley Sobre Mensajes de Datos y Firmas Electrónicas (LSMDFE), el PSC APACUANA debe garantizar la integridad, disponibilidad y accesibilidad de la información y documentos relacionados con los servicios que proporciona. En este sentido, el PSC APACUANA realizará publicaciones de toda aquella

información considerada de dominio público, la cual estará disponible a través de la página Web: https://pub.apacuana.com/docs/

3. Frecuencia de publicación

La publicación del Certificado del PSC APACUANA, se efectuará una vez obtenida la acreditación por parte de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) en el repositorio público del PSC APACUANA https://pub.apacuana.com/ac-raiz, su período de validez será de diez (10) años y se regirá de acuerdo a los siguientes parámetros:

1.1 Publicación de los certificados emitidos por el PSC APACUANA

La publicación de todos los certificados electrónicos emitidos mediante el PSC APACUANA, serán publicados diariamente, los 365 días del año mientras el psc Apacuana se encuentre en operaciones https://portal.apacuana.com/ce.

1.2 Lista de certificados revocados (LCR)

La lista de certificados revocados del PSC APACUANA, será publicada cada veinticuatro (24) horas o cada vez que sea revocado un certificado. Dicha Lista de certificados revocados estará disponible en el portal de APACUANA https://pub.apacuana.com/lcr/ACAPACUANA.crl.

1.3 Versiones anteriores y actualizaciones de la DPC y PC

El PSC APACUANA a fin de garantizar la disponibilidad de los documentos vigentes a sus usuarios, llevará un control de versiones y en caso de actualización de alguno de estos lo identificara con la palabra “vigente”, adicionalmente la

publicación de la Declaración de Prácticas de Certificación y Políticas de Certificación del PSC APACUANA, se encontrará en la dirección electrónica https://pub.apacuana.com/docs/dpc-pc/ una vez hayan sido aprobados y certificados los cambios por SUSCERTE.

1.4 Los datos de contacto de la AC

Los datos de contacto del PSC APACUANA, se encuentran especificados en el Capítulo XI "POLÍTICAS DE ADMINISTRACIÓN DE LA AC", apartado N° 2 "Persona contacto" del presente manual.

En caso, de existir algún cambio de los datos del contacto del PSC APACUANA, los cambios se notificarán mediante la publicación de la noticia en el portal web: https://www.apacuana.com/nosotros y adicionalmente se efectuarán todos los cambios necesarios para la actualización de la documentación correspondiente.

4. Controles de acceso al repositorio de certificados

La información publicada por el PSC APACUANA en su sitio web, está clasificada de acuerdo a su uso y está firmada electrónicamente, sólo podrá ser consultada por personas interesadas. La actualización de la información del PSC Apacuana sólo será realizada por el personal designado del PSC Apacuana en su estructura organizativa.

XIII. IDENTIFICACIÓN Y AUTENTICACIÓN

1. Registro de nombres

El PSC APACUANA 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 del PSC APACUANA es la siguiente:

Campos del certificado	Valor del certificado
Versión	V3 (Número de versión del certificado).
Número de Serie **Serial Number**	(Identificador único menor de 25 caracteres hexadecimales.)
Algoritmo de Firma (signatureAlgorithm)	ecdsa-with-SHA512
Datos del emisor	
CN	SUSCERTE
O	Sistema Nacional de Certificación Electrónica
País (countryName)	VE
Datos de validez	
No Antes (notBefore)	Fecha (UTC)
No Después (notAfter)	Fecha (UTC)
Datos del titular (Subject)	
Nombre Común (commonName)	PSC APACUANA
Correo Electrónico (emailAddress)	contacto@apacuana.com
Teléfono (telephoneNumber)	+58 424 2258248
Departamento	SOLUCIONES TECNOLOGICAS APACUANA

(organizationalUnitName)	
Organización (organizationName)	Sistema Nacional de Certificación Electrónica
Localidad (localityName)	Caracas
Estado (stateOrProvinceName)	Miranda
País (countryName)	VE
Información de Clave Pública del Titular (subjectPublicKey)	
Algoritmo de Firma (signatureAlgorithm)	id-ecPublicKey
NIST CURVE	P-521
Extensiones	
Restricciones Básicas (basicConstraints)	**X**
Autoridad de Certificación (AC)	TRUE
Uso de la llave (keyUsage)	**X**
Firma de certificado	keyCertSign(5)
Firma de LCR	cRLSign (6)
Firma digital	digitalSignature
Puntos de Distribución de las LCR (cRLDistributionPoints)	
Punto de distribución LCR (distributionPoint)	https://pub.apacuana.com/lcr/APACUANA.crl

Políticas de Certificación (PolicyInformation)	
PolicyInformation (PC o CP)	
policy identifier(s)	<OID Autorizado por SUSCERTE> 1.3.6.1.5.5.7.14
cPSuir	<Dirección donde se puede descargar la PC >
PolicyInformation (DPC o CPS)	
policyIdentifier	(OID Autorizado por SUSCERTE) 1.3.6.1.5.5.7.2.1
cPSuir	https://pub.apacuana.com/docs/dpc-pc/dpc.pdf
Identificador de clave de autoridad certificadora	
Id. de clave	48:82:34:4E:E6:31:11:03:E6:53:2C:81:23:D1:47:46:B5:EA:94:6E
AIA (authorityInfoAccess)	
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP] https://pub.apacuana.com/ocsp
Firma	
Algoritmo de Firma (signatureAlgorithm)	ecdsa-with-SHA512
Firma(signature)	<Contenido de la Firma>

El PSC APACUANA posee una plataforma de certificación auditada y autorizada por la SUSCERTE la cual cumple con los estándares internacionales para operación de una

infraestructura de clave pública bajo estándar X-509 V3. Además, se encuentra en capacidad de emitir certificados electrónicos para distintos usos. La SUSCERTE previa evaluación de cumplimiento de los requisitos de Ley, firma una petición de certificado con la plataforma del certificado raíz del estado venezolano. Una vez firmado el certificado, el PSC APACUANA se constituye en una autoridad de certificación de segundo nivel y se encuentra subordinada a la SUSCERTE.

El certificado raíz generado por la SUSCERTE, debe ser integrado por el PSC APACUANA, dentro de su plataforma de certificación a los efectos de poder a su vez generar y asignar los certificados electrónicos bajo los parámetros del decreto ley sobre mensajes de datos y firmas electrónicas (LSMDFE) y su reglamento (RLSMDFE).
El PSC APACUANA debe generar cada veinticuatro (24) horas una lista de certificados revocados (LCR), la cual se constituye en un mecanismo de validación y comprobación del estado de los certificados electrónicos y verificar cuales se encuentran revocados.

Nombre del campo	Valor
Versión	V2 (Número de versión del certificado).
Algoritmo de Firma:	sha512WithECDSAEncryption (Algoritmo de Firma)
Datos del emisor	
Nombre Común (commonName)	PSC APACUANA
Correo Electrónico (emailAddress)	contacto@apacuana.com
Teléfono (telephoneNumber)	+58 424 2258248

Departamento (organizationalUnitName)	SOLUCIONES TECNOLOGICAS APACUANA
Organización (organizationName)	Sistema Nacional de Certificación Electrónica
Localidad (localityName)	Caracas
Estado (stateOrProvinceName)	Miranda
País (countryName)	VE
Período de validez	
Última Fecha de Actualización (thisUpdate o lastUpdate)	Fecha (UTC)
Siguiente Fecha de Actualización (nextUpdate)	Fecha (UTC)
Extensiones de LCR	
Identificador de clave de Autoridad Certificadora (AuthorityKeyIdentifier)	
Clave de Autoridad (keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>
Número de LCR (CRL Number)	CertificateSerialNumber (Contiene el número de LCR emitidos)
Puntos de Distribución de las LCR (IssuingdistributionPoint)	**X**
Punto distribución LCR	https://pub.apacuana.com/lcr/ACAPACUANA.crl
Certificados Revocados	

Certificados revocados (Revoked Certificates)	
Serial del Certificado (Serial Number)	Entero Hexadecimal (Serial de certificado revocado)
Fecha de revocación (RevocationDate)	Fecha (fecha y hora en formato UTC)
Razón de Revocación (CRL ReasonCode)	Razón de Revocación (Anexo G Norma 32-05/24)
Firma	
Algoritmo de Firma (signatureAlgorithm)	sha512WithECDSAEncryption
Firma(signature)	<Contenido de la Firma>

1.1. Tipo de nombres

El PSC APACUANA, sólo genera y firma certificados acorde al estándar X509.v3 y los mismos se estructurará de la siguiente manera:

1.1.1 PSC APACUANA:

Campo del Certificado	Valor del Certificado
CN:	PSC-APACUANA
O:	Sistema Nacional de Certificación Electrónica
OU:	APACUANA
C:	VE
E:	contacto@apacuana.com
L:	Caracas

S:	Distrito Capital

1.1.2 Nombre alternativo:

Campo del Certificado	Valor del Certificado
DNS Name:	apacuana.com
OID:	(Código de identificación del PSC-APACUANA) OID por definir … RIF: J-501459053

1.1.3 Para los usuarios:

Los atributos definidos para los certificados de los usuarios, se regirán de acuerdo a lo establecido en la norma técnica 022 de Suscerte sobre las Políticas de Certificados del PSC APACUANA y de acuerdo a las características del mismo.

1.2. Necesidad de Nombres Significativos

La AR asignará los nombres significativos de acuerdo a lo siguiente:

- Si el suscriptor o solicitante es una persona física (Natural), el nombre asignado al atributo “Common Name” (documentIdentifier) debe ser los nombres y apellidos completos que figuran en la cédula de identidad laminada vigente que posea el solicitante, emitida por el Servicio Administrativo de Identificación, Migración y Extranjería (SAIME). La cédula de identidad deberá incluir como prefijo un literal asociado a la nacionalidad del titular (V o E) y seguido a este literal los dígitos que lo identifican usando el siguiente formato: V-00000000 o E-00000000 según sea el caso.

- En caso de ser una institución privada o ente gubernamental (Jurídica), el nombre asignado a “Common Name” será el RIF o Registro Único de Información Fiscal según el formato del ente emisor, ejemplo: V-00000000, G-000000000, J-000000000, correspondiente a su razón social emitida por el Servicio Integrado de Administración Aduanera y Tributaria (SENIAT), según la norma 032, "sección 4.1 Anexo A: Uso del DN Serial Number".

1.3. Interpretación de formatos de nombres

Las reglas utilizadas para la interpretación de los nombres significativos en los certificados emitidos, están descritos en la ISO/IEC 9595 (X.500) Distinguished Name (DN). Adicionalmente todos los certificados emitidos utilizan codificación UTF8 para todos los atributos, según la RFC 3280 (“Internet X.509 V3 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”).

1.4. Unicidad de los nombres

El nombre significativo para los certificados electrónicos emitidos por el PSC APACUANA, será único para cada certificado. En el caso que, exista la duplicidad de nombres para un suscriptor, el PSC APACUANA establece mecanismos de validación mediante otro atributo DN (según la la norma 032, "sección 4.1 Anexo A: Uso del DN Serial Number"), document Identifier (Cédula de Identidad, la cual debe incluir como prefijo un literal asociado a la nacionalidad del titular “V o E” y seguido a este literal los dígitos que lo identifican usando el siguiente formato: V-00000000 o E-00000000 según sea el caso, en caso de persona natural; o RIF - Registro Único de Información Fiscal - según el formato del ente emisor, ejemplo: V-00000000, G-000000000, J-000000000, correspondiente a su razón social, en caso de persona jurídica), para distinguir la unicidad del certificado de acuerdo a la información registrada en los sistemas de identificación de la República Bolivariana de Venezuela.

1.5. Resolución de conflictos relativos a nombres

En caso de existir conflictos de nombres por parte de los usuarios, la AR se basará en los documentos legales de identificación de la República Bolivariana de Venezuela, para efectuar la distinción de los mismos, considerando los mecanismos que se aplican en el apartado 1.4. Unicidad de los nombres.

2. Validación inicial de la identidad

2.1 Métodos de prueba de posesión de la clave privada

El esquema de operación del PSC APACUANA usando su plataforma tecnológica de certificación se encuentra configurada para que el suscriptor de un certificado electrónico (CE) genere su par de claves (pública y privada). En virtud de esto, una vez que se ha emitido cada certificado electrónico, el signatario pasa a tener la custodia y resguardo de su clave privada. Esto presupone que el signatario asume el resguardo del CE y su clave privada, obligándose conforme a la ley, salvo denuncia de el mismo signatario cuando se haya comprometido su CE y su clave privada, caso en el cual éste procederá a realizar la revocación de la firma o certificado electrónico que corresponda.

2.2 Autenticación de la identidad de la organización

Toda solicitud de certificado para personas jurídicas, debe ser efectuada por el representante legal de la organización, mediante la consignación de los siguientes documentos:

2.2.1 Acta constitutiva

2.2.2 Modificación de los estatutos en donde se designe al representante legal y sus atribuciones (De ser el caso).

2.2.3 Fotocopia del Registro de información fiscal (Rif)

2.2.4 Fotocopia de la cédula de identidad del o los representantes legales de la organización.

2.2.5 Poder debidamente registrado (De ser el caso).

Una vez consignado, los documentos anteriormente la AR-APACUANA, deberá validar la veracidad de la información suministrada previo a la firma del certificado electrónico.

2.3 Autenticación de la identidad de personas naturales

La autenticación de la identidad de suscriptores de tipo persona natural, estará sujeta al tipo de solicitud que se efectúe. En tal sentido, se regirá de acuerdo a las políticas de certificación establecidas por el PSC APACUANA. Sin embargo para todos los casos, los requisitos mínimos son:

2.3.1 Cédula de Identidad vigente en caso de ser venezolano

2.3.2 Pasaporte válido, en caso de ser extranjero y no tener Cédula de Identidad

2.4 Comprobación de las facultades de representación

La comprobación de las facultades de representación se efectuará de acuerdo a lo establecido en el apartado 2.2 del presente capítulo.

3. Identificación y autenticación de las solicitudes de renovación de clave

3.1 Generación del nuevo par de claves

La generación de un nuevo par de llaves del certificado, se debe realizar utilizando las técnicas definidas para la autenticación e identificación inicial. Una vez efectuado este procedimiento el suscriptor podrá generar su par de claves (privada y pública), con el fin de culminar el ciclo de la firma del certificado.

3.2 Generación de nuevo certificado – posterior a revocación

La política de identificación y autenticación para la renovación de un certificado después de una revocación sin compromiso de la clave será efectuada de la misma manera que en el registro inicial.

Adicionalmente, la AR podrá negar la renovación extraordinaria de un certificado para un usuario.

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

La AR, validará la identificación y autenticación de las solicitudes de revocación de la clave, mediante el procedimiento referido en el apartado denominado 1.6 Procedimiento para realizar una solicitud de revocación de un certificado del Capítulo XIV. CICLO DE VIDA DE LOS CERTIFICADOS de esta misma DPC. Adicionalmente, el PSC APACUANA está en la potestad de revocar cualquier certificado emitido por esta entidad, si se comprueba que el usuario está haciendo mal uso del mismo.

XIV. EL CICLO DE VIDA DE LOS CERTIFICADOS (REQUERIMIENTOS OPERATIVOS)

1. Solicitudes de certificados

1.1. Ciclo de vida de los certificados

El ciclo de vida de los certificados emitidos por el PSC APACUANA, se clasifica de la siguiente manera:

a) Certificado de Firma Electrónica para Persona Natural: Validez de un (01) año.
b) Certificado de Firma Electrónica para Profesional Titulado: Validez de un (01) año.
c) Certificado de Firma Electrónica para Representante de Empresa Pública: Validez de un año.
d) Certificado de Firma Electrónica para Empleado de Institución Pública (Funcionario Público): Validez de un (01) año.
e) Certificado de Firma Electrónica para Representante de Empresa Privada: Validez de un (01) año.
f) Certificado de Firma Electrónica para Empleado de Empresa Privada: Validez de un (01) año.

1.2. Proceso de generación de solicitud de certificado electrónico.

1.2.2. Acceder a la Página Web de APACUANA: El suscriptor ingresa al portal.apacuana.com accede al formulario para registrar la solicitud del certificado electrónico, llenando con sus datos los siguientes campos, indicando:

a) Correo electrónico

b) Tipo de documento de identidad

c) Número de documento de identidad

d) Clave de usuario

e) Confirmación de clave de usuario

1.2.3. Al completar los datos en el formulario para registrar la solicitud, visualizará en la interfaz los "Términos y condiciones de uso" del servicio, el solicitante podrá acceder al documento.

1.2.4. Si el suscriptor acepta los "Términos y condiciones de uso", recibirá a través del correo electrónico el código de verificación numérico, el cual transcribe en la pantalla de registro de la solicitud del certificado electrónico, ingresando al portal de Apacuana.

1.2.5. Al acceder al portal de Apacuana, se despliega la pantalla donde el usuario selecciona en el nomenclador el Tipo de Certificado que pretende adquirir.

1.2.6. La selección del tipo de certificado electrónico por parte del usuario determina los requisitos exigidos:

1.2.6.1. **Selección del Certificado de firma electrónica para Persona Natural:** se inicia la solicitud rellenando los campos del formulario, indicando Nombres, Apellidos, tipo de Documento de Identidad, número de Documento de Identidad, Correo electrónico (email), fecha y lugar de nacimiento, número de teléfono

contacto, número de RIF, y datos de la dirección de domicilio. El número telefónico es validado mediante el envío de un SMS con un código de verificación numérico a ese teléfono.

Se procede solicitando al usuario ingresar una foto digital o video con el rostro del usuario, que se utiliza como prueba de vida, el material se analizará y validará en tiempo real mediante el uso de herramientas de IA.

Consignados por el usuario los documentos escaneados del registro, se le asigna el status de pendiente, enviándolo a la AR para su proceso de verificación y aprobación.

La verificación de los datos en la AR consiste en dos fases:

1.2.6.1.1. Validación usando motor IA: el motor de IA valida la autenticidad de los documentos de identificación, cédula de identidad y RIF, verifica los datos suministrados por el usuario y compara los contenidos en el formulario registro de la solicitud. Posteriormente, procede a contrastar la foto extraída de la prueba de vida con la foto del documento de identidad. Esto termina arrojando un valor de validación a la solicitud.

1.2.6.1.2. El Operador de la AR, ingresa con su credencial a la interfaz de la AR. a través de la URL backoffice.apacuana.com

1.2.6.1.3. Accede a la sección de Clientes, ubicada en el menú lateral izquierdo.

1.2.6.1.4. Busca la solicitud del usuario en el listado de solicitudes pendientes.

1.2.6.1.5. Escoge la opción 'Ver Detalles'; accediendo a la pestaña de "Resultado" para verificar que la solicitud esté en estado "Completa".

1.2.6.1.6. En el icono de 'Información General', accede al campo 'Fe de Vida' para validar que estará en el estado 'Completa'.

1.2.6.1.7. Se despliega en una nueva pestaña del navegador la foto digital del rostro o la extraída del video consignado en el proceso de registro.

1.2.6.1.8. A continuación, se desplaza a la pestaña 'DOCUMENTOS DE VERIFICACIÓN' y abre el documento de identidad del usuario en una nueva pestaña del navegador.

1.2.6.1.9. El operador de la AR, pasará a comprobar que la foto digital o video del rostro del usuario se corresponde a la del documento de identificación. En caso de no conformidad con el documento de identidad, el operador marcará en el botón de 'Solicitar' que se encuentra al

lado izquierdo del campo 'Documento de identidad' en la pestaña 'DOCUMENTOS DE VERIFICACIÓN', lo cual habilitará una sección al final de 'Requerimiento' en la cual el operador debe escribir los motivos de la solicitud, y presionar el botón 'Solicitar Recaudos.

1.2.6.1.10. En caso de no conformidad con la foto del rostro, el operador procederá a ponerse en contacto vía correo electrónico o telefónica con el usuario, para agendar una videollamada. Cerrará la pestaña del navegador con la foto del rostro.

1.2.6.1.11. En caso de que la validación sea satisfactoria, continuará con los siguientes pasos.

1.2.6.1.12. Usando como referencia la información del documento de identidad, procederá a validar la información ubicada en la pestaña 'DATOS PERSONALES': Nombres, Apellidos, Número de Cédula de Identidad, Fecha de Nacimiento. En caso de no conformidad con alguno de los datos de los campos y la información del documento de identidad, el operador marcará en el botón de 'Solicitar' que se encuentra al lado izquierdo del campo requerido, dentro de la pestaña 'DATOS PERSONALES', y presionar el botón 'Solicitar Recaudos'.

1.2.6.1.13. A continuación, debe desplazarse a la pestaña denominada 'DOCUMENTOS DE VERIFICACIÓN' y proceder a abrir el RIF cargado por el usuario. Esto desplegará en una nueva pestaña del navegador el RIF.

1.2.6.1.14. Usando como referencia la información del RIF, procederá a validar la información ubicada en la pestaña 'DATOS PERSONALES': Registro único de información (RIF), y procederá a validar la información ubicada en la pestaña 'DATOS DE DOMICILIO': Estado, Municipio, Parroquia, Código postal, y Dirección Fiscal. En caso de no conformidad con alguno de los datos de los campos y la información del RIF, el operador marcará en el botón de 'Solicitar' que se encuentra al lado izquierdo del campo requerido, dentro de las pestañas 'DATOS PERSONALES' y/o 'DATOS DOMICILIO', y presionar el botón 'Solicitar Recaudos'. En caso de que la validación sea satisfactoria, continuará con los siguientes pasos.

1.2.6.1.15. Si la validación previa de los datos proporcionados por el suscriptor fue satisfactoria, el operador AR procederá a presionar el botón 'Verificar identidad' que se encuentra al final de la pantalla. Esto hará que

se despliegue un diálogo de confirmación '¿Estás seguro de que deseas continuar?', el operador debe seleccionar la opción 'Aceptar'. Aparecerá un mensaje 'Se ha actualizado exitosamente'. En caso de no estar seguro, regresará al paso inicial.

1.2.6.1.16. Una vez verificado los datos del usuario, el Operador AC facultado, procede a revisar la solicitud, para ello, ingresa con sus credenciales en la AR: backoffice.apacuana.com

1.2.6.1.17. Se dirige a la sección de Clientes, ubicada en el menú lateral izquierdo.

1.2.6.1.18. Selecciona la solicitud del suscriptor de la lista de solicitudes pendientes y presiona el enlace de 'Ver Detalles'.

1.2.6.1.19. Se desplaza hasta la sección "DATOS PERSONALES" y valida que todo esté "aprobado".

1.2.6.1.20. Luego, selecciona la pestaña "DATOS DOMICILIO" y valida que todo esté "aprobado".

1.2.6.1.21. Por último, selecciona la pestaña "DOCUMENTOS DE IDENTIFICACIÓN" y valida que todo esté "aprobado".

1.2.6.1.22. Una vez validado todo lo anterior, procede a desplazar hasta la parte inferior de la pantalla,

donde aparecerá el botón “Aprobar Emisión”, que estará aprobando la emisión del certificado

1.2.6.1.23. El sistema enviará una notificación vía correo electrónico al usuario indicando que su solicitud ha sido aprobada y debe autenticarse en el portal de Apacuana, donde realizó su registro.

1.2.6.1.24. El suscriptor se autentica con las credenciales registradas.

1.2.6.1.25. El sistema le solicita una “contraseña” que será usada para proteger la clave privada que se generará en el navegador. Con esta acción del lado del suscriptor, se genera un “request” en formato PKCS10 que será enviado a la AR como petición de emisión de certificado.

1.2.6.1.26. Se recibe en la AR la petición y el sistema prepara los datos de registro junto el PKCS10, para enviar la petición hacia la AC.

1.2.6.1.27. La AC recibe la información y procede a generar el certificado con los datos recibidos del perfil del suscriptor. El detalle de la operación de la AC se encuentra detallado en el STA-DO-021-Manual de Operación de la Autoridad de Certificación (AC).

1.2.6.1.28. Una vez generado el certificado en formato (.pem), es devuelto a la AR, para ser entregado al suscriptor este documento.

1.2.6.1.29. El suscriptor recibe el certificado, que posteriormente unifica con la Clave Privada previamente generada en el navegador, para generar el certificado en formato PKCS12.

1.2.6.1.30. El certificado final generado, será resguardado por el cliente en el dispositivo que utilizó para realizar la solicitud.

1.2.6.2. **Selección del Certificado de firma electrónica para Profesional Titulado**: se inicia la solicitud rellenando los campos del formulario, indicando Nombres, Apellidos, tipo de Documento de Identidad, número de Documento de Identidad, Correo electrónico (email), fecha y lugar de nacimiento, número de teléfono contacto, número de RIF, y datos de la dirección de domicilio, así como el Título profesional y el documento de colegiatura correspondiente. El número telefónico es validado mediante el envío de un SMS con un código de verificación numérico a ese teléfono.

Se procede solicitando al usuario ingresar una foto digital o video con el rostro del usuario, que se utiliza como prueba de vida, el material se analizará y validará en tiempo real mediante el uso de herramientas de IA.

Consignados por el usuario los documentos escaneados del registro, se le asigna el status de

pendiente, enviándolo a la AR para su proceso de verificación y aprobación.

La verificación de los datos en la AR consiste en dos fases:

1.2.6.2.1. Validación usando motor IA: el motor de IA valida la autenticidad de los documentos de identificación, cédula de identidad y RIF, verifica los datos suministrados por el usuario y compara los contenidos en el formulario registro de la solicitud. Posteriormente, procede a contrastar la foto extraída de la prueba de vida con la foto del documento de identidad. Esto termina arrojando un valor de validación a la solicitud.

1.2.6.2.2. El Operador de la AR, ingresa con su credencial a la interfaz de la AR. a través de la URL backoffice.apacuana.com

1.2.6.2.2.1. Accede a la sección de Clientes, ubicada en el menú lateral izquierdo.

1.2.6.2.2.2. Busca la solicitud del usuario en el listado de solicitudes pendientes.

1.2.6.2.2.3. Escoge la opción ‘Ver Detalles’; accediendo a la pestaña de “Resultado” para verificar que la solicitud esté en estado “Completa”.

1.2.6.2.2.4. En el icono de 'Información General', accede al campo 'Fe de Vida' para validar que estará en el estado 'Completa'.

1.2.6.2.2.5. Se despliega en una nueva pestaña del navegador la foto digital del rostro o la extraída del video consignado en el proceso de registro.

1.2.6.2.2.6. A continuación, se desplaza a la pestaña 'DOCUMENTOS DE VERIFICACIÓN' y abre el documento de identidad del usuario en una nueva pestaña del navegador.

1.2.6.2.2.7. El operador de la AR, pasará a comprobar que la foto digital o video del rostro del usuario se corresponde a la del documento de identificación. En caso de no conformidad con el documento de identidad, el operador marcará en el botón de 'Solicitar' que se encuentra al lado izquierdo del campo 'Documento de identidad' en la pestaña 'DOCUMENTOS DE VERIFICACIÓN', lo cual habilitará una sección al final de 'Requerimiento' en la cual el operador debe escribir los motivos de la solicitud, y presionar el botón 'Solicitar Recaudos.

1.2.6.2.2.8. En caso de no conformidad con la foto del rostro, el operador procederá a ponerse en contacto vía correo electrónico o telefónica con el usuario,

para agendar una videollamada. Cerrará la pestaña del navegador con la foto del rostro.

1.2.6.2.2.9. En caso de que la validación sea satisfactoria, continuará con los siguientes pasos.

1.2.6.2.2.10. Usando como referencia la información del documento de identidad, procederá a validar la información ubicada en la pestaña 'DATOS PERSONALES': Nombres, Apellidos, Número de Cédula de Identidad, Fecha de Nacimiento. En caso de no conformidad con alguno de los datos de los campos y la información del documento de identidad, el operador marcará en el botón de 'Solicitar' que se encuentra al lado izquierdo del campo requerido, dentro de la pestaña 'DATOS PERSONALES', y presionar el botón 'Solicitar Recaudos'.

1.2.6.2.2.11. A continuación, debe desplazarse a la pestaña denominada 'DOCUMENTOS DE VERIFICACIÓN' y proceder a abrir el RIF cargado por el usuario. Esto desplegará en una nueva pestaña del navegador el RIF.

1.2.6.2.2.12. Usando como referencia la información del RIF, procederá a validar la información ubicada en la pestaña 'DATOS PERSONALES': Registro único de información (RIF), y procederá a validar la información ubicada en la pestaña 'DATOS DE

DOMICILIO': Estado, Municipio, Parroquia, Código postal, y Dirección Fiscal. En caso de no conformidad con alguno de los datos de los campos y la información del RIF, el operador marcará en el botón de 'Solicitar' que se encuentra al lado izquierdo del campo requerido, dentro de las pestañas 'DATOS PERSONALES' y/o 'DATOS DOMICILIO', y presionar el botón 'Solicitar Recaudos'. En caso de que la validación sea satisfactoria, continuará con los siguientes pasos.

1.2.6.2.2.13. A continuación, debe desplazarse a la pestaña denominada 'DOCUMENTOS DE VERIFICACIÓN' y proceder a abrir el Título Profesional y el documento de colegiatura cargado por el usuario. Esto desplegará en una nueva pestaña del navegador el contenido de los documentos.

1.2.6.2.2.14. Usando como referencia la información del Título profesional, procederá a validar la información contra el documento de colegiatura. En caso de no conformidad con la información del Título profesional, el operador marcará en el botón de 'Solicitar' que se encuentra al lado izquierdo del campo requerido y presionar el botón 'Solicitar Recaudos'. En caso de que la validación sea satisfactoria, continuará con los siguientes pasos.

1.2.6.2.2.15. Si la validación previa de los datos proporcionados por el suscriptor fue satisfactoria, el operador AR procederá a presionar el botón 'Verificar identidad' que se encuentra al final de la pantalla. Esto hará que se despliegue un diálogo de confirmación '¿Estás seguro de que deseas continuar?', el operador debe seleccionar la opción 'Aceptar'. Aparecerá un mensaje 'Se ha actualizado exitosamente'. En caso de no estar seguro, regresará al paso inicial.

1.2.6.2.3. Una vez verificado los datos del usuario, el Operador AC facultado, procede a revisar la solicitud, para ello, ingresa con sus credenciales en la AR: backoffice.apacuana.com

1.2.6.2.3.1. Se dirige a la sección de Clientes, ubicada en el menú lateral izquierdo.

1.2.6.2.3.2. Selecciona la solicitud del suscriptor de la lista de solicitudes pendientes y presiona el enlace de 'Ver Detalles'.

1.2.6.2.3.3. Se desplaza hasta la sección "DATOS PERSONALES" y valida que todo esté "aprobado".

1.2.6.2.3.4. Luego, selecciona la pestaña "DATOS DOMICILIO" y valida que todo esté "aprobado".

1.2.6.2.3.5. Por último, selecciona la pestaña “DOCUMENTOS DE IDENTIFICACIÓN” y valida que todo esté “aprobado”.

1.2.6.2.3.6. Una vez validado todo lo anterior, procede a desplazar hasta la parte inferior de la pantalla, donde aparecerá el botón “Aprobar Emisión”, que estará aprobando la emisión del certificado

1.2.6.2.4. El sistema enviará una notificación vía correo electrónico al usuario indicando que su solicitud ha sido aprobada y debe autenticarse en el portal de Apacuana, donde realizó su registro.

1.2.6.2.4.1. El suscriptor se autentica con las credenciales registradas.

1.2.6.2.4.2. El sistema le solicita una “contraseña” que será usada para proteger la clave privada que se generará en el navegador. Con esta acción del lado del suscriptor, se genera un “request” en formato PKCS10 que será enviado a la AR como petición de emisión de certificado.

1.2.6.2.4.3. Se recibe en la AR la petición y el sistema prepara los datos de registro junto el PKCS10, para enviar la petición hacia la AC.

1.2.6.2.5. La AC recibe la información y procede a generar el certificado con los datos recibidos del perfil del suscriptor. El detalle de la operación de la AC se encuentra detallado en el

STA-DO-021-Manual de Operación de la Autoridad de Certificación (AC).

1.2.6.2.6. Una vez generado el certificado en formato (.pem), es devuelto a la AR, para ser entregado al suscriptor este documento.

1.2.6.2.7. El suscriptor recibe el certificado, que posteriormente unifica con la Clave Privada previamente generada en el navegador, para generar el certificado en formato PKCS12.

1.2.6.2.8. El certificado final generado, será resguardado por el cliente en el dispositivo que utilizó para realizar la solicitud.

1.2.6.3. **Selección del Certificado de firma electrónica para Representante Legal de Empresa Pública**: se inicia la solicitud rellenando los campos del formulario, indicando Nombres, Apellidos, tipo de Documento de Identidad, número de Documento de Identidad, Correo electrónico (email), fecha y lugar de nacimiento, número de teléfono contacto, número de RIF, y datos de la dirección de domicilio, así como el RIF de la empresa, publicación en gaceta y última declaración fiscal. El número telefónico es validado mediante el envío de un SMS con un código de verificación numérico a ese teléfono.

Se procede solicitando al usuario ingresar una foto digital o video con el rostro del usuario, que se utiliza como prueba de vida, el material se analizará y validará en tiempo real mediante el uso de herramientas de IA.

Consignados por el usuario los documentos escaneados del registro, se le asigna el status de pendiente, enviándolo a la AR para su proceso de verificación y aprobación.

La verificación de los datos en la AR consiste en dos fases:

1.2.6.3.1. Validación usando motor IA: el motor de IA valida la autenticidad de los documentos de identificación, cédula de identidad y RIF, verifica los datos suministrados por el usuario y compara los contenidos en el formulario registro de la solicitud. Posteriormente, procede a contrastar la foto extraída de la prueba de vida con la foto del documento de identidad. Esto termina arrojando un valor de validación a la solicitud.

1.2.6.3.2. El Operador de la AR, ingresa con su credencial a la interfaz de la AR. a través de la URL backoffice.apacuana.com

1.2.6.3.2.1. Accede a la sección de Clientes, ubicada en el menú lateral izquierdo.

1.2.6.3.2.2. Busca la solicitud del usuario en el listado de solicitudes pendientes.

1.2.6.3.2.3. Escoge la opción 'Ver Detalles'; accediendo a la pestaña de "Resultado" para verificar que la solicitud esté en estado "Completa".

1.2.6.3.2.4. En el icono de 'Información General', accede al campo 'Fe de Vida' para validar que estará en el estado 'Completa'.

1.2.6.3.2.5. Se despliega en una nueva pestaña del navegador la foto digital del rostro o la extraída del video consignado en el proceso de registro.

1.2.6.3.2.6. A continuación, se desplaza a la pestaña 'DOCUMENTOS DE VERIFICACIÓN' y abre el documento de identidad del usuario en una nueva pestaña del navegador.

1.2.6.3.2.7. El operador de la AR, pasará a comprobar que la foto digital o video del rostro del usuario se corresponde a la del documento de identificación. En caso de no conformidad con el documento de identidad, el operador marcará en el botón de 'Solicitar' que se encuentra al lado izquierdo del campo 'Documento de identidad' en la pestaña 'DOCUMENTOS DE VERIFICACIÓN', lo cual habilitará una sección al final de 'Requerimiento' en la cual el operador debe escribir los motivos

de la solicitud, y presionar el botón 'Solicitar Recaudos.

1.2.6.3.2.8. En caso de no conformidad con la foto del rostro, el operador procederá a ponerse en contacto vía correo electrónico o telefónica con el usuario, para agendar una videollamada. Cerrará la pestaña del navegador con la foto del rostro.

1.2.6.3.2.9. En caso de que la validación sea satisfactoria, continuará con los siguientes pasos.

1.2.6.3.2.10. Usando como referencia la información del documento de identidad, procederá a validar la información ubicada en la pestaña 'DATOS PERSONALES': Nombres, Apellidos, Número de Cédula de Identidad, Fecha de Nacimiento. En caso de no conformidad con alguno de los datos de los campos y la información del documento de identidad, el operador marcará en el botón de 'Solicitar' que se encuentra al lado izquierdo del campo requerido, dentro de la pestaña 'DATOS PERSONALES', y presionar el botón 'Solicitar Recaudos'.

1.2.6.3.2.11. A continuación, debe desplazarse a la pestaña denominada 'DOCUMENTOS DE VERIFICACIÓN' y proceder a abrir el RIF cargado por el usuario. Esto desplegará en una nueva pestaña del navegador el RIF.

1.2.6.3.2.12. Usando como referencia la información del RIF, procederá a validar la información ubicada en la pestaña 'DATOS PERSONALES': Registro único de información (RIF), y procederá a validar la información ubicada en la pestaña 'DATOS DE DOMICILIO': Estado, Municipio, Parroquia, Código postal, y Dirección Fiscal. En caso de no conformidad con alguno de los datos de los campos y la información del RIF, el operador marcará en el botón de 'Solicitar' que se encuentra al lado izquierdo del campo requerido, dentro de las pestañas 'DATOS PERSONALES' y/o 'DATOS DOMICILIO', y presionar el botón 'Solicitar Recaudos'. En caso de que la validación sea satisfactoria, continuará con los siguientes pasos.

1.2.6.3.2.13. A continuación, debe desplazarse a la pestaña denominada 'DOCUMENTOS DE VERIFICACIÓN' y proceder a abrir los documentos RIF de la empresa, publicación en gaceta y última declaración fiscal. cargado por el usuario. Esto desplegará en una nueva pestaña del navegador el contenido de los documentos.

1.2.6.3.2.14. Usando como referencia la información del RIF de la empresa, procederá a validar la información contra la última declaración fiscal. En caso de no

conformidad con la información de alguno o más de los documentos, el operador marcará en el botón de 'Solicitar' que se encuentra al lado izquierdo del campo requerido y presionar el botón 'Solicitar Recaudos'. En caso de que la validación sea satisfactoria, continuará con los siguientes pasos.

1.2.6.3.2.15. Si la validación previa de los datos proporcionados por el suscriptor fue satisfactoria, el operador AR procederá a presionar el botón 'Verificar identidad' que se encuentra al final de la pantalla. Esto hará que se despliegue un diálogo de confirmación '¿Estás seguro de que deseas continuar?', el operador debe seleccionar la opción 'Aceptar'. Aparecerá un mensaje 'Se ha actualizado exitosamente'. En caso de no estar seguro, regresará al paso inicial.

1.2.6.3.3. Una vez verificado los datos del usuario, el Operador AC facultado, procede a revisar la solicitud, para ello, ingresa con sus credenciales en la AR: backoffice.apacuana.com

1.2.6.3.3.1. Se dirige a la sección de Clientes, ubicada en el menú lateral izquierdo.

1.2.6.3.3.2. Selecciona la solicitud del suscriptor de la lista de solicitudes pendientes y presiona el enlace de 'Ver Detalles'.

1.2.6.3.3.3. Se desplaza hasta la sección “DATOS PERSONALES” y valida que todo esté “aprobado”.

1.2.6.3.3.4. Luego, selecciona la pestaña “DATOS DOMICILIO” y valida que todo esté “aprobado”.

1.2.6.3.3.5. Por último, selecciona la pestaña “DOCUMENTOS DE IDENTIFICACIÓN” y valida que todo esté “aprobado”.

1.2.6.3.3.6. Una vez validado todo lo anterior, procede a desplazar hasta la parte inferior de la pantalla, donde aparecerá el botón “Aprobar Emisión”, que estará aprobando la emisión del certificado

1.2.6.3.4. El sistema enviará una notificación vía correo electrónico al usuario indicando que su solicitud ha sido aprobada y debe autenticarse en el portal de Apacuana, donde realizó su registro.

1.2.6.3.5. El suscriptor se autentica con las credenciales registradas.

1.2.6.3.6. El sistema le solicita una “contraseña” que será usada para proteger la clave privada que se generará en el navegador. Con esta acción del lado del suscriptor, se genera un “request” en formato PKCS10 que será enviado a la AR como petición de emisión de certificado.

1.2.6.3.7. Se recibe en la AR la petición y el sistema prepara los datos de registro junto el PKCS10, para enviar la petición hacia la AC.

1.2.6.3.8. La AC recibe la información y procede a generar el certificado con los datos recibidos del perfil del suscriptor. El detalle de la operación de la AC se encuentra detallado en el STA-DO-021-Manual de Operación de la Autoridad de Certificación (AC).

1.2.6.3.9. Una vez generado el certificado en formato (.pem), es devuelto a la AR, para ser entregado al suscriptor este documento.

1.2.6.3.10. El suscriptor recibe el certificado, que posteriormente unifica con la Clave Privada previamente generada en el navegador, para generar el certificado en formato PKCS12.

1.2.6.3.11. El certificado final generado, será resguardado por el cliente en el dispositivo que utilizó para realizar la solicitud.

1.2.6.4. **Selección del Certificado de firma electrónica para Empleado de Institución Pública (Funcionario Público)**: En el caso de empleado de empresa pública, el llenado del formulario para la solicitud está condicionado a que previamente esté registrado un representante legal de dicha empresa y éste haga llegar una invitación. Una vez recibida la invitación por

correo electrónico, se inicia la solicitud rellenando los campos del formulario, indicando Nombres, Apellidos, tipo de Documento de Identidad, número de Documento de Identidad, Correo electrónico (email), fecha y lugar de nacimiento, número de teléfono contacto, número de RIF, y datos de la dirección de domicilio. El número telefónico es validado mediante el envío de un SMS con un código de verificación numérico a ese teléfono.

Se procede solicitando al usuario ingresar una foto digital o video con el rostro del usuario, que se utiliza como prueba de vida, el material se analizará y validará en tiempo real mediante el uso de herramientas de IA.

Consignados por el usuario los documentos escaneados del registro, se le asigna el status de pendiente, enviándolo a la AR para su proceso de verificación y aprobación.

La verificación de los datos en la AR consiste en dos fases:

1.2.6.4.1. Validación usando motor IA: el motor de IA valida la autenticidad de los documentos de identificación, cédula de identidad y RIF, verifica los datos suministrados por el usuario y compara los contenidos en el formulario registro de la solicitud. Posteriormente, procede

a contrastar la foto extraída de la prueba de vida con la foto del documento de identidad. Esto termina arrojando un valor de validación a la solicitud.

1.2.6.4.2. El Operador de la AR, ingresa con su credencial a la interfaz de la AR. a través de la URL backoffice.apacuana.com

1.2.6.4.2.1. Accede a la sección de Clientes, ubicada en el menú lateral izquierdo.

1.2.6.4.2.2. Busca la solicitud del usuario en el listado de solicitudes pendientes.

1.2.6.4.2.3. Escoge la opción 'Ver Detalles'; accediendo a la pestaña de "Resultado" para verificar que la solicitud esté en estado "Completa".

1.2.6.4.2.4. En el icono de 'Información General', accede al campo 'Fe de Vida' para validar que estará en el estado 'Completa'.

1.2.6.4.2.5. Se despliega en una nueva pestaña del navegador la foto digital del rostro o la extraída del video consignado en el proceso de registro.

1.2.6.4.2.6. A continuación, se desplaza a la pestaña 'DOCUMENTOS DE VERIFICACIÓN' y abre el documento de identidad del usuario en una nueva pestaña del navegador.

1.2.6.4.2.7. El operador de la AR, pasará a comprobar que la foto digital o video del rostro del usuario se

corresponde a la del documento de identificación. En caso de no conformidad con el documento de identidad, el operador marcará en el botón de 'Solicitar' que se encuentra al lado izquierdo del campo 'Documento de identidad' en la pestaña 'DOCUMENTOS DE VERIFICACIÓN', lo cual habilitará una sección al final de 'Requerimiento' en la cual el operador debe escribir los motivos de la solicitud, y presionar el botón 'Solicitar Recaudos.

1.2.6.4.2.8. En caso de no conformidad con la foto del rostro, el operador procederá a ponerse en contacto vía correo electrónico o telefónica con el usuario, para agendar una videollamada. Cerrará la pestaña del navegador con la foto del rostro.

1.2.6.4.2.9. En caso de que la validación sea satisfactoria, continuará con los siguientes pasos.

1.2.6.4.2.10. Usando como referencia la información del documento de identidad, procederá a validar la información ubicada en la pestaña 'DATOS PERSONALES': Nombres, Apellidos, Número de Cédula de Identidad, Fecha de Nacimiento. En caso de no conformidad con alguno de los datos de los campos y la información del documento de identidad, el operador marcará en el botón de 'Solicitar' que se encuentra al lado izquierdo del

campo requerido, dentro de la pestaña 'DATOS PERSONALES', y presionar el botón 'Solicitar Recaudos'.

1.2.6.4.2.11. A continuación, debe desplazarse a la pestaña denominada 'DOCUMENTOS DE VERIFICACIÓN' y proceder a abrir el RIF cargado por el usuario. Esto desplegará en una nueva pestaña del navegador el RIF.

1.2.6.4.2.12. Usando como referencia la información del RIF, procederá a validar la información ubicada en la pestaña 'DATOS PERSONALES': Registro único de información (RIF), y procederá a validar la información ubicada en la pestaña 'DATOS DE DOMICILIO': Estado, Municipio, Parroquia, Código postal, y Dirección Fiscal. En caso de no conformidad con alguno de los datos de los campos y la información del RIF, el operador marcará en el botón de 'Solicitar' que se encuentra al lado izquierdo del campo requerido, dentro de las pestañas 'DATOS PERSONALES' y/o 'DATOS DOMICILIO', y presionar el botón 'Solicitar Recaudos'. En caso de que la validación sea satisfactoria, continuará con los siguientes pasos.

1.2.6.4.2.13. Si la validación previa de los datos proporcionados por el suscriptor fue satisfactoria,

el operador AR procederá a presionar el botón 'Verificar identidad' que se encuentra al final de la pantalla. Esto hará que se despliegue un diálogo de confirmación '¿Estás seguro de que deseas continuar?', el operador debe seleccionar la opción 'Aceptar'. Aparecerá un mensaje 'Se ha actualizado exitosamente'. En caso de no estar seguro, regresará al paso inicial.

1.2.6.4.3. Una vez verificado los datos del usuario, el Operador AC facultado, procede a revisar la solicitud, para ello, ingresa con sus credenciales en la AR: backoffice.apacuana.com

1.2.6.4.4. Se dirige a la sección de Clientes, ubicada en el menú lateral izquierdo.

1.2.6.4.5. Selecciona la solicitud del suscriptor de la lista de solicitudes pendientes y presiona el enlace de 'Ver Detalles'.

1.2.6.4.6. Se desplaza hasta la sección "DATOS PERSONALES" y valida que todo esté "aprobado".

1.2.6.4.7. Luego, selecciona la pestaña "DATOS DOMICILIO" y valida que todo esté "aprobado".

1.2.6.4.8. Por último, selecciona la pestaña "DOCUMENTOS DE IDENTIFICACIÓN" y valida que todo esté "aprobado".

1.2.6.4.9. Una vez validado todo lo anterior, procede a desplazar hasta la parte inferior de la pantalla, donde aparecerá el botón “Aprobar Emisión”, que estará aprobando la emisión del certificado

1.2.6.4.10. El sistema enviará una notificación vía correo electrónico al usuario indicando que su solicitud ha sido aprobada y debe autenticarse en el portal de Apacuana, donde realizó su registro.

1.2.6.4.11. El suscriptor se autentica con las credenciales registradas.

1.2.6.4.12. El sistema le solicita una “contraseña” que será usada para proteger la clave privada que se generará en el navegador. Con esta acción del lado del suscriptor, se genera un “request” en formato PKCS10 que será enviado a la AR como petición de emisión de certificado.

1.2.6.4.13. Se recibe en la AR la petición y el sistema prepara los datos de registro junto el PKCS10, para enviar la petición hacia la AC.

1.2.6.4.14. La AC recibe la información y procede a generar el certificado con los datos recibidos del perfil del suscriptor. El detalle de la operación de la AC se encuentra detallado en el STA-DO-021-Manual de Operación de la Autoridad de Certificación (AC).

1.2.6.4.15. Una vez generado el certificado en formato (.pem), es devuelto a la AR, para ser entregado al suscriptor este documento.

1.2.6.4.16. El suscriptor recibe el certificado, que posteriormente unifica con la Clave Privada previamente generada en el navegador, para generar el certificado en formato PKCS12.

1.2.6.4.17. El certificado final generado, será resguardado por el cliente en el dispositivo que utilizó para realizar la solicitud.

1.2.6.5. **Selección del Certificado de firma electrónica para Representante Legal de Empresa Privada**: se inicia la solicitud rellenando los campos del formulario, indicando Nombres, Apellidos, tipo de Documento de Identidad, número de Documento de Identidad, Correo electrónico (email), fecha y lugar de nacimiento, número de teléfono contacto, número de RIF, y datos de la dirección de domicilio, así como el Acta constitutiva de la empresa, actas de asambleas que lo acrediten como representante legal y última declaración fiscal. El número telefónico es validado mediante el envío de un SMS con un código de verificación numérico a ese teléfono.

Se procede solicitando al usuario ingresar una foto digital o video con el rostro del usuario, que se utiliza como prueba de vida, el material se analizará y

validará en tiempo real mediante el uso de herramientas de IA.

Consignados por el usuario los documentos escaneados del registro, se le asigna el status de pendiente, enviándolo a la AR para su proceso de verificación y aprobación.

La verificación de los datos en la AR consiste en dos fases:

1.2.6.5.1. Validación usando motor IA: el motor de IA valida la autenticidad de los documentos de identificación, cédula de identidad y RIF, verifica los datos suministrados por el usuario y compara los contenidos en el formulario registro de la solicitud. Posteriormente, procede a contrastar la foto extraída de la prueba de vida con la foto del documento de identidad. Esto termina arrojando un valor de validación a la solicitud.

1.2.6.5.2. El Operador de la AR, ingresa con su credencial a la interfaz de la AR. a través de la URL backoffice.apacuana.com

1.2.6.5.2.1. Accede a la sección de Clientes, ubicada en el menú lateral izquierdo.

1.2.6.5.2.2. Busca la solicitud del usuario en el listado de solicitudes pendientes.

1.2.6.5.2.3. Escoge la opción ‘Ver Detalles’; accediendo a la pestaña de “Resultado” para verificar que la solicitud esté en estado “Completa”.

1.2.6.5.2.4. En el icono de ‘Información General’, accede al campo ‘Fe de Vida’ para validar que estará en el estado ‘Completa’.

1.2.6.5.2.5. Se despliega en una nueva pestaña del navegador la foto digital del rostro o la extraída del video consignado en el proceso de registro.

1.2.6.5.2.6. A continuación, se desplaza a la pestaña ‘DOCUMENTOS DE VERIFICACIÓN’ y abre el documento de identidad del usuario en una nueva pestaña del navegador.

1.2.6.5.2.7. El operador de la AR, pasará a comprobar que la foto digital o video del rostro del usuario se corresponde a la del documento de identificación. En caso de no conformidad con el documento de identidad, el operador marcará en el botón de ‘Solicitar’ que se encuentra al lado izquierdo del campo ‘Documento de identidad’ en la pestaña ‘DOCUMENTOS DE VERIFICACIÓN’, lo cual habilitará una sección al final de ‘Requerimiento’ en la cual el operador debe escribir los motivos de la solicitud, y presionar el botón ‘Solicitar Recaudos.

1.2.6.5.2.8. En caso de no conformidad con la foto del rostro, el operador procederá a ponerse en contacto vía correo electrónico o telefónica con el usuario, para agendar una videollamada. Cerrará la pestaña del navegador con la foto del rostro.

1.2.6.5.2.9. En caso de que la validación sea satisfactoria, continuará con los siguientes pasos.

1.2.6.5.2.10. Usando como referencia la información del documento de identidad, procederá a validar la información ubicada en la pestaña 'DATOS PERSONALES': Nombres, Apellidos, Número de Cédula de Identidad, Fecha de Nacimiento. En caso de no conformidad con alguno de los datos de los campos y la información del documento de identidad, el operador marcará en el botón de 'Solicitar' que se encuentra al lado izquierdo del campo requerido, dentro de la pestaña 'DATOS PERSONALES', y presionar el botón 'Solicitar Recaudos'.

1.2.6.5.2.11. A continuación, debe desplazarse a la pestaña denominada 'DOCUMENTOS DE VERIFICACIÓN' y proceder a abrir el RIF cargado por el usuario. Esto desplegará en una nueva pestaña del navegador el RIF.

1.2.6.5.2.12. Usando como referencia la información del RIF, procederá a validar la información ubicada en la

pestaña ‘DATOS PERSONALES’: Registro único de información (RIF), y procederá a validar la información ubicada en la pestaña ‘DATOS DE DOMICILIO’: Estado, Municipio, Parroquia, Código postal, y Dirección Fiscal. En caso de no conformidad con alguno de los datos de los campos y la información del RIF, el operador marcará en el botón de ‘Solicitar’ que se encuentra al lado izquierdo del campo requerido, dentro de las pestañas ‘DATOS PERSONALES’ y/o ‘DATOS DOMICILIO’, y presionar el botón ‘Solicitar Recaudos’. En caso de que la validación sea satisfactoria, continuará con los siguientes pasos.

1.2.6.5.2.13. A continuación, debe desplazarse a la pestaña denominada ‘DOCUMENTOS DE VERIFICACIÓN’ y proceder a abrir los documentos Acta constitutiva de la empresa, actas de asambleas que lo acrediten como representante legal y última declaración fiscal. cargado por el usuario. Esto desplegará en una nueva pestaña del navegador el contenido de los documentos.

1.2.6.5.2.14. Usando como referencia la información del Acta constitutiva de la empresa, actas de asambleas que lo acrediten como representante legal y última declaración fiscal. En caso de no

conformidad con la información de alguno o más de los documentos, el operador marcará en el botón de 'Solicitar' que se encuentra al lado izquierdo del campo requerido y presionar el botón 'Solicitar Recaudos'. En caso de que la validación sea satisfactoria, continuará con los siguientes pasos.

1.2.6.5.2.15. Si la validación previa de los datos proporcionados por el suscriptor fue satisfactoria, el operador AR procederá a presionar el botón 'Verificar identidad' que se encuentra al final de la pantalla. Esto hará que se despliegue un diálogo de confirmación '¿Estás seguro de que deseas continuar?', el operador debe seleccionar la opción 'Aceptar'. Aparecerá un mensaje 'Se ha actualizado exitosamente'. En caso de no estar seguro, regresará al paso inicial.

1.2.6.5.3. Una vez verificado los datos del usuario, el Operador AC facultado, procede a revisar la solicitud, para ello, ingresa con sus credenciales en la AR: backoffice.apacuana.com

1.2.6.5.3.1. Se dirige a la sección de Clientes, ubicada en el menú lateral izquierdo.

1.2.6.5.3.2. Selecciona la solicitud del suscriptor de la lista de solicitudes pendientes y presiona el enlace de 'Ver Detalles'.

1.2.6.5.3.3. Se desplaza hasta la sección “DATOS PERSONALES” y valida que todo esté “aprobado”.

1.2.6.5.3.4. Luego, selecciona la pestaña “DATOS DOMICILIO” y valida que todo esté “aprobado”.

1.2.6.5.3.5. Por último, selecciona la pestaña “DOCUMENTOS DE IDENTIFICACIÓN” y valida que todo esté “aprobado”.

1.2.6.5.3.6. Una vez validado todo lo anterior, procede a desplazar hasta la parte inferior de la pantalla, donde aparecerá el botón “Aprobar Emisión”, que estará aprobando la emisión del certificado

1.2.6.5.4. El sistema enviará una notificación vía correo electrónico al usuario indicando que su solicitud ha sido aprobada y debe autenticarse en el portal de Apacuana, donde realizó su registro.

1.2.6.5.5. El suscriptor se autentica con las credenciales registradas.

1.2.6.5.6. El sistema le solicita una “contraseña” que será usada para proteger la clave privada que se generará en el navegador. Con esta acción del lado del suscriptor, se genera un “request” en formato PKCS10 que será enviado a la AR como petición de emisión de certificado.

1.2.6.5.7. Se recibe en la AR la petición y el sistema prepara los datos de registro junto el PKCS10, para enviar la petición hacia la AC.

1.2.6.5.8. La AC recibe la información y procede a generar el certificado con los datos recibidos del perfil del suscriptor. El detalle de la operación de la AC se encuentra detallado en el STA-DO-021-Manual de Operación de la Autoridad de Certificación (AC).

1.2.6.5.9. Una vez generado el certificado en formato (.pem), es devuelto a la AR, para ser entregado al suscriptor este documento.

1.2.6.5.10. El suscriptor recibe el certificado, que posteriormente unifica con la Clave Privada previamente generada en el navegador, para generar el certificado en formato PKCS12.

1.2.6.5.11. El certificado final generado, será resguardado por el cliente en el dispositivo que utilizó para realizar la solicitud.

1.2.6.6. **Selección del Certificado de firma electrónica para Empleado de Empresa Privada**: En el caso de empleado de empresa pública, el llenado del formulario para la solicitud está condicionado a que previamente esté registrado un representante legal de dicha empresa y éste haga llegar una invitación. Una vez recibida la invitación por correo electrónico, se inicia la solicitud rellenando los campos del formulario, indicando Nombres, Apellidos, tipo de Documento de Identidad, número de Documento de Identidad, Correo electrónico (email), fecha y lugar de nacimiento, número de teléfono contacto, número de RIF, y datos de la dirección de domicilio. El número telefónico es validado mediante el envío de un SMS con un código de verificación numérico a ese teléfono.

Se procede solicitando al usuario ingresar una foto digital o video con el rostro del usuario, que se utiliza como prueba de vida, el material se analizará y validará en tiempo real mediante el uso de herramientas de IA.

Consignados por el usuario los documentos escaneados del registro, se le asigna el status de pendiente, enviándolo a la AR para su proceso de verificación y aprobación.

La verificación de los datos en la AR consiste en dos fases:

1.2.6.6.1. Validación usando motor IA: el motor de IA valida la autenticidad de los documentos de identificación, cédula de identidad y RIF, verifica los datos suministrados por el usuario y compara los contenidos en el formulario registro de la solicitud. Posteriormente, procede a contrastar la foto extraída de la prueba de vida con la foto del documento de identidad. Esto termina arrojando un valor de validación a la solicitud.

1.2.6.6.2. El Operador de la AR, ingresa con su credencial a la interfaz de la AR. a través de la URL backoffice.apacuana.com

1.2.6.6.2.1. Accede a la sección de Clientes, ubicada en el menú lateral izquierdo.

1.2.6.6.2.2. Busca la solicitud del usuario en el listado de solicitudes pendientes.

1.2.6.6.2.3. Escoge la opción ‘Ver Detalles’; accediendo a la pestaña de “Resultado” para verificar que la solicitud esté en estado “Completa”.

1.2.6.6.2.4. En el icono de ‘Información General’, accede al campo ‘Fe de Vida’ para validar que estará en el estado ‘Completa’.

1.2.6.6.2.5. Se despliega en una nueva pestaña del navegador la foto digital del rostro o la extraída del video consignado en el proceso de registro.

1.2.6.6.2.6. A continuación, se desplaza a la pestaña ‘DOCUMENTOS DE VERIFICACIÓN’ y abre el documento de identidad del usuario en una nueva pestaña del navegador.

1.2.6.6.2.7. El operador de la AR, pasará a comprobar que la foto digital o video del rostro del usuario se corresponde a la del documento de identificación. En caso de no conformidad con el documento de identidad, el operador marcará en el botón de ‘Solicitar’ que se encuentra al lado izquierdo del campo ‘Documento de identidad’ en la pestaña ‘DOCUMENTOS DE VERIFICACIÓN’, lo cual habilitará una sección al final de ‘Requerimiento’ en la cual el operador debe escribir los motivos de la solicitud, y presionar el botón ‘Solicitar Recaudos.

1.2.6.6.2.8. En caso de no conformidad con la foto del rostro, el operador procederá a ponerse en contacto vía correo electrónico o telefónica con el usuario, para agendar una videollamada. Cerrará la pestaña del navegador con la foto del rostro.

1.2.6.6.2.9. En caso de que la validación sea satisfactoria, continuará con los siguientes pasos.

1.2.6.6.2.10. Usando como referencia la información del documento de identidad, procederá a validar la información ubicada en la pestaña ‘DATOS

PERSONALES': Nombres, Apellidos, Número de Cédula de Identidad, Fecha de Nacimiento. En caso de no conformidad con alguno de los datos de los campos y la información del documento de identidad, el operador marcará en el botón de 'Solicitar' que se encuentra al lado izquierdo del campo requerido, dentro de la pestaña 'DATOS PERSONALES', y presionar el botón 'Solicitar Recaudos'.

1.2.6.6.2.11. A continuación, debe desplazarse a la pestaña denominada 'DOCUMENTOS DE VERIFICACIÓN' y proceder a abrir el RIF cargado por el usuario. Esto desplegará en una nueva pestaña del navegador el RIF.

1.2.6.6.2.12. Usando como referencia la información del RIF, procederá a validar la información ubicada en la pestaña 'DATOS PERSONALES': Registro único de información (RIF), y procederá a validar la información ubicada en la pestaña 'DATOS DE DOMICILIO': Estado, Municipio, Parroquia, Código postal, y Dirección Fiscal. En caso de no conformidad con alguno de los datos de los campos y la información del RIF, el operador marcará en el botón de 'Solicitar' que se encuentra al lado izquierdo del campo requerido, dentro de las pestañas 'DATOS PERSONALES'

y/o 'DATOS DOMICILIO', y presionar el botón 'Solicitar Recaudos'. En caso de que la validación sea satisfactoria, continuará con los siguientes pasos.

1.2.6.6.2.13. Si la validación previa de los datos proporcionados por el suscriptor fue satisfactoria, el operador AR procederá a presionar el botón 'Verificar identidad' que se encuentra al final de la pantalla. Esto hará que se despliegue un diálogo de confirmación '¿Estás seguro de que deseas continuar?', el operador debe seleccionar la opción 'Aceptar'. Aparecerá un mensaje 'Se ha actualizado exitosamente'. En caso de no estar seguro, regresará al paso inicial.

1.2.6.6.3. Una vez verificado los datos del usuario, el Operador AC facultado, procede a revisar la solicitud, para ello, ingresa con sus credenciales en la AR: backoffice.apacuana.com

1.2.6.6.3.1. Se dirige a la sección de Clientes, ubicada en el menú lateral izquierdo.

1.2.6.6.3.2. Selecciona la solicitud del suscriptor de la lista de solicitudes pendientes y presiona el enlace de 'Ver Detalles'.

1.2.6.6.3.3. Se desplaza hasta la sección "DATOS PERSONALES" y valida que todo esté "aprobado".

1.2.6.6.3.4. Luego, selecciona la pestaña “DATOS DOMICILIO” y valida que todo esté “aprobado”.

1.2.6.6.3.5. Por último, selecciona la pestaña “DOCUMENTOS DE IDENTIFICACIÓN” y valida que todo esté “aprobado”.

1.2.6.6.3.6. Una vez validado todo lo anterior, procede a desplazar hasta la parte inferior de la pantalla, donde aparecerá el botón “Aprobar Emisión”, que estará aprobando la emisión del certificado

1.2.6.6.4. El sistema enviará una notificación vía correo electrónico al usuario indicando que su solicitud ha sido aprobada y debe autenticarse en el portal de Apacuana, donde realizó su registro.

1.2.6.6.5. El suscriptor se autentica con las credenciales registradas.

1.2.6.6.6. El sistema le solicita una “contraseña” que será usada para proteger la clave privada que se generará en el navegador. Con esta acción del lado del suscriptor, se genera un “request” en formato PKCS10 que será enviado a la AR como petición de emisión de certificado.

1.2.6.6.7. Se recibe en la AR la petición y el sistema prepara los datos de registro junto el PKCS10, para enviar la petición hacia la AC.

1.2.6.6.8. La AC recibe la información y procede a generar el certificado con los datos recibidos del perfil

del suscriptor. El detalle de la operación de la AC se encuentra detallado en el STA-DO-021-Manual de Operación de la Autoridad de Certificación (AC).

1.2.6.6.9. Una vez generado el certificado en formato (.pem), es devuelto a la AR, para ser entregado al suscriptor este documento.

1.2.6.6.10. El suscriptor recibe el certificado, que posteriormente unifica con la Clave Privada previamente generada en el navegador, para generar el certificado en formato PKCS12.

1.2.6.6.11. El certificado final generado, será resguardado por el cliente en el dispositivo que utilizó para realizar la solicitud.

1.2.7. Proceso de firma del certificado

La AC, firmará aquellos certificados que hayan sido verificados los datos del suscriptor o signatario por el Operador AR y haya sido aprobado por un Operador AC la emisión del certificado.

El PSC APACUANA, una vez validada la identidad del signatario por la AR y la AC aprobado desde el sistema de certificación la emisión del certificado para la firma del mismo, seguirá el proceso siguiente:

a) El Encargado de la AR notifica al Encargado de la AC la verificación de identidad del suscriptor o signatario, para proceder con el siguiente paso.

b) El Encargado de la AC revisa la verificación de identidad previa del suscriptor o signatario y procede a aprobar la emisión del certificado electrónico
c) El Suscriptor o Signatario, suministra clave de 6 dígitos a través del sistema lo que permite generar el certificado y ser firmado electrónicamente.

1.2.8. Proceso de generación de la solicitud de renovación de un certificado y sus claves El proceso de generación de solicitud de renovación de las claves del certificado, deberá efectuarse por el usuario del certificado del mismo modo que se efectúa para la generación del certificado. Es decir, ingresando a la dirección electrónica https://portal.apacuana.com/, generando la solicitud del certificado que desea renovar de acuerdo a los procedimientos previamente establecidos.

Es necesario, destacar que en este caso la petición de renovación del certificado debe ser efectuada por el supervisor inmediato del usuario con un (01) mes de antelación a la fecha de expiración del mismo.

Así mismo, el sistema envía notificación vía correo al suscriptor o signatario indicando que está próxima la fecha de expiración del certificado electrónico

1.5 Procedimiento para realizar una solicitud de renovación de un certificado

El proceso para la renovación de un certificado electrónico de un usuario será el mismo que para la solicitud de generación por primera vez de un certificado electrónico.

1.6 Procedimiento para realizar una solicitud de revocación de un certificado

La revocación de certificados se realiza cuando la persona natural o jurídica signataria ha dejado de existir, ha cesado en las actividades por las cuales se le otorgó el certificado, o en caso de que la seguridad de la llave privada se haya visto comprometida. La solicitud de revocación de un certificado electrónico será admitida si la petición la origina cualquier de los siguientes solicitantes:

1. Titular signatario de un certificado electrónico
2. Responsable autorizado de una persona jurídica que sea signataria de un certificado electrónico.
3. Persona jurídica signataria y titular del certificado electrónico a través de un funcionario debidamente autorizado.
4. Personas habilitadas por el titular signatario de un certificado electrónico vía escrito formal y firmado electrónicamente
5. Autoridades judiciales con competencia legal.
6. La alta dirección del PSC APACUANA.

Los certificados generados por el PSC APACUANA, podrán ser revocados por las siguientes razones:

1. Caducidad o expiración.
2. Extravío o pérdida.
3. Cuando la clave privada se considera comprometida.
4. Despido o suspensión por procedimiento administrativo del usuario.
5. Violación de la seguridad.
6. Fin de la relación laboral de cualquiera de los usuarios.
7. De acuerdo a los establecido en las leyes que regulan la materia.

8. Otras que considere necesarias el PSC APACUANA.

Las formas permitidas por el PSC Apacuana para generar la revocación de un certificado son las siguientes:

1.6.1 Solicitud de revocación por parte del usuario desde portal web:

- El Usuario deberá ingresar al portal.apacuana.com y autenticarse con sus credenciales.
- Una vez autenticado, deberá ir a la opción del menú para revocar su certificado.
- Para cumplir con la petición, deberá seleccionar una de las opciones que se desplegará en el menú, que mejor describa el motivo por el cual desea revocar su certificado.
- Hace clic en proceder y la solicitud queda registrada en el sistema
- Un operador AC recibirá la solicitud de revocación del usuario, procederá a revisar y posteriormente a aprobar
- Una vez aprobada, se envía la petición a la PKI, donde se revoca el certificado y se actualizará el listado de certificados revocados, que estará disponible desde la URL https://pub.apacuana.com/lcr/

1.6.2. Solicitud de revocación por parte del usuario directo a oficina Apacuana

- El usuario deberá asistir a la oficina para solicitar la revocación de su certificado
- Será atendido por un operador de AR, el cual validará la información del usuario dentro del sistema
- El operador luego registrará la solicitud de revocación del certificado del usuario, indicando el motivo de la revocación para que sea atendido por la AC del PSC Apacuana.
- Se registra la solicitud y luego el operador debe confirmar la aprobación de revocación del certificado en cuestión.
- Una vez aprobada, se envía la petición a la PKI, donde se revoca el certificado y se actualizará el listado de certificados revocados, que estará disponible desde la URL https://pub.apacuana.com/lcr/.

El PSC APACUANA procesa las solicitudes de revocación dentro de las veinticuatro (24) horas de haber recibido una decisión definitiva de la raíz de certificación de la autoridad de certificación (AC).

1.7. Procedimiento para realizar una solicitud de suspensión de un certificado

El procedimiento para la suspensión de certificados está limitado solo a los perfiles de los siguientes certificados:

1.7.1. Representante de Empresa Pública

En el caso de Representante de Empresa Pública se puede solicitar la suspensión del certificado electrónico cuando el suscriptor propietario del mismo deba ausentarse de su cargo por un determinado periodo, lo cual deberá indicar en el sistema el motivo de la ausencia y definir el periodo por el cual durará la suspensión del certificado. Este periodo no podrá exceder la duración de noventa (90) días continuos. Para realizar esta solicitud, el suscriptor deberá ingresar al portal https://portal.apacuana.com, autenticarse con sus credenciales. Una vez dentro de su perfil, tendrá la opción para suspender su certificado. Deberá indicar el motivo y la duración del periodo de suspensión. Una vez realizada la solicitud, se confirmará la acción con el código temporal enviado al correo electrónico del suscriptor para validar la solicitud. Una vez verificado el código, la solicitud quedará aprobada inmediatamente. Durante el periodo que se indicó para la suspensión, el suscriptor no podrá utilizar su certificado electrónico para firmar dentro del sistema del PSC Apacuana.

1.7.2. Empleado de Institución Pública (Funcionario Público)

En el caso de Empleado de Empresa Pública se puede solicitar la suspensión del certificado electrónico cuando el suscriptor propietario del mismo deba ausentarse de su cargo por un determinado periodo, lo cual deberá indicar en el sistema el motivo de la ausencia y definir el periodo por el cual durará la suspensión del certificado. Este periodo no podrá exceder la duración de noventa (90) días continuos.

Para realizar esta solicitud, el suscriptor deberá ingresar al portal https://portal.apacuana.com, autenticarse con sus credenciales. Una vez dentro de su perfil, tendrá la opción para suspender su certificado. Deberá indicar el motivo y la duración del periodo de suspensión. Una vez realizada la solicitud, se confirmará la acción

con el código temporal enviado al correo electrónico del suscriptor para validar la solicitud. Una vez verificado el código, la solicitud quedará aprobada inmediatamente.

Durante el periodo que se indicó para la suspensión, el suscriptor no podrá utilizar su certificado electrónico para firmar dentro del sistema del PSC Apacuana.

1.7.3. Representante de Empresa Privada

En el caso de Representante de Empresa Privada se puede solicitar la suspensión del certificado electrónico cuando el suscriptor propietario del mismo deba ausentarse de su cargo por un determinado periodo, lo cual deberá indicar en el sistema el motivo de la ausencia y definir el periodo por el cual durará la suspensión del certificado. Este periodo no podrá exceder la duración de noventa (90) días continuos.

Para realizar esta solicitud, el suscriptor deberá ingresar al portal https://portal.apacuana.com, autenticarse con sus credenciales. Una vez dentro de su perfil, tendrá la opción para suspender su certificado. Deberá indicar el motivo y la duración del periodo de suspensión. Una vez realizada la solicitud, se confirmará la acción con el código temporal enviado al correo electrónico del suscriptor para validar la solicitud. Una vez verificado el código, la solicitud quedará aprobada inmediatamente. Durante el periodo que se indicó para la suspensión, el suscriptor no podrá utilizar su certificado electrónico para firmar dentro del sistema del PSC Apacuana.

1.7.4. Empleado de Empresa Privada

En el caso de Empleado de Empresa Privada se puede solicitar la suspensión del certificado electrónico cuando el suscriptor propietario del mismo deba ausentarse de su cargo por un determinado periodo, lo cual deberá indicar en el sistema el motivo de la ausencia y definir el periodo por el cual durará la suspensión del certificado. Este periodo no podrá exceder la duración de noventa (90) días continuos.

Para realizar esta solicitud, el suscriptor deberá ingresar al portal https://portal.apacuana.com, autenticarse con sus credenciales. Una vez dentro de su perfil, tendrá la opción para suspender su certificado. Deberá indicar el motivo y la duración del periodo de suspensión. Una vez realizada la solicitud, se confirmará la acción con el código temporal enviado al correo electrónico del suscriptor para validar la solicitud. Una vez verificado el código, la solicitud quedará aprobada inmediatamente.

Durante el periodo que se indicó para la suspensión, el suscriptor no podrá utilizar su certificado electrónico para firmar dentro del sistema del PSC Apacuana.

2. **Tramitación de solicitud de un certificado**

En este apartado se especifican las funciones que cumplirá la AR para la tramitación de la solicitud de un certificado por parte de los suscriptores.

Las funciones de autenticación por parte de la AR, se establecerán de acuerdo a los procesos definidos, el cual se describe a continuación.

El Operador de la AR, ingresa con su credencial a la interfaz de la AR. a través de la URL backoffice.apacuana.com

Adicionalmente, se regirá de acuerdo al tipo de certificado y a lo establecido en las Políticas de Certificación del PSC APACUANA.

2.1. Realización de las funciones de identificación y autenticación

Las funciones de identificación y autenticación de los suscriptores que optan a la adquisición de una firma o certificado, está asignada a la autoridad de registro (AR) del PSC APACUANA. La autoridad de registro (AR) del PSC APACUANA cuando se trate de firmas electrónicas que acrediten empresas o entes públicos procederá de la manera siguiente:

2.1.1. Ente público: El Operador de la Autoridad de Registro (AR) procederá a comprobar la publicación en la gaceta oficial de la república bolivariana de Venezuela de la resolución que crea a la entidad o empresa pública. Todo certificado electrónico de organización deberá estar asociado a un responsable humano por dicho certificado. La autoridad de registro (AR) del PSC APACUANA cumplirá los pasos de verificación y comprobación de identidad y representación. Una vez comprobadas la identidad de la organización y las facultades de representación se procederá a validar el resto de la información solicitada por el sistema de contratación del PSC APACUANA y cumplido el procedimiento exitosamente, la autoridad

de registro (AR) comunicará a la autoridad de certificación (AC) del PSC APACUANA, su conformidad respecto a los datos para que se proceda a la generación del certificado electrónico contratado por el suscriptor.

2.1.2. Ente privado: La autoridad de registro (AR) procederá a comprobar la existencia de la empresa privada a través de la revisión de su documento constitutivo-estatutario, debidamente inscrito en la oficina del registro mercantil correspondiente a la circunscripción judicial del domicilio de la empresa Privada, como de la publicación del registro de empresa en un diario mercantil. Todo certificado electrónico de organización deberá estar asociado a un responsable humano por dicho certificado. La autoridad de registro (AR) del PSC APACUANA cumplirá los pasos de verificación y comprobación de identidad y representación. Una vez comprobadas la identidad de la organización y las facultades de representación se procederá a validar el resto de la información solicitada por el sistema de contratación del PSC APACUANA y cumplido el procedimiento exitosamente, la autoridad de registro (AR) comunicará a la autoridad de certificación (AC) del PSC APACUANA, su conformidad respecto a los datos para que se proceda a la generación del certificado electrónico contratado por el suscriptor.

2.2. Aprobación o negación de un certificado

Serán objeto de aprobación todos aquellos certificados que cumplan con los requisitos exigidos por el PSC APACUANA, tanto de validación, como firmas de convenios y otros descritos en las Políticas de Certificación de acuerdo al tipo de certificado a ser otorgado. Por otra parte, el PSC APACUANA se reserva el derecho de negar un certificado, en los siguientes casos:2.2.1 No cumpla con los requisitos debidamente exigidos por el PSC APACUANA en su DPC y PC respectivas.

2.2.2. Otros que el PSC APACUANA considere pertinente de acuerdo al marco legal vigente.

2.3. Plazo para la tramitación de un certificado

El plazo para la tramitación de un certificado por parte del PSC APACUANA, será a lo sumo de tres (03) días hábiles para la firma del mismo. En este período se lleva a cabo el proceso de autenticación y validación de los datos suministrados y, en caso de ser exitosa dicha validación, su posterior firma.

3. **Emisión de certificados**

En este apartado, se mencionan los requerimientos establecidos por el PSC APACUANA para la firma y notificación de la emisión de un certificado a los signatarios.

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

La AC para la emisión de sus certificados validará que se hayan cumplido todos los procedimientos de autenticación y validación de la información suministrada por los usuarios, de acuerdo al apartado 1.2 Proceso de solicitud de generación de certificado. Una vez culminado este proceso, los operadores de la AC del PSC Apacuana, procederán a firmar los certificados correspondientes y a remitir los mismos.

3.2. 3.2. Notificación al solicitante por parte del PSC APACUANA acerca de la emisión de su certificado electrónico

La AC, notificará a los usuarios sobre la emisión de sus certificados vía electrónica, adicionalmente efectuará la actualización de las listas de certificados emitidos, en la siguiente dirección electrónica https://portal.apacuana.com/ce

4. **Aceptación de certificados**

En este apartado se definen los procedimientos para la aceptación de los certificados y publicación de los mismos.

4.1. Forma en la que se acepta el certificado

Para la aceptación del certificado, el signatario deberá recibir el archivo firmado por el PSC APACUANA, y continuar con los siguientes procedimientos de acuerdo al tipo de certificado:

a. Sí el certificado posee dentro de sus atributos la autenticación: El signatario deberá instalar el certificado en el navegador y cumplir con los demás requisitos de seguridad establecidos en el documento de Políticas de Certificación.
b. Sí el certificado posee dentro de sus atributos firma o cifrado: El signatario deberá concatenar el certificado dentro de la cadena de confianza, crear el archivo KEY, y convertirlo en PEM, para la instalación en el medio de almacenamiento que cumpla con las características de seguridad requeridas por el PSC APACUANA, previamente definidas en el documento de Políticas de Certificación.

4.2. Publicación del certificado por el PSC APACUANA

El PSC APACUANA, publicará la lista de certificados emitidos y válidos, una vez, se haya efectuado la operación en la siguiente dirección electrónica: https://portal.apacuana.com/ce, en el caso de los certificados revocados, los mismos serán publicados en la siguiente dirección electrónica: https://pub.apacuana.com/lcr/

4.3. Notificación de la emisión del certificado a otras autoridades

En caso de terceros interesados que requieran información relacionada con la emisión de certificados por parte el PSC APACUANA

5. Uso de par de claves y del certificado

Los procedimientos establecidos para el uso de par de claves y certificados emitidos por el PSC APACUANA, son los que se detallan a continuación:

5.1. Uso de la clave privada del certificado

La clave privada del certificado, será exclusiva del usuario y de su absoluta responsabilidad. En tal sentido, se deberá establecer mecanismos de seguridad que aseguren el uso del certificado emitido y el resguardo del mismo los cuales están contemplados en la PC respectiva que rige el certificado y en el modelo de contrato que se

suscribe entre el signatario y el PSC Apacuana en el momento de aprobar la solicitud de emisión del certificado.

5.2. Uso de la clave pública y del certificado por los terceros de buena fe

El uso de la clave pública será responsabilidad del signatario, en tal sentido el mismo deberá establecer mecanismos de seguridad para su resguardo. Así mismo, es responsable de compartir su clave pública sólo con el PSC- APACUANA para efectuar las operaciones de cifrado y descifrado de las operaciones con la Empresa Apacuana. En el caso de los terceros de buena fe deben verificar el estado del certificado previo a depositar su confianza y conocer los usos de este establecidos en la presente DPC.

6. **Renovación del certificado**

La renovación de los certificados emitidos por el PSC APACUANA, estarán sujetos a lo siguiente:

6.1. Causas para la renovación

La causa por la cual se efectuará la renovación de un certificado, será por la caducidad del mismo.

6.2. Entidad que puede solicitar la renovación de un certificado

La renovación de un certificado podrá ser solicitada por el signatario al cual le fue emitido el certificado por el PSC-APACUANA.

6.3. Procedimiento de solicitud para la renovación de un certificado

El procedimiento establecido para la renovación de un certificado será el mismo que se efectúa para la solicitud de un certificado por primera vez, definido en este documento en el apartado N.º XIV. Sobre el “CICLO DE VIDA DE LOS CERTIFICADOS (REQUERIMIENTOS OPERATIVOS)”, sección 1.2 del “Proceso de la generación de la solicitud de certificados y responsabilidades”.

6.4. Notificación de la emisión de un nuevo certificado

Cuando un signatario desee incorporar un nuevo certificado para la tramitación de operaciones con la Empresa Apacuana, se

deberá efectuar su solicitud de acuerdo a lo establecido en el presente documento en el apartado N° XIV. Sobre el "CICLO DE VIDA DE LOS CERTIFICADOS (REQUERIMIENTOS OPERATIVOS)", sección 1.2 del "Proceso de la generación de la solicitud de certificados y responsabilidades".

6.5. Publicación de los certificados renovados por el PSC APACUANA

La información correspondiente a la renovación de los certificados emitidos por el PSC APACUANA, estará disponible en la siguiente dirección electrónica: https://portal.apacuana.com/

6.6. Notificación de la emisión del certificado a otras entidades

Por políticas internas del PSC APACUANA, sólo se efectuará la notificación de la renovación de los certificados al signatario correspondiente.

7. **Nueva clave del certificado**

Los certificados electrónicos emitidos por el PSC APACUANA, deberán mantener su integridad durante su tiempo de vigencia. En caso, que el signatario requiera la modificación de su par de claves, deberá justificar su solicitud. El PSC APACUANA, estudiará el caso y de ser procedente, efectuará la revocación del certificado actual y el signatario realizará el proceso de registro inicial para generar un nuevo certificado, de acuerdo al apartado N.° XIV. Sobre el "CICLO DE VIDA DE LOS CERTIFICADOS (REQUERIMIENTOS OPERATIVOS)", sección 1.2 del "Proceso de la generación de la solicitud de certificados y responsabilidades".

8. **Modificación de certificados**

Los certificados electrónicos emitidos por el PSC APACUANA, deberán mantener su utilidad de acuerdo a la PC que regula su objetivo durante su tiempo de vigencia. En caso, que el signatario requiera la modificación del mismo deberá efectuar su solicitud debidamente justificada. El PSC APACUANA, estudiará el caso y de ser procedente, efectuará la

revocación del certificado actual y el signatario realizará el proceso de registro inicial para generar un nuevo certificado, de acuerdo al apartado N.º XIV. Sobre el "CICLO DE VIDA DE LOS CERTIFICADOS (REQUERIMIENTOS OPERATIVOS)", sección 1.2 del "Proceso de la generación de la solicitud de certificados y responsabilidades".

9. **Revocación de un certificado**

Las circunstancias por las cuales se regirá el PSC APACUANA, para efectuar la revocación de certificados, serán las siguientes:

9.1. Circunstancias para la revocación del certificado

La atención a la revocación de un certificado se realizará de acuerdo al apartado N.º XIV. Sobre el "CICLO DE VIDA DE LOS CERTIFICADOS (REQUERIMIENTOS OPERATIVOS)", sección 1.6 Procedimiento para realizar una solicitud de revocación de un certificado.

9.2. Entidad que puede solicitar la revocación de un certificado

La entidad que puede solicitar la revocación de un certificado se realizará de acuerdo al apartado N.º XIV. Sobre el "CICLO DE VIDA DE LOS CERTIFICADOS (REQUERIMIENTOS OPERATIVOS)", sección 1.6 Procedimiento para realizar una solicitud de revocación de un certificado.

9.3. Procedimiento de solicitud de revocación de certificado electrónico

El procedimiento para la solicitud de revocación de un certificado electrónico se realizará de acuerdo al apartado N.º XIV. Sobre el "CICLO DE VIDA DE LOS CERTIFICADOS (REQUERIMIENTOS OPERATIVOS)", sección 1.6 Procedimiento para realizar una solicitud de revocación de un certificado.

9.4. Límites del período de la solicitud de revocación

La entidad que puede solicitar la revocación de un certificado se realizará de acuerdo al apartado N.º XIV. Sobre el "CICLO DE VIDA DE LOS CERTIFICADOS (REQUERIMIENTOS OPERATIVOS)", sección 1.6 Procedimiento para realizar una solicitud de revocación de un certificado.

9.5. Circunstancias para la suspensión

La circunstancias para la suspensión de certificados se define en el apartado "1.7 Procedimiento para realizar una solicitud de suspensión de un certificado" del presente documento.

9.6. Entidad que puede solicitar la suspensión

La entidad que puede solicitar la suspensión de certificados se define en el apartado "1.7 Procedimiento para realizar una solicitud de suspensión de un certificado" del presente documento.

9.7. Procedimientos para la Solicitud de Suspensión

El procedimiento para la solicitud de suspensión de certificados se define en el apartado "1.7 Procedimiento para realizar una solicitud de suspensión de un certificado" del presente documento.

9.8. Límites del Período de Suspensión de un Certificado

El límite de periodo para la suspensión de certificados se define en el apartado "1.7 Procedimiento para realizar una solicitud de suspensión de un certificado" del presente documento.

9.9. Frecuencia de emisión de listas de certificados revocados

El PSC APACUANA, actualiza su lista de certificados revocados una vez que se haya efectuado está operación, dicha información será actualizada cada cuatro (4) horas o cada vez que sea revocado un certificado y estará disponible en el portal Web https://pub.apacuana.com/lcr/

9.10. Requisitos para la comprobación de la lista de certificados revocados

Los requisitos que deben cumplir los signatarios o terceros de buena fe para comprobar la lista de certificados es ingresar a la siguiente dirección electrónica: https://pub.apacuana.com/lcr/ , dado que la lista de certificados revocados es de carácter público.

En tal sentido el PSC APACUANA, mantendrá actualizadas las listas de revocación, de forma que los signatarios o terceros de buena fe puedan obtener la información requerida respecto a los certificados, mediante los medios de publicación anteriormente establecidos.

9.11. Disponibilidad de comprobación en línea del servicio de revocación del estado del certificado

Con el fin de garantizar la disponibilidad de comprobación en línea del servicio de revocación del certificado, el PSC APACUANA dispondrá de una dirección electrónica, https://pub.apacuana.com/lcr/ en donde los signatarios y demás interesados podrán visualizar el estado en línea del servicio de revocación de todos los certificados emitidos por el PSC APACUANA.

Adicionalmente, se notificará a través de correo electrónico el estatus de sus certificados a los signatarios correspondientes cuando el signatario así lo solicite a la dirección de correo contacto@apacuana.com

9.12. Requisitos de Comprobación en línea del estado de revocación

Tal como se especificó en el punto N.º 9.11 de este apartado, el usuario o terceros de buena fe interesado en comprobar en línea el estado de revocación de un certificado, sólo deberá ingresar a la siguiente dirección electrónica: https://pub.apacuana.com/lcr/

9.13. Otras formas disponibles para la divulgación de la revocación

Tal como se mencionó en el punto Nº 9.11 de este apartado, el PSC APACUANA también efectuará la notificación al signatario sobre la revocación de los certificados emitidos

9.14. Requisitos para la Verificación de Otras Formas de Divulgación de Revocación

No se tienen contemplados requisitos para la verificación de otras formas de divulgación de revocación adicionales.

9.15 Requisitos Específicos para Casos de Compromiso de Claves

En caso de compromiso de la clave privada, el signatario deberá notificar de manera inmediata el acontecimiento mediante el correo electrónico contacto@apacuana.com, a fin de que el PSC APACUANA efectúe los trámites correspondientes.

10. Servicio de comprobación de estado de certificados

10.1. Características operativas

El servicio de comprobación se realiza mediante el protocolo OCSP (Online Certificate Status Protocol), el cual proporciona la información actualizada sobre el estado de los certificados emitidos por el PSC Apacuana https://pub.apacuana.com/ocsp.

10.2. Disponibilidad del Servicio

El PSC APACUANA, mantiene los servicios de las listas de certificados del protocolo OCSP disponibles las 24 horas del día y los 365 días del año.

10.3. Características adicionales

No se encuentran definidas características adicionales para el servicio OCSP.

11. Finalización de la suscripción

La finalización de la suscripción de los certificados emitidos por el PSC APACUANA, serán causados por el vencimiento o revocación de los mismos de acuerdo a los parámetros definidos dentro de las PC de cada tipo de certificado.

12. Custodia y recuperación de la clave

12.1. Prácticas y políticas de recuperación de la clave

La clave privada del PSC APACUANA se almacena y se custodia en el dispositivo criptográfico HSM ("Hardware Security Module" o Módulo de Seguridad de Hardware), en caso de recuperación de la misma se realizará a través de la implementación de controles de autorización. Para el acceso al repositorio de claves privadas es necesario el uso de tarjetas inteligentes con el respectivo quórum para activar el dispositivo y operar, estás son asignadas al personal con Rol de Oficial de Cumplimiento y/o Custodio de la Autoridad de Certificación responsable de la AC, con la compartición de secretos, donde la llave como tal es dividida en partes y se da a conocer a cada uno una sola parte de la misma, siendo necesaria la presencia de n de m (3 de 5) participantes, al momento de requerirse la recuperación de la llave de la AC.

Por otro lado, el esquema de operación del PSC APACUANA y su plataforma tecnológica de certificación se encuentran configurados para que el suscriptor cliente genere su par de claves (pública y privada). Siempre y en todo caso el compromiso de clave derivará del mismo suscriptor cliente pues el PSC APACUANA no genera el par de claves (pública y privada).

Los signatarios serán responsables de su par de claves (privada y pública), esto debido a que dichas claves no son almacenadas por el PSC APACUANA y en caso de extravío o pérdida se deberá emitir un nuevo certificado de acuerdo a las políticas establecidas.

En virtud de lo anterior, si el suscriptor extravía su clave privada, se deberá proceder a la emisión de un nuevo certificado y deberá cumplir el proceso de contratación del PSC Apacuana a tales efectos. La clave pública siempre estará en el repositorio, de conformidad con lo señalado en el presente documento de declaración de prácticas de certificación (DPC).

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

1. Controles de seguridad física

1.1. Construcción y localización de las instalaciones

En función de validar las condiciones físicas de las instalaciones donde opera el PSC Apacuana, se cuentan con diversas medidas de seguridad, tales como:

1.1.1. El PSC Apacuana se encuentra instalado en un centro de datos con altos mecanismos de seguridad respecto a su estructura física, tal como se indica en los planos de funcionamiento del hosting, Ver anexo DAYCOHOST (Apartado “VII. Continuidad Operativa de Daycohost”).

1.1.2. El control de acceso a las instalaciones donde funciona el centro de datos del PSC Apacuana se realiza mediante el uso de tarjeta de proximidad en el último anillo de seguridad. Mientras que en la entrada se emplea una tarjeta de acceso y luego de proximidad hacia el centro de datos.

1.1.3. Existe un sistema de protección y prevención de incendios donde funciona el centro de datos del PSC Apacuana con detectores de humo, extintores, formación del personal para

actuar ante incendios, entre otros, de acuerdo al Convenio de Contratación de Servicios de Daycohost.

1.1.4. Existe un puesto de vigilancia en zonas cercanas al centro de datos donde funciona el PSC Apacuana.

1.1.5. Se tiene una Bitácora de Acceso al centro de datos donde funciona el PSC Apacuana.

1.1.6. Existe un sistema de control de acceso donde funciona el centro de datos del PSC Apacuana restringido sólo a los trabajadores autorizados a través de tarjeta de proximidad.

1.1.7. Funciona un circuito cerrado de televisión en todas las áreas críticas o de acceso restringido donde funciona el centro de datos del PSC Apacuana

1.2. Acceso Físico

El acceso a las instalaciones del PSC APACUANA dentro del centro de datos está restringido sólo al personal autorizado para tal fin. En este sentido, sólo tendrá acceso a estas instalaciones los trabajadores que por el desempeño de sus funciones así lo amerite, Ver anexo DAYCOHOST (Apartado “VII. Continuidad Operativa de Daycohost”).

Las áreas sensibles y críticas se resguardan mediante el empleo de controles de acceso físico al Centro de Datos de Daycohost a fin de permitir el acceso sólo al personal autorizado. Estos controles de acceso físico tienen las siguientes características, soportadas en el contrato de SLA, reflejadas en el VIII (pág. 71) contemplando lo siguiente:

1. Supervisión y vigilancia con cámaras de seguridad a los visitantes de áreas donde estarán ubicados los servidores de la plataforma de Certificación. Registrar la fecha y horario de su ingreso y egreso.
2. Control y limitaciones de acceso a la información clasificada y a las instalaciones de la plataforma de Certificación, exclusivamente a las personas autorizadas. Se mantiene un registro para permitir auditar todos los accesos.
3. Revisión y actualización de los cambios en los derechos de acceso a

las áreas protegidas, documentados y firmados por el Director de Tecnología.

4. Revisión y auditoría según lo contemplado en el plan de seguridad y riesgos para la efectiva ejecución de los controles de acceso a las áreas protegidas. Esta tarea la realizará la unidad de auditoría interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información del PSC Apacuana.

1.3. Alimentación Eléctrica y Aire Acondicionado

El centro de datos del hosting donde se encuentra el PSC Apacuana, cuenta con una (01) unidad de UPS y un banco de baterías de 40 minutos, además de un (01) PDU, sistemas de aire acondicionado de precisión de manera redundante, una (01) planta eléctrica, a fin de asegurar el funcionamiento continúo y óptimo de los equipos que allí reposan Ver anexo DAYCOHOST (Apartado "III. Infraestructura Data Center Multisite, Geo-Distribuido (DCI) de Daycohost")

El equipamiento eléctrico del centro de datos de DaycoHost provee protección con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones y funcionamiento descrito en los Niveles de Servicios SLA de Daycohost. Para asegurar la continuidad del suministro de energía, a continuación, se mencionan algunas medidas de control tomadas en cuenta:

1. Disposición de múltiples enchufes o líneas de suministro en la línea donde se encuentra el rack de operaciones del PSC Apacuana para evitar un único punto de falla en el suministro de energía.
2. Suministro de energía continua al rack del PSC Apacuana a través de un "Uninterruptible Power Supply" (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas de la empresa. La determinación de dichas operaciones críticas, será el resultado del análisis integral de riesgos y seguridad realizado por la empresa.

3. Disponibilidad de un generador de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía en el centro de datos de Daycohost.
4. Planificación de mantenimiento de los generadores a fin de que sean inspeccionados y probados periódicamente para asegurar que funcionen según lo previsto en los planes de contingencia del centro de datos DaycoHost

1.4. Exposición al Agua

Las instalaciones del hosting donde se encuentra el PSC APACUANA, cuentan con diversos mecanismos de protección como detectores de humedad, entre otros, para evitar las exposiciones al agua y asegurar la continuidad de las operaciones, Ver anexo DAYCOHOST (Apartado "III. Infraestructura Data Center Multisite, Geo-Distribuido (DCI) de Daycohost").

1.5. Prevención y Protección Contra Incendios

Las instalaciones del hosting donde se encuentra el PSC APACUANA disponen de mecanismos de seguridad contra incendio tanto de equipos como de cableados, Ver anexo DAYCOHOST (Apartado "III. Infraestructura Data Center Multisite, Geo-Distribuido (DCI) de Daycohost").

1.6. Sistemas de Almacenamiento

La información referente al PSC APACUANA, se encuentra almacenada en arreglos de discos en el centro de datos de DaycoHost de forma redundante que garantizan su disponibilidad en caso de fallos, con cifrado de la información, dependiendo de su naturaleza del activo de información contempaldo dentro de la politica de seguridad, considerando que la documentación se encuentra en sistemas donde se resguardan las diversas versiones que deben mantenerse cifradas y almacenadas, para el caso del software de certificación

electrónica que se encuentra en los servidores del centro de datos DaycoHost donde se encuentra la ICP del PSC Apacuana.

1.7. Eliminación de residuos

La eliminación de residuos, se lleva a cabo de acuerdo a los mecanismos de seguridad establecidos por el PSC APACUANA, con el fin de garantizar que la información confidencial o interna que se encuentre eliminada no pueda ser recuperada bajo ningún mecanismo.

1.8. Almacenamiento de copias de seguridad

Las copias de seguridad se almacenan en Daycohost, fuera de las instalaciones del hosting donde se encuentra el PSC APACUANA de forma cifrada en una caja de seguridad, la cual posee características altamente seguras, para evitar daños y accesos no autorizados, cumpliendo con los estándares de seguridad establecidos en la ISO/IEC 27001 e ISO/IEC 27002.

2. Controles de procedimientos

2.1. Definición de roles confiables

La administración del PSC APACUANA, estará a cargo del Director de Operaciones, será el responsable de aplicar las estrategias necesarias para la operación del PSC APACUANA, según las políticas establecidas y la normativa jurídica vigente que regula la materia. También, estarán bajo la supervisión de la Dirección de Tecnología. Los roles confiables dentro del PSC Apacuana se constituyen en las funciones de los custodios, operadores de la AR y AC, Oficial de Cumplimiento, Auditor Interno y Coordinador de Infraestructura, de acuerdo a la pertinencia de estos roles, los cuales son de revisión y decisión de la alta gerencia y se encuentran descritos en el documento de STA-DO-024-Estructura Organizativa del PSC APACUANA.

Por otro lado, la verificación periódica del cumplimiento de los controles establecidos estará a cargo tanto de la Dirección de

Seguridad de la Información y de la Dirección de Auditoría Interna del PSC APACUANA como de SUSCERTE.

2.2. Separación de funciones

Con el fin de maximizar la transparencia del proceso de certificación electrónica ejecutado por el PSC APACUANA, los operadores de la AR no ejecutarán las funciones relacionadas a la AC y viceversa, ni tampoco podrán ejercer cargos de custodios de AR y AC simultáneamente, ni ejercer como oficial de cumplimiento o auditor interno, segregando ambas responsabilidades sobre distintos trabajadores de la Dirección de Seguridad de la Información. El perfil y roles del personal encargado están descritos en el documento STA-DO-024-Estructura Organizativa del PSC APACUANA.

2.3. Número de personas requeridas por rol

El número de personas requeridas por rol será definido por la Dirección de Seguridad de la Información del PSC APACUANA, de acuerdo a las necesidades institucionales. La cantidad de personas en cada rol y el rol están definidos en el documento STA-DO-024-Estructura Organizativa PSC APACUANA.

2.4. Identificación y autenticación para cada rol

La identificación y autenticación para cada rol, será definido por el PSC APACUANA, en tal sentido, serán quienes asignan los roles a cumplir por cada uno de los trabajadores asignados y asimismo le otorgarán los accesos a los sistemas y estructuras físicas correspondientes. Los accesos determinados para cada rol serán asignados por la Dirección de Tecnología de acuerdo con las políticas de seguridad de la información del PSC Apacuana.

3. Controles de seguridad personal

3.1. Requerimientos de antecedentes, calificación, experiencia y acreditación

El trabajador que presta sus servicios en el PSC APACUANA, realizará funciones profesionales exclusivas asociadas al Servicio de Certificación Electrónica y su Infraestructura de Clave Pública. Éste debe poseer los conocimientos, experiencia y formación suficiente, para el mejor cometido de las funciones asignadas.

En este sentido, la Coordinación de Capital Humano de APACUANA, debe llevar a cabo los procesos de selección de personal correspondientes, con el objeto de que el perfil profesional del empleado se adecue a las características propias de las tareas a desarrollar.

Entre los requisitos - para los empleados de la ICP del PSC Apacuana - tenemos:

3.1.1. Conocimientos asociados al tema de certificación electrónica.

3.1.2. Conocimientos básicos sobre seguridad en sistemas de información.

3.1.3. Profesional universitario en el área de informática, computación o carreras afines.

3.2. Requerimientos de formación.

Los trabajadores que laboran para el PSC APACUANA, posee asignado un rol que va dirigido al cumplimiento de políticas de seguridad del PSC APACUANA. De igual modo, los conocimientos, cualificación y experiencia aseguran su capacidad para llevar a cabo cada una de sus obligaciones.

En este sentido, el PSC APACUANA cuenta con planes de formación para el personal, a fin de elevar la capacidad de los mismos, los cuales se encuentran referenciados en las STA-DO-006-Políticas de Seguridad de la Información, entre los cuales se incluyen:

3.2.1. Documentación de la Infraestructura de Clave Pública (ICP).

3.2.2. Seguridad de la Información.

3.2.3. Gestión de incidentes.

3.2.4. Certificación electrónica.
3.2.5. Software libre
3.2.6. Declaración de Prácticas y Políticas de Certificación.
3.2.7. Manuales de Operación.
3.2.8. Plan de Recuperación ante Desastres.
3.2.9. Manuales de Políticas de Seguridad de la Información.
3.2.10. Políticas de Confidencialidad.
3.2.11. Descripción de Cargo.
3.2.12. Acuerdo de confidencialidad.
3.2.13. Manual de procedimientos internos.
3.2.14. Otras que considere pertinentes.

3.3. Requerimientos y frecuencia de actualización de la formación

La actualización de la formación de los trabajadores del PSC APACUANA, estará acorde a la detección de necesidades anuales efectuada por la Coordinación de Capital Humano de APACUANA especificadas en las STA-DO-006-Políticas de Seguridad de la Información del PSC Apacuana

3.4. Frecuencia y secuencia de rotación de tareas

La frecuencia de rotación de las tareas para los operadores de la AC y AR, será definida por el Director de Seguridad de la Información, con lapsos de rotación no mayores a seis (06) meses, previa aprobación de la Dirección Ejecutiva. Para mantener la operatividad se dispone de la siguiente relación de personas por rol:

- Oficial de Cumplimiento y/o Custodio de la AC (3) Tres de cinco (5) personas, de acuerdo con el apartado 12.1 Realización de las Funciones de Identificación y Autenticación, relacionado con los quórum de tarjetas inteligentes y la activación y/u operación de la llave pública.
- Operador de Autoridad de Certificación de AC (2) dos personas, para garantizar siempre la disponibilidad del personal.

- Operador de Autoridad de Registro (2) Dos personas, para garantizar siempre la disponibilidad del personal.

3.5. Sanciones por acciones no autorizadas

Las sanciones establecidas para el personal del PSC APACUANA por acciones no autorizadas, se regirán de acuerdo a lo establecido en los Manuales de Políticas de Seguridad de la Información del PSC APACUANA.

3.6. Documentación proporcionada al personal

El PSC APACUANA, debe proporcionar a sus trabajadores, una serie de documentos que apoyen su gestión diaria. Dentro de los cuales se encuentran:

3.6.1. Declaración de Prácticas y Políticas de Certificación.
3.6.2. Manuales de Operación.
3.6.3. Documentación relacionada a la (ICP)
3.6.4. Plan de Recuperación ante Desastres.
3.6.5. Manuales de Políticas de Seguridad de la Información.
3.6.6. Políticas de Confidencialidad.
3.6.7. Descripción de Cargo.
3.6.8. Acuerdo de confidencialidad.
3.6.9. Manual de procedimientos internos.
3.6.10. Otras que considere pertinentes.

4. Procedimientos de control de seguridad

4.1. Tipos de eventos registrados

4.1.1. Los eventos registrados son los detallados a continuación:

4.1.1.1 Registros de autenticación.
4.1.2.1 Registros de auditoría.
4.1.3.1 Registros de Aplicaciones.
4.1.4.1 Registros del Sistema Operativo.
4.1.5.1 Registros de Bases de Datos.
4.1.6.1 Registros de envío y recepción de correos.

4.1.2. Todos estos registros, se encuentran definidos de acuerdo a los estándares de seguridad establecidos por el PSC Apacuana con el fin de robustecer su plataforma tecnológica y garantizar la seguridad de la información que maneja, además de cumplir con las políticas y estándares de seguridad para mantener la confidencialidad y disponibilidad de los servicios ofrecidos. Dentro de estos registros se toman en cuenta los siguientes eventos:

4.1.2.1 Inicialización de los sistemas de certificación.

4.1.2.2 Tentativas de remover, modificar, realizar o definir cualquier cambio de privilegios de los sistemas del PSC APACUANA.

4.1.2.3 Cambios de configuración o nuevas claves.

4.1.2.4 Cambios en las políticas de creación de certificados.

4.1.2.5 Operaciones de escritura o lectura en el repositorio de certificados y en otros repositorios.

4.1.2.6 Operaciones descritas en el repositorio.

Estos registros deberán almacenar todos los datos necesarios, tales como: hora del evento, identificación del usuario que lo originó, entre otros. Adicionalmente, el manejo de tipo de eventos se encuentra con los procesos complementarios en el Manual de Políticas de Seguridad de la Información en el apartado relativo a 15.5. Gestión de Incidentes de Seguridad de la Información.

4.2. Frecuencia de procesamiento de los registros de log de auditoría

El procesamiento de los registros de “Logs”, por parte del PSC APACUANA, se efectúa de manera constante durante las veinticuatro (24) horas del día.

4.3. Períodos de resguardo de los log de auditoría

El PSC APACUANA, debe mantener todos los registros de auditoría generado por el sistema, por un período mínimo desde la fecha de su creación de:

- Seis (06) meses en línea.
- Cinco (05) años en cintas de respaldo.

4.4. Protección de los “Log” de auditoría

El acceso a los “Log” de auditoría del PSC APACUANA, sólo lo tendrá el personal autorizado para tal fin de acuerdo a la estructura organizativa y la descripción de funciones. Asimismo, esta información se resguarda en cintas de respaldo de forma cifrada, en las instalaciones del Centro de Datos de DaycoHost mediante la utilización de caja fuerte de seguridad con pin de seguridad de 4 dígitos.

4.5. Procedimiento de respaldo de los Log de auditoría

Para garantizar la disponibilidad e integridad de los “Log” de auditoría, se estableció el siguiente procedimiento de respaldo:

4.5.1 Dos respaldos incrementales de forma diaria.

Se dispondrá de una unidad de respaldo para almacenar los log de auditoría, de forma incremental diario, mediante el siguiente procedimiento:

1. Realizar una copia completa inicial de todos los datos y archivos log.

2. Identificar y respaldar únicamente los archivos que han sufrido modificaciones desde la última copia.

3. Actualizar y guardar los cambios en una ubicación segura destinada al almacenamiento de los respaldos.

Es importante tener en cuenta que el respaldo incremental se debe realizar de forma periódica para asegurar la protección de los datos más actualizados y minimizar la pérdida de información en caso de fallos o errores.

4.5.2 Un respaldo completo de forma semanal.
Se dispondrá de una unidad de respaldo para almacenar los log de auditoría, de forma incremental diario, mediante el siguiente procedimiento:

1. Realizar una copia completa inicial de todos los datos y archivos log.

Los mismos son almacenados en formatos cifrados y se realizan de forma desatendida.

4.6. Sistema de recopilación de información de auditoría

El sistema de recopilación de la información de autoría, se realiza mediante el dispositivo Luna Backup HSM 7. Registro de eventos del HSM, lo que le permite auditar el uso del HSM y la AC del PSC APACUANA. El registro de eventos de HSM solo es visible y configurable mediante la función de usuario de auditoría.

4.7. Notificación de eventos significativos:

1. Intentos de acceso al registro (inicios de sesión)
2. Registrar la gestión de HSM
3. Eventos de gestión de claves (creación/eliminación de claves)
4. Registrar mensajes de ca_ log externo
5. Registrar eventos relacionados con la configuración del registro

4.8. Análisis de vulnerabilidades

4.8.1 Revisión de actualizaciones de librerías, y herramientas

Periódicamente, se realiza revisión de actualizaciones disponibles de librerías de código de aplicación y herramientas que componen la plataforma tecnológica APACUANA, para garantizar que en todo momento se tenga la tecnología más actualizada y prevenir riesgos por vulnerabilidades en herramientas desactualizadas

4.8.2 Revisión de versiones de código fuente

Se estableció procedimiento interno de revisión y análisis de código fuente para detectar vulnerabilidades y riesgos operacionales que permiten prevenir que dichos riesgos sean desplegados en los servidores cuando sean detectados

4.8.3 Pruebas de penetración y hacking ético

Se estableció con frecuencia de cada 6 meses, pruebas intensivas de penetración y hacking ético de hardware y software que componen la plataforma tecnológica APACUANA, con el fin de detectar posibles vulnerabilidades que representen un riesgo a la operación del PSC APACUANA, permitiendo actuar de manera preventiva en la corrección de vulnerabilidades antes que sean detectadas y explotadas por terceros malintencionados

5. Archivo de informaciones y registros

1.5.1 Tipos de Registros Archivados

Los tipos de registros archivados son los emitidos por la plataforma tecnológica por el PSC APACUANA, según lo establecido en la clasificación indicada en el apartado N.º 4.1 Tipos de eventos registrados del presente capítulo.

1.5.2 Período de Resguardo de un Archivo

El período de retención de los archivos será de acuerdo a lo establecido en el apartado N.º 4.3 Períodos de resguardo de los log de auditoría del presente capítulo.

1.5.3 Método de Protección del Archivo

El método de protección de los archivos del PSC APACUANA, será de acuerdo a lo establecido en el apartado N.º 4.4 Protección de los “Log” de auditoría del presente capítulo.

1.5.4 Procedimientos del Backup del Archivo

El procedimiento de respaldo de los archivos será el predefinido en el apartado N.º 4.5 Procedimiento de respaldo de los Log de auditoría del presente capítulo

1.5.5 Sistema de Repositorios de Archivos (Externo-Interno)

Los sistemas de repositorios de archivos de auditoría para el PSC Apacuana, están constituidos por los logs automáticos que se generan dentro de la plataforma tecnológica del PSC Apacuana asociados a software y hardware que se registran de acuerdo a lo indicado en el apartado 4.1 Tipos de Eventos Registrados. Posteriormente, se realizan

los respaldos cifrados en cintas magnéticas. El PSC APACUANA, almacena los archivos de auditoría de forma cifrada en cintas de respaldo cifrados, en la caja fuerte de seguridad ubicadas dentro y fuera de la Empresa de acuerdo a lo pautado en el apartado 4.4. Protección de los "Log" de auditoría.

1.5.6 Procedimiento para Obtener y Verificar Información de Archivos

La integridad de los archivos respaldados, se garantizará a través del firmado de los mismos y su acceso será validado por el Director de Seguridad de la Información.

1.6. Cambio de clave

Los cambios de clave de los certificados electrónicos emitidos por el PSC APACUANA, no podrán realizarse. En tal sentido, en caso de compromiso de la clave y necesidad de efectuar un cambio, el certificado actual se revocará y será sustituido por uno nuevo.

1.7. Plan de recuperación ante desastres

1.7.1 Procedimientos de Gestión de Incidentes y Vulnerabilidades

El plan de recuperación ante desastres (PRD), del PSC APACUANA, tiene como propósito establecer una serie de procedimientos a seguir en caso de presentarse situaciones de anomalía que impactan la disponibilidad normal del servicio. En tal sentido, el comité de continuidad de negocio es el responsable de tomar la decisión de declarar un escenario de desastre. La primera función, será reunirse de forma inmediata para analizar la situación, determinar la magnitud del desastre, su impacto y comunicar oficialmente el tipo de desastre, para así, activar el apartado Plan de Contingencia.

Cabe destacar, que los procedimientos para la Gestión de Incidentes y Vulnerabilidades, se encuentran en el documento de "Plan de Continuidad de Negocio y Recuperación ante Desastre", donde a partir del Tipo de Desastres y Tipo de Escenario determinados se procederá a realizar una serie actividades que son responsabilidad del Comité de Continuidad de Negocio

1.7.2 Alteración de los Recursos (Hardware, Software y/o Datos)

Esta consideración se encuentra incluida en los Tipos de Escenarios para la activación del Plan de Contingencia dentro del Plan de Continuidad de Negocio y Recuperación ante Desastre y su Comité respectivo. Si los recursos de Hardware, Software, y/o datos se alteran o se sospecha que han sido alterados, se detendrá el funcionamiento del PSC APACUANA hasta el restablecimiento de un entorno seguro, con la incorporación de nuevos componentes de eficiencia acreditable. De forma paralela se debe realizar una auditoría para identificar la causa de la alteración y asegurar la reproducción de la misma. El PSC APACUANA en el plan de continuidad de negocio y recuperación ante desastres (Revisar el documento STA-DO-007), contempla este escenario considerando esto como una afectación al compromiso parcial o total de la infraestructura de clave pública (ICP). El plan de recuperación ante desastres es revisado periódicamente a medida de los cambios riesgos en el ambiente. En caso de fallas de componentes físicos o sistemas hay un paso a paso, y de verse afectados los certificados emitidos, se notifica el hecho de manera inmediata a los suscriptores de los mismos, debiéndose realizar una nueva emisión.

1.7.3 Procedimiento de actuación ante la vulnerabilidad de la clave privada del PSC APACUANA.

Esta consideración se encuentra incluida en los Tipos de Escenarios para la activación del Plan de Contingencia dentro del Plan de Continuidad de Negocio y Recuperación ante Desastre y su Comité respectivo. En caso que la clave privada del PSC APACUANA, se vea comprometida se activará del Plan de Contingencia de acuerdo al Tipo de Desastres y Tipo de Escenario y quedará sujeto al Comité de Continuidad de Negocio las acciones correctivas a ejecutarse. De forma inmediata se generará el cese del servicio de venta y generación de certificados electrónicos y se procederá a ejecutar los siguientes pasos

1.7.3.1. Declaración del PSC APACUANA del escenario de desastre.

1.7.3.2. Notificación a la SUSCERTE del compromiso de la clave, para la inmediata revocación del certificado del PSC APACUANA.

1.7.3.3. Publicación del evento en la Página Web del PSC APACUANA.

1.7.3.4. Notificación a los suscriptores del PSC APACUANA vía e-mail.

1.7.3.5. Notificar a la compañía aseguradora que mantiene la fianza de operación del PSC APACUANA.

1.7.3.6. Analizar el motivo del compromiso y realizar un informe técnico detallando las razones por las que se vio comprometida la clave privada del PSC APACUANA.

1.7.3.7. Acordar junto con la SUSCERTE las acciones a tomar para la reactivación del servicio de emisión de certificados.

1.7.4 Seguridad de las instalaciones ante un desastre natural o de otro tipo

Esta consideración se encuentra incluida en los Tipos de Escenarios para la activación del Plan de Contingencia detallado de acuerdo al Plan de Continuidad de Negocio y Recuperación ante Desastre y su comité respectivo. En caso de desastre natural o limitación de acceso a las instalaciones del PSC APACUANA por un período superior o igual a veinticuatro (24) horas, se procederá a la activación del plan de recuperación ante desastres.

1.8. Cese de las actividades del PSC APACUANA

En caso del cese de las operaciones del PSC APACUANA, todos los certificados emitidos por el mismo, serán revocados en un lapso de un (01) mes. De igual forma se notificará la decisión del cese de las operaciones y la revocación de los certificados a los signatarios, terceros usuarios, otros Proveedores de Servicios de Certificación y demás usuarios vinculados mediante la publicación de la noticia en el portal “Web” de Apacuana, correos y otros medios de difusión.

Asimismo, la lista de certificados revocados se encontrará disponible en la siguiente dirección electrónica: https://pub.apacuana.com/lcr/.

En caso de cese de actividad comercial de certificación electrónica, el PSC Apacuana tiene contemplado varios supuestos que al ocurrir pueden causar la cesación de operaciones, son los siguientes supuestos:

1. Extinción por vencimiento de acreditación.

2. Extinción por cese de operaciones.
3. 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
4. Extinción derivada de aspectos tecnológicos.

En el caso de ocurrencia de cualquiera de los supuestos antes indicados el PCS Apacuana, estará en la obligación de colocar a disposición de la SUSCERTE el repositorio de todos los archivos y certificados emitidos durante su gestión, incluyendo el estatus de cada uno de ellos. En este sentido, cuando el PSC Apacuana decida cesar en sus actividades, lo notificará a la Superintendencia de Servicios de Certificación Electrónica -SUSCERTE, al menos con treinta (30) días de anticipación a la fecha de cesación.

En el caso de Inhabilitación Técnica, el Proveedor de Servicios de Certificación notificará inmediatamente a la Superintendencia de Servicios de Certificación Electrónica. Entonces, cuando ocurran y se notifique cualesquiera de las causas señaladas, la Superintendencia de Servicios de Certificación Electrónica emitirá un acto por el cual se declare públicamente la cesación de actividades del PSC Apacuana como prestador de ese servicio. Sin embargo, el PSC APACUANA tomará las medidas que fueren necesarias con el objeto de salvaguardar los derechos de los usuarios. En consecuencia, el PSC APACUANA realizará los trámites que considere necesarios para hacer del conocimiento público (a usuarios, a terceros, a SUSCERTE y demás interesados) la cesación de sus actividades, y garantizar la conservación de la información que fuere de interés para sus usuarios y el público en general. En todo caso, el cese de las actividades del PSC APACUANA realizará un proceso de retiro del registro llevado por la SUSCERTE, tal y como lo establece la LSMDFE, en su artículo 37.

XVI. CONTROLES DE SEGURIDAD TÉCNICA

1. Generación e Instalación del par de Claves

El PSC APACUANA, tiene como objetivo mantener controles que aseguren de forma confiable que su par de claves se generan de acuerdo a los estándares

internacionales y a las recomendaciones de SUSCERTE. Los pares de claves (privada y pública) para los componentes internos de la **"ICP"** de APACUANA, específicamente la AC, se generan en módulos de **"Hardware"** criptográficos que cumplen los requisitos establecidos en un perfil de protección de dispositivo seguro de firma electrónica de autoridad, de acuerdo con **"ITSEC"** y **"FIPS"** 140-2. Los sistemas de **"Hardware"** y **"Software"** que se emplean son conformes a las normas CWA 14167-1 y CWA 14167-2. La clave en el HSM es tipeada, considerando que el HSM no cuenta con PED (Pin Entry Device) o con tarjeta CHIP. La clave pública del PSC APACUANA está codificada de acuerdo al estándar RFC 3280, PKCS#1 ó PKC#11. El algoritmo de generación de claves es el **"SHA 512"** con algoritmo de cifrado **"ECDSA".** La verificación de la calidad de la clave privada y pública se realiza de acuerdo con el informe especial del ETSI SR 002 176, que indica la calidad de los algoritmos de firma electrónica. Los algoritmos y parámetros utilizados por el PSC APACUANA para la firma de certificados electrónicos son los siguientes:

- Algoritmo de firma con algoritmo de cifrado ECDSA.
- Algoritmo de firma con la P521**.**
- Funciones criptográficas de resumen **"SHA-512"**

Para la generación del par de claves se consideran los siguientes aspectos:

a) La responsabilidad de la generación de claves del PSC Apacuana es el personal de las áreas involucradas: Dirección de Operaciones (ICP y Certificación electrónica) y la Dirección de Tecnología o Consultoría Jurídica.

b) Los métodos de generación de claves del PSC Apacuana, se efectúan por hardware criptográfico. Es decir, mediante el HSM por appliance.

c) Los métodos de distribución de la clave pública del PSC Apacuana en forma segura, mediante el portal Web de https://pub.apacuana.com/ac-raiz/, el cual se publicarán los certificados públicos, CRL (lista de certificados revocados) y protocolo OCSP (consulta en línea)

d) Las características y tamaño de las claves que se generan por el PSC Apacuana y controles efectuados sobre las mismas: SHA-512 con ECDSA. Tamaño de la clave 521. Los mismos controles del HSM

e) Los propósitos para los cuales pueden ser utilizadas las claves y restricciones para dicha utilización es solo para la generación de certificados

1.1. Generación del par de claves

El PSC APACUANA, realizará la generación de su par de claves (Privada y Pública), mediante un mecanismo criptográfico usando ECDSA con curva P521, la misma será almacenada en un dispositivo criptográfico (HSM) FIPS 140-2 Nivel 3. Este proceso se describe en el capítulo XVI. EL CICLO DE VIDA DE LOS CERTIFICADOS, apartado 1.2. Proceso de generación de solicitud de certificado electrónico.

Para el caso, de la generación del par de claves por parte de los suscriptores, los mismos serán responsables de su emisión, uso y resguardo. En caso de pérdida o extravío de la clave se procederá a la revocación y generación de un nuevo certificado, de acuerdo a lo establecido en el presente documento.

1.2. Entrega de la clave privada al usuario

Tal como se especificó en el punto anterior, el suscriptor es el responsable de generar su par de claves. En tal sentido, el PSC APACUANA, en ningún momento efectúa la entrega de la clave privada a sus suscriptores. Este proceso se describe en el capítulo XVI. EL CICLO DE VIDA DE LOS CERTIFICADOS, apartado 1.2. Proceso de generación de solicitud de certificado electrónico.

1.3. Entrega de la clave pública al emisor del certificado

En este caso, el PSC APACUANA hará la entrega de la clave pública a sus usuarios de acuerdo al tipo de certificado emitido y a lo establecido en las (PC). Tomando en cuenta que una vez firmados los certificados la clave pública siempre se encontrará en los repositorios. Este proceso se describe en el capítulo XVI. EL CICLO DE VIDA DE LOS CERTIFICADOS, apartado 1.2. Proceso de generación de solicitud de certificado electrónico.

1.4. Disponibilidad de las claves públicas del PSC APACUANA para los usuarios

Las claves públicas de los certificados emitidos por el PSC APACUANA, estarán disponibles en los repositorios y en las direcciones electrónicas definidas previamente (https://portal.apacuana.com/ce).

1.5. Tamaño de las claves

El certificado del PSC APACUANA, será generado con una clave ECDSA curva P521. En el caso de los usuarios las mismas serán emitidas de acuerdo al tipo de certificado y a lo establecido en las (PC).

1.6. Parámetros de generación de la clave pública y verificación de la calidad

El parámetro utilizado por el PSC APACUANA, para la generación de claves asimétricas será el ECDSA. La verificación de calidad será efectuada una vez emitido el certificado, a través del PSC APACUANA.

1.7. Generación de claves por hardware y software

El estándar utilizado por el PSC APACUANA para la generación del par de claves y certificados es el X.509 V3, adicionalmente se utiliza un módulo criptográfico (HSM) para su almacenamiento, el cual posee las siguientes especificaciones:

1.7.1. API's PKCS#11 CSP for Microsoft, OpenSSL, Java JCA/JCE CSP, BHAPI, nCore API C or JAVA, CHIL

1.7.2. Algoritmo de Criptografía: Simétricos: DES, triple DES, CAAST, AES-Rijndael, ARC Tour Compatible con RC4.

1.7.3. Asimétrico: RSA, DSA, ECDSA, El Gamal.

1.7.4. Funciones de Hash y HMAS: MD2, MD5, RIPEMD 160, SHA2 (128-256-384-512), SHA3-512ECDSA.

1.7.5. Certificaciones: FIPS 140-2, level 3, FCC, CFRT47, Part 15, Subpart B, Class A, CE: EN55022, Class, A EN55024-1 EN60950.

1.8. Propósito de utilización de la clave privada

La clave privada de los certificados emitidos por el PSC APACUANA, podrán cumplir las funciones de firmar, descifrar, autenticar y no repudio de acuerdo al tipo de certificado y a lo establecido en las (PC).

2. Protección de la clave privada

2.1. Estándares para módulos criptográficos

El estándar empleado para el módulo criptográfico tanto para la generación como cifrado del par de claves será el Fips-140-2 Nivel 3.

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

La clave privada del HSM del PSC APACUANA está protegida mediante controles rigurosos que garantizan la autenticación entre varias partes para su activación. Se implementa un

procedimiento autenticación de multifactor (quórum (M de N), donde múltiples partes autorizadas deben colaborar para completar la validación requerida. Este enfoque asegura que la clave privada solo puede activarse en presencia simultánea de los custodios designados de un total de m partes de la clave, proporcionando así un nivel adicional de seguridad y control sobre el acceso a la misma. En el contexto del sistema utilizado, se emplea una configuración específica de claves en bloques para respaldar esta funcionalidad, asegurando la integridad, disponibilidad y confidencialidad de la clave privada en todas las operaciones pertinentes. En particular, se requieren n = 3 custodios de m = 6 partes de la clave. Se requiere la presencia de los 3 custodios para poder activar el mundo de seguridad del HSM.

a) Los responsables de la generación de claves está constituido por el personal de las áreas involucradas en la Dirección de Operaciones, de acuerdo a las funciones descritas en la Estructura Organizativa.

b) El método de generación de claves, se efectúan por hardware criptográfico, es decir, mediante el HSM por appliance.

c) El método de distribución de la clave pública del Proveedor de Servicios de Certificación en forma segura, se realiza mediante el portal Web de https://pub.apacuana.com/, el cual se publicarán los certificados públicos, CRL (lista de certificados revocados) y protocolo OCSP (consulta en línea).

d) Las características y tamaño de las claves y controles efectuados sobre las mismas son SHA-512 con ECDSA. Tamaño de la clave 4096, con los mismos controles del HSM

e) El propósito para el cual pueden ser utilizadas las claves y restricciones es solo para la generación de certificados.

2.3. Custodia de la clave privada

La clave privada del PSC APACUANA, estará protegida mediante el módulo criptográfico (HSM) anteriormente descrito.

La clave privada del PSC APACUANA se custodia en un dispositivo criptográfico HSM. Para el acceso al repositorio de claves privadas es necesario el uso de controles duales de autenticación a través de procedimientos de claves conjuntas a través de la presencia de los custodios designados, tal como se describe en el apartado 2.2. El esquema de operación del PSC APACUANA y su plataforma tecnológica de certificación se encuentran configurados para que el suscriptor

genere su par de claves (pública y privada). Siempre y en todo caso el compromiso de clave derivará del mismo suscriptor pues el PSC APACUANA no genera el par de claves (pública y privada).

En virtud de lo anterior, si el suscriptor extravía su clave privada, se deberá proceder a la emisión de un nuevo certificado y deberá cumplir el proceso de contratación del PSC APACUANA a tales efectos. La clave pública siempre estará en el repositorio, de conformidad con lo señalado en el presente documento de declaración de prácticas de certificación (DPC).

2.4. Copia de seguridad de la clave privada

Los procedimientos y controles empleados para realizar la copia de seguridad de la clave, son:

1. Se debe autenticar en el HSM mediante clave PED (Pin Entry Device), por los menos 3 custodios.
2. Se resguarda la clave privada de la AC.

2.5. Archivo de la clave privada

La clave privada del PSC APACUANA se encuentra resguardada, de acuerdo a lo establecido en el apartado 1.3 del presente capítulo.

2.6. Inserción de claves privadas en módulos criptográficos

El PSC APACUANA generará la petición de certificados a través del módulo de seguridad HSM y luego que SUSCERTE efectúe la firma de la misma, ésta se instalará y activará en el PSC APACUANA bajo la modalidad de subordinada.

La clave PED (Pin Entry Device) es el único medio para autenticar roles, dominios y la administración del Luna Network HSM 7, autenticado por quórum multifactor.

El quórum multifactor aplicado es M de N, es decir, 3 de 6 según el personal responsable de la custodia o responsables de la clave PED, que se describen a continuación:

1. Director de Operaciones
2. Director de Seguridad de la Información
3. Director de Tecnología

4. Coordinador de Autoridad de Certificación

5. Coordinador de Seguridad de la Información

Es decir, mediante el HSM por appliance. La distribución de la clave pública del Proveedor de Servicios de Certificación en forma segura se realiza mediante el portal Web de https://pub.apacuana.com, en el cual se publicarán los certificados públicos, CRL (lista de certificados revocados) y protocolo OCSP (consulta en línea). Estas claves serán generadas vía el algoritmo SHA-512 con ECDSA, con un tamaño de clave correspondiente a la curva P521. Los controles del HSM para los cuales pueden ser utilizadas las claves y restricciones para dicha utilización es solo para la generación de certificados.

2.7. Método de activación de la clave privada

La clave privada del PSC APACUANA, se activará mediante la aplicación de mecanismos de autenticación multifactor a través del uso de claves PED, aplicando el quórum multifactor 2 de 6, como se describe en el apartado 2.6, del presente documento de DPC.

2.8. Método de desactivación de la clave privada

La clave privada del PSC APACUANA, se desactiva mediante la aplicación de mecanismos de autenticación multifactor a través del uso de claves PED, aplicando el quórum multifactor 2 de 6, como se describe en el apartado 2.6, del presente documento de DPC.

2.9. Método de destrucción de la clave privada

Para realizar la destrucción de la clave privada del PSC APACUANA, se eliminarán todos los respaldos de la misma y se restaurará el equipo HSM a su estado inicial de fábrica, garantizando que está no pueda ser recuperada bajo ningún mecanismo. Toda clave con el HSM es mediante mecanismos de autenticación multifactor a través del uso de claves PED, aplicando el quórum multifactor 2 de 6. Son responsables de la destrucción de la clave privada el Director de Operaciones, el Director de Seguridad de la Información, Director de Tecnología, Coordinador de la Autoridad de Certificación y el Coordinador de Seguridad de la Información. La

generación de claves, se efectúan por hardware criptográfico. Es decir, mediante el HSM por appliance.

La clave privada de origen de la autoridad de certificación (AC) puede ser destruida retornando al HSM a su estado original de fábrica y borrando todos los símbolos de respaldo.

3. **Otros aspectos de la gestión del par de claves**

3.1. Archivo de la clave pública

La clave pública del PSC APACUANA, será almacenada en el Hardware Criptográfico (HSM) destinados para tal fin, bajo estrictos controles de seguridad que garanticen su integridad y disponibilidad por un período de diez (10) años.

3.2. Períodos operativos de los certificados y períodos de uso para el par de claves (privada y pública)

Los períodos operativos, uso de los certificados y par de claves, se regirán de acuerdo a lo siguiente:

- En el caso de la clave pública la misma tendrá una vigencia de diez (10) años.
- En el caso de la clave privada para los certificados de usuario emitidos por el PSC APACUANA tendrá una vigencia de un año para todos los tipos de certificados. La clave privada del PSC APACUANA será de diez (10) años.

4. Datos de activación

4.1. Generación e instalación de datos de activación

La generación y resguardo de las claves privadas de los usuarios será de la exclusiva responsabilidad de los mismos. En caso de que esta, haya sido comprometida el usuario debe notificar inmediatamente al PSC APACUANA para su revocación.

La generación del par de claves (pública y privada) que utiliza la plataforma de certificación de la autoridad de certificación (AC) PSC APACUANA 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:

2.1.8.1.1. La validación de la identidad del individuo se ejecuta por parte de la autoridad de registro (AR) la cual le envía a la autoridad de certificación (AC) la información necesaria para que la creación del usuario dentro del sistema de y de esta forma garantizar la vinculación de identidad de la persona con su clave pública. El usuario final debe ingresar a la página web de APACUANA (https://www.apacuana.com) y presionar click sobre el enlace Certificados Electrónicos, luego pulsar sobre el cuadro que señala el Sistema de Certificación (https://portal.apacuana.com), acceder y registrarse en el sistema de certificación.

2.1.8.1.2. 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.

2.1.8.1.3. 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.

2.1.8.1.4. Al presionar el botón Generar se crean el par de claves (pública y privada), y automáticamente es enviada la petición de certificado a la autoridad de registro para que sea validada presencialmente la identidad del usuario que está realizando la solicitud.

2.1.8.1.5. El procedimiento de generación de par de claves mencionado, garantiza la privacidad de la clave privada del usuario, ya que el usuario es quien la genera,

PSC APACUANA solo garantiza la vinculación del individuo con la clave pública, dicha clave pública está asociada a su vez a la clave privada.

2.1.8.1.1.6. Una vez validada la identidad por la Autoridad de Registro (AR) y generado el certificado por la Autoridad de Certificación (AC), el suscriptor procede a descargar la firma o certificado electrónico en el repositorio de su computadora, aceptando la fuente de emisión del certificado.

2.1.1.1 Protección de datos de activación

La activación del certificado emitido es realizada utilizando el sistema de certificación del PSC APACUANA, limitándose en el equipo o dispositivo donde se hayan generado el par de claves. Por lo tanto, cada usuario es responsable de la protección de la clave privada al momento de su activación, de acuerdo al tipo de certificado y a lo establecido en las (PC).

2.1.2 Controles de seguridad del computador

2.1.2.1 Requisitos técnicos específicos

Los requisitos establecidos por el PSC APACUANA, son los siguientes:

2.1.2.2 Mecanismos de conexión segura hacia la AR y AC.

2.1.2.3 Aplicación del "Hardening" o reforzamiento de la protección correspondiente que garantice la seguridad de los mismos.

2.1.2.4 Segregación de funciones entre los operadores de la AR y AC.

2.1.2.5 Activación de "Log" de auditoría.

2.1.2.6 Implementación de mecanismos de control de acceso por roles y funciones.

2.1.2.7 Calificaciones de seguridad informática

El PSC APACUANA, utiliza productos certificados, al menos, por el Nivel E3 de las normas ITSEC. Asimismo, se tiene certificación de:

a) Control de acceso a los servicios y roles de certificación.
b) Separación de funciones para los roles de certificación.
c) Identificación y autenticación de los roles de certificación.
d) Re-utilización o separación para memoria de acceso aleatorio.

Los equipos destinados para la operación de la AR y AC, estarán sujetos a auditorías internas y externas de manera de garantizar el cumplimiento de los controles establecidos.

2.1.3 Controles de seguridad del ciclo de vida

2.1.3.1 Controles del desarrollo de sistemas

Los desarrollos realizados dentro de APACUANA, se basan en los estándares de calidad y seguridad establecidos, así como a través de la implementación de mecanismos de control de cambios y versiones.
El software AC, usado por la infraestructura de clave pública (ICP) de APACUANA para la emisión de certificado y el manejo del ciclo de vida, ha sido desarrollado de acuerdo con los requerimientos de la Criterios de Evaluación de Seguridad de tecnología de Información (ITSEC por sus siglas en inglés) Nivel E3. El HSM utilizado por la infraestructura de clave pública (ICP) y las Autoridades de Certificación, cumple con los requerimientos FIPS 140-2.

2.1.3.2 Controles de Administración de Seguridad

Todas las actividades realizadas sobre el PSC APACUANA relacionadas con la administración de seguridad, son registradas de acuerdo a lo establecido en las Políticas de Seguridad de la Información de APACUANA.

2.1.10.3. Calificaciones de Seguridad del Ciclo de Vida

El ciclo de vida de los certificados será auditado de forma anual, a través de los auditores externos acreditados por SUSCERTE o cada vez que este así lo requiera. Durante todo el ciclo de vida de las claves se implementan controles de seguridad que permitan instrumentar y

auditar cada fase de los sistemas de la autoridad de certificación (AC) del PSC APACUANA.

2.1.10.4. Controles de seguridad de la red

Los servidores que conforman el PSC APACUANA, se encuentran protegidos tanto de la red externa como interna, según lo especificado en el documento de Plataforma Tecnológica, Ver anexo DAYCOHOST (Apartado "III. Infraestructura Data Center Multisite, Geo-Distribuido (DCI) de Daycohost").

El hardware y software para la infraestructura de clave pública (ICP) de la autoridad de certificación (AC) son mantenidos "off-line" en una instalación de alta seguridad en Daycohost, usando un exhaustivo control de seguridad y rigurosos controles de acceso interno.

Se mantiene sofisticados sistemas de detección contra intrusos para notificar al personal de seguridad sobre cualquier violación a los controles de acceso.

Adicionalmente, la raíz de certificación de la autoridad de certificación (AC) se mantiene fuera de línea y no se alcanza o relaciona con ningún componente externo.

XVII. PERFILES DE CERTIFICADOS (LCR/OCSP)

1. Perfil del certificado

Los certificados AC, LCR y OCSP emitidos por el PSC APACUANA, están alineados a lo establecido en los estándares nacionales e internacionales como el establecido en el estándar ITU X.509 V3 y a la Norma 032 de SUSCERTE.

Los certificados del PSC APACUANA 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.

2. Perfiles de certificados LCR / OCSP

La lista de certificados revocados del PSC APACUANA, son emitidas según lo establecido en el estándar ITU X.509 V3 y a la Norma 032 de SUSCERTE.

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

2.2. Extensiones del certificado: Las extensiones de los certificados del PSC APACUANA permiten codificar información adicional en los certificados. 2.3. Las extensiones estándar X.509 definen los siguientes campos: i) SubjectKeyIdentifier; ii) AuthorityKeyIdentifier; iii) BasicConstraints; iv) Certificate Policies; v) KeyUsage; vi) LCRDistribucionPoint; vii) SubjectAlternativeName; y viii) AuthorityInformationAccess.

2.4. Identificadores de objeto (OID) de los algoritmos: El OID del algoritmo criptográfico utilizado por el PSC APACUANA es: SHA512 with ECDSA Encryption.

2.5. Formatos de nombres: El formato y significado asignado a los nombres en cada uno de las firmas y certificados electrónicos generados por el PSC APACUANA se encuentran detallados en el apartado XIV del presente documento de la declaración de prácticas de certificación (DPC).

2.6. Identificador de objeto (OID) de la PC: PSC APACUANA, utilizará la definición de política de asignación de OID’s según el árbol privado de numeración asignado por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).

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

Dicha lista está firmada electrónicamente por la propia autoridad de certificación (AC) que la emitió.

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

La lista de certificados revocados (LCR) es una lista de firmas y certificados electrónicos, en la cual concretamente, se muestran los números de serie de las firmas o certificados electrónicos revocados por una autoridad de certificación (AC), los números de serie que han sido revocados ya no son válidos, y por ende el usuario no debe confiar en ningún certificado incluido en la LCR del sistema. Una (LCR) es un archivo que contiene:

1. Nombre del emisor de la LCR
2. Números de serie de la firma o certificado
3. Fecha de revocación de las firmas o certificados
4. La fecha efectiva y la fecha de la próxima actualización
5. Motivo de la revocación.

La lista está firmada electrónicamente por la propia autoridad de certificación (AC) que la emitió.

Cuando un usuario desea comprobar la validez de un certificado debe descargar e instalar la LCR actualizada desde los servidores de la misma autoridad de certificación (AC) que emitió la firma o certificado, al realizar esto, las firmas o certificados que se encuentren instalados en el computador en donde se halla instalado la LCR, automáticamente se validan, si los mismos se encuentran revocados, se invalidan; también se puede

comprobar a través del número de serie ubicado en la LCR el status de algún otro certificado. Se comprueba la autenticidad de la lista gracias a la firma electrónica de la autoridad de certificación.

Nombre del campo	Valor
Versión	V2 (Número de versión del certificado).
Algoritmo de Firma:	SHA-512ECDSA (Algoritmo de Firma)
Datos del emisor	
CN	PSC APACUANA
O	Sistema Nacional de Certificación Electrónica
OU	APACUANA
C	VE
E	contacto@apacuana.com
L	Caracas
ST	MIRANDA
Período de validez	
Última Actualización:	Fecha y hora emisión LCR.
Próxima Actualización:	Fecha próxima LCR.
Lista de certificados revocados	
Certificados Revocados	Contiene la lista de certificados revocados (número de serie y fecha de revocación).
Extensiones	

Identificación clave autoridad certificadora	Proporciona un medio para identificar la clave pública que corresponde a la clave privada utilizada para firmar una LCR (ID DE CLAVE)
Nombre alternativo del emisor	
Punto distribución LCR	https://pub.apacuana.com/lcr/
Información del emisor	https://pub.apacuana.com/ocsp
Política de certificados	https://pub.apacuana.com/docs/dpc-pc/

Certificado electrónico para OCSP:

Los Certificados para OCSP se utilizan dentro de la Infraestructura de Clave Pública del PSC APACUANA, a los fines de dar cumplimiento al estándar nacional e internacional y nos permiten validar el estado de los certificados emitidos por el PSC APACUANA. Comprobando que es correcto y que no está revocado, permitiendo una mayor seguridad en las transacciones. El uso asignado al certificado para OCSP es el siguiente:

- Determinar el estado de vigencia de un certificado digital X.509 usando otros medios que no sean el uso de CRL.

- Brindar confianza en el usuario de los certificados emitidos por el PSC APACUANA.

Estructura Certificado de Servidor de OCSP

Nombre del campo	Valor
Versión	**V4** (Número de versión).
Serial number	**(Identificador único menor de 32 caracteres hexadecimales.)**
Algoritmo de Firma	**SHA-512ECDSA** (Algoritmo de Firma)
Algoritmo del hash de Firma	**SHA512**
Datos del emisor	
CN	PSC APACUANA
C	VE
O	Sistema Nacional de Certificación Electrónica
OU	Soluciones Tecnológica APACUANA
S	Distrito Capital
L	Caracas
E	contacto@apacuana.com
Período de validez	
Valid From	Fecha de emisión del Certificado
Valid To	Fecha de vencimiento del certificado
SUJETO	

CN	portal.apacuana.com
O	PSC APACUANA
C	VE
Clave Pública	RSA (1024 Bits) (ID DE CLAVE)
Uso Extendido de la llave	OCSP SIGNING
OCSP non revocation cheking	
Identificados de la llave del sujeto	(Identificador de las subject key en el certificado)
Identificador de la llave de la autoridad	
Key ID	(Identificador de la Clave)
Certificate Iusser	(Datos del emisor)
E	contacto@apacuana.com
OU	Soluciones Tecnológicas Apacuana, S.A.
O	Sistema Nacional de Certificación Electrónica
S	Distrito Capital

L	Caracas
C	VE
CN	PSC APACUANA
~~**Certificate**~~ **Serial number**	- (Número de Serial)
Basic Constraints	
Subject Type	End Entity
Path Length Constraint	None
Certificate Policy	
Policy Identifier	2.16.862.11.2.1
Policy Qualifier Info	
Policy Qualifier ID	CPS
Qualifier	https://pub.apacuana.com/docs/dpc-pc/dpc.pdf
Issuer Alternative Name	
DNS Name	apacuana.com
OID (Asignado por SUSCERTE)	(Código del PSC APACUANA asignado por SUSCERTE)
OID (Asignado por SUSCERTE)	(RIF de APACUANA)
Key Usage	Digital Signature

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

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

3. Auditoría

La auditoría de conformidad del PSC APACUANA, podrá ser efectuada por SUSCERTE en el momento que lo considere necesario y adicionalmente deberá ser efectuada anualmente por un auditor externo acreditado por dicha entidad, previa contratación del mismo.

En las auditorías externas, los aspectos a ser evaluados por los mismos serán aquellos que se encuentren relacionados al funcionamiento y servicio que ofrece el PSC APACUANA, de acuerdo a lo establecido en la Ley de Mensajes de Datos y Firmas Electrónicas y en las Normas 040 y 027 de SUSCERTE, además de otros requisitos que este ente dictamine.

Adicionalmente, el PSC APACUANA deberá ser auditado de forma periódica según el cronograma establecido por la Dirección de Auditoría Interna del PSC APACUANA, con el fin de garantizar el cumplimiento de las políticas y procedimientos establecidos.

Tomando en cuenta que, los auditores internos deben cumplir con los siguientes requisitos:

a) Poseer una adecuada capacitación y experiencia en (ICP), seguridad, procesos de auditorías y tecnologías criptográficas.

b) Poseer Independencia a nivel organizativo de los Operadores del PSC APACUANA.

c) Emitir informe sobre los hallazgos encontrados e informar a los involucrados en el proceso.

En caso, que el auditor interno encuentre alguna deficiencia durante la ejecución de la auditoría, deberá notificar de manera inmediata, al PSC APACUANA a fin de que el mismo, efectúe las medidas correctivas pertinentes para solventarlas en el menor tiempo posible.

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

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

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

3.4. Relación entre el auditor y la autoridad auditada: Entre el PSC APACUANA y el auditor seleccionado, solamente existe una relación comercial que no causa dependencia. El PSC APACUANA contratará la auditoría de seguimiento ordenada por la SUSCERTE y el auditor

prestará el servicio con la obligación de generar un informe de cumplimiento, el cual entregará al PSC APACUANA y a la SUSCERTE, y de mantener en todo momento la confidencialidad de la información a la cual tuvo acceso durante el proceso de auditoría.

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

3.5.1. Seguridad física.

3.5.2. Evaluación de tecnología.

3.5.3. Administración de servicios CA.

3.5.4. Investigación de personal.

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

3.5.6. Contratos.

3.5.7. Protección de datos y consideraciones sobre privacidad.

3.5.8. Planificación de recuperación ante desastres.

3.6. Acciones a tomar como resultado de una deficiencia

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

3.7. Comunicación del resultado: Los resultados de las auditorías se consideran información comercial sensitiva. A menos que esté estipulado en el contrato, serán protegidos como información

confidencial de acuerdo con la sección 4.3 de este documento de la declaración de prácticas de certificación (DPC).

4. Requisitos comerciales y legales

4.1. Aranceles

Los certificados emitidos por el PSC APACUANA, tendrán un costo asociado al tipo de certificado electrónico. Los Certificados Electrónicos (Firmas electrónicas) tienen como clientes objetivo a: Sector bancario nacional, Sector asegurador, Personas jurídicas domiciliadas en el país, Profesionales titulados en el país y Personas naturales. Además, las tarifas para emisión de certificado, renovación, revocación y otros productos o servicios son variables, dependiendo del perfil del suscriptor, sobre lo cual se aplicaría revisión de la cantidad de documentos a firmar anualmente o el modelo en que se valide la cantidad de firmas electrónicas que se utilicen por un suscriptor en el momento que este seleccione el tipo de certificado que va a utilizar.

4.2. Responsabilidad financiera del PSC APACUANA

La responsabilidad financiera del PSC APACUANA, será asumida por la empresa. Los límites de la responsabilidad del PSC APACUANA hacia sus potenciales clientes, está regulada mediante acuerdos contractuales con dichos suscriptores. La responsabilidad del PSC APACUANA para con los suscriptores, partes dependientes y cualquier otra entidad usuaria de firmas o certificados electrónicos generados por el PSC, está limitada contra reclamos de cualquier tipo, incluyendo los contractuales, ilegales, extra contractual y de naturaleza delictiva, en cada certificado en particular sin importar el número de transacciones, firmas electrónicas es o causas de acción que surjan o estén relacionadas con dicho certificado o cualquier servicio prestado con respecto a dicho certificado y en forma acumulativa.

Todos y cada uno de los reclamos que surjan de la infraestructura de clave pública (ICP) con relación a un certificado (sin reparar en la

entidad causante de los daños), estarán sujetos a los límites de responsabilidad aplicables a éstos de acuerdo con este documento de la declaración de prácticas de certificación (DPC) y política de certificados (PC).

Sujeto a las limitaciones anteriores, el límite de responsabilidad agregada de la autoridad de certificación (AC) PSC APACUANA hacia todos los suscriptores, partes dependientes y cualquier otra entidad, ni por todo el período de validez de un certificado emitido por la autoridad de certificación (AC) (a menos que sea revocado o suspendido antes de su expiración), hacia todas las personas con relación a dicho certificado es un valor o cantidad basada en unidades tributarias. En ningún caso la responsabilidad de la autoridad de certificación (AC) excederá el límite antes mencionado.

De igual forma, mediante los contratos con los suscriptores para la emisión de certificados, quedan establecidas todas estas condiciones.

4.3 Políticas de confidencialidad

El PSC APACUANA, se compromete a proteger todos los datos a los que tenga acceso como consecuencia de su actividad. En tal sentido, sólo tendrán acceso a la información confidencial los trabajadores que por el ejercicio de sus funciones así lo requieran de acuerdo a la estructura organizativa del PSC Apacuana

Toda la recopilación y uso de la información compilada por la autoridad de certificación (AC) del PSC APACUANA es realizada cumpliendo con la legislación de la venezolana y basándose en las distinciones suministradas en este documento de la política de certificación y declaración de prácticas de certificación (DPC). El PSC Apacuana cumple con el estándar mínimo contemplado en este documento de la declaración de prácticas de certificación (DPC) y política de certificados (PC). 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.

En todo caso, el PSC Apacuana busca el almacenamiento y disponibilidad de los datos a los fines de mantener la condición de servicios de certificación a los suscriptores correspondientes. Los detalles sobre cómo PSC APACUANA recopila, procesa y almacena datos personales se encuentran en la política de modelo de operación de la autoridad de registro (AR) de la autoridad de certificación (AC) del PSC APACUANA.

4.3.1. Información confidencial

En adición a lo antes expuesto, se señala que la información de identificación es la información obtenida para identificar positivamente una entidad y suministrar los servicios de certificación que ésta solicita. La información de identificación será tratada como información confidencial a menos que la entidad a la cual se refiere la información dé su consentimiento de manera explícita. Se considera información confidencial, aquella que cumpla con las siguientes características:

4.3.1.1. Información de registros y todos los datos relativos al certificado.

4.3.1.2. La información suministrada por sus proveedores y otras personas con la que el PSC APACUANA, tiene el deber de guardar la confidencialidad establecida legal o convencionalmente.

4.3.1.3. Proceso de ejecución del certificado.

4.3.1.4. Mecanismos de gestión e interconexión del PSC APACUANA.

4.3.1.5. Otras características del proceso que establezca el PSC APACUANA.

4.3.2. Información Pública – o Información no confidencial

Tipos de información no considerados confidenciales.

4.3.2.1. Resumen de información.

4.3.2.2. Contenido de los certificados solicitados.

4.3.2.3. Lista de certificados revocados (LCR).

4.3.2.4. Clave pública del PSC APACUANA.

4.3.2.5. Las versiones de la DPC y PC.

4.3.2.6. Reglamentos y políticas de funcionamiento.

4.3.2.7. Otras características del proceso que establezca el PSC APACUANA.

4.3.3. Publicación de información sobre la revocación de un certificado

La información sobre la revocación de los certificados emitidos por el PSC APACUANA, LCR (List of Certificates Revocation), a sus usuarios estará disponible en la siguiente dirección electrónica, las veinticuatro (24) horas del día y trescientos sesenta y cinco 365 días del año. https://pub.apacuana.com/lcr/.

4.3.4. Divulgación de Información a Autoridades Judiciales

Cada una de las Partes conviene en notificar a la otra tan pronto reciba cualquier solicitud de divulgación de la Información Confidencial como consecuencia de una medida dictada por organismos judiciales, administrativos o gubernamentales, de manera tal que la Parte cuya información ha sido requerida, pueda ejercer algún método de protección de dicha información previo a su entrega de acuerdo a lo permitido por la ley.

Costos: Cada una de las Partes deberá enfrentar a su propio costo todos los esfuerzos para prevenir la divulgación hacia terceros de la Información Confidencial confiada a ella por la otra parte.

La razón o razones para la suspensión o revocación de un certificado pueden hacerse públicas de acuerdo con la ley aplicable o bajo la responsabilidad única y absoluta del PSC APACUANA. La información sobre suspensión de certificados será revelada sólo al suscriptor propietario del certificado o a la SUSCERTE bajo requerimiento derivado de proceso judicial y bajo mandato de cumplimiento. Ningún documento o registro en poder de la autoridad de certificación (AC) o la autoridad de registro (AR) del PSC APACUANA 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 autoridad de certificación (AC) y autoridad de registro (AR) del PSC APACUANA es entregado a ninguna persona excepto donde: i) Se produzca una solicitud de información debidamente documentada (Ej. que haya cumplido con todos los procedimientos legales); y ii) La persona que requiere la información es una persona autorizada para hacerlo y está debidamente identificada. Los servicios de certificación prestados bajo la autoridad de terceros pueden ser objeto de este tipo de solicitudes de información, como evidencia civil o para propósitos de descubrimiento, relacionados con la autoridad de certificación (AC) del PSC APACUANA en cualquier jurisdicción donde los procedimientos legales apropiados se hayan cumplido.

4.3.5. Protección de la información Interna

4.3.5.1. Información considerada privada

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

32.10.2. Información considerada no privada: Tipos de información no considerados confidenciales: i) resumen de información; ii) todos los certificados emitidos por la infraestructura de clave pública (ICP) para uso público pueden ser divulgados públicamente; y iii) todos los certificados emitidos por la autoridad de certificación (AC) en su condición servicios de certificación a terceros también pueden ser divulgados públicamente.

4.3.6. Responsabilidad de proteger la información confidencial

El PSC APACUANA tiene la obligación de mantener a resguardo la información suministrada por los suscriptores contratantes de firmas o certificados electrónicos generados por el PSC APACUANA. 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 suscriptores estará limitado al representante de la autoridad de registro (AR) y al Director Ejecutivo del PSC APACUANA.

4.3.7. Consentimiento previo para el uso de información privada/secreta

La información dispuesta en archivos por el PSC APACUANA será manejada como información confidencial y la misma no será suministrada a terceros distintos al suscriptor propietario de la firma o certificado electrónico, salvo que medie aprobación expresa y autenticada en notaría pública por parte del suscriptor cuya información se trate, autorización realizada por escrito vía correo electrónico firmado o certificado por el suscriptor propietario de la firma o certificado electrónico o derivado de mandato judicial impuesto por Tribunal y derivado de causa en proceso.

4.3.8. 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 de la Declaración de Prácticas de Certificación (DPC).

4.3.9. Derecho de propiedad intelectual

Todo lo establecido en el presente documento, en las PC, documentación técnica, operativa y de seguridad de la información, de aplicaciones y sistemas, arquitecturas y diseños de operaciones, modelos y manuales asociados a la PKI, publicaciones realizadas en las páginas web www.apacuana.com, así como los componentes de la PKI y sus especificaciones detalladas en diferentes documentos, que conforman la infraestructura de claves públicas del PSC APACUANA, son de propiedad exclusiva de APACUANA, bajo ningún concepto puede copiarse ni

reproducirse Todos los documentos marcados y versionados se mantienen bajo exclusiva propiedad intelectual y de marca de Apacuana.

4.3.9.1. 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, listas de certificados revocados (LCR) y certificados; a menos que explícitamente se indique lo contrario, todas las prácticas, política, los documentos operacionales y de seguridad referentes a la infraestructura de clave pública (ICP) del PSC APACUANA (electrónicos o no) así como los contratos, le pertenecen y seguirán siendo propiedad de PSC APACUANA. Mediante los contratos correspondientes para la prestación de servicios de certificación, PSC APACUANA podrá otorgar una licencia a terceros para el uso de certificados, listas de certificados revocados (LCR) y otras prácticas autorizadas y documentos de política en la medida que lo requieran para la prestación de servicios de certificación de acuerdo con el presente documento de la declaración de prácticas de certificación (DPC).

4.3.9.2. Claves pública y privada: Todos los derechos de propiedad intelectual de las claves pública y privada generadas estarán amparados por la entidad por la cual dichas claves fueron generadas o por la entidad designada por esta. Los servicios de certificación operados bajo la autoridad de suscriptores finales no obtendrán ningún derecho en lo absoluto en relación con los certificados, su contenido, formato o estructura.

4.3.9.3. Certificado: En todo momento PSC APACUANA se reserva el derecho de suspender o revocar cualquier certificado de acuerdo con los procedimientos y las políticas establecidas en el presente documento de la declaración de prácticas de certificación (DPC) y política de certificados (PC).

4.3.9.4. Nombres distinguidos: Los derechos de propiedad intelectual en nombres distinguidos y números de identificación de suscriptores

no son responsabilidad del PSC APACUANA a menos que se especifique lo contrario en un contrato o acuerdo.

4.3.9.5. Propiedad intelectual: La propiedad intelectual del presente documento de la declaración de prácticas de certificación (DPC) y política de certificados (PC), así como de toda la información, publicaciones y documentos generados por el PSC APACUANA y contenidos o no dentro de su página web (www.apacuana.com), son propiedad exclusiva del PSC APACUANA.

4.3.10 Responsabilidad del PSC APACUANA

El PSC APACUANA, es responsable por los daños que se pudieran ocasionar en el desarrollo de sus operaciones, excluyendo las mencionadas en el siguiente punto:

Excepciones de responsabilidad

El PSC APACUANA, no asumirá ninguna responsabilidad en los siguientes casos:

- Uso indebido o fraudulento de los certificados.
- Cuando el usuario o tercero de buena fe no compruebe la veracidad de los documentos con firma electrónica, no tenga en cuenta las restricciones que figuren en el certificado en cuanto a sus posibles usos, cuando no tenga en cuenta la pérdida de vigencia del certificado publicado en la (LCR) o cuando no verifique la firma electrónica.
- Causas de fuerza mayor.

4.3.10.1. Plazo y finalización

El presente documento y las Políticas de Certificación emitidas por el PSC APACUANA, estarán vigentes a partir de la acreditación según Gaceta Oficial por parte de SUSCERTE.

Asimismo, el PSC APACUANA, deberá publicar todas las versiones de las (PC) y DPC e identificar la última versión con la palabra “Vigente”.

4.3.10.2. Terminación

El presente documento y las (PC), emitidas por el PSC APACUANA dejarán de tener validez, en caso del cese de las funciones como Proveedor de Servicios de Certificación (PSC APACUANA).

4.3.10.3. Modificaciones

Cambio de especificaciones

El PSC APACUANA, estará en la plena capacidad de efectuar modificaciones a los documentos definidos, en caso de existir algún cambio que requiera la modificación de estos de cualquier tipo.

Asimismo, estos cambios no estarán vigentes hasta tanto SUSCERTE no haya aprobado los cambios para su posterior publicación.

4.3.10.4. Publicación y notificación

Una vez aprobados los cambios por SUSCERTE, el PSC APACUANA publicará la noticia a través de su portal web, de manera que los usuarios de certificados electrónicos emitidos por el PSC APACUANA, estén al tanto de los cambios efectuados.

4.3.10.5. Aprobación

La aprobación estará bajo la responsabilidad de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).

4.3.10.6. Legislación aplicable

La DPC y PC del PSC APACUANA, se encuentran enmarcadas en lo establecido en la LSMDFE y otras normas complementarias dictadas por SUSCERTE.

XVIII. OBLIGACIONES Y RESPONSABILIDAD CIVIL

3.1. Obligaciones del PSC APACUANA

Las obligaciones del PSC Apacuana, son las establecidas en el Art.35 de la LSMDFE, que especifica:

a. Recibir solicitudes de emisión y revocación de certificados.
b. Confirmar la identidad del signatario y la validez de la solicitud de acuerdo con los requisitos establecidos en el presente documento y en las (PC).

c. Adoptar las medidas necesarias para determinar la exactitud de los Certificados Electrónicos que proporcionen y la identidad del Signatario.
d. Informar antes de la emisión de un certificado al suscriptor de las obligaciones que asume, la forma que debe custodiar los datos de creación de firma, el procedimiento que debe seguir para comunicar la pérdida o utilización indebida de los datos o dispositivos de creación y de verificación de firma, de las condiciones precisas para la utilización del certificado, de sus limitaciones de uso, de la forma en que garantizan su posible responsabilidad patrimonial y de los datos de la página Web donde pueden consultar cualquier información.
e. Realizar todos los mecanismos para aprobar las solicitudes de las emisiones y revocaciones de certificado en correspondencia con el intercambio de datos entre nodos.
f. Utilizar VPN o SSL o cualquier otro protocolo tecnológico que brinde igual o mayor nivel de seguridad y privacidad, al momento de tener disponible los servicios del PSC Apacuana a los signatarios de los certificados electrónicos en la web.
g. Informar a las organizaciones titulares de certificados la emisión o revocación de sus certificados electrónicos.
h. Garantizar la disponibilidad de los certificados emitidos por el PSC APACUANA.
i. Solicitar la revocación de un certificado cuando tenga conocimiento o sospecha del compromiso de una clave privada.
j. Mantener bajo estricto control las herramientas de tramitación de certificados electrónicos y notificar a SUSCERTE, cualquier falla en el funcionamiento u otra eventualidad que pudiera salirse del comportamiento normal esperado.
k. Cumplir con la obligación de confidencialidad, durante la ejecución de sus funciones.
l. Garantizar la validez, vigencia y legalidad del Certificado Electrónico que proporcione.

m. Mantener en medios electrónicos o magnéticos, para su consulta, por diez (10) años siguientes al vencimiento de los Certificados Electrónicos que proporcionen, un archivo cronológico con la información relacionada con los referidos Certificados Electrónicos.

n. Garantizar a los Signatarios un medio para notificar el uso indebido de sus Firmas Electrónicas.

o. Informar a los interesados en sus servicios de certificación, utilizando un lenguaje comprensible en su página en la Internet o en cualquier otra red mundial de acceso público, los términos precisos y condiciones para el uso del Certificado Electrónico y, en particular, de cualquier limitación sobre su responsabilidad, así como de los procedimientos especiales existentes para resolver cualquier controversia.

p. Garantizar la integridad, disponibilidad y accesibilidad de la información y documentos relacionados con los servicios que proporcione. A tales efectos, deberán mantener un respaldo confiable y seguro de dicha información.

q. Garantizar la adopción de las medidas necesarias para evitar la falsificación de Certificados Electrónicos y de las Firmas Electrónicas que proporcionen.

r. Efectuar las notificaciones y publicaciones necesarias para informar a los signatarios y personas interesadas acerca del vencimiento, revocación, suspensión o cancelación de los Certificados Electrónicos que proporcione, así como de cualquier otro aspecto de relevancia para el público en general, en relación con dichos Certificados Electrónicos.

2. Notificar a la Superintendencia de Servicios de Certificación Electrónica cuando tenga conocimiento de cualquier hecho que pueda conllevar a su Inhabilitación Técnica.

3. Otras inherentes al funcionamiento del PSC APACUANA.

3.2. Obligaciones del usuario

Todos los signatarios del PSC APACUANA, están en la obligación de cumplir con las políticas establecidas para el uso de los certificados. En tal sentido, los mismos se limitarán a efectuar operaciones con APACUANA y deberán establecer mecanismos de seguridad para el resguardo de los certificados emitidos por el PSC APACUANA, así como garantizar la seguridad de la clave privada de sus certificados electrónicos.

3.3. Obligaciones de terceros de buena fe

Es responsabilidad de un tercero de buena fe, verificar la validez y vigencia del certificado, mediante la comprobación de los siguientes datos:

- Aceptación de los términos y condiciones de la emisión, revocación y renovación especificados esta DPC y las PC los certificados emitidos por el PSC Apacuana.
- Verificar que el certificado no se encuentra en la lista de revocación del PSC APACUANA.
- Verificar que el certificado electrónico no haya sido suspendido o expirado.
- Verificar la validez de un certificado emitido por un PSC APACUANA.
- Velar por el cumplimiento del uso correcto del certificado electrónico emitido por el PSC Apacuana.
- El incumplimiento de esta comprobación, no acarrea responsabilidad alguna sobre el certificado emitido por el PSC APACUANA.

Adicionalmente, los terceros de buena fe deberán acatar las normas y políticas establecidas en el presente documento respecto al uso, validación y otros términos de su interés.

3.4. Responsabilidad del proveedor de servicios de certificación

Es responsabilidad del PSC APACUANA garantizar la continuidad de las operaciones a sus usuarios mediante el uso de sus certificados, siempre y cuando el uso de estos se efectúe de acuerdo a las políticas y normas establecidas en el presente documento y en las PC, considerando el apartado 4.3.6. Responsabilidad de proteger la información confidencial, así como lo

indicado 4.3.10 Responsabilidad del PSC APACUANA y en el Reglamento Parcial de la LSMDFE señala en su Artículo 11 la responsabilidad del PSC por los perjuicios causados por la revocación.

3.5. Responsabilidad del usuario

Es responsabilidad del usuario, garantizar el resguardo de su certificado y de su par de claves, mediante la implementación de mecanismos establecidos en las (PC), los cuales pueden ser objeto de revisión en el momento que el PSC APACUANA, lo considere necesario o sospeche del mal uso de los certificados otorgados. Debe garantizar los usos permitidos de acuerdo al apartado XIX. USO DE LOS CERTIFICADOS, 3. Usos permitidos. y 9.15 Requisitos Específicos para Casos de Compromiso de Claves.

3.6. Responsabilidad de terceros de buena fe

Los terceros de buena fe son responsables de cumplir con las obligaciones descritas en el punto N.º 3 del presente apartado. En tal sentido, el PSC APACUANA, no se responsabiliza si el tercero de buena fe no cumple con los requisitos de validación de los certificados de seguridad emitidos, según lo establecido en el presente documento y en las políticas de certificación.