AUTHENTICSING C.A.

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

2025

Resumen de Información.

Empresa	**AUTHENTICSING C.A.**		
Documento	Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC).		
Tipo de Documento	Documentación sobre la Infraestructura de Clave Pública		
ID	DIF-002		
Autor	Ing. Carlos García.		
Colaboradores			
Revisado por	Abog. Samuel Gómez.	**Fecha de creación**	2024 enero
Aprobado por	Abog. Zolangel González.	**Fecha aprobación**	29/02/2024
Versión/Edición	3.0v	**Nº Total de Páginas**	**- 147 -**
Tipo de Uso	**Uso Interno** ☐ **Uso Público** ☒		

CONTROL DE DISTRIBUCIÓN

Nombre y Apellidos
Ing. Farewell Beatriz Hernández González – Cargo. Auditor Teléfono 0412-7214122 Email fhernandez@authenology.com.ve
Ing. Carlos Vicente García Gómez – Cargo. Coordinador de la Infraestructura de la Clave Pública Teléfono 0412-6049988 Email cvgcvg@gmail.com
Lic. Detriana Barrios A. – Cargo. Coordinador de Seguridad de la Información y Plataforma Teléfono 0424-218-31-97 Email detrianab@gmail.com
M.Sc. Elvis R, Chourio M. - Cargo Coordinador de Plataforma y Soporte a Usuarios Teléfono 04146017005 Email Echurio@gmail.com

ÍNDICE

1. CONTROL DE VERSIONES.

Control de Cambio			
Versión	**Revisión**	**Fecha**	**Observaciones**
1	1	Enero de 2024	Versión inicial
2	2	Agosto de 2024	Segunda edición, con actualizaciones
3	3	Septiembre de 2025	Tercera edición, con actualizaciones

2. TÍTULO.

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

3. CÓDIGO DEL DOCUMENTO.

DIF-002

4. INTRODUCCIÓN.

AUTHENTICSING C.A., bajo su marca comercial Authenology, es un Proveedor de Servicios de Certificación (PSC) debidamente registrado, acreditado y autorizado por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).”

Como parte de sus procesos y funciones, AUTHENTICSING presenta el documento **“Declaración de Prácticas de Certificación (DPC) y Política de Certificados” (DIF-002).** Este documento tiene como objetivo definir y documentar los requisitos y procedimientos para la generación, publicación y administración de los certificados electrónicos emitidos por AUTHENTICSING. Su propósito es garantizar la transparencia y facilitar la comprensión de estos procesos por parte de la Junta Directiva, clientes, proveedores, personal y demás partes interesadas.

Para cumplir con los estándares nacionales, este documento adopta la estructura recomendada por el Gobierno de Venezuela para documentos relacionados con la seguridad de la información, tal como se establece en la guía de la AC Raíz de Venezuela (SUSCERTE). Esta estructura, que diferencia de la RFC 3647, incluye

cuerpo, encabezado y apéndice.

5. OBJETIVO.

La presente documentación establece el marco normativo para la gestión integral de certificados electrónicos, abarcando desde su generación hasta su revocación, conforme a las prácticas establecidas por PSC AUTHENTICSING C.A.

6. ALCANCE.

Dirigida a autoridades y clientes, esta DPC y PC proporciona una descripción detallada de los procesos técnicos involucrados en la emisión de certificados digitales por parte de AUTHENTICSING C.A. Se definen los roles de la AC y AR, el modelo de confianza empleado y se categorizan los distintos tipos de certificados que serán emitidos.

7. TÉRMINOS Y DEFINICIONES.

Con el propósito de garantizar la claridad y precisión en la interpretación de este documento, se incluyen las siguientes definiciones de términos clave:

- **Authenology:** Representa la identidad corporativa de AUTHENTICSING C.A., sirviendo como un distintivo o marca que individualiza nuestros productos y servicios en el mercado, asociándolos con calidad y confianza.
- **Activos de Información:** Son bienes relacionados a un sistema de información en cualquiera de sus etapas. Ejemplos de activos son:
  - Información: Bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, resultados de proyectos de investigación, entre otros.
  - Software: Software de aplicaciones, software de sistemas, herramientas de desarrollo, entre otros.
  - Activos físicos: Computadoras, equipamiento de redes y comunicaciones, medios de almacenamiento, mobiliario, lugares de emplazamiento.
- **Administración de Riesgos:** Administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.
- **Aplicación:** Sistema informático, tanto desarrollado por AUTHENTICSING C.A como por terceros, o al sistema operativo o software de base, que integren los sistemas de información o donde estos estén alojados.
- **Autoridad de Certificación (AC):** Autoridad en la cual confían los clientes para crear, emitir y manejar el ciclo de vida de los certificados, la cual a los efectos del

decreto ley de mensajes de datos y firmas electrónicas debe contar con la acreditación otorgada por SUSCERTE.

- **Autoridad de Registro (AR):** Entidad cuyo propósito es suministrar apoyo local a la infraestructura de clave pública (ICP) de una Autoridad de Certificación (AC). La Autoridad de Registro desempeña un conjunto de funciones orientadas a la validación, comprobación y conformación de la documentación suministrada, así como la identidad física de un cliente que opte a la compra de una firma electrónica o certificado electrónico generado por el PSC AUTHENTICSING.
- **Certificado:** Estructura de datos que utiliza el estándar CCITT ITU X.509, que contiene la clave pública de una entidad junto a información asociada y presentada como "un-forgettable" (inolvidable), mediante una firma electrónica de la autoridad de certificación que la generó.
- **Cifrado:** Es el proceso mediante el cual los datos simples de un texto son transformados para ocultar su significado.
- **Clave Asimétrico:** Es el par de claves relacionadas, en el cual la clave privada define la modificación privada y la clave pública define la transformación pública.
- **Cliente:** Es la entidad que ha solicitado la emisión de un certificado dentro de la Infraestructura de Clave Pública (ICP) del PSC AUTHENTICSING C.A. A los fines del Decreto Ley de Mensajes de Datos y Firmas Electrónicas y su Reglamento el Cliente será entendido como el Signatario y viceversa.
- **Comité de Seguridad de la Información:** Es un cuerpo destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad. En AUTHENTICSING C.A esta función es cumplida por la Comisión de Seguridad de la Información. Dentro de esta Política los términos Comité de Seguridad de la Información y Comisión de Seguridad de la Información son considerados equivalentes.
- **Evaluación de Riesgos:** Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria de AUTHENTICSING C.A.
- **Firma Electrónica:** Es el dato añadido o una transformación criptográfica de una unidad de dato que permite al receptor de la unidad de dato probar la fuente y la integridad del dato y protegerse contra falsificaciones, por ejemplo, del destinatario.
- **Generación de Certificado:** Proceso de crear un certificado a partir de datos de entrada que son específicos a la aplicación y al cliente.
- **Incidente de Seguridad:** Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.
- **Información de Identificación:** Cuando se **verifica** la identidad de una entidad, se

procede a **otorgar** los servicios de certificación solicitados.

- **Infraestructura de clave pública (ICP):** Es la infraestructura necesaria que genera, distribuye, maneja y archiva claves, certificados y listas de revocación de certificado de protocolo para la condición del certificado en-línea (PECL).
- **Infraestructura Operacional:** Es la Infraestructura tecnológica mediante la cual se suministran los servicios de certificación.
- **Integridad de Datos:** Es la condición de ser preciso, completo y válido de no ser alterado o destruido de manera no autorizada.
- **Lista de Certificados Revocados (LCR):** Es la lista de certificados que han sido revocados o suspendidos por el PSC AUTHENTICSING C.A.
- **Manejo de Clave:** Es la administración y el uso de la generación, inscripción, certificación, la desincorporación, distribución, instalación, almacenamiento, archivo, revocación, derivación y destrucción del material de clave de acuerdo con la política de seguridad.
- **Norma:** Regla de comportamiento dictada por una autoridad competente que se debe seguir o a la que se deben ajustar las conductas, tareas, actividades, etc.
- **Par Clave:** Son las claves de un sistema criptográfico asimétrico, y que tienen como función que uno de los pares de claves descifrará lo que el otro par de clave cifra.
- **Par de claves asimétrico:** Es el par de claves relacionadas donde la clave privada define la transformación privada y la clave pública define la transformación pública.
- **Parte interesada:** Es la organización o persona que tiene interés en el desempeño o éxito del PSC AUTHENTICSING C.A.
- **Procedimiento:** Acciones que se realizan, con una serie común de pasos claramente definidos, que permiten realizar correctamente una tarea o alcanzar un objetivo. Se distinguen dos clases de procedimientos: obligatorios y recomendados. Estos últimos representan “buenas prácticas”, que son aconsejables, pero no requeridas. Si en un procedimiento no se utiliza la palabra “recomendado” se asume que es obligatorio.
- **Proceso de Información:** Conjunto de tareas relacionadas lógicamente que se realizan para lograr un resultado determinado en un Sistema de Información.
- **Proceso de Verificación:** Es todo proceso que toma como entrada de datos un mensaje firmado, la clave de verificación y los parámetros de dominio que arroja como salida el resultado de verificación de la firma, si es válida o inválida.
- **Propietario de un Activo Físico:** Es el responsable patrimonial del bien.
- **Propietario de un Proceso de Información:** Es el responsable por la creación, puesta en funcionamiento y mantenimiento de un proceso de Información.
- **Propietarios de la Información:** Son los funcionarios, unidades académicas o dependencias responsables de la generación o recopilación de la información, con competencia jurídica para administrar y disponer de su contenido.
- **Protocolo de Estatus de Certificado En-línea (Online Certificate Status**

Protocol): Es un protocolo utilizado para validar el estado de un certificado en tiempo real. La respuesta de las solicitudes incluye tres estados: valido, revocado o desconocido. Su definición en Idioma Inglés es OCSP (Online Certificate Status Protocol).

- **Proveedor:** Es una organización o persona que suministra un producto o servicio para los PSC (Proveedor de Servicios de certificación)
- **PSC:** Proveedor de Servicios de Certificación
- **Registro:** Conjunto de datos relacionados entre sí, que constituyen una unidad de información en una base de datos, informatizada o no. A los efectos de esta Política se clasifican en:
    - Registros de Funcionamiento: Son los asociados con las actividades de soporte a las actividades principales (directores, gerentes y personal técnico) del PSC AUTHENTICSING.
    - Registros Personales: Son los relacionados con las personas físicas o jurídicas.
    - Registros de Producción: Son los asociados a las actividades de Authenticsing o de alguno de sus miembros.
- **Registro de Auditoría:** Es la unidad de dato discreta para el rastro de auditoría cuando ocurre un evento que es examinado y registrado.
- Responsable de la Unidad de Auditoría Interna: Auditor Interno Titular.
- **Responsable de la Unidad Organizativa:** Director o Gerente General, secretario, Gerente de unidad o director responsable del funcionamiento de la Unidad Organizativa.
- **Responsable del Área Informática:** director del departamento de Informática.
- **Responsable de una Aplicación:** Encargado de la instalación y mantenimiento de la aplicación.
- **Responsable del Área Legal:** Director de Asuntos Jurídicos.
- **Responsable del Área de Recursos Humanos:** Director General de Personal dependiente del departamento de RRHH.
- **Responsable de Seguridad Informática:** Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes de Authenticsing que así lo requieran.
- **Responsable de un Sistema de Información:** Encargado de velar por la puesta en marcha y el correcto funcionamiento del Sistema de Información o en su defecto el responsable de la Unidad Organizativa.
- **Revocación:** Es el cambio de estatus de un certificado válido o suspendido a “revocado” a partir de una fecha específica en adelante.
- **Revocación de Certificado:** Son los procesos que consisten en cambiar el estatus de un certificado válido o suspendido o revocado. Cuando un certificado tiene un estado revocado, esto significa que una entidad ya no es confiable para ningún

objetivo.

- **Seguridad de la Información:** La seguridad de la información se entiende como la preservación de las siguientes características:
  - Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
  - Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
  - Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
  - Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
  - Auditabilidad: Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
  - Protección a la duplicación: Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
  - No repudio: Garantiza que una entidad no pueda negar haber enviado o recibido información, protegiendo así la integridad de las comunicaciones
  - Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta al PSC AUTHENTICSING C.A.
  - Confiabilidad de la Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
  - Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
  - Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
  - Tecnología de la Información: Se refiere al hardware y software operados por la PSC AUTHENTICSING o por un tercero que procese información en su nombre, para llevar a cabo una función propia del PSC AUTHENTICSING, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo

- **Seguridad Física:** Es la medida utilizada para proveer protección física a los recursos contra amenazas intencionales y accidentales.
- **Servicios de Certificación:** Son los servicios que pueden proporcionar con respecto al manejo del ciclo de vida de un certificado para cualquier tipo de nivel de jerarquía de la ICP, esto incluye servicios auxiliares, tales como; servicios OCPS, servicios de tiempo compartido, servicios de verificación de identidad, hospedaje de lista de certificados revocados (LCR), etc.
- **Sociedad Mercantil o Sociedad de Capital:** Persona jurídica que se crea para iniciar una actividad comercial con fines de lucro. En este sentido, se agrupan una o más personas físicas o morales, según la legislación mercantil, convirtiéndose ahora en socios para desempeñar una actividad económica.
- **Solicitante:** La persona física o jurídica que solicita (o pretende renovar) un Certificado. Una vez que se emite el Certificado, el Solicitante se denomina Suscriptor. Para los Certificados emitidos a dispositivos, el Solicitante es la entidad que controla u opera el dispositivo mencionado en el Certificado, incluso si el dispositivo envía la solicitud de certificado real.
- **Solicitud de Certificado:** Es la solicitud autenticada de una entidad por su autoridad matriz para emitir un certificado que une la identidad de esa entidad a una clave pública.
- **Unidades Organizativas:** Las Unidades Organizativas del PSC AUTHENTICSING son las unidades y las áreas de la administración central que dependen directamente del Director o Gerente General. Las Unidades Organizativas se detallarán en la estructura organizativa de la empresa.
- **Uso del Certificado:** Conjunto de reglas que indican la aplicabilidad del certificado de una comunidad en particular y/o la clase de aplicación con requerimientos de seguridad comunes.
- **Validación:** Es un proceso que lleva a cabo la verificación de validez de un Certificado en términos de su estatus o condición (Ej. si es suspendido o revocado).

8. SÍMBOLOS Y ABREVIATURAS

9. COMUNIDAD DE USUARIOS Y APLICABILIDAD.

Está incluye las distintas entidades que cumplen roles con relación al certificado y cuya integración se encuentre prevista para el cumplimiento de la actividad de certificación.

PC	Política de Certificados.
PSC	Proveedor de Servicios de Certificación.
SUSCERTE	Superintendencia de Servicios de Certificación Electrónica.
OCSP	Protocolo de estado de certificados en línea.
OID	Identificador de Objeto.
LSMDFE	Ley Sobre Mensajes de Datos y Firmas Electrónicas.
LCR	Lista de Certificados Revocados.
ICP/PKI	Infraestructura de clave pública
DPC/CPS	Declaración de Prácticas de Certificación.

9.1 Autoridad de certificación (AC)

El PSC AUTHENTICSING C.A. es una Autoridad de Certificación (AC) constituida bajo las leyes venezolanas para emitir y gestionar certificados digitales. En cumplimiento con el Decreto Ley de Mensaje de Datos y Firmas Electrónicas (LMDFE) y normativa vigente, su reglamentación o los cuerpos normativos que sustituyan a estos. Las principales funciones como AC son:

- Ofrecer certificados electrónicos y firmas electrónicas a personas naturales y jurídicas, tanto del sector público como privado,
- Prestar el servicio técnico y de soporte a las aplicaciones para firmas y certificados electrónicos

Realizar acciones de adiestramiento en materia de firmas y certificados electrónicos, comercio electrónico y demás aplicaciones. Esto incluye los usos de; desarrollo, mantenimiento, y ofrecer aplicaciones para tramites en línea con entes de la administración pública, gobernaciones y municipios de la República

Bolivariana de Venezuela.

9.1.1 Modelo de operación del PSC AUTHENTICSING.

9.1.1.1 Sede Administrativa.

La sede administrativa de Authenticsing centralizará las operaciones de la compañía, incluyendo los procesos financieros, administrativos, fiscales, de recursos humanos y operativos. Desde esta sede, se gestionará tanto la **Autoridad de Registro (AR)** como la **Autoridad de Certificación (AC)**. La AR será responsable de validar la documentación e identidad de los clientes y usuarios, emitiendo una afirmación pública sobre la veracidad de los datos proporcionados. La AC, por su parte, se encargará de emitir, gestionar y revocar los certificados digitales.

La dirección física de la sede administrativa es la siguiente:

DATOS DE LA EMPRESA/DIRECCIÓN FÍSICA.	
Nombre	**Proveedor de Certificados AUTHENTICSING**
Dirección	Calle Bolívar, Edificio Don David, PB – Ofic. 001, Municipio Chacao del estado Miranda de la República Bolivariana de Venezuela
Código Postal	1060
Correo electrónico	contacto@authenology.com.ve
Número de teléfono	+58 – 0212 - 2647658
Numero de Fax	+58 – 0212 - 2647658
Página web-*-	www.authenology.com.ve
Horario de atención al publico	8:00 a.m. a 12:00 m y de 1:00 p.m. a 5:00 p.m. de lunes a viernes.
	AUTHENTICSING emitirá certificados electrónicos de firma a todas las personas naturales o jurídicas que cumplan con los requisitos establecidos en el Decreto Ley de Mensaje de Datos y Firmas Electrónicas y su reglamento, y que hayan suscrito exitosamente el contrato de prestación de servicios. La vigencia inicial de los certificados será de un (1) año.

9.1.2 Certificado raíz del PSC AUTHENTICSING.

El PSC AUTHENTICSING es una AC de nivel superior y se encuentra subordinada a la autoridad de certificación raíz del estado venezolano y solamente estará en funcionamiento durante la realización de las operaciones para las que se establece. La estructura del certificado raíz del PSC AUTHENTICSING es la siguiente:

ESTRUCTURA DE DATOS DEL CERTIFICADO RAIZ	
NOMBRE DEL PUNTO	**VALOR**
Versión	V3 (Número de versión del certificado)
Número de serie (SerialNumber)	(Identificador único menor de 20 caracteres hexadecimales)
Algoritmo de firma (signatureAlgorithm)	sha512WithECDSAEncryption
DATOS DEL EMISOR	
CN (commonName)	Autoridad de Certificación Raíz del Estado Venezolano (SUSCERTE)
O (organizationName)	Sistema Nacional de Certificación Electrónica
C (countryName)	VE
PERIODO DE VALIDEZ	
Valido desde:	Fecha (UTC)
Válido hasta:	Fecha (UTC)
DATOS DEL TITULAR	
CN (commonName)	AUTHENTICSING
O (organizationName)	Sistema Nacional de Certificación Electrónica
OU (organizationName)	PROVEEDOR DE CERTIFICADOS AUTHENTICSING
C (countryName)	VE
INFORMACIÓN DE CLAVE PUBLICA	
Algoritmo clave pública (algorithm)	ecdsaEncryption (Algoritmo utilizado para generar la clave pública)
NIST CURVE	521
Extensiones	
Restricciones básicas (basicConstraints)	
Autoridad de Certificación	AC: True
Uso de la llave (keyUsage)	
Firma de certificado	KeyCertSign(5)
Firma de LCR	cRLSign (6)
Firma digital	digitalSignature
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)	
Clave de Autoridad (keyIdentifier)	Identificador de la clave

Puntos de Distribución de la LCR (cRLDistributionPoints)	
Punto de distribución LCR (distributionPoint)	https://www.authenology.com.ve/ac-raiz/authenologycrl.crl
AIA (authorityInfoAccess)	
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [ocsp] http://ocsp.authenology.com.ve/
Políticas de Certificación (PolicyInformation)	
PolicyInformation (PC)	
Identificador de Política (policyIdentifier)	<OID Autorizado por SUSCERTE> 1.3.6.1.5.5.7.14
Identificador de recurso uniforme (cPSuri)	https://www.authenology.com.ve/normativas/
PolicyInformation (DPC)	
Identificador de Política (policyIdentifier)	<OID Autorizado por SUSCERTE> 1.3.6.1.5.5.7.2.1
Identificador de recurso uniforme (cPSuri)	https://www.authenology.com.ve/normativas/
Firma	
Algoritmo de Firma (signatureAlgorithm)	sha512WithECDSAEncryption
Firma(signature)	<Contenido de la Firma>

9.1.3 Raíz de certificación del PSC AUTHENTICSING.

PSC AUTHENTICSING cuenta con una plataforma de certificación conforme a los estándares internacionales X.509 V3 y autorizada por SUSCERTE. Esta plataforma permite emitir certificados electrónicos para diversos usos. Los usuarios generan sus propias claves criptográficas a través de los navegadores web (OCSP), y SUSCERTE valida el cumplimiento de los requisitos legales antes de firmar la solicitud de certificado. De esta manera, AUTHENTICSING opera como una Autoridad de Certificación subordinada bajo la supervisión de SUSCERTE.

AUTHENTICSING, en cumplimiento con el LMDFE y su reglamento, integrará el certificado raíz de SUSCERTE en su plataforma para emitir certificados electrónicos válidos. Para garantizar la seguridad, se generará una Lista de Certificados Revocados (LCR) diaria, la cual será notificada mensualmente a SUSCERTE y almacenada de forma segura. Los titulares de los certificados serán informados por correo electrónico sobre cualquier revocación.

9.1.1.2 Relación con proveedores de tecnología y demás compañías relacionadas.

El PSC AUTHENTICSING mantiene asociaciones estratégicas con las siguientes empresas:

- DAYCOHOST

9.1.1.3 Página y Aplicativo Web.

El aplicativo web de AUTHENTICSING, accesible en **https://app.authenology.com.ve** , presenta una interfaz intuitiva con los siguientes módulos de navegación:

- Información de contacto AUTHENTICSING.
- Firma de documentos.
- Tipos de certificados.
- DPC y PC.
- Lista de Certificados Revocados (LCR).
- Firmas electrónicas
- Planes y Servicios.
- Inicio de Sección.
- Registros.

9.1.1.4 Centro de datos.

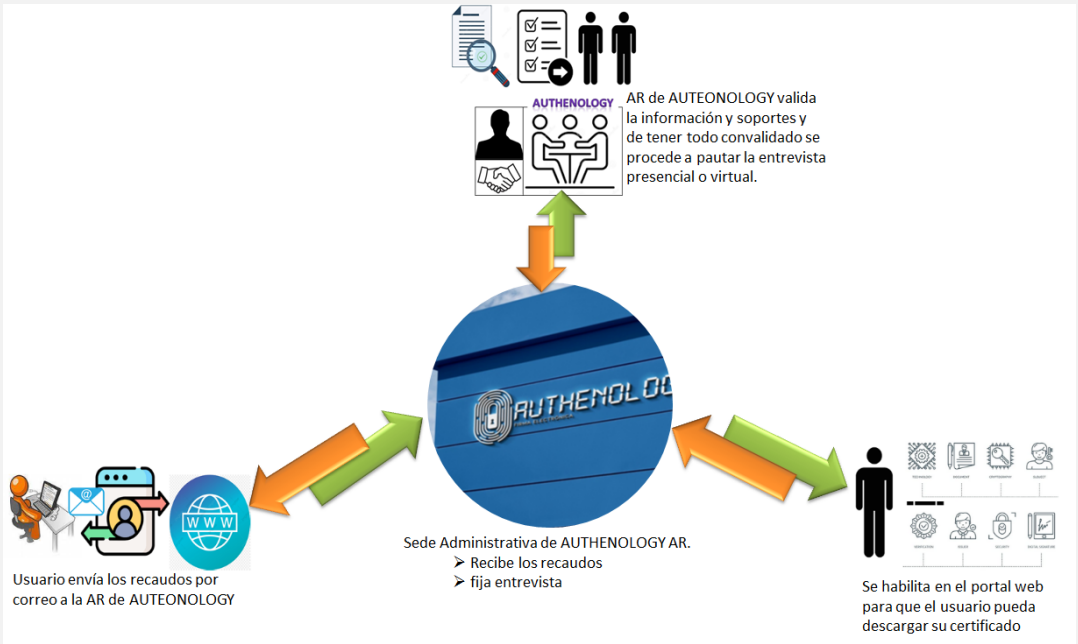
AUTHENTICSING provee un esquema operativo orientado a garantizar una constancia funcional y prestación de servicios con estándares de calidad, oportunidad y seguridad. El centro de datos se constituye en la sede de Daycohost. Opera las veinticuatro (24) horas del día, los trescientos sesenta y cinco (365) días del año y mantiene una autonomía y/o independencia operacional superior a los dos (2) meses. Adicionalmente, el centro de datos reúne condiciones y características de construcción antisísmica y de prevención de incendio e inundaciones, mantiene un perímetro de seguridad y cuenta con siete (7) niveles de seguridad de acceso.

El centro de datos donde opera el PSC AUTHENTICSING mantiene las pólizas o instrumentos emitidos por empresas de seguros solventes y reconocidos, a los efectos de mantener un respaldo en caso de ocurrencia de una contingencia que afecta la integridad física de la referida sede administrativa y pueda ofrecer de esa manera una garantía de su continuidad operacional. La autoridad de certificación (AC)

mantiene contrato de operación de centro alterno en caso de daño permanente que imposibilite y restrinja la operación regular del centro de datos.

9.1.1.5 Esquema del modelo operacional de AUTHENTICSING

Imagen #1



Esquema de Operación

9.2 Autoridad de Registro (AR).

La Autoridad de Registro (AR) es una entidad o persona responsable de verificar y registrar la información de identificación del solicitante para un certificado electrónico antes de que se emita el certificado. La AR actúa como intermediario entre el solicitante y la entidad emisora del certificado, Autoridad Certificado (AC), verificando la identidad del solicitante y proporcionando la información necesaria a la AC para emitir el certificado.

La función de la AR es fundamental para garantizar la autenticidad y la integridad de los certificados digitales emitidos, ya que la AC se basa en la información proporcionada por la AR para emitir el certificado. La AR también puede ser responsable de comprobar la validez de los documentos de identificación presentados por el solicitante y de garantizar que se cumplan los requisitos de

seguridad y privacidad aplicables.

AUTHENTICSING ha implementado un sistema innovador para la validación de identidad, eliminando la necesidad de una Autoridad de Registro (AR/RA presencial). Nuestro proceso es 100% automatizado, seguro y eficiente, garantizando la máxima confiabilidad en la emisión de certificados electrónicos.

Este enfoque automatizado permite validar y comprobar la identificación de personas jurídicas o naturales que solicitan o renuevan certificados electrónicos, otorgando la fe pública sobre la identidad del cliente y estableciendo la prueba legal de las responsabilidades y obligaciones derivadas del uso del certificado, conforme al Decreto Ley de Mensajes de Datos y Firmas Electrónicas y su Reglamento.

- Proceso de Validación Integrado en AUTHENTICSING:
  A diferencia de los modelos tradicionales, en AUTHENTICSING la función de validación de identidad está completamente integrada dentro de nuestro sistema automatizado de registro y certificación de clientes.

- Todos los interesados en obtener un certificado electrónico, bajo las normativas del Decreto Ley de Mensajes de Datos y Firmas Electrónicas, su Reglamento y SUSCERTE, deben seguir el siguiente proceso digital:

  - Acceso a la Plataforma: El usuario accede a la página web de AUTHENTICSING (www.authenology.com.ve).

  - Registro en Línea: Se completa un formulario digital donde se incluyen datos personales y se adjunta una fotografía digital de la cédula de identidad, así como otra información requerida según el tipo de persona (natural o jurídica).

  - Verificación de Correo Electrónico: El sistema envía un token de verificación al correo electrónico del usuario, que debe ser confirmado para activar la cuenta.

  - Validación Biométrica Facial en Tiempo Real: Este es el paso clave de nuestra automatización. El sistema realiza una verificación facial biométrica en tiempo real. Durante este proceso, se compara el rostro del solicitante con la fotografía de la cédula de identidad previamente cargada, solicitando gestos específicos (como mirar a la izquierda, a la derecha y abrir la boca brevemente) para asegurar la vivacidad y

autenticidad del usuario.

- ❖ Generación de Certificado: Una vez que la validación de identidad biométrica es exitosa, el sistema permite al usuario generar su certificado digital de forma inmediata.

Este proceso automatizado elimina por completo la necesidad de citas presenciales, entrega de documentación física o cualquier interacción humana para la validación de identidad.

- ➢ Almacenamiento y Vigencia de la Documentación:
  AUTHENTICSING almacena de forma segura la documentación digital y los registros del proceso de validación durante el período de vigencia del certificado electrónico o de cualquiera de sus renovaciones. Los registros de archivo digital de certificados tendrán una vigencia total de diez (10) años antes de proceder a su desincorporación, asegurando la trazabilidad y cumplimiento legal.

De ser aprobada la conexión por parte de la AC en adelante todos los datos que viajen desde la AR a la AC serán firmados digitalmente por la AR, incluidas las solicitudes de generación y revocación.

9.2.1 Modelo de Operación de la AR

9.2.1.1 Sede Administrativa.

La AR del PSC AUTHENTICSING conserva un esquema de gestión orientado a asegurar y garantizar la constancia funcional y servicios con amplios estándares de seguridad y calidad. La AR elabora desde la ubicación administrativa del PSC AUTHENTICSING y es el encargado de dar consentimiento, conformidad y validación acerca de la autenticidad de los clientes contratantes de certificados electrónicos, y una vez verificada la información e identidad de los clientes, se procederá con el registro y posteriormente a la generación de los certificados electrónicos.

9.2.1.2 Proceso de validación de identidad automatizada.

El proceso de validación de identidad es un pilar fundamental para AUTHENTICSING, esencial para la emisión segura y legal de certificados digitales. Este proceso, totalmente automatizado y sin intervención de una Autoridad de Registro (AR) presencial, garantiza la autenticidad del

cliente y del potencial signatario. Su diseño responde a la necesidad de proteger la seguridad de los usuarios y la integridad de las transacciones, siendo aplicable tanto a personas naturales como jurídicas, incluyendo individuos y representantes de organizaciones públicas o privadas.

AUTHENTICSING ha desarrollado un sistema de validación de identidad digital robusto que integra diversas tecnologías para asegurar la máxima fiabilidad:

- Para Personas Naturales:
  I. Verificación de Documento de Identidad: El sistema analiza la fotografía digital de la cédula de identidad (o pasaporte) cargada por el usuario para confirmar su vigencia, autenticidad y extraer sus datos clave de forma automática.
  II. Validación Biométrico-Facial en Tiempo Real: Se realiza una comparación biométrica del rostro del solicitante con la imagen de su documento de identidad. Este proceso incluye la detección de vivacidad mediante el análisis de gestos específicos (ej. mirar a la izquierda, a la derecha, abrir la boca brevemente), garantizando que la persona presente es la misma que aparece en el documento.
  III. Consulta Automatizada con Registros Oficiales: El sistema puede realizar consultas automatizadas con bases de datos oficiales, como el padrón electoral (CNE), para convalidar la identificación y los datos proporcionados por el cliente.

- Para Personas Jurídicas:
  IV. Consulta Automatizada de Identificación Legal: El sistema se integra con bases de datos públicas, como las del SENIAT, para verificar la identificación y el estatus de la persona jurídica.
  V. Validación del Representante Legal: A través del proceso biométrico-facial, se valida la identidad del representante legal de la persona jurídica, comparándola con su documento de identidad y convalidando su poder de representación según la documentación digital cargada y las bases de datos oficiales.

Este proceso de validación se ejecuta de manera continua y automatizada desde el momento en que el cliente completa la solicitud y carga la información requerida a través del portal web de

AUTHENTICSING (www.authenology.com.ve). No se requieren entrevistas programadas ni atención presencial.

9.2.1.3 Confirmación y Comunicación Digital:

La comunicación con el cliente se realiza de forma totalmente digital a través del correo electrónico. Todos los mensajes importantes enviados por AUTHENTICSING estarán firmados con firma electrónica para garantizar su autenticidad e integridad. Los correos podrán solicitar información adicional no predecible, que solo el cliente conoce, para fortalecer la seguridad del proceso de validación. El sistema también puede verificar automáticamente el número de teléfono proporcionado, cruzándolo con registros públicos oficiales de compañías telefónicas.

9.2.1.4 Almacenamiento Seguro y Auditorías:

AUTHENTICSING mantiene los documentos digitales y los registros del proceso de validación almacenados de forma segura en repositorios de bóvedas electrónicas. Esta documentación se conserva durante el período de vigencia del certificado o de sus renovaciones, con un archivo digital que se extiende por diez (10) años antes de su desincorporación, asegurando el cumplimiento de la normativa.

Se planifican auditorías de control anuales para la validación de la documentación e identidad de los clientes que contratan certificados electrónicos, garantizando la mejora continua y el apego a las regulaciones.

9.2.1.5 Verificación de Certificados Extranjeros:

Con relación a la verificación y validación de certificados extranjeros, AUTHENTICSING mantiene actualizada la data de las entidades con las cuales se tiene relación de reconocimiento y validación, de acuerdo con el Decreto Ley de Mensajes de Datos y Firmas Electrónicas (LSMDFE) y su Reglamento, evitando el uso de certificados revocados.

9.2.1.6 Diagrama del modelo de AR.

Imagen #1

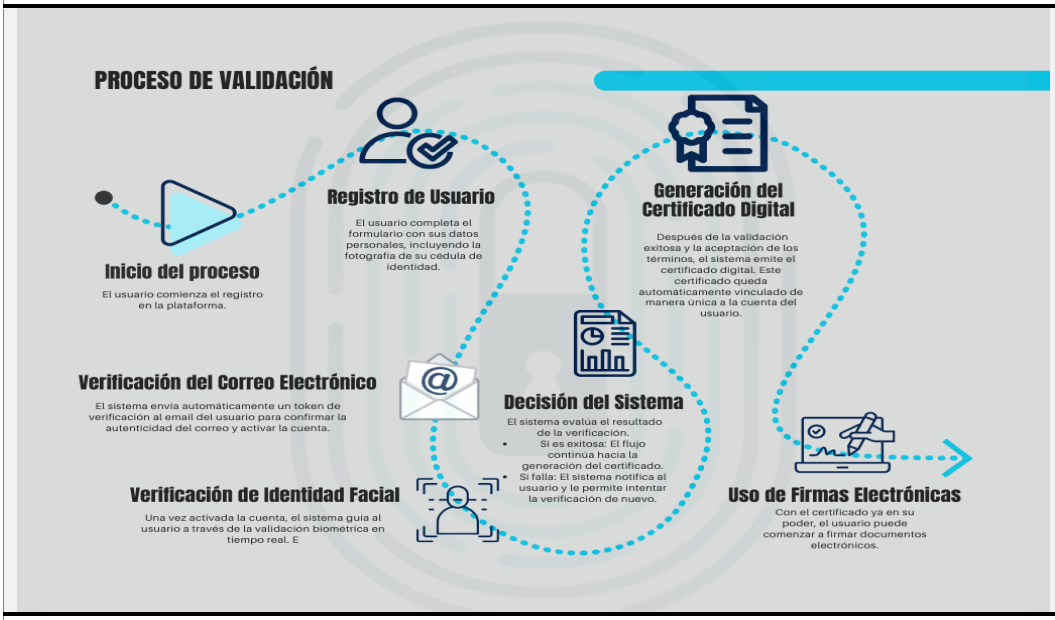


Diagrama de validación

9.3 Signatario

En el contexto de la firma y certificados electrónico, un signatario puede ser una persona natural o jurídica que firma un documento digitalmente utilizando una firma electrónica. En este caso, la firma electrónica se considera equivalente a una firma manuscrita y es legalmente vinculante de acuerdo con las leyes y regulaciones aplicables.

9.4 Tercero de buena fe.

Los terceros de buena fe, son entidades jurídicas que confían en una firma electrónica, certificado electrónico, registro de certificados revocados o información generada por el PSC AUTHENTICSING y sobre las cuales pueden depositar su seguridad y confianza de acuerdo con el actual documento de la la Política de Certificados (PC) y Declaración de Prácticas de Certificación (DPC).

La Infraestructura de Clave Pública (ICP) del PSC AUTHENTICSING, está reconocida y obligada, directa o indirectamente (mediante cadena de contratos) con todos los proveedores, clientes y/o parte interesada, usuarios de firmas electrónicas y certificados electrónicos generados por el PSC AUTHENTICSING. De esta manera corresponder a una comunidad cerrada y depositar su confianza en sus

servicios, se requiere precisamente de la aprobación de los clientes (terceros de buena Fe), a las condiciones del contrato de adquisición de firmas electrónicas o certificados electrónicos generados por el PSC AUTHENTICSING

10. USO DE LOS CERTIFICADOS.

10.1 Usos permitidos.

La gestión de los certificados subordinados emitidos por PSC AUTHENTICSING se encuentra regulada por políticas específicas para cada tipo de certificado. Se advierte que el uso no autorizado o fraudulento de estos certificados puede dar lugar a responsabilidades legales y económicas. En consecuencia, se recomienda encarecidamente a los usuarios el cumplimiento estricto de las condiciones de uso establecidas.

A continuación, se presenta una clasificación de los diferentes tipos de certificados emitidos por esta entidad:

10.1.1 Certificado de firma electrónica para empleado de empresa privada.

El uso asignado para este tipo de certificado son los siguientes puntos:

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

ESTRUCTURA DEL CERTIFICADO ELECTRÓNICO DE FIRMA PARA EMPLEADO DE EMPRESA PRIVADA	
NOMBRE DEL PUNTO	**VALOR**
Versión	V3 (Número de versión del certificado)
Número de serie (SerialNumber)	(Identificador único menor de 20 caracteres hexadecimales)
Algoritmo de firma (signatureAlgorithm)	Sha384WithECDSAEncryption
DATOS DEL EMISOR	
Nombre común (commonName)	AUTHENTICSING
Organización (organizationName)	Sistema Nacional de Certificación Electrónica

OU (organizationName)	PROVEEDOR DE CERTIFICADOS AUTHENTICSING
C (countryName)	VE
PERIODO DE VALIDEZ	
Válido desde:	Fecha (UTC)
Válido hasta:	Fecha (UTC)
DATOS DEL TITULAR	
Nombre común (commonName)	[Nombre1, Nombre2, Apellido1 y Apellido2]
Organización (organizationName)	Nombre completo de la persona jurídica tal cual aparece en el documento constitutivo de la empresa
Título(title)	Título(title) Título y/o cargo del empleado
Correo Electrónico (emailAddress)	Dirección de correo electrónico del Titular
Estado (stateOrProvinceName)	Estado de ubicación del Titular
Departamento (organizationalUnitName)	Nombre del departamento, dirección o unidad de trabajo al cual pertenece el titular
País (countryName)	VE
SerialNumber (DN)	Cédula de identidad (V o E), Registro Único de Información Fiscal (G o J) o Número de Pasaporte
INFORMACIÓN DE CLAVE PUBLICA	
Algoritmo clave pública (algorithm)	ecdsaEncryption (Algoritmo utilizado para generar la clave pública)
NIST CURVE	384
Extensiones	
Restricciones básicas (basicConstraints)	
Autoridad de Certificación	AC: False
Uso de la llave (keyUsage)	
Firma digital	digitalSignature(0)
Compromiso de contenido (contentCommitment)	contentCommitment(1) (Antes No Repudio)
Cifrado de clave	keyEncipherment
Cifrado de datos	dataEncipherment
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)	
Clave de Autoridad (keyIdentifier)	Identificador de la clave
Usos Extendidos de la Clave (extKeyUsage)	
Adobe PDF Signing (adobePdfSigning)	1.2.840.113583 Adobe Acrobat Reader
Microsoft Document Signing	1.3.6.1.4.1.311.10.3.12 documentSigning
Puntos de Distribución de la LCR (cRLDistributionPoints)	
Punto de distribución LCR (distributionPoint)	https://www.authenology.com.ve/ac-raiz/authenologycrl.crl
AIA (authorityInfoAccess)	

Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [ocsp]
Dirección de Acceso (accessLocation)	http://ocsp.authenology.com.ve/
Políticas de Certificación (PolicyInformation)	
PolicyInformation (DPC)	
Identificador de Política (policyIdentifier)	<OID Autorizado por SUSCERTE> 1.3.6.1.5.5.7.2.1
Identificador de recurso uniforme (cPSuri)	https://www.authenology.com.ve/normativas/
Firma	
Algoritmo de Firma (signatureAlgorithm)	Sha384WithECDSAEncryption
Firma(signature)	<Contenido de la Firma>

- El uso del certificado de firma electrónica para empleado de empresa privada emitido por el PSC **AUTHENTICSING** estará limitado según el tipo de certificado, y a continuación se menciona el uso del mismo:

Tipo de certificado	Uso	Uso mejorado
Certificado de firma electrónica para empleado de empresa privada	Firma digital, compromiso de contenido, cifrado de clave, cifrado de datos	Firma de documentos

10.1.2 Certificado de firma electrónica para representante de empresa pública.

El uso asignado para este tipo de certificado es el siguiente:

- Transacciones en línea públicas o privadas, en representación de Entidades de Derecho Público o Empresas.
- Comercio electrónico en representación de Entidades de Derecho Público o Empresas.
- Certificar a una persona como representante legal de una entidad jurídica publica
- Comunicaciones privadas o públicas en representación de Entidades de Derecho Público o Empresas.
- Declaraciones o trámites en línea ante gobierno en representación de Entidades de Derecho Público o Empresas.

ESTRUCTURA DEL CERTIFICADO ELECTRÓNICO DE FIRMA PARA REPRESENTANTE DE EMPRESA PÚBLICA	
NOMBRE DEL PUNTO	**VALOR**

Versión	V3 (Número de versión del certificado)
Número de serie (SerialNumber)	(Identificador único menor de 20 caracteres hexadecimales)
Algoritmo de firma (signatureAlgorithm)	Sha384WithECDSAEncryption
DATOS DEL EMISOR	
Nombre común (commonName)	AUTHENTICSING
Organización (organizationName)	Sistema Nacional de Certificación Electrónica
OU (organizationName)	PROVEEDOR DE CERTIFICADOS AUTHENTICSING
C (countryName)	VE
PERIODO DE VALIDEZ	
Válido desde:	Fecha (UTC)
Válido hasta:	Fecha (UTC)
DATOS DEL TITULAR	
Nombre común (commonName)	[Nombre1, Nombre2, Apellido1 y Apellido2]
Organización (organizationName)	Nombre completo de la persona jurídica tal cual aparece en el decreto de creación o en el documento constitutivo de la organización
Título(title)	Título(title) Título y/o cargo del empleado
Correo Electrónico (emailAddress)	Dirección de correo electrónico de contacto del Titular
Estado (stateOrProvinceName)	Estado de ubicación del Titular
Departamento (organizationalUnitName)	Nombre del departamento, dirección o unidad de trabajo al cual pertenece el titular
País (countryName)	VE
SerialNumber (DN)	Cédula de identidad (V o E), Registro Único de Información Fiscal (G o J) o Número de Pasaporte
INFORMACIÓN DE CLAVE PUBLICA	
Algoritmo clave pública (algorithm)	ecdsaEncryption (Algoritmo utilizado para generar la clave pública)
NIST CURVE	384
Extensiones	
Restricciones básicas (basicConstraints)	
Autoridad de Certificación	AC: False
Uso de la llave (keyUsage)	
Firma digital	digitalSignature(0)
Compromiso de contenido (contentCommitment)	contentCommitment(1) (Antes No Repudio)
Cifrado de clave	keyEncipherment
Cifrado de datos	dataEncipherment
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)	
Clave de Autoridad (keyIdentifier)	Identificador de la clave

Usos Extendidos de la Clave (extKeyUsage)	
Adobe PDF Signing (adobePdfSigning)	1.2.840.113583 Adobe Acrobat Reader
Microsoft Document Signing	1.3.6.1.4.1.311.10.3.12 documentSigning
Puntos de Distribución de la LCR (cRLDistributionPoints)	
Punto de distribución LCR (distributionPoint)	https://www.authenology.com.ve/ac-raiz/authenologycrl.crl
AIA (authorityInfoAccess)	
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [ocsp]
Dirección de Acceso (accessLocation)	http://ocsp.authenology.com.ve/
Políticas de Certificación (PolicyInformation)	
PolicyInformation (DPC)	
Identificador de Política (policyIdentifier)	<OID Autorizado por SUSCERTE> 1.3.6.1.5.5.7.2.1
Identificador de recurso uniforme (cPSuri)	https://www.authenology.com.ve/normativas/
Firma	
Algoritmo de Firma (signatureAlgorithm)	Sha384WithECDSAEncryption
Firma(signature)	<Contenido de la Firma>

- El uso del certificado de firma electrónica para representante de empresa pública emitido por el PSC AUTHENTICSING estará limitado según el tipo de certificado, y a continuación se menciona el uso del mismo:

Tipo de certificado	Uso	Uso mejorado
Certificado de firma electrónica para representante de empresa pública	Firma digital, compromiso de contenido, cifrado de clave, cifrado de datos	Firma de documentos

10.1.3 Certificado de firma electrónica para funcionario público (empleado de institución público).

El uso asignado para este tipo de certificado es el siguiente:

- Transacciones en línea públicas o privadas, en representación de Entidades de Derecho Público o Empresas.
- Comercio electrónico en representación de Entidades de Derecho Público o Empresas.
- Certificar a una persona como representante legal de una entidad jurídica publica

- Comunicaciones privadas o públicas en representación de Entidades de Derecho Público o Empresas.
- Declaraciones o trámites en línea ante gobierno en representación de Entidades de Derecho Público o Empresas.

ESTRUCTURA DEL CERTIFICADO ELECTRÓNICO DE FIRMA PARA FUNCIONARIO PÚLICO	
NOMBRE DEL PUNTO	**VALOR**
Versión	V3 (Número de versión del certificado)
Número de serie (SerialNumber)	(Identificador único menor de 20 caracteres hexadecimales)
Algoritmo de firma (signatureAlgorithm)	Sha384WithECDSAEncryption
DATOS DEL EMISOR	
Nombre común (commonName)	AUTHENTICSING
Organización (organizationName)	Sistema Nacional de Certificación Electrónica
OU (organizationName)	PROVEEDOR DE CERTIFICADOS AUTHENTICSING
C (countryName)	VE
PERIODO DE VALIDEZ	
Válido desde:	Fecha (UTC)
Válido hasta:	Fecha (UTC)
DATOS DEL TITULAR	
Nombre común (commonName)	[Nombre1, Nombre2, Apellido1 y Apellido2]
Organización (organizationName)	Nombre completo de la persona jurídica tal cual aparece en el documento constitutivo de la empresa
Título(title)	Título(title) Título y/o cargo del funcionario
Correo Electrónico (emailAddress)	Dirección de correo electrónico de contacto del Titular
Identificador de documento (documentIdentifier)	Especificar documento que lo acredita como empleado
Estado (stateOrProvinceName)	Estado de ubicación del titular
Departamento (organizationalUnitName)	Nombre del departamento, dirección o unidad de trabajo al cual pertenece el titular
País (countryName)	VE
SerialNumber (DN)	Cédula de identidad (V o E), Registro Único de Información Fiscal (G o J) o Número de Pasaporte
INFORMACIÓN DE CLAVE PUBLICA	
Algoritmo clave pública (algorithm)	**ecdsaEncryption (Algoritmo utilizado para generar la clave pública)**
NIST CURVE	384
Extensiones	
Restricciones básicas (basicConstraints)	

Autoridad de Certificación	**AC: False**
Uso de la llave (keyUsage)	
Firma digital	digitalSignature(0)
Compromiso de contenido (contentCommitment)	contentCommitment(1) (Antes No Repudio)
Cifrado de clave	keyEncipherment
Cifrado de datos	dataEncipherment
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)	
Clave de Autoridad (keyIdentifier)	**Identificador de la clave**
Usos Extendidos de la Clave (extKeyUsage)	
Adobe PDF Signing (adobePdfSigning)	1.2.840.113583 Adobe Acrobat Reader
Microsoft Document Signing	1.3.6.1.4.1.311.10.3.12 documentSigning
Puntos de Distribución de la LCR (cRLDistributionPoints)	
Punto de distribución LCR (distributionPoint)	https://www.authenology.com.ve/ac-raiz/authenologycrl.crl
AIA (authorityInfoAccess)	
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [ocsp]
Dirección de Acceso (accessLocation)	http://ocsp.authenology.com.ve/
Políticas de Certificación (PolicyInformation)	
PolicyInformation (DPC)	
Identificador de Política (policyIdentifier)	<OID Autorizado por SUSCERTE> 1.3.6.1.5.5.7.2.1
Identificador de recurso uniforme (cPSuri)	https://www.authenology.com.ve/normativas/
Firma	
Algoritmo de Firma (signatureAlgorithm)	Sha384WithECDSAEncryption
Firma(signature)	<Contenido de la Firma>

- El uso del certificado de firma electrónica para funcionario público emitido por el PSC AUTHENTICSING estará limitado según el tipo de certificado, y a continuación se menciona el uso del mismo:

Tipo de certificado	Uso	Uso mejorado
Certificado de firma electrónica para funcionario público	Firma digital, compromiso de contenido, cifrado de clave, cifrado de datos	Firma de documentos

10.1.4 Certificado de firma electrónica para representante legal de empresa privada.

El uso asignado para este tipo de certificado es el siguiente:

- Transacciones en línea públicas o privadas, en representación de Entidades de Derecho Público o Empresas.
- Comercio electrónico en representación de Entidades de Derecho Público o Empresas.
- Certificar a una persona como representante legal de una entidad jurídica publica
- Comunicaciones privadas o públicas en representación de Entidades de Derecho Público o Empresas.
- Declaraciones o trámites en línea ante gobierno en representación de Entidades de Derecho Público o Empresas.

ESTRUCTURA DEL CERTIFICADO ELECTRÓNICO DE FIRMA PARA REPRESENTANTE LEGAL DE EMPRESA PRIVADA	
NOMBRE DEL PUNTO	**VALOR**
Versión	V3 (Número de versión del certificado)
Número de serie (SerialNumber)	(Identificador único menor de 20 caracteres hexadecimales)
Algoritmo de firma (signatureAlgorithm)	Sha384WithECDSAEncryption
DATOS DEL EMISOR	
Nombre común (commonName)	AUTHENTICSING
Organización (organizationName)	Sistema Nacional de Certificación Electrónica
OU (organizationName)	PROVEEDOR DE CERTIFICADOS AUTHENTICSING
C (countryName)	VE
PERIODO DE VALIDEZ	
Válido desde:	Fecha (UTC)
Válido hasta:	Fecha (UTC)
DATOS DEL TITULAR	
Nombre común (commonName)	[Nombre1, Nombre2, Apellido1 y Apellido2]
Organización (organizationName)	Nombre completo de la persona jurídica tal cual aparece en el documento constitutivo de la empresa
Título(title)	Título(title) Título y/o cargo del empleado
Correo Electrónico (emailAddress)	Dirección de correo electrónico de contacto del Titular

Estado (stateOrProvinceName)	Estado de ubicación del Titular
Departamento (organizationalUnitName)	Nombre del departamento, dirección o unidad de trabajo al cual pertenece el titular
País (countryName)	VE
SerialNumber (DN)	Cédula de identidad (V o E), Registro Único de Información Fiscal (G o J) o Número de Pasaporte
INFORMACIÓN DE CLAVE PUBLICA	
Algoritmo clave pública (algorithm)	ecdsaEncryption (Algoritmo utilizado para generar la clave pública)
NIST CURVE	384
Extensiones	
Restricciones básicas (basicConstraints)	
Autoridad de Certificación	AC: False
Uso de la llave (keyUsage)	
Firma digital	digitalSignature(0)
Compromiso de contenido (contentCommitment)	contentCommitment(1) (Antes No Repudio)
Cifrado de clave	keyEncipherment
Cifrado de datos	dataEncipherment
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)	
Clave de Autoridad (keyIdentifier)	Identificador de la clave
Usos Extendidos de la Clave (extKeyUsage)	
Adobe PDF Signing (adobePdfSigning)	1.2.840.113583 Adobe Acrobat Reader
Microsoft Document Signing	1.3.6.1.4.1.311.10.3.12 documentSigning
Puntos de Distribución de la LCR (cRLDistributionPoints)	
Punto de distribución LCR (distributionPoint)	https://www.authenology.com.ve/ac-raiz/authenologycrl.crl
AIA (authorityInfoAccess)	
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [ocsp]
Dirección de Acceso (accessLocation)	http://ocsp.authenology.com.ve/
Políticas de Certificación (PolicyInformation)	
PolicyInformation (DPC)	
Identificador de Política (policyIdentifier)	<OID Autorizado por SUSCERTE> 1.3.6.1.5.5.7.2.1
Identificador de recurso uniforme (cPSuri)	https://www.authenology.com.ve/normativas/
Firma	
Algoritmo de Firma (signatureAlgorithm)	Sha384WithECDSAEncryption

Firma(signature)	<Contenido de la Firma>

- El uso del certificado de firma electrónica para representante legal de empresa privada emitido por el PSC **AUTHENTICSING** estará limitado según el tipo de certificado, y a continuación se menciona el uso del mismo:

Tipo de certificado	Uso	Uso mejorado
Certificado de firma electrónica para representante legal de empresa privada	Firma digital, compromiso de contenido, cifrado de clave, cifrado de datos	firma de documentos

10.1.5 Certificado de firma electrónica para profesionales titulados.

El uso asignado para este tipo de certificado es el siguiente:

- Transacciones en línea asociadas al ejercicio de profesión u oficio con colegiatura y reconocimiento legal dentro de la República Bolivariana de Venezuela.
- Comunicaciones privadas o públicas asociadas al ejercicio de profesión u oficio con colegiatura y reconocimiento dentro de la República Bolivariana de Venezuela.
- Comercio electrónico asociadas al ejercicio de profesión u oficio con colegiatura y reconocimiento dentro de la República Bolivariana de Venezuela.
- Certificar a una persona como representante legal de una entidad jurídica publica
- Comunicaciones privadas o públicas en representación de Entidades de Derecho Público o Empresas.
- Declaraciones o trámites en línea ante gobierno asociadas al ejercicio de profesión u oficio con colegiatura y reconocimiento dentro de la República Bolivariana de Venezuela.

ESTRUCTURA DEL CERTIFICADO ELECTRÓNICO DE FIRMA PARA PROFESIONALES TITULADOS	
NOMBRE DEL PUNTO	**VALOR**
Versión	V3 (Número de versión del certificado)
Número de serie (SerialNumber)	(Identificador único menor de 20 caracteres hexadecimales)
Algoritmo de firma (signatureAlgorithm)	Sha384WithECDSAEncryption
DATOS DEL EMISOR	
Nombre común (commonName)	AUTHENTICSING

Organización (organizationName)	Sistema Nacional de Certificación Electrónica
OU (organizationName)	PROVEEDOR DE CERTIFICADOS AUTHENTICSING
C (countryName)	VE
PERIODO DE VALIDEZ	
Válido desde:	Fecha (UTC)
Válido hasta:	Fecha (UTC)
DATOS DEL TITULAR	
Nombre común (commonName)	Número de colegiatura
Nombre (givenName)	Nombre 1 Nombre 2
Apellido (surName)	Apellido 1 Apellido 2
Título (title)	Nombre del Título registrado ante la Colegiatura
Correo Electrónico (emailAddress)	Dirección de correo electrónico de contacto del Titular
Estado (stateOrProvinceName)	Estado de ubicación del Titular
País (countryName)	VE
SerialNumber (DN)	Cédula de identidad (V o E), Registro Único de Información Fiscal (G o J) o Número de Pasaporte
INFORMACIÓN DE CLAVE PUBLICA	
Algoritmo clave pública (algorithm)	ecdsaEncryption (Algoritmo utilizado para generar la clave pública)
NIST CURVE	384
Extensiones	
Restricciones básicas (basicConstraints)	
Autoridad de Certificación	AC: False
Uso de la llave (keyUsage)	
Firma digital	digitalSignature(0)
Compromiso de contenido (contentCommitment)	contentCommitment(1) (Antes No Repudio)
Cifrado de clave	keyEncipherment
Cifrado de datos	dataEncipherment
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)	
Clave de Autoridad (keyIdentifier)	Identificador de la clave
Usos Extendidos de la Clave (extKeyUsage)	
Adobe PDF Signing (adobePdfSigning)	1.2.840.113583 Adobe Acrobat Reader
Microsoft Document Signing	1.3.6.1.4.1.311.10.3.12 documentSigning
Puntos de Distribución de la LCR (cRLDistributionPoints)	
Punto de distribución LCR (distributionPoint)	https://www.authenology.com.ve/ac-raiz/authenologycrl.crl

AIA (authorityInfoAccess)	
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [ocsp]
Dirección de Acceso (accessLocation)	http://ocsp.authenology.com.ve/
Políticas de Certificación (PolicyInformation)	
PolicyInformation (DPC)	
Identificador de Política (policyIdentifier)	<OID Autorizado por SUSCERTE> 1.3.6.1.5.5.7.2.1
Identificador de recurso uniforme (cPSuri)	https://www.authenology.com.ve/normativas/
Firma	
Algoritmo de Firma (signatureAlgorithm)	Sha384WithECDSAEncryption
Firma(signature)	<Contenido de la Firma>

- El uso del certificado de firma electrónica para profesionales titulados emitido por el PSC **AUTHENTICSING** estará limitado según el tipo de certificado, y a continuación se menciona el uso del mismo:

Tipo de certificado	Uso	Uso mejorado
Certificado de firma electrónica para profesionales titulados.	Firma digital, compromiso de contenido, cifrado de clave, cifrado de datos	firma de Documentos

10.1.6 Certificado electrónico de firma para persona natural.

El uso asignado para este tipo de certificado es el siguiente:

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

ESTRUCTURA DEL CERTIFICADO ELECTRÓNICO DE FIRMA PARA PERSONA NATURAL	
NOMBRE DEL PUNTO	VALOR
Versión	V3 (Número de versión del certificado)
Número de serie (SerialNumber)	(Identificador único menor de 20 caracteres hexadecimales)
Algoritmo de firma (signatureAlgorithm)	Sha384WithECDSAEncryption
DATOS DEL EMISOR	

Nombre común (commonName)	AUTHENTICSING
Organización (organizationName)	Sistema Nacional de Certificación Electrónica
OU (organizationName)	PROVEEDOR DE CERTIFICADOS AUTHENTICSING
País (countryName)	VE
PERIODO DE VALIDEZ	
Válido desde:	Fecha (UTC)
Válido hasta:	Fecha (UTC)
DATOS DEL TITULAR	
Nombre común (commonName)	[Nombre1, Nombre2, Apellido1 y Apellido2]
Correo Electrónico (emailAddress)	Dirección de correo electrónico de contacto del Titular
Estado (stateOrProvinceName)	Estado de ubicación del Titular
Localidad (localityName)	Ciudad de residencia del Titular
País (countryName)	VE
SerialNumber (DN)	Cédula de identidad (V o E), Registro Único de Información Fiscal (G o J) o Número de Pasaporte
INFORMACIÓN DE CLAVE PUBLICA	
Algoritmo clave pública (algorithm)	ecdsaEncryption (Algoritmo utilizado para generar la clave pública)
NIST CURVE	384
Extensiones	
Restricciones básicas (basicConstraints)	
Autoridad de Certificación	AC: False
Uso de la llave (keyUsage)	
Firma digital	digitalSignature(0)
Compromiso de contenido (contentCommitment)	contentCommitment(1) (Antes No Repudio)
Cifrado de clave	keyEncipherment
Cifrado de datos	dataEncipherment
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)	
Clave de Autoridad (keyIdentifier)	Identificador de la clave
Usos Extendidos de la Clave (extKeyUsage)	
Adobe PDF Signing (adobePdfSigning)	1.2.840.113583 Adobe Acrobat Reader
Microsoft Document Signing	1.3.6.1.4.1.311.10.3.12 documentSigning
Puntos de Distribución de la LCR (cRLDistributionPoints)	
Punto de distribución LCR (distributionPoint)	https://www.authenology.com.ve/ac-raiz/authenologycrl.crl
AIA (authorityInfoAccess)	

Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [ocsp]
Dirección de Acceso (accessLocation)	http://ocsp.authenology.com.ve/
Políticas de Certificación (PolicyInformation)	
PolicyInformation (DPC)	
Identificador de Política (policyIdentifier)	<OID Autorizado por SUSCERTE> 1.3.6.1.5.5.7.2.1
Identificador de recurso uniforme (cPSuri)	https://www.authenology.com.ve/normativas/
Firma	
Algoritmo de Firma (signatureAlgorithm)	Sha384WithECDSAEncryption
Firma(signature)	<Contenido de la Firma>

- El uso del certificado de firma electrónica para persona natural emitido por el PSC AUTHENTICSING estará limitado según el tipo de certificado, y a continuación se menciona el uso del mismo:

Tipo de certificado	Uso	Uso mejorado
Certificado de firma electrónica para persona natural	Firma digital, Compromiso de contenido, cifrado de clave, cifrado de datos	Firma de Documentos

10.1.7 Certificado de Servidor de OCSP.

El uso asignado para este tipo de certificado es el siguiente:

- Se debe colocar una estructura de Certificado de servidor OCSP para firmar respuestas generadas del servicio OCSP de una AC.
- Las restricciones básicas debe ser la AC= [false]

ESTRUCTURA DEL CERTIFICADO ELECTRÓNICO DE FIRMA PARA OCSP	
NOMBRE DEL PUNTO	**VALOR**
Versión	V3 (Número de versión del certificado)
Número de serie (SerialNumber)	(Identificador único menor de 20 caracteres hexadecimales)
Algoritmo de firma (signatureAlgorithm)	Sha384WithECDSAEncryption
DATOS DEL EMISOR	
Nombre común (commonName)	AUTHENTICSING
Organización (organizationName)	Sistema Nacional de Certificación Electrónica

OU (organizationName)	PROVEEDOR DE CERTIFICADOS AUTHENTICSING
C (countryName)	VE
PERIODO DE VALIDEZ	
Válido desde:	Fecha de emisión del Certificado
Válido hasta:	Fecha de vencimiento del Certificado
SUJETO	
Nombre común (commonName)	authenology.com.ve
Organización (organizationName)	Sistema Nacional de Certificación Electrónica
País (countryName)	VE
Algoritmo clave pública (algorithm)	Algoritmo utilizado para generar la clave pública
Uso de la llave (KeyUsage)	
Firma digital	digitalSignature(0)
Usos Extendidos de la Clave (extKeyUsage)	
Firma de OCSP	ocspSigning 1.3.6.1.5.5.7.3.9
Puntos de Distribución de las LCR (cRLDistributionPoints)	
Punto de distribución LCR (distributionPoint)	https://www.authenology.com.ve/ac-raiz/authenologycrl.crl
AIA (authorityInfoAccess)	
Dirección de Acceso (accessLocation)	http://ocsp.authenology.com.ve/
OCSP non revocation cheking	
Identificados de la llave del sujeto	Identificador de las subject key en el certificado
Identificador de la llave de autoridad	
Key id	Identificador de la clave
Certificate Iuseer	Datos del emisor
OU (organizationName)	PROVEEDOR DE CERTIFICADOS AUTHENTICSING
Correo Electrónico (emailAddress)	contacto@authenology.com.ve
Organización (organizationName)	Sistema Nacional de Certificación Electrónica
C (countryName)	VE
Serial number(DN)	Número de serial
Certificate Policy	
Policy Identifier	1.3.6.1.5.5.7.14
Policy Qualifier Info	

Policy Qualifier ID	CPS(DPC)
Qualifier	https://www.authenology.com.ve/normativas/
Issuer Alternative Name	
DNS Name	authenology.com.ve
OID (asignado por suscerte)	Código del PSC AUTHENTICSING asignado por la SUSCERTE
OID (asignado por suscerte)	RIF J-503240237 (AUTHENTICSING)

- El uso del certificado de firma electrónica para servidor OCSP emitido por el PSC AUTHENTICSING estará limitado según el tipo de certificado, y a continuación se menciona el uso del mismo:

Tipo de certificado	Uso	Uso mejorado
Certificado de firma electrónica para servidor OCSP	Firma electrónica	Firma OSCP

10.1.8 Certificado de firma electrónica para SSL (Secure Sockets Layer).

El uso asignado para este tipo de certificado es el siguiente:

- Asegurar la seguridad de las comunicaciones digitales entre los diversos elementos de una infraestructura tecnológica unificada, protegiendo los datos transmitidos de accesos no autorizados y alteraciones.
- Implementar medidas de seguridad para proteger los datos sensibles transmitidos durante las transacciones electrónicas en un entorno de sistemas interconectados.

ESTRUCTURA DEL CERTIFICADO ELECTRÓNICO DE FIRMA PARA SSL (SECURE SOCKETS LAYER)	
NOMBRE DEL PUNTO	**VALOR**
Versión	V3 (Número de versión del certificado)
Número de serie (SerialNumber)	(Identificador único menor de 20 caracteres hexadecimales)
Algoritmo de firma (signatureAlgorithm)	Sha384WithECDSAEncryption
DATOS DEL EMISOR	
Nombre común (commonName)	AUTHENTICSING
Organización (organizationName)	Sistema Nacional de Certificación Electrónica
OU (organizationName)	PROVEEDOR DE CERTIFICADOS AUTHENTICSING

País (countryName)	VE
PERIODO DE VALIDEZ	
Válido desde:	Fecha (UTC)
Válido hasta:	Fecha (UTC)
DATOS DEL TITULAR	
Nombre Común (commonName)	Nombre de dominio del sitio web que protege el certificado <No se permiten direcciones IP privadas>
Organización (organizationName)	Nombre de la empresa
Correo Electrónico (emailAddress)	Dirección de correo electrónico
Departamento(organizationalUnitName)	Departamento de origen del SSL
Localidad (localityName)	Ciudad de residencia del titular del certificado
Estado (stateOrProvinceName)	Estado de residencia del titular del certificado
País (countryName)	VE
INFORMACIÓN DE CLAVE PUBLICA	
Algoritmo clave pública (algorithm)	ecdsaEncryption (Algoritmo utilizado para generar la clave pública)
NIST CURVE	384
Extensiones	
Restricciones básicas (basicConstraints)	
Autoridad de Certificación	AC: False
Uso de la llave (keyUsage)	
Compromiso de contenido (contentCommitment)	contentCommitment(1) (Antes No Repudio)
Cifrado de clave	keyEncipherment
Cifrado de datos	dataEncipherment
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)	
Clave de Autoridad (keyIdentifier)	Identificador de la clave
Usos Extendidos de la Clave (extKeyUsage)	
Autenticación de Servidor	id-kp-serverAuth [RFC5280]
Puntos de Distribución de la LCR (cRLDistributionPoints)	
Punto de distribución LCR (distributionPoint)	https://www.authenology.com.ve/ac-raiz/authenologycrl.crl
AIA (authorityInfoAccess)	
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [ocsp]
Dirección de Acceso (accessLocation)	http://ocsp.authenology.com.ve/
Políticas de Certificación (PolicyInformation)	
PolicyInformation (DPC)	

Identificador de Política (policyIdentifier)	<OID Autorizado por SUSCERTE> 1.3.6.1.5.5.7.2.1
Identificador de recurso uniforme (cPSuri)	https://www.authenology.com.ve/normativas/
Firma	
Algoritmo de Firma (signatureAlgorithm)	Sha384WithECDSAEncryption
Firma(signature)	<Contenido de la Firma>

- El uso del certificado de firma electrónica para SSL emitido por el PSC AUTHENTICSING estará limitado según el tipo de certificado, y a continuación se menciona el uso del mismo:

Tipo de certificado	Uso	Uso mejorado
Certificado de firma electrónica para SSL	Compromiso de contenido, cifrado de clave, cifrado de datos	Autenticación del servidor

10.1.9 Certificado Electrónico de firma para Redes Virtuales (VPN).

El uso asignado para este tipo de certificado es el siguiente:

- Cifrado de datos para establecer conexiones seguras y cifradas entre los dispositivos y la red VPN. Esto garantiza que los datos transmitidos estén protegidos contra interceptaciones y manipulaciones.
- Gestión de dispositivos como teléfonos móviles o laptops para permitir o restringir el acceso a la VPN.

ESTRUCTURA DEL CERTIFICADO ELECTRÓNICO DE FIRMA PARA REDES VIRTUALES (VPN)	
NOMBRE DEL PUNTO	**VALOR**
Versión (version)	V3 (Número de versión del certificado)
Serial (serialNumber)	Identificador único menor de 20 caracteres hexadecimales
Algoritmo de Firma (signatureAlgorithm)	Sha384WithECDSAEncryption
DATOS DEL EMISOR	
Nombre común (commonName)	AUTHENTICSING
Organización (organizationName)	Sistema Nacional de Certificación Electrónica
OU (organizationalUnitName)	PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN
Pais (countryName)	VE
PERIODO DE VALIDEZ	
Válido desde:	Fecha (UTC)

Válido hasta:	Fecha (UTC)
DATOS DEL TITULAR	
Nombre Común (commonName)	Nombre que identifica el servicio de Dominio o Dirección IP
Organización(organizationName)	Nombre de la organización
Correo Electrónico (emailAddress)	Dirección de correo electrónico
Departamento (organizationalUnitName)	Nombre del departamento o unidad organizativa
Localidad(localityName)	Dirección de residencia del titular del certificado
Estado(stateOrProvinceName)	Estado de residencia del titular del certificado
País (countryName)	VE
INFORMACIÓN DE CLAVE PÚBLICA DEL TITULAR (SUBJECTPUBLICKEY)	
Algoritmo de clave pública (algorithm)	Id-ecdsaPublicKey
NIST CURVE	384
Extensiones	
Restricciones Básicas (basicConstraints)	
Autoridad de Certificación (AC)	Booleano [false]
Uso de la clave (keyUsage)	
Firma digital	digitalSignature(0)
Compromiso de Contenido (contentCommitment)	contentCommitment(1) - (No Repudio)
Cifrado de clave	keyEncipherment
Cifrado de datos	dataEncipherment
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)	
Clave de Autoridad (keyIdentifier)	<Identificador de la clave pública de la AC Raíz>
Usos Extendidos de la Clave (extKeyUsage)	
Autenticación de Servidor	id-kp-serverAuth [RFC5280]
Autenticación de Cliente	idkpclientAuth [RFC5280]
Uso mejorado de la clave	Seguridad IP y cifrado
Puntos de Distribución de las LCR (cRLDistributionPoints)	
Punto de distribución LCR (distributionPoint)	https://www.authenology.com.ve/ac-raiz/authenologycrl.crl
AIA (authorityInfoAccess)	
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]
Dirección de Acceso (accessLocation)	http://ocsp.authenology.com.ve/
Políticas de Certificación (PolicyInformation)	

PolicyInformation (DPC)	
policyIdentifier	<OID Autorizado por SUSCERTE> 1.3.6.1.5.5.7.2.1
Identificador de recurso uniforme (cPSuri)	https://www.authenology.com.ve/normativas/
Firma	
Algoritmo de Firma (signatureAlgorithm)	Sha384WithECDSAEncryption
Firma(signature)	<Contenido de la Firma>

- El uso del certificado de firma electrónica para VPN emitido por el PSC AUTHENTICSING estará limitado según el tipo de certificado, y a continuación se menciona el uso del mismo:

Tipo de certificado	Uso	Uso mejorado
Certificado de firma electrónica para VPN	Firma digital, compromiso de contenido, cifrado de clave, cifrado de datos	Autenticación de servidor y de cliente, seguridad IP y cifrado

10.1.10 Certificado Electrónico para la Firma de software

El uso asignado para este tipo de certificado es el siguiente:

- Protección contra la manipulación alertando al titular de que la aplicación podría estar comprometida.
- Distribución segura del software, facilitando la distribución segura de software a través de internet.

ESTRUCTURA DEL CERTIFICADO ELECTRÓNICO DE FIRMA DE SOFTWARE	
NOMBRE DEL PUNTO	**VALOR**
Versión (version)	V3 (Número de versión del certificado)
Serial (serialNumber)	Identificador único menor de 20 caracteres hexadecimales
Algoritmo de Firma (signatureAlgorithm)	Sha384WithECDSAEncryption
DATOS DEL EMISOR	
Nombre común (commonName)	AUTHENTICSING
Organización (organizationName)	Sistema Nacional de Certificación Electrónica
OU (organizationalUnitName)	PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN
Pais (countryName)	VE
PERIODO DE VALIDEZ	
Válido desde:	Fecha (UTC)

Válido hasta:	Fecha (UTC)
DATOS DEL TITULAR	
Nombre Común	Identificación del objeto
Organización(organizationName)	Nombre de la organización responsable
Correo Electrónico (emailAddress)	Dirección de correo electrónico
Departamento (organizationalUnitName)	Nombre de la unidad organizativa
Localidad(localityName)	Ciudad de residencia o dirección
Estado(stateOrProvinceName)	Estado de residencia
País (countryName)	VE
Información de Clave Pública del Titular (subjectPublicKey)	
Algoritmo de clave pública (algorithm)	Id-ecdsaPublicKey
NIST CURVE	384
Extensiones	
Restricciones Básicas (basicConstraints)	
Autoridad de Certificación (AC)	Booleano [false]
Uso de la clave (keyUsage)	
Firma digital	digitalSignature(0)
Compromiso de Contenido (contentCommitment)	contentCommitment(1) - (No Repudio)
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)	
Clave de Autoridad (keyIdentifier)	<Identificador de la clave pública de la AC Raíz>
Usos Extendidos de la Clave (extKeyUsage)	
Autenticación de Servidor	id-kp-servertAuth [RFC5280]
Puntos de Distribución de las LCR (cRLDistributionPoints)	
Punto de distribución LCR (distributionPoint)	https://www.authenology.com.ve/ac-raiz/authenologycrl.crl
AIA (authorityInfoAccess)	
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]
Dirección de Acceso (accessLocation)	http://ocsp.authenology.com.ve/
Políticas de Certificación (PolicyInformation)	
PolicyInformation (DPC)	
policyIdentifier	<OID Autorizado por SUSCERTE> 1.3.6.1.5.5.7.2.1

Identificador de recurso uniforme (cPSuri)	https://www.authenology.com.ve/normativas/
Firma	
Algoritmo de Firma (signatureAlgorithm)	Sha384WithECDSAEncryption
Firma(signature)	<Contenido de la Firma>

- El uso del certificado de firma electrónica para firma de software por el PSC AUTHENTICSING estará limitado según el tipo de certificado, y a continuación se menciona el uso del mismo:

Tipo de certificado	Uso	Uso mejorado
Certificado de firma electrónica para firma de software	Firma digital, compromiso de contenido	Autenticación de servidor

10.1.11 Certificado Electrónico para la firma de transacción.

El uso asignado para este tipo de certificado es el siguiente:

- Cifrado de extremo a extremo
- Evidencia digital irrefutable
- Verificación de la autenticidad
- Imposibilidad de negar la autoría vinculando al firmante con la transacción
- Autenticación de archivos digitales

ESTRUCTURA DEL CERTIFICADO ELECTRÓNICO DE FIRMA DE TRANSACCIÓN	
NOMBRE DEL PUNTO	**VALOR**
Versión (version)	V3 (Número de versión del certificado)
Serial (serialNumber)	Identificador único menor de 20 caracteres hexadecimales
Algoritmo de Firma (signatureAlgorithm)	Sha384WithECDSAEncryption
DATOS DEL EMISOR	
Nombre común (commonName)	AUTHENTICSING
Organización (organizationName)	Sistema Nacional de Certificación Electrónica
OU (organizationalUnitName)	PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN
Pais (countryName)	VE

PERIODO DE VALIDEZ	
Válido desde:	Fecha (UTC)
Válido hasta:	Fecha (UTC)
DATOS DEL TITULAR	
Nombre Común	Identificación del objeto
Organización(organizationName)	Nombre de la organización responsable
Correo Electrónico (emailAddress)	Dirección de correo electrónico
Departamento (organizationalUnitName)	Nombre de la unidad organizativa
Localidad(localityName)	Ciudad de residencia o dirección
Estado(stateOrProvinceName)	Estado de residencia
País (countryName)	VE
INFORMACIÓN DE CLAVE PÚBLICA DEL TITULAR (SUBJECTPUBLICKEY)	
Algoritmo de clave pública (algorithm)	Id-ecdsaPublicKey
NIST CURVE	384
Extensiones	
Restricciones Básicas (basicConstraints)	
Autoridad de Certificación (AC)	Booleano [false]
Uso de la clave (keyUsage)	
Firma digital	digitalSignature(0)
Compromiso de Contenido (contentCommitment)	contentCommitment(1) - (No Repudio)
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)	
Clave de Autoridad (keyIdentifier)	<Identificador de la clave pública de la AC Raíz>
Usos Extendidos de la Clave (extKeyUsage)	
Uso mejorado de la clave	Firma de documento
Puntos de Distribución de las LCR (cRLDistributionPoints)	
Punto de distribución LCR (distributionPoint)	https://www.authenology.com.ve/ac-raiz/authenologycrl.crl
AIA (authorityInfoAccess)	
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]
Dirección de Acceso (accessLocation)	http://ocsp.authenology.com.ve/

Políticas de Certificación (PolicyInformation)	
PolicyInformation (DPC)	
policyIdentifier	<OID Autorizado por SUSCERTE> 1.3.6.1.5.5.7.2.1
Identificador de recurso uniforme (cPSuri)	https://www.authenology.com.ve/normativas/
Firma	
Algoritmo de Firma (signatureAlgorithm)	Sha384WithECDSAEncryption
Firma(signature)	<Contenido de la Firma>

- El uso del certificado de firma electrónica para firma de transacción por el PSC AUTHENTICSING estará limitado según el tipo de certificado, y a continuación se menciona el uso del mismo:

Tipo de certificado	Uso	Uso mejorado
Certificado de firma electrónica para firma de transacción	Firma digital, compromiso de contenido	Firma de documento

10.1.12 Certificado electrónico de factura electrónica.

El uso asignado para este tipo de certificado es el siguiente:

- Autenticidad y veracidad de los datos.
- Confirmación de que la información no ha sido alterada.
- Garantía de la integridad de los datos.
- Seguridad en la información transmitida.

ESTRUCTURA DEL CERTIFICADO ELECTRÓNICO DE FACTURA ELECTRÓNICA	
NOMBRE DEL PUNTO	**VALOR**
Versión (version)	V3 (Número de versión del certificado)
Serial (serialNumber)	Identificador único menor de 20 caracteres hexadecimales
Algoritmo de Firma (signatureAlgorithm)	Sha384WithECDSAEncryption
DATOS DEL EMISOR	
Nombre común (commonName)	AUTHENTICSING
Organización (organizationName)	Sistema Nacional de Certificación Electrónica
OU (organizationalUnitName)	PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN
Correo Electrónico (emailAddres)	contacto@authenology.com.ve

Localidad (localityName)	Caracas
Estado (stateOrProvinceName)	Miranda
Pais (countryName)	VE
PERIODO DE VALIDEZ	
Válido desde:	Fecha (UTC)
Válido hasta:	Fecha (UTC)
DATOS DEL TITULAR	
Nombre Común	Entidad a la que se le otorgará la certificación
Organización(organizationName)	Nombre de la entidad responsable
Correo Electrónico (emailAddress)	Dirección de correo electrónico de la entidad responsable
Departamento (organizationalUnitName)	Nombre de la unidad organizativa
Localidad(localityName)	Ciudad de residencia o dirección
Estado(stateOrProvinceName)	Estado de residencia
Pais (countryName)	VE
SerialNumber (DN)	Registro Único de Información Fiscal (RIF)
INFORMACIÓN DE CLAVE PÚBLICA DEL TITULAR (SUBJECTPUBLICKEY)	
Algoritmo de clave pública (algorithm)	Id-ecdsaPublicKey
NIST CURVE	384
Extensiones	
Restricciones Básicas (basicConstraints)	
Autoridad de Certificación (AC)	Booleano [false]
Uso de la clave (keyUsage)	
Firma digital	digitalSignature(0)
Compromiso de Contenido (contentCommitment)	contentCommitment(1) - (No Repudio)
Cifrado de clave	keyEncipherment
Cifrado de datos	dataEncipherment
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)	
Clave de Autoridad (keyIdentifier)	<Identificador de la clave pública de la AC Raíz>
Puntos de Distribución de las LCR (cRLDistributionPoints)	

Punto de distribución LCR (distributionPoint)	https://www.authenology.com.ve/ac-raiz/authenologycrl.crl
AIA (authorityInfoAccess)	
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]
Dirección de Acceso (accessLocation)	http://ocsp.authenology.com.ve/
Políticas de Certificación (PolicyInformation)	
PolicyInformation (DPC)	
policyIdentifier	<OID Autorizado por SUSCERTE> 1.3.6.1.5.5.7.2.1
Identificador de recurso uniforme (cPSuri)	https://www.authenology.com.ve/normativas/
Firma	
Algoritmo de Firma (signatureAlgorithm)	Sha384WithECDSAEncryption
Firma(signature)	<Contenido de la Firma>

- El uso del certificado de firma electrónica para firma de factura electrónica por el PSC AUTHENTICSING estará limitado según el tipo de certificado, y a continuación se menciona el uso del mismo:

Tipo de certificado	Uso	Uso mejorado
Certificado de firma electrónica para firma de factura electrónica	Firma digital, compromiso de contenido, cifrado de clave, cifrado de datos	N/A

10.1.13 Certificado electrónico para el control de acceso lógico.

El uso asignado para este tipo de certificado es el siguiente:

- Seguridad de la información.

ESTRUCTURA DEL CERTIFICADO ELECTRÓNICO PARA EL CONTROL DE ACCESO LÓGICO	
NOMBRE DEL PUNTO	**VALOR**
Versión (version)	V3 (Número de versión del certificado)
Serial (serialNumber)	Identificador único menor de 20 caracteres hexadecimales
Algoritmo de Firma (signatureAlgorithm)	Sha384WithECDSAEncryption
DATOS DEL EMISOR	
Nombre común (commonName)	AUTHENTICSING

Organización (organizationName)	Sistema Nacional de Certificación Electrónica
OU (organizationalUnitName)	PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN
Pais (countryName)	VE
PERIODO DE VALIDEZ	
Válido desde:	Fecha (UTC)
Válido hasta:	Fecha (UTC)
DATOS DEL TITULAR	
Nombre Común	Entidad a la que se le otorgará la certificación
Organización(organizationName)	Nombre de la entidad responsable
Correo Electrónico (emailAddress)	Dirección de correo electrónico de la entidad responsable
Departamento (organizationalUnitName)	Nombre de la unidad organizativa
Localidad(localityName)	Ciudad de residencia o dirección
Estado(stateOrProvinceName)	Estado de residencia
Pais (countryName)	VE
dNSName	Nombre de dominio completo del servicio de autenticación <No se permite dirección IP privada>
INFORMACIÓN DE CLAVE PÚBLICA DEL TITULAR (SUBJECTPUBLICKEY)	
Algoritmo de clave pública (algorithm)	Id-ecdsaPublicKey
NIST CURVE	384
Extensiones	
Restricciones Básicas (basicConstraints)	
Autoridad de Certificación (AC)	Booleano [false]
Uso de la clave (keyUsage)	
Firma digital	digitalSignature(0)
Compromiso de Contenido (contentCommitment)	contentCommitment(1) - (No Repudio)
Cifrado de clave	keyEncipherment
Cifrado de datos	dataEncipherment
Usos Extendidos de la Clave (extKeyUsage)	
Autenticación de cliente	id-kp-clientAuth
Uso mejorado	Autenticación con tarjeta inteligente

Identificador de clave de Autoridad Certificadora (Authority Key Identifier)	
Clave de Autoridad (keyIdentifier)	<Identificador de la clave pública de la AC Raíz>
Puntos de Distribución de las LCR (cRLDistributionPoints)	
Punto de distribución LCR (distributionPoint)	https://www.authenology.com.ve/ac-raiz/authenologycrl.crl
AIA (authorityInfoAccess)	
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]
Dirección de Acceso (accessLocation)	http://ocsp.authenology.com.ve/
Políticas de Certificación (PolicyInformation)	
PolicyInformation (DPC)	
policyIdentifier	<OID Autorizado por SUSCERTE> 1.3.6.1.5.5.7.2.1
Identificador de recurso uniforme (cPSuri)	https://www.authenology.com.ve/normativas/
Firma	
Algoritmo de Firma (signatureAlgorithm)	Sha384WithECDSAEncryption
Firma(signature)	<Contenido de la Firma>

- El uso del certificado de firma electrónica para el control de acceso lógico por el PSC AUTHENTICSING estará limitado según el tipo de certificado, y a continuación se menciona el uso del mismo:

Tipo de certificado	Uso	Uso mejorado
Certificado de firma electrónica para el control de acceso lógico	Firma digital, compromiso de contenido, cifrado de clave, cifrado de datos	Autenticación de cliente, autenticación de tarjeta inteligente

10.1.14 Certificado electrónico de dispositivos móviles.

El uso asignado para este tipo de certificado es el siguiente:

- Autenticación
- Cifrado de comunicaciones
- Integridad de los datos

ESTRUCTURA DEL CERTIFICADO ELECTRÓNICO DE DISPOSITIVOS MÓVILES	
NOMBRE DEL PUNTO	**VALOR**
Versión (version)	V3 (Número de versión del certificado)
Serial (serialNumber)	Identificador único menor de 20 caracteres hexadecimales
Algoritmo de Firma (signatureAlgorithm)	Sha384WithECDSAEncryption
DATOS DEL EMISOR	
Nombre común (commonName)	AUTHENTICSING
Organización (organizationName)	Sistema Nacional de Certificación Electrónica
OU (organizationalUnitName)	PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN
Pais (countryName)	VE
PERIODO DE VALIDEZ	
Válido desde:	Fecha (UTC)
Válido hasta:	Fecha (UTC)
DATOS DEL TITULAR	
Nombre Común (commonName)	Nombre1, Nombre2, Apellido1, Apellido2
Organización(organizationName)	Entidad a la que pertenece el sujeto del certificado
Correo Electrónico (emailAddress)	Dirección de correo electrónico
Departamento (organizationalUnitName)	Departamento de la entidad a la que pertenece el sujeto del certificado
Localidad(localityName)	Dirección fiscal de la empresa o titular
Estado(stateOrProvinceName)	Estado de residencia de la empresa o titular
Pais (countryName)	VE
Serial(serialNumber)	IMEI del dispositivo movil
INFORMACIÓN DE CLAVE PÚBLICA DEL TITULAR (SUBJECTPUBLICKEY)	
Algoritmo de clave pública (algorithm)	Id-ecdsaPublicKey
NIST CURVE	384
Extensiones	
Restricciones Básicas (basicConstraints)	
Autoridad de Certificación (AC)	Booleano [false]
Uso de la clave (keyUsage)	
Firma digital	digitalSignature(0)

Compromiso de Contenido (contentCommitment)	contentCommitment(1) - (No Repudio)
Cifrado de claves	keyEncipherment(2)
Acuerdo de claves	keyAgreement(4)
Usos Extendidos de la Clave (extKeyUsage)	
Autenticación de Servidor	id-kp-serverAuth [RFC5280]
Autenticacdión del cliente	id-kp-clientAuth [RFC5280]
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)	
Clave de Autoridad (keyIdentifier)	<Identificador de la clave pública de la AC Raíz>
Puntos de Distribución de las LCR (cRLDistributionPoints)	
Punto de distribución LCR (distributionPoint)	https://www.authenology.com.ve/ac-raiz/authenologycrl.crl
AIA (authorityInfoAccess)	
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]
Dirección de Acceso (accessLocation)	http://ocsp.authenology.com.ve/
Políticas de Certificación (PolicyInformation)	
PolicyInformation (DPC)	
policyIdentifier	<OID Autorizado por SUSCERTE> 1.3.6.1.5.5.7.2.1
Identificador de recurso uniforme (cPSuri)	https://www.authenology.com.ve/normativas/
Firma	
Algoritmo de Firma (signatureAlgorithm)	Sha384WithECDSAEncryption
Firma(signature)	<Contenido de la Firma>

- El uso del certificado de firma electrónica para dispositivos móviles por el PSC AUTHENTICSING estará limitado según el tipo de certificado, y a continuación se menciona el uso del mismo:

Tipo de certificado	Uso	Uso mejorado
Certificado de firma electrónica para dispositivos móviles	Firma digital, compromiso de contenido, cifrado de clave, cifrado de dato	Autenticación de servidor y cliente

10.1.15 Certificado electrónico de servidor (general)

El uso asignado para este tipo de certificado es el siguiente:

- Cifrado de comunicación
- Autenticación del servidor
- Integridad de los datos

ESTRUCTURA DEL CERTIFICADO ELECTRÓNICO DE SERVIDOR(GENERAL)	
NOMBRE DEL PUNTO	**VALOR**
Versión (version)	V3 (Número de versión del certificado)
Serial (serialNumber)	Identificador único menor de 20 caracteres hexadecimales
Algoritmo de Firma (signatureAlgorithm)	Sha384WithECDSAEncryption
DATOS DEL EMISOR	
Nombre común (commonName)	AUTHENTICSING
Organización (organizationName)	Sistema Nacional de Certificación Electrónica
OU (organizationalUnitName)	PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN
Pais (countryName)	VE
PERIODO DE VALIDEZ	
Válido desde:	Fecha (UTC)
Válido hasta:	Fecha (UTC)
DATOS DEL TITULAR	
Nombre Común (commonName)	Identificación del servidor, dominio o aplicación
Organización(organizationName)	Entidad a la que pertenece el sujeto del certificado
Correo Electrónico (emailAddress)	Dirección de correo electrónico
Departamento (organizationalUnitName)	Nombre del departamento, dirección o unidad de trabajo al cual pertenece el titular
Localidad (localityName)	Ciudad donde se ubica la organización propietaria del certificado
Estado (stateOrProvinceName)	Estado de residencia de la empresa o titular
Pais (countryName)	VE
Serial (serialNumber)	RIF de la organización o empresa suscriptora del certificado
INFORMACIÓN DE CLAVE PÚBLICA DEL TITULAR (SUBJECTPUBLICKEY)	
Algoritmo de clave pública (algorithm)	Id-ecdsaPublicKey
NIST CURVE	384
EXTENSIONES	

Restricciones Básicas (basicConstraints)	
Autoridad de Certificación (AC)	Booleano [false]
Uso de la clave (keyUsage)	
Firma digital	digitalSignature(0)
Compromiso de Contenido (contentCommitment)	contentCommitment(1) - (No Repudio)
Cifrado de claves	keyEncipherment(2)
Acuerdo de claves	keyAgreement(4)
Usos Extendidos de la Clave (extKeyUsage)	
Autenticación de Servidor	id-kp-serverAuth [RFC5280]
Puntos de Distribución de las LCR (cRLDistributionPoints)	
Punto de distribución LCR (distributionPoint)	https://www.authenology.com.ve/ac-raiz/authenologycrl.crl
AIA (authorityInfoAccess)	
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]
Dirección de Acceso (accessLocation)	http://ocsp.authenology.com.ve/
Políticas de Certificación (PolicyInformation)	
PolicyInformation (DPC)	
policyIdentifier	<OID Autorizado por SUSCERTE> 1.3.6.1.5.5.7.2.1
Identificador de recurso uniforme (cPSuri)	https://www.authenology.com.ve/normativas/
Firma	
Algoritmo de Firma (signatureAlgorithm)	Sha384WithECDSAEncryption
Firma(signature)	<Contenido de la Firma>

- El uso del certificado de firma electrónica para servidor por el PSC AUTHENTICSING estará limitado según el tipo de certificado, y a continuación se menciona el uso del mismo:

Tipo de certificado	Uso	Uso mejorado
Certificado de firma electrónica para servidor (General)	Firma digital, compromiso de contenido, cifrado de clave, cifrado de dato	Autenticación de servidor

10.1.16 Certificado de firma electrónica para cédula electrónica.

El uso asignado para este tipo de certificado es el siguiente:

- Trámites Gubernamentales en Línea
- No Repudio

ESTRUCTURA DEL CERTIFICADO ELECTRÓNICO PARA CÉDULA ELECTRÓNICA	
NOMBRE DEL PUNTO	**VALOR**
Versión	V3 (Número de versión del certificado)
Número de serie (SerialNumber)	(Identificador único menor de 20 caracteres hexadecimales)
Algoritmo de firma (signatureAlgorithm)	Sha384WithECDSAEncryption
DATOS DEL EMISOR	
Nombre común (commonName)	AUTHENTICSING
Organización (organizationName)	Sistema Nacional de Certificación Electrónica
OU (organizationName)	PROVEEDOR DE CERTIFICADOS AUTHENTICSING
País (countryName)	VE
PERIODO DE VALIDEZ	
Válido desde:	Fecha (UTC)
Válido hasta:	Fecha (UTC)
DATOS DEL TITULAR	
Nombre Común (commonName)	Nombre1, Nombre2, Apellido1 y Apellido2
SerialNumber (DN)	Cédula de identidad (V o E), Registro Único de Información Fiscal (G o J) o Número de Pasaporte
Correo Electrónico (emailAddress)	Dirección de correo electrónico
Teléfono (telephoneNumber)	Télefono de contacto del titular
Calle (streetAddress)	Calle de residencia del Titular
Localidad (localityName)	Ciudad de residencia del titular
Estado (stateOrProvinceName)	Estado de residencia del titular
País (countryName)	VE
INFORMACIÓN DE CLAVE PUBLICA	
Algoritmo clave pública (algorithm)	ecdsaEncryption (Algoritmo utilizado para generar la clave pública)
NIST CURVE	384
ATRIBUTOS ADICIONALES DEL TITULAR (SUBJECTDIRECTORYATTRIBUTES)	

Fecha de Nacimiento (dateOfBirth)	Fecha de Nacimiento del Titular
Lugar de Nacimiento (placeOfBirth)	Lugar de Nacimiento del Titular
Género (gender)	male (masculino) o female (femenino)
País de Ciudadanía (countryOfCitizenship)	VE
Extensiones	
Restricciones básicas (basicConstraints)	
Autoridad de Certificación	AC: False
Uso de la llave (keyUsage)	
Firma digital	digitalSignature(0)
Compromiso de contenido (contentCommitment)	contentCommitment(1) (Antes No Repudio)
Cifrado de clave	keyEncipherment
Cifrado de datos	dataEncipherment
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)	
Clave de Autoridad (keyIdentifier)	Identificador de la clave
Usos Extendidos de la Clave (extKeyUsage)	
Autenticación de Servidor	id-kp-serverAuth [RFC5280]
Autenticación de Cliente	idkpclientAuth [RFC5280]
Uso mejorado de la clave	Firma de documento
Puntos de Distribución de la LCR (cRLDistributionPoints)	
Punto de distribución LCR (distributionPoint)	https://www.authenology.com.ve/ac-raiz/authenologycrl.crl
AIA (authorityInfoAccess)	
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [ocsp]
Dirección de Acceso (accessLocation)	http://ocsp.authenology.com.ve/
Políticas de Certificación (PolicyInformation)	
PolicyInformation (DPC)	
Identificador de Política (policyIdentifier)	<OID Autorizado por SUSCERTE> 1.3.6.1.5.5.7.2.1
Identificador de recurso uniforme (cPSuri)	https://www.authenology.com.ve/normativas/
Firma	
Algoritmo de Firma (signatureAlgorithm)	Sha384WithECDSAEncryption
Firma(signature)	<Contenido de la Firma>

- El uso del certificado electrónico para cédula electrónica emitido por el PSC AUTHENTICSING estará limitado según el tipo de certificado, y a continuación se menciona el uso del mismo:

Tipo de certificado	Uso	Uso mejorado
Certificado electrónico para cédula electrónica	Firma digital, compromiso de contenido, cifrado de clave, cifrado de datos	Autenticación del servidor, autenticación de cliente y firma de documento

10.1.17 Certificado de firma electrónica de banca electrónica

El uso asignado para este tipo de certificado es el siguiente:

- Validación de la identidad del usuario.
- Firma electrónica.
- Seguridad de pagos electrónicos.
- Justificante legal de una transacción digital.
- Preservación de la integridad de los datos.
- No repudio.

ESTRUCTURA DEL CERTIFICADO ELECTRÓNICO DE BANCA ELECTRÓNICA	
NOMBRE DEL PUNTO	**VALOR**
Versión (version)	V3 (Número de versión del certificado)
Serial (serialNumber)	Identificador único menor de 20 caracteres hexadecimales
Algoritmo de Firma (signatureAlgorithm)	Sha384WithECDSAEncryption
DATOS DEL EMISOR	
Nombre común (commonName)	AUTHENTICSING
Organización (organizationName)	Sistema Nacional de Certificación Electrónica
OU (organizationalUnitName)	PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN
Pais (countryName)	VE
PERIODO DE VALIDEZ	
Válido desde:	Fecha (UTC)
Válido hasta:	Fecha (UTC)
DATOS DEL TITULAR	
Nombre Común (commonName)	Nombre de la empresa o usuario a certificar
Organización(organizationName)	Nombre de entidad bancaria

Correo Electrónico (emailAddress)	Dirección de correo electrónico de contacto del Titular
Departamento (organizationalUnitName)	Nombre del representante de Empresa o de la persona natural
Localidad(localityName)	Dirección fiscal de la Entidad Bancaria
Estado(stateOrProvinceName)	Estado de residencia
Pais (countryName)	VE
INFORMACIÓN DE CLAVE PÚBLICA DEL TITULAR (SUBJECTPUBLICKEY)	
Algoritmo de clave pública (algorithm)	Id-ecdsaPublicKey
NIST CURVE	384
Extensiones	
Restricciones Básicas (basicConstraints)	
Autoridad de Certificación (AC)	Booleano [false]
Uso de la clave (keyUsage)	
Firma digital	digitalSignature(0)
Compromiso de Contenido (contentCommitment)	contentCommitment(1) - (No Repudio)
Cifrado de clave	keyEncipherment
Cifrado de datos	dataEncipherment
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)	
Clave de Autoridad (keyIdentifier)	<Identificador de la clave pública de la AC Raíz>
Puntos de Distribución de las LCR (cRLDistributionPoints)	
Punto de distribución LCR (distributionPoint)	https://www.authenology.com.ve/acraiz/authenologycrl.crl
AIA (authorityInfoAccess)	
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]
Dirección de Acceso (accessLocation)	http://ocsp.authenology.com.ve/
Políticas de Certificación (PolicyInformation)	
PolicyInformation (DPC)	
policyIdentifier	<OID Autorizado por SUSCERTE> 1.3.6.1.5.5.7.2.1
Identificador de recurso uniforme (cPSuri)	https://www.authenology.com.ve/normativas/
Firma	

Algoritmo de Firma (signatureAlgorithm)	Sha384WithECDSAEncryption
Firma(signature)	<Contenido de la Firma>

- El uso del certificado de firma electrónica de banca electrónica por el PSC AUTHENTICSING estará limitado según el tipo de certificado, y a continuación se menciona el uso del mismo:

Tipo de certificado	Uso	Uso mejorado
Certificado de firma electrónica de banca electrónica	Firma digital, compromiso de contenido, cifrado de clave, cifrado de datos	N/A

10.2 Usos no permitidos

Se prohíbe al titular del certificado electrónico utilizar este más allá de los fines permitidos expresamente en el apartado 10.1.

El titular del certificado asume la responsabilidad de cumplir con todas las condiciones establecidas en el contrato. En caso de incumplimiento, AUTHENTICSING se reserva el derecho de revocar el certificado y exigir una indemnización por los daños y perjuicios ocasionados.

11. POLÍTICAS DE ADMINISTRACIÓN DE AUTHENTICSING

Con el objetivo de garantizar la seguridad y transparencia en la gestión de certificados electrónicos, el PSC AUTHENTICSING ha establecido un conjunto de normas y procedimientos que regulan la emisión, administración y uso de los mismos. Esta información es proporcionada a todos nuestros clientes para asegurar su comprensión y cumplimiento.

11.1 Estructura y organización administrativa

Esta sección detalla las responsabilidades del equipo encargado de registrar, mantener y actualizar la Declaración de Prácticas de Certificación (DPC) y la Política de Certificados (PC) dentro de PSC AUTHENTICSING."

DATOS DE LA EMPRESA	
Nombre	Junta directiva de Authenticsing.
Correo	contacto@authenology.com.ve

electrónico	
Número de teléfono	+58 – 0212 - 2647658
Numero de Fax	+58 – 0212 - 2647658
Página web	www.authenology.com.ve

11.2 Persona Contacto.

Sobre esta Declaración de Prácticas de Certificación o los certificados emitidos por el PSC AUTHENTICSING, los interesados pueden comunicarse a través de los siguientes datos de contacto:

DATOS DEL CONTACTO	
Nombre	PSC AUTHENTICSING.
Correo electrónico	contacto@authenology.com.ve
Número de teléfono	+58 – 0212 – 2647658
Numero de Fax	+58 – 0212 - 2647658
Página web	www.authenology.com.ve

11.3 Competencia para determinar la adecuación de la DPC y las políticas

Con el fin de cumplir con los requisitos establecidos por SUSCERTE, AUTHENTICSING ha desarrollado esta Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC). Esta normativa se aplica a todos los procesos de certificación y reafirma nuestro compromiso con la excelencia en materia de seguridad.

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

12.1 Repositorios

El PSC AUTHENTICSING ofrece acceso ininterrumpido a los servicios de publicación, los cuales funcionan las veinticuatro (24) horas del día, todos los días del año. Ante cualquier eventualidad que interrumpa el servicio, nos comprometemos a restablecerlo en un plazo máximo de cuarenta y ocho (48) horas. Los repositorios de certificados están disponibles en:

- La información completa sobre la Autoridad de Certificación raíz subordinada, así como su Política de Certificación y Declaración de Prácticas de Certificación, se encuentra disponible de manera permanente en el sitio web: www.authenology.com.

- Certificado emitido por la AC Subordinada AUTHENTICSING, junto con los certificados que emite y su correspondiente Declaración de Prácticas de Certificación (DPC): https://www.authenology.com.ve/ac-raiz/
- Lista de Certificados Revocados: https://www.authenology.com.ve/ac-raiz/authenologycrl.crl

- Servicio de validación en línea (OCSP): http://ocsp.authenology.com.ve/

- La información almacenada en el repositorio público de AUTHENTICSING es de acceso libre y no compromete la privacidad.

12.2 Autenticidad de publicación

Con el objetivo de fomentar la transparencia y la confianza en nuestros servicios, el PSC AUTHENTICSING publica de manera periódica en su página web toda la información pertinente sobre los procesos y estatus de los certificados emitidos:

- Lista de Certificados Revocados (LCR), es válido y funcional en formato CRL en:

  https://www.authenology.com.ve/ac-raiz/authenologycrl.crl

- El actual documento se encuentra útil y disponible en:

  https://www.authenology.com.ve/normativas/

- El certificado de la AC Subordinada AUTHENTICSING está a disposición en:

  https://www.authenology.com.ve/ac-raiz/

- Los certificados emitidos por la AC Subordinada AUTHENTICSING se encuentran en:

  https://www.authenology.com.ve/ac-raiz/

- La información de contacto del PSC AUTHENTICSING se ubica en:

https://www.authenology.com.ve

- La acreditación y documentación técnica del PSC AUTHENTICSING está disponible en la siguiente dirección:

  https://www.authenology.com.ve

12.3 Frecuencia de publicación

12.3.1 Certificados del Proveedor de Servicio de Certificación (PSC).

La emisión de los certificados se realizará únicamente después de obtener la aprobación y certificación de SUSCERTE. La validez de estos certificados será de diez (10) años.

12.3.2 Lista de Certificados Revocados (LCR)

La publicación de la Lista de Certificados Revocados (LCR) se actualizará y ejecutará cada veinticuatro (24) horas o cada vez que sea revocado un certificado.

12.3.3 Versiones y actualizaciones de la DPC y PC.

Salvo indicación expresa en contrario contenida en este documento, las nuevas versiones de la DPC y PC serán publicadas en el sitio web de AUTHENTICSING https://www.authenology.com.ve/normativas/ una vez hayan sido aprobadas por SUSCERTE.

12.3.4 Controles de acceso al repositorio de certificados.

La información publicada por PSC AUTHENTICSING tiene carácter consultivo y está protegida contra modificaciones no autorizadas. La actualización de la información, como la LCR, el servidor OCSP y el presente documento, se realizará de manera periódica y controlada por el personal especializado de AUTHENTICSING, garantizando así la integridad y disponibilidad de los datos.

13. IDENTIFICACION Y AUTENTICACIÓN.

13.1 Registro de nombres.

13.1.1 Tipo de nombres.

La estructura de los certificados digitales emitidos por AUTHENTICSING se basa en el estándar X.509 V3. En particular, los campos de 'Nombre del sujeto' y 'Nombre alternativo del sujeto' se utilizan para identificar de forma única al

titular del certificado.

- El Nombre Distintivo (DN) del PSC AUTHENTICSING está compuesto por:

Nombre de punto	Valor
CN	AUTHENTICSING
O	Sistema Nacional de Certificacion Electrónica
E	contacto@authenology.com.ve
C	VE

- La composición del nombre alternativo (AN) del PSC AUTHENTICSING es la siguiente:

Nombre de punto	Valor
DNSName	authenology.com.ve
OID 2.16.862	RIFJ-503240237 (AUTHENTICSING)
OID 2.16.862.2.1	Por definir

- Para los Signatarios: Los atributos de los certificados de usuario se ajustarán a los lineamientos establecidos en la norma técnica 022 (manual de actualización y aprobación de políticas y prácticas de certificación) de Suscerte sobre las Políticas de Certificados del PSC AUTHENTICSING, considerando las características específicas de cada certificado

13.1.2 Necesidad de que los nombres sean significativos.

Como requisito indispensable para la contratación de firmas o certificados electrónicos, el PSC AUTHENTICSING exigirá a sus clientes la presentación de sus nombres y apellidos completos, los cuales deberán coincidir exactamente con los datos reflejados en su cédula de identidad laminada. El campo correspondiente a la nacionalidad en la cédula de identidad deberá indicar, mediante el uso de las letras 'V' o 'E', la condición migratoria del titular, seguido de su número de identificación personal, según el formato establecido:

V00000000 o E00000000.

Para identificar organizaciones, empresas públicas o privadas se debe utilizar el Registro Único de Información Fiscal (R.I.F). El Registro Único de Información Fiscal (R.I.F.) deberá seguir el formato del ente emisor, ejemplo: V00000000, G00000000, J000000000, C000000000.

El uso del DN Serial Number se rige por la norma 032 (infraestructura nacional de certificación electrónica: estructura, certificados y listas de certificados revocados), sección 7.1 Anexo A.

13.1.3 Interpretación de formatos de nombres.

Para interpretar los nombres que identifican a las entidades en los certificados, se utiliza el estándar internacional ISO/IEC 9595 (X.500). Además, todos los datos contenidos en los certificados están codificados en UTF-8, siguiendo las recomendaciones de la RFC 3280, un estándar ampliamente utilizado en el ámbito de la infraestructura de clave pública (PKI).

13.1.4 Unicidad de nombres.

SUSCERTE establece que el campo DN del CA debe servir como una identificación única y clara. En el caso de PSC AUTHENTICSING, se utilizará el nombre comercial de la empresa para cumplir con este requisito. Asimismo, para proteger la privacidad de los clientes, la información personal asociada a cada certificado se mantendrá consistente y no se permitirán duplicidades

13.1.5 Resolución de Conflictos relativos a nombres.

En caso de que dos o más clientes de AUTHENTICSING tengan el mismo nombre y apellido, la Autoridad de Registro utilizará el número de cédula de identidad y el RIF para identificar de manera única a cada uno y resolver cualquier conflicto.

13.2 Validación inicial de la identidad

13.2.1 Método de prueba de posesión de la clave privada.

Con el fin de garantizar la seguridad y la integridad del proceso, AUTHENTICSING ha implementado un sistema en el que el cliente genera y firma su propio par de claves, asegurando así la autenticidad de la solicitud de certificación.

El cliente asume la custodia y garantía de su clave privada desde el momento de la emisión del certificado. En cumplimiento de la normativa vigente, el cliente se compromete a resguardar esta información de manera segura. En caso de que el cliente detecte o sospeche que su clave privada ha sido comprometida, deberá notificarlo a AUTHENTICSING para que se proceda a la revocación del certificado correspondiente

13.2.2 Autenticación de la identidad de la organización.

La Autoridad de Registro (AR) del PSC AUTHENTICSING en el momento de que se trate de firmas electrónicas que autentiquen y acrediten empresas o entes públicos se ejecutará de la siguiente manera:

13.2.1.1 Entidad pública.

La AR realizará las diligencias necesarias para autenticar la existencia legal de la entidad solicitante, conforme a lo publicado en Gaceta Oficial. Asimismo, se garantizará la asignación de un titular responsable para cada certificado electrónico emitido.

Una vez verificada la identidad de la organización y la autoridad de quien la representa, se evaluará la documentación presentada de acuerdo con los procedimientos establecidos. Si toda la información es correcta y cumple con los requisitos, la Autoridad de Registro dará el visto bueno a la Autoridad de Certificación para generar el certificado electrónico solicitado.

13.2.1.2 Entidad privada.

La Autoridad de Registro (AR) realizará una diligencia de verificación para confirmar la existencia legal de la empresa privada, consultando su documento constitutivo en el registro mercantil correspondiente y corroborando su publicación en un diario oficial. Todo certificado electrónico emitido a una organización requerirá la designación de un responsable, cuya identidad y autoridad serán debidamente comprobadas por la AR de AUTHENTICSING.

Una vez corroborada la identidad y representación legal de la organización, se validarán los datos restantes proporcionados. Si la información resulta conforme, la Autoridad de Registro notificará a la Autoridad de Certificación para que proceda con la emisión del certificado electrónico.

13.2.3 Autenticación de la identidad de Personas Naturales.

Los requisitos para autenticar la identidad de personas naturales dependerán del tipo de solicitud y se ajustarán a las políticas de certificación de AUTHENTICSING. En todos los casos, se requerirá como mínimo la presentación de la cédula de identidad vigente (para venezolanos) o el pasaporte válido (para extranjeros sin cédula). El proceso de autenticación consta de los siguientes pasos:

- **Recopilación de información de identificación:** La persona interesada en obtener un certificado electrónico CE debe proporcionar información de identificación, como su nombre completo, dirección, fecha de nacimiento, cedula de identificación, etc.

- **Verificación de la información de identificación:** AUTHENTICSING verificará la identidad de los solicitantes mediante la consulta de registros gubernamentales (SENIAT, SAIME, CNE), la revisión de documentos y otros métodos como videoconferencias o validación por terceros.

- **Verificación de la identidad en persona:** La Autoridad de Registro de AUTHENTICSING se reserva el derecho de requerir una verificación de identidad presencial, la cual podrá incluir la presentación de documentos físicos y la captura de una imagen del solicitante.

- **Verificación de la autenticidad de los documentos:** La AR de PSC AUTHENTICSING se reserva el derecho de solicitar documentación complementaria para verificar la identidad del solicitante. Dicha documentación podrá incluir, a modo de ejemplo, pasaportes, licencias de conducir o documentos de identidad oficiales

13.2.4 Comprobación de las facultades de representación.

Para verificar las facultades de representación, el signatario deberá exhibir los documentos originales ante el operador de autenticación del PSC AUTHENTICSING, ya sea en nuestras oficinas o de forma remota.

Así mismo la aplicación AR, valida la identidad del signatario a través de su serial de validación y correo electrónico, para la autenticación en la AR, previa a la emisión del CE por parte de la AC de AUTHENTICSING.

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

13.3.1 Generación de nuevo Par de Claves.

La generación de un nuevo par de claves es un proceso importante para garantizar la seguridad y la integridad de las comunicaciones y transacciones electrónicas. Un par de claves es un conjunto de dos claves criptográficas, una clave pública y una clave privada, que se utilizan en la criptografía de clave pública para cifrar y descifrar datos y para proporcionar una firma electrónica segura y legalmente vinculante.

Para el PSC AUTHENTICSING la renovación del CE debe ser efectuada por el signatario con su clave de revocación desde el Sitio Web de la AR en la sede administrativa de Authenticsing.

En el caso de que el signatario no recuerde la clave de revocación debe presentarse con sus documentos para el tipo de CE, en la sede administrativa del PSC AUTHENTICSING con los operadores AR.

13.3.2 Generación de Nuevo Certificado (Posterior a Revocación).

PSC AUTHENTICSING exige la generación de una nueva clave privada al momento de renovar un Certificado Electrónico (CE), incluso cuando la clave anterior no se encuentre comprometida. Este procedimiento, llevado a cabo en nuestras instalaciones por personal especializado, garantiza la máxima seguridad del sistema. La plataforma tecnológica está diseñada para que el usuario sea el único responsable de la generación y custodia de su par de claves criptográficas.

Para renovar un certificado tras su revocación, el solicitante deberá acreditar nuevamente su identidad y autenticidad, siguiendo el mismo procedimiento establecido para la solicitud inicial. Asimismo, deberá demostrar fehacientemente a PSC AUTHENTICSING que las razones que motivaron la revocación previa han cesado.

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

La revocación de un certificado suele ser solicitada por el signatario, quien debe ponerse en contacto con la Autoridad de Registro (AR) para programar una cita y presentar su clave de revocación. No obstante, la PC puede establecer procedimientos correspondientes.

En el supuesto de que el titular del certificado electrónico no recuerde la

contraseña de revocación, deberá presentar los documentos exigidos para el tipo de certificado en las oficinas de nuestra entidad

Debido a las restricciones actuales, la renovación de certificados no está disponible a través de medios electrónicos. Es necesario gestionar la solicitud de forma presencial.

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

En este capítulo se detallan los procedimientos técnicos necesarios para gestionar los certificados digitales desde su creación hasta su finalización

14.1 Solicitud de certificados.

Los procedimientos establecidos por la AC de PSC AUTHENTICSING para la recepción y evaluación de las solicitudes de certificados digitales.

14.1.1 Ciclo de vida de los certificados.

La validez de cada certificado listado en la sección **10.1** de la presente DPC será de un año a partir de su emisión.

14.1.2 Procedimiento para la solicitud de certificados y responsabilidades.

Todos los requerimientos para la obtención de un certificado digital deben ser iniciados exclusivamente por el suscriptor del servicio o su representante legal autorizado, de forma directa y completamente en línea a través de nuestra plataforma.

- Proceso Digital para la Obtención de tu Certificado Electrónico: AUTHENTICSING ofrece un proceso 100% online y automatizado para que el usuario obtenga su certificado digital de manera rápida y segura. Para ello es necesario seguir los siguientes pasos:

VI. Acceso e Iniciar Sesión:

VII. Acceder al portal web: www.authenology.com.ve

VIII. Ingresar a la aplicación directamente en: https://app.authenology.com.ve/

IX. Si no hay registro, registrarse y completar el formulario con

los datos solicitados.

- Explorar y Seleccionar:

X. Revisar los diferentes tipos de certificados y planes disponibles. La sección 10.1 de este documento detalla una lista completa de los perfiles a emitir por Authenticsing.

XI. Tipos de Certificados Disponibles (Ejemplos): Certificados de Firma Electrónica (para Persona Natural, Empleado, Representante Legal, Funcionario Público, Profesionales Titulados). Certificados de Servidor (OCSP, SSL, General). Certificados para Seguridad (VPN, Control de Acceso Lógico, Dispositivos Móviles). Certificados para Aplicaciones Específicas (Firma de Software, Transacciones, Factura Electrónica, Banca Electrónica, Cédula Electrónica).

- Completar la Solicitud Online:

XII. Seleccionar el tipo de certificado deseado.

XIII. Envíar los requisitos y la documentación digital solicitada (según el tipo de certificado) directamente a través de la plataforma.

XIV. Aceptar los términos y condiciones del contrato para la adquisición del certificado.

- Validación Automatizada de Identidad:

XV. El sistema realizará una validación de identidad facial en tiempo real utilizando tecnología biométrica, comparando el rostro del usuario con el documento de identidad digital que proporcionó durante el registro. Este proceso es automatizado y no requiere intervención humana ni citas presenciales.

- Emisión del Certificado:

XVI. Una vez completada exitosamente la validación de identidad, el sistema procederá a la generación automática de las claves criptográficas y del certificado digital. Este certificado

será incorporado a la infraestructura de clave pública, y el usuario adquirirá la condición de signatario autorizado.

AUTHENTICSING se reserva la facultad de requerir, a su discreción y a través del sistema, cualquier documentación digital complementaria a la establecida en el Manual de Operaciones, con el fin de corroborar la identidad de los solicitantes de certificados electrónicos de forma automatizada y transparente.

14.1.3 Proceso de firma del certificado.

Para el PSC AUTHENTICSING, el proceso de firma del certificado electrónico sigue el siguiente proceso de firma del certificado:

- **Identificación y autenticación:** Para realizar la solicitud, el solicitante deberá proporcionar la información de identificación personal y/o institucional requerida. En algunos casos, PSC AUTHENTICSING podrá solicitar documentación adicional para verificar y autenticar la identidad del solicitante, de acuerdo con los requisitos establecidos por la Autoridad de Registro (AR).

- **Solicitud de certificado:** El proceso de solicitud de certificado se inicia una vez completada la identificación y autenticación del solicitante. A continuación, se podrá formalizar la solicitud, bien a través de la plataforma digital del PSC AUTHENTICSING o presencialmente en las oficinas.

- **Verificación de la solicitud:** El AR verifica la solicitud y realiza las validaciones necesarias para asegurarse de que la solicitud sea válida.

- **Generación de la clave privada y pública:** El AR genera una clave privada y una clave pública para el solicitante. La clave privada es utilizada por el titular del certificado para firmar documentos electrónicos y la clave pública es utilizada por las partes que desean verificar la autenticidad de la firma digital del titular.

- **Firma del certificado:** El signatario firma digitalmente el certificado utilizando su propia clave privada para garantizar la autenticidad del certificado.

- **Entrega del certificado:** Para facilitar el uso del certificado electrónico,

PSC AUTHENTICSING entregará al titular, en nuestras oficinas, un dispositivo USB con todo lo necesario: el certificado, el software y un manual de instrucciones detallado.

14.1.4 Proceso de generación de la solicitud de renovación de las claves del certificado.

En AUTHENTICSING, todo proceso de renovación de certificados implica obligatoriamente el cambio de claves. Este procedimiento se aplica independientemente del motivo de la renovación.

Para renovar su Certificado Electrónico (CE), se debe seguir los mismos pasos que se realizó en la primera solicitud. Es importante iniciar el proceso de renovación al menos 20 días antes de la fecha de vencimiento indicada en el certificado actual:

- **De manera presencial en las oficinas de AUTHENTICSING:** Para renovar el certificado electrónico, el signatario deberá acudir a la oficina administrativa de AUTHENTICSING y solicitar la renovación. El proceso de renovación seguirá los mismos pasos que una solicitud inicial. La Autoridad de Registro (AR) se pondrá en contacto con el signatario para programar una cita y finalizar el trámite.

- **De forma electrónica por medio del correo electrónico *contacto@authenology.com.ve*:** Para solicitar la renovación de su certificado electrónico, el signatario deberá enviar una solicitud por correo electrónico a la autoridad de registro (AR). Una vez recibida la solicitud, la AR se comunicará con el signatario para programar una cita y llevar a cabo el proceso de generación del nuevo certificado.

- **Proporcionar información de identificación:** Para renovar el certificado, se deberá proporcionar nuevamente la documentación de identificación y cumplir con los requisitos específicos según el tipo de certificado solicitado.

- **Verificar la información y envió de solicitud:** Antes de enviar la solicitud de renovación, el signatario debe verificar que toda la información proporcionada sea correcta. Esto es importante para evitar errores y retrasos en el proceso de renovación. Una vez que se ha completado la solicitud de renovación y se ha verificado la información, se debe enviar la solicitud PSC.

- **Confirmación de cita:** Después de enviar la solicitud de renovación, se debe esperar la confirmación de cita por parte del PSC AUTHENTICSING. En algunos casos, se puede requerir que se proporcione más información o se realice un proceso de verificación adicional antes de otorgar la renovación.

- **Generación del nuevo certificado:** Si la renovación es aprobada, el PSC AUTHENTICSING proporcionará un nuevo certificado con las claves renovadas, cumpliendo con el proceso y protocolo de generación del par de claves.

14.1.5 Procedimiento para realizar una solicitud de renovación de un certificado.

Para renovar un certificado electrónico, los usuarios deberán seguir el mismo procedimiento que se utiliza para solicitar un certificado nuevo.

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

El procedimiento para suspender un certificado está sujeto a variaciones según las características propias de cada caso

La suspensión de un certificado electrónico se realizará a solicitud escrita del signatario o de la alta gerencia de PSC AUTHENTICSING. Únicamente el administrador de AUTHENTICSING podrá tramitar dicha solicitud, la cual deberá ser presentada por alguno de los siguientes medios:

- **De manera presencial en las oficinas de AUTHENTICSING:** Para solicitar la suspensión de su certificado electrónico, el signatario deberá acudir a la oficina administrativa de AUTHENTICSING. Deberá presentar la documentación requerida para su identificación, la cual será verificada por la Autoridad de Registro (AR).

- **De forma electrónica por medio del correo electrónico *contacto@authenology.com.ve*:** El signatario podrá solicitar la suspensión de su certificado electrónico mediante correo electrónico. La Autoridad de Registro (AR) se pondrá en contacto con él para coordinar los procedimientos necesarios.

14.2 Tramitación de solicitud de un certificado

14.2.1 Realización de las funciones de identificación y autenticación

A continuación, se detallan las funciones específicas de la Autoridad de Registro (AR) en el proceso de solicitud de certificados, incluyendo los procedimientos de autenticación.

Los operadores de registro deben utilizar un dispositivo de firma segura (tarjeta de funcionario) para garantizar el acceso controlado a la aplicación y asegurar la integridad y no repudio de todas las operaciones y transacciones realizadas.

La Autoridad de Registro (AR) de Authenticsing se encargará de verificar la identidad y representación de los solicitantes de Certificados de Firma Electrónica. Para ello, los solicitantes deberán presentar la documentación requerida, que será debidamente registrada y conservada por la AR.

14.2.2 Aprobación o denegación de un certificado

Se aprobarán las solicitudes de certificación de aquellas personas naturales o jurídicas que cumplan íntegramente con los requisitos técnicos, económicos y legales establecidos en esta Declaración de Prácticas de Certificación. Todos los certificados emitidos estarán vinculados a la cadena de confianza de la Infraestructura Nacional de Certificación Electrónica, garantizando así su validez y seguridad.

La aprobación o rechazo de una solicitud de firma o certificado electrónico es decisión exclusiva de la Autoridad de Certificación (AC) de PSC AUTHENTICSING. Para ser aprobada, toda solicitud debe ser previamente homologada por la Autoridad de Registro (AR) y cumplir con todos los requisitos establecidos por la AC:

- Validar el pago realizado por el cliente.
- Verificar la información emitida por la Autoridad de Registro (AR).
- Determinar el tipo de certificado requerido y gestionar su emisión ante la Universal Register Authority (URA). Este proceso corresponde al módulo de posterioridad y generación de certificados.

Luego de estar comprobados y logrado con los pasos mencionados con anterioridad, la Autoridad de Certificación (AC) del PSC AUTHENTICSING se

procederá a la firma o certificado electrónico y según sea el caso.

14.2.3 Plazo para la tramitación de un certificado

PSC AUTHENTICSING, tras verificar la documentación presentada para la solicitud de un certificado electrónico, emitirá una respuesta en un plazo máximo de veinte (20) días hábiles.

14.3 Emisión de certificados

14.3.1 Acciones del PSC durante la emisión de un certificado

Una vez aprobada la solicitud por parte de PSC AUTHENTICSING, se procederá a generar y emitir de manera segura el certificado electrónico, el cual será puesto a disposición del solicitante.

PSC AUTHENTICSING emite los certificados digitales. Una vez validada la información del solicitante por la AR, el sistema de certificación inicia automáticamente el proceso de emisión. A través de una conexión segura HTTPS, se solicita a la Autoridad de Certificación la firma de la clave pública correspondiente al certificado. La AC firma el certificado y lo envía al software de certificación usando igualmente la comunicación del https. Posteriormente después de emitir el certificado el suscriptor tendrá que proceder a descargar e instalar.

14.3.2 Notificación al solicitante por parte del PSC acerca de la emisión de su certificado electrónico

El PSC AUTHENTICSING, en su rol de Autoridad de Certificación, notificará al cliente por correo electrónico la fecha y hora para que se acerque a nuestras oficinas a retirar su certificado. En esta cita, se le proporcionará el dispositivo con el certificado almacenado y se le guiará en la generación de su par de claves y el uso del aplicativo para la firma de documentos.

14.4 Aceptación de certificados

14.4.1 Forma en la que se acepta el certificado

El proceso de emisión de un certificado electrónico por parte de PSC AUTHENTICSING culmina con su publicación en el repositorio de infraestructura. Con esta acción, se considera que el signatario ha aceptado los términos y condiciones de uso, habiendo recibido previamente el certificado, el aplicativo para firmas electrónicas y el manual de usuario

14.4.2 Publicación del certificado

El PSC AUTHENTICSING mantiene disponible, con acceso público, el repositorio de publicación de los Certificados Electrónicos el cual podrán ser consultados en la lista de certificados electrónicos (LCR) y también con el Protocolo de estado de certificado en línea (OCSP) en el portal web www.authenology.com.ve

14.4.3 Notificación de la emisión del certificado a otras autoridades

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

14.5 Uso de par de claves y del certificado

14.5.1 Uso de la clave privada del certificado

El PSC AUTHENTICSING no guarda las claves privadas de los certificados emitidos. La custodia, uso y protección de estas claves son responsabilidad exclusiva del titular del certificado.

El titular sólo puede utilizar la clave privada y el certificado para lo cual fue adquirido los usos autorizados y estipulado en la presente DPC.

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

Los terceros de buena fe sólo pueden depositar su confianza en los certificados electrónicos para aquello que establece esta DPC. Los terceros de buena fe pueden realizar operaciones de clave pública de manera satisfactoria confiando en el certificado emitido por la cadena de confianza. Así mismo, deben asumir la responsabilidad de verificar el estado del certificado utilizando los medios que se establecen en esta DPC.

14.6 Renovación del certificado

14.6.1 Causas para la renovación

La principal causa de renovación de un certificado electrónico emitido por PSC AUTHENTICSING es el vencimiento de su plazo de validez.

Las presentes Políticas establecen que PSC AUTHENTICSING no realiza renovaciones de certificados con la misma clave. Cada solicitud de renovación generará un nuevo certificado con una clave distinta. El proceso a seguir es

idéntico al descrito en el apartado 13.1 para la obtención de un certificado inicial.

14.6.2 Entidad que puede solicitar la renovación de un certificado

Bajo las presentes Políticas de Certificación, el PSC AUTHENTICSIG no renueva Certificados electrónicos, manteniendo la Clave pública del mismo.

14.6.3 Procedimiento de solicitud para la renovación de un certificado

Los signatarios deben cumplir nuevamente con el proceso de solicitud de Certificado Electrónicos para solicitar la renovación de un certificado electrónico. Por tal motivo, el procedimiento es el mismo cuando se realiza por primera vez el proceso de un certificado nuevo, el cual se describe en el apartado 13.1.

14.6.4 Notificación de la emisión de un nuevo certificado

Las presentes Políticas de Certificación establecen que PSC AUTHENTICSING no renovará los certificados sin realizar un cambio de clave pública.

AUTHENTICSING notificará por medio de un correo electrónico al signatario la pronta caducidad del certificado electrónico y que requerirá realizar el mismo procedimiento cuando realizo por primera vez el proceso de un certificado nuevo, el cual se describe en el apartado 13.1.

14.6.5 Publicación del certificado renovado por el PSC

Bajo las presentes Políticas de Certificación, el PSC AUTHENTICSIG no renueva Certificados manteniendo la Clave pública del mismo.

14.6.6 Notificación de la emisión del certificado a otras entidades

AUTHENTICSING enviará una notificación por correo electrónico al titular del certificado cuando este esté próximo a expirar, recordándole los pasos a seguir para su renovación, detallados en el apartado 13.1

14.7 Nueva clave del certificado

Bajo las presentes Políticas de Certificación, el PSC AUTHENTICSIG no renueva clave para Certificados Electrónicos, manteniendo la Clave pública del mismo.

14.8 Modificación de certificados

Para garantizar la seguridad y la integridad de las transacciones, los Certificados Electrónicos emitidos por AUTHENTICSING no pueden ser alterados una vez generados. Cualquier modificación implica la solicitud de un nuevo certificado.

14.9 Revocación y suspensión de un certificado

14.9.1 Circunstancias para la Revocación del certificado del signatario

La revocación de un certificado electrónico emitido por PSC AUTHENTICSING C.A. puede producirse por diversas causas, las cuales se detallan a continuación:

- **Compromiso del certificado:** Ante cualquier sospecha de compromiso o vulneración del certificado, es fundamental revocarlo de inmediato para prevenir el uso fraudulento de la información protegida.

- **Cambio de circunstancias:** Si las circunstancias que rodearon la emisión del certificado han cambiado de alguna manera, como la terminación de la relación laboral con la organización para la cual se emitió el certificado, puede ser necesario revocar el certificado para garantizar que la información protegida por el certificado no se utilice de manera inapropiada.

- **Pérdida o robo del dispositivo de seguridad:** Si el dispositivo de seguridad que almacena el certificado se ha perdido o ha sido robado, es importante revocar el certificado para evitar su uso fraudulento y proteger la información protegida por el certificado.

- **Caducidad del certificado:** Una vez caducado el certificado, es fundamental solicitar su revocación para prevenir su uso indebido y garantizar la seguridad de la información

- **Clave privada comprometida:** Si el signatario sospecha que su clave privada ha sido comprometida, debe revocar inmediatamente el certificado para prevenir el uso no autorizado de su identidad digital y proteger la confidencialidad de la información

- **Error en los datos del certificado:** Si se identifica algún error en los datos del certificado, como información incorrecta del titular o de la organización, se debe proceder a su revocación para garantizar la exactitud y confiabilidad de la información asociada.

- **Incapacidad sobrevenida o fallecimiento del signatario:** Ante el fallecimiento o la incapacidad del signatario electrónico.

14.9.2 Entidad que puede solicitar la Revocación

Al verse comprometida la clave del Certificado Electrónico, se rompe la cadena de confianza, en esos casos, las entidades autorizadas para solicitar la revocación del certificado electrónico son:

- La autoridad competente a la conformidad con la LSMDFE
- Un encargado del PSC AUTHENTICSING a quién expresadamente tenga lugar como autoridad para ejecutar la solicitud de suspensión o revocación.
- La decisión de un tribunal por medio el cual se proclame aplicablemente una decisión preventiva o ejecutoria solicitando la revocación de una firma electrónica o certificado electrónico emitido por AUTHENTICSING.

14.9.3 Procedimientos de Solicitud de la Revocación

Para garantizar la seguridad y la integridad de la información, es necesario seguir los siguientes pasos al solicitar la revocación de un certificado electrónico:

- **Proporcionar información de identificación:** Es necesario proporcionar información de identificación adecuada para identificar al titular del certificado y demostrar que se tiene la autoridad para solicitar la revocación del certificado. Esto puede incluir el nombre completo del titular del certificado, la organización a la que pertenece (si corresponde), la dirección de correo electrónico y la información de contacto del solicitante.

- **Proporcionar una justificación para la revocación:** Es importante proporcionar una justificación para la solicitud de revocación del certificado, como la sospecha de compromiso del certificado, la pérdida o el robo del dispositivo de seguridad que almacena el certificado, o un cambio en las circunstancias que rodean la emisión del certificado.

- **Proporcionar documentación de soporte:** Es posible que se requiera documentación de soporte para demostrar la justificación de la solicitud de revocación. Esto puede incluir copias de una denuncia de robo o pérdida, una declaración jurada, o cualquier otra documentación relevante.

- **Realizar la solicitud de revocación.**

14.9.4 Límites del período de la Solicitud de Revocación

El periodo de tiempo para tramitar la solicitud de revocación de un certificado electrónico emitido por el PSC AUTHENTICSING es de tres (3) días hábiles luego de su finalidad o antes de finalizar PSC decretara si el certificado debe ser revocado o restablecido como válido.

14.9.5 Circunstancias para la Suspensión

La suspensión de un certificado electrónico puede ser necesaria en ciertas circunstancias para garantizar la seguridad y la integridad de la información protegida por el certificado. Algunas de las circunstancias comunes para la suspensión de un certificado electrónico son:

- **Compromiso del certificado:** Ante la sospecha de un compromiso del certificado, es fundamental revocarlo de inmediato para prevenir su uso fraudulento y salvaguardar la integridad de la información protegida.

- **Cambio de circunstancias:** Si las circunstancias que rodearon la emisión del certificado han cambiado de alguna manera, como la terminación de la relación laboral con la organización para la cual se emitió el certificado, puede ser necesario revocar el certificado para garantizar que la información protegida por el certificado no se utilice de manera inapropiada.

- **Pérdida o robo del dispositivo de seguridad:** Si el dispositivo de seguridad que almacena el certificado se ha perdido o ha sido robado, es importante revocar el certificado para evitar su uso fraudulento y proteger la información protegida por el certificado.

- **Caducidad del certificado:** Si el certificado ha caducado, es importante revocarlo para evitar su uso fraudulento después de su fecha de vencimiento.

- **Clave privada comprometida:** Si el signatario considera que su clave privada está comprometida, es importante revocar el certificado para evitar su uso fraudulento y proteger la información protegida por el certificado.

- **Error en los datos del certificado:** Si se ha detectado un error en los datos del certificado, como información incorrecta del titular o la organización, puede ser necesario revocar el certificado para garantizar

que la información protegida por el certificado sea precisa y confiable.

- **Incapacidad sobrevenida del signatario:** En caso de que el signatario de un documento electrónico se encuentra incapacitado temporalmente y le sea incapaz de firmar por cualquier razón.

14.9.6 Entidad que puede solicitar la Suspensión

La suspensión de un Certificado Electrónico emitido por PSC AUTHENTICSING podrá ser solicitada por el signatario, la Alta Dirección de Authenticsing, los operadores de la AR o la AC ante el compromiso de la clave privada, las circunstancias descritas en el apartado 13.9.5 o cualquier otro hecho que justifique la revocación según la política de certificación aplicable.

14.9.7 Procedimientos para la Solicitud de Suspensión

La suspensión temporal del certificado implica la pérdida de su validez, impidiendo su uso para cualquier fin. Para solicitar la suspensión, el signatario debe comunicarse telefónicamente al número (+58 – 0212 – 2647658) en el horario establecido (8:30 AM a 12:00 PM y 1:00 PM a 4:30 PM).

Es importante destacar que la suspensión tiene una duración de veinte (20) días, durante los cuales el certificado quedará inhabilitado. Al finalizar este período, el signatario deberá acudir a nuestras oficinas para formalizar la revocación o reactivación del certificado.

14.9.8 Límites del Período de Suspensión de un Certificado

La Lista de Certificados Revocados (LCR) se actualiza cada 24 horas o inmediatamente después de una revocación. Está disponible en todo momento en la página web de AUTHENTICSING (https://www.authenology.com.ve). Además, ofrecemos un servicio OCSP para verificar el estado de los certificados en línea

14.9.9 Frecuencia de Emisión de Listas de Certificados Revocados

La Lista de Certificados Revocados (LCR) se actualiza y publica cada 24 horas, o con mayor frecuencia en caso de revocaciones urgentes. Podrá consultarse en línea a través de la página web de AUTHENTICSING (https://www.authenology.com.ve/). Además, se ofrece un servicio OCSP para verificar el estado de los certificados en tiempo real.

14.9.10 Requisitos para la comprobación de la Lista de Certificados Revocados

La publicación de las Listas de Revocación se realiza en el momento de generación de dichas Listas, por lo que el periodo de latencia o comprobación entre la generación de la LCR y su publicación es prácticamente nulo.

14.9.11 Disponibilidad de comprobación en Línea del Servicio de Revocación del Estado del Certificado

La información sobre el estado de los certificados se encuentra disponible en línea de forma ininterrumpida. En caso de presentarse alguna eventualidad que afecte la disponibilidad del sistema, se activará el Plan de Continuidad del Negocio para restablecer el servicio a la brevedad y garantizar la seguridad de la información.

14.9.12 Requisitos de comprobación en Línea del Estado de Revocación

La comprobación en línea del estado de revocación de los Certificados AC subordinadas o de entidad final puede realizarse mediante el Servicio de información del estado de los certificados, ofrecido a través de OCSP.

14.9.13 Otras Formas Disponibles para la Divulgación de la Revocación

No definidas.

14.9.14 Requisitos para la Verificación de Otras Formas de Divulgación de Revocación

No definidas.

14.9.15 Requisitos Específicos para Casos de Compromiso de Claves

Si AUTHENTICSING sospecha que la clave privada de un Suscriptor ha sido comprometida, empleará todos los medios a su alcance para notificarlo de inmediato. En caso de confirmarse el incidente, se procederá a la revocación del certificado correspondiente, según lo establecido en el apartado 13.9.1, con el fin de proteger la seguridad de la información del Suscriptor.

14.10 Servicio de comprobación de estado de certificados

14.10.1 Características operativas

La comprobación del estado de un Certificado Electrónico se lleva a cabo utilizando los protocolos OCSP y/o CRL. Estos mecanismos proporcionan información actualizada sobre la validez del certificado.

14.10.2 Disponibilidad del servicio

El servicio de comprobación de certificados electrónicos opera de forma continua, con la salvedad de los períodos de mantenimiento programados. Estos no superarán las cuatro (4) horas por mantenimiento ni las treinta y seis (36) horas anuales en total.

14.10.3 Características adicionales

No definidas.

14.11 FINALIZACIÓN DE LA SUSCRIPCIÓN

La extinción de la validez de un Certificado Electrónico, se produce en los siguientes casos:

- El certificado electrónico será revocado en caso de que se cumpla alguna de las condiciones establecidas en el apartado 13.9.1

- Al llegar a su fecha de caducidad

14.12 Custodia y recuperación de la clave

14.12.1 Prácticas y políticas de recuperación de la clave

Con el fin de garantizar la máxima seguridad, la clave privada de la AC de Authenticsing se ha dividido en cinco fragmentos independientes. Para su activación, se requiere la combinación de al menos tres de estos fragmentos, lo que dificulta significativamente su acceso no autorizado.

Para mitigar riesgos, PSC AUTHENTICSING mantiene copias de seguridad de la clave privada de la AC en dispositivos criptográficos, sujetos a estrictos controles de acceso y medidas de seguridad adicionales.

El signatario del Certificado Electrónico CE, generado por PSC AUTHENTICSING, es responsable de la custodia de la clave privada asociada. En caso de pérdida, robo o sospecha de compromiso de esta clave, debe

solicitar de inmediato la revocación del certificado.

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

15.1 Controles de seguridad física

15.1.1 Controles de seguridad física y estructural del PSC.

Con el fin de garantizar la seguridad de la información, PSC AUTHENTICSING mantiene todos sus sistemas críticos en zonas de alta seguridad, protegidos tanto física como lógicamente.

La AC de PSC AUTHENTICSING está diseñada para ofrecer servicios de certificación de manera continua, segura y oportuna, siempre cumpliendo con los más altos estándares de calidad y satisfaciendo las necesidades de sus clientes

El centro de datos se dispone en la sede operacional de la Autoridad de Certificación (AC) AUTHENTICSING y por consiguiente en donde opera la plataforma de emisión de certificados.

Diseñado para garantizar la máxima seguridad, el centro de datos cumple con los estándares internacionales, las leyes venezolanas y las regulaciones de SUSCERTE en materia de protección de datos.

En conjunto con la Gerencia General y el asesor de tecnología de Informática, el equipo de operaciones de PSC AUTHENTICSING se encarga de la gestión, mantenimiento y operación de la plataforma tecnológica de generación de certificados, ubicada en el Centro de Datos Daycohost (Calle Londres, entre Caroní y Nueva York, Torre Dayco, Las Mercedes, Caracas).

El centro de datos opera ininterrumpidamente las veinticuatro (24) horas del día, los trescientos sesenta y cinco (365) días del año, garantizando una autonomía superior a dos meses. Cumple con las más estrictas normas de seguridad antisísmica, contra incendios e inundaciones, y cuenta con un perímetro y siete niveles de acceso controlados.

Cumpliendo con los estándares de seguridad requeridos, el centro de datos de la Autoridad de Certificación dispone de pólizas de seguros que cubren posibles pérdidas o daños que pudieran afectar sus operaciones.

Con el objetivo de asegurar la continuidad de sus operaciones y proteger

los datos de sus clientes, AUTHENTICSING dispone de un centro de datos de respaldo que entrará en funcionamiento en caso de fallas o desastres que afecten al centro principal

15.1.2 Acceso físico.

En cumplimiento con las normativas vigentes, AUTHENTICSING ha implementado rigurosos protocolos de seguridad física, los cuales se detallan a lo largo de este capítulo, demostrando así su compromiso con la protección de sus activos y la información.

Con el fin de reducir significativamente el riesgo de incidentes de seguridad, se han definido perímetros de seguridad diferenciados, cada uno con sus respectivos controles de acceso, para proteger las áreas donde se desarrollan actividades sensibles.

La sede de AUTHENTICSING, estratégicamente ubicada en DAYCOHOST, está protegida por un sistema de seguridad integral que incluye controles de acceso físicos, vigilancia tecnológica avanzada y la colaboración con fuerzas de seguridad especializadas. Esta combinación de medidas garantiza la máxima protección de la infraestructura y los datos de la Autoridad de Certificación. Las salas e instalaciones cuentan con un sistema de seguridad integral que combina controles de acceso perimetrales con múltiples medidas de seguridad interior, como videovigilancia, detección de intrusos y de incendios. Además, se dispone de personal de seguridad para monitorear y responder ante cualquier eventualidad

Para garantizar la seguridad de los equipos, el acceso al interior de los racks se limitará al personal del PSC AUTHENTICSING, debidamente autorizado y controlado. El centro de datos cuenta con las siguientes Características:

- Se dispone de un exhaustivo sistema de controles físicos de personas a la entrada y salida que conforman diversos anillos de seguridad.

- Todas las operaciones críticas del Prestador de Servicios de Confianza se realizan dentro de un recinto físicamente seguro con diversos niveles de seguridad para acceder a las máquinas y aplicaciones críticas.

- Los sistemas están físicamente separados de otros sistemas, de forma que exclusivamente el personal autorizado pueda acceder a ellos y se garantice la independencia de otras redes de propósito general.
- La cerca perimetral fija y determina el ingreso físico a la sede del centro de

datos.

- Se implementa un sistema de vigilancia integral, operando las 24 horas del día, los 7 días de la semana, los 365 días del año. Este sistema combina la presencia de personal de seguridad con tecnología de videovigilancia, permitiendo identificar y registrar el ingreso de equipos portátiles.
- Para acceder al área de servidores, se requiere una triple autenticación de la identidad de cada persona, autorizada previamente por AUTHENTICSING, garantizando así un control estricto del acceso.

- El dispositivo biométrico, sensible al calor y diseñado para autenticar la identidad, tiene como objetivo restringir el acceso al área de servidores únicamente al personal autorizado y acompañado cuando sea necesario por técnicos o personal de operaciones.

- El carnet magnético de seguridad es el único medio válido para acceder al área de control de servidores. Este dispositivo garantiza que solo el personal autorizado, debidamente identificado, pueda ingresar a esta zona restringida.

- Para garantizar la seguridad del cuarto de servidores, el acceso está restringido y controlado por operadores autorizados. Estos verifican la identidad de las personas y mantienen un registro detallado de los accesos.

- El personal de AUTHENTICSING es el único autorizado a acceder al rack de servidores, siendo responsables de la custodia y seguridad de los equipos y de la Autoridad de Certificación.

- El acceso a los servidores de AUTHENTICSING está restringido a personal autorizado mediante un sistema de seguridad en la puerta del rack, garantizando así la protección de la plataforma de certificación.

15.1.3 Suministro de electricidad y acondicionador de aire.

El rack donde se encuentra instalados los servidores de la plataforma de certificación de la Autoridad de Certificación (AC) AUTHENTICSING cuenta con dos (2) líneas de tensión diferentes, una general o principal y otra auxiliar, las líneas de tensión están unidas a dos (2) sistemas de alimentación ininterrumpida (UPS “Uninterruptable Power Supply”), por lo tanto, a su vez están unidas a dos (2) plantas productoras y generadoras de energía eléctrica.

La distribución eléctrica garantiza un suministro continuo, incluyendo la energía necesaria para el funcionamiento del aire acondicionado. A continuación, se presenta un diagrama que ilustra de forma esquemática las conexiones eléctricas del sistema:

Imagen #2

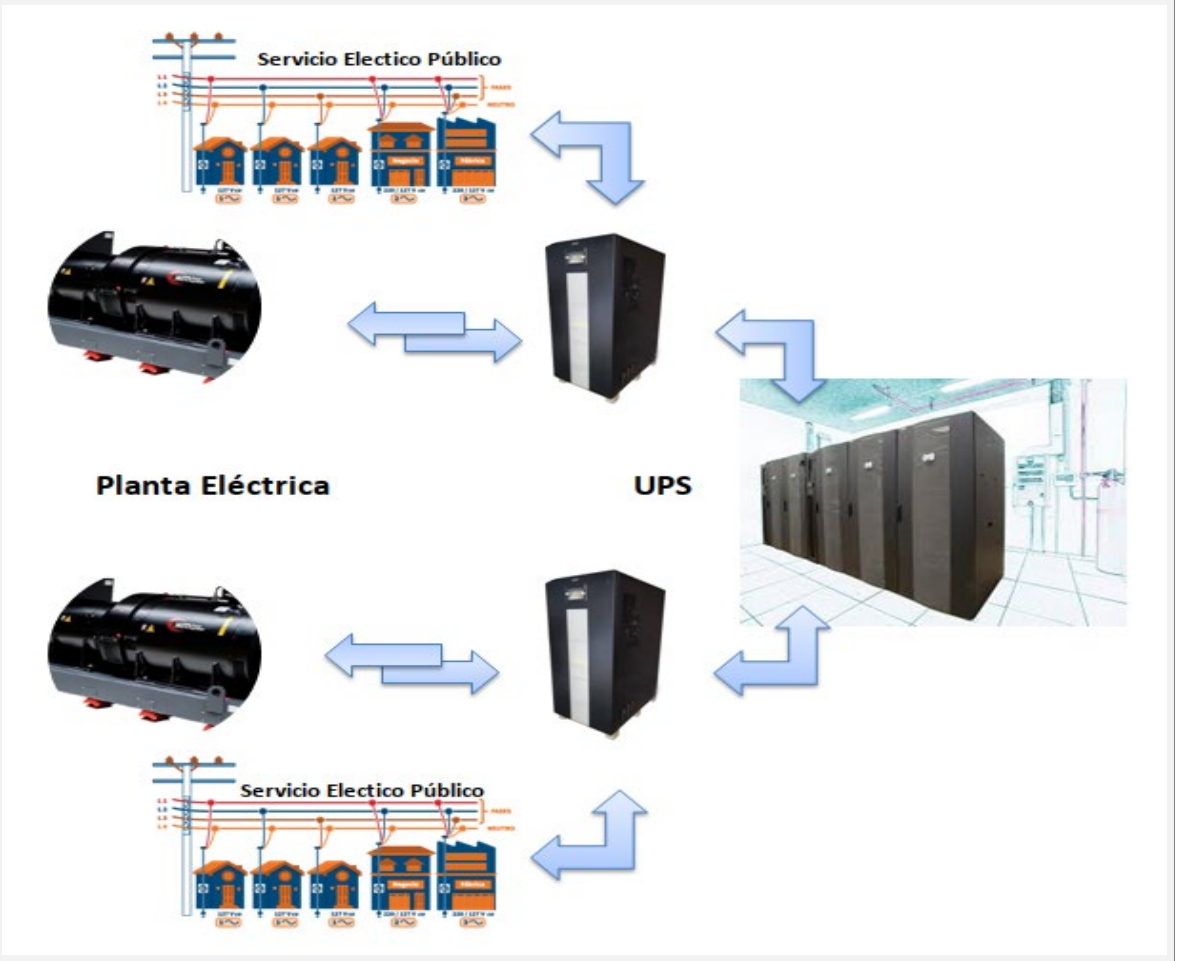


Diagrama del sistema de alimentación eléctrica.

15.1.4 Exposición de agua

Diseñado para garantizar la máxima seguridad, nuestro centro de datos opera en estricta conformidad con los estándares internacionales de seguridad de la información, las leyes venezolanas y los requerimientos de SUSCERTE.

15.1.5 Protección y prevención de incendios

El centro de datos cumple cabalmente con todos los requisitos operativos establecidos en la normativa internacional de seguridad de la información, la legislación venezolana y las disposiciones específicas de SUSCERTE.

Dispone de sistemas redundantes de detección y extinción de incendios, tanto para equipos como para infraestructura de red.

15.1.6 Sistemas y técnicas de almacenamiento.

El centro de datos reúne y mantiene cada uno de los requisitos de operación, para este tipo de compresibilidad informa la normativa internacional en tema de seguridad asociada a la tecnología de información, la ley de la república bolivariana de Venezuela y las normas impuesta por SUSCERTE.

15.1.7 Sistemas de almacenamiento

El centro de datos reúne y mantiene cada uno de los requisitos de operación, para este tipo de compresibilidad informa la normativa internacional en tema de seguridad asociada a la tecnología de información, la ley de la república bolivariana de Venezuela y las normas impuesta por SUSCERTE.

El centro de datos DaycoHost alberga la información del PSC AUTHENTICSING en sistemas de almacenamiento redundantes y cifrados. Toda documentación se encuentra protegida y almacenada en servidores seguros, cumpliendo con los estándares de seguridad establecidos.

15.1.8 Eliminación de residuos

En cumplimiento con las normativas de seguridad de la información, PSC AUTHENTICSING implementa procedimientos de eliminación de residuos diseñados para garantizar la destrucción completa y definitiva de datos confidenciales, evitando cualquier posibilidad de recuperación.

15.1.9 Almacenamiento de copias de seguridad

Las copias de seguridad se encuentran encriptadas y almacenadas en un entorno seguro y externo a nuestras instalaciones, específicamente en Daycohost. Este almacenamiento cumple con los estándares internacionales como la ISO/IEC 27001 e ISO/IEC 27002, garantizando la protección de los datos contra cualquier tipo de acceso no autorizado o daño.

16. CONTROLES DE PROCEDIMIENTOS

16.1 Definición de roles confiables

La Autoridad de Certificación (AC) y Autoridad de Registro (AR) mantendrán y guardarán un esquema o diseño de administración y operación apoyado en una estructura plana, respaldada y reforzada sobre la interrelación e interdependencia del equipo en sus diversos roles y funciones. La operación regular del PSC AUTHENTICSING será dividida en funciones del procedimiento y administración.

La alta dirección se establece en el nivel con mayor poder de decisión y mando dentro de la organización. Las actividades de operación y administración serán coordinadas por el Gerente general y el asesor de tecnología del PSC AUTHENTICSING, lo cual comunicarán directamente a la alta dirección.

La administración, monitoreo y seguimiento continuos de la plataforma tecnológica de certificación serán responsabilidad del equipo de operadores de informática, bajo la supervisión del encargado designado por la gerencia general y el consultor de tecnología.

El equipo de operadores de informática estará incorporado por un total de hasta cuatro (4) operadores, por lo cual estarán en capacidades de atender y solucionar cada uno de los requerimientos operacionales de la plataforma tecnológica de certificación.

Se asignará un encargado específico para la gestión de la Autoridad de Registro (AR). Este encargado, junto con un asistente administrativo, reportarán al Gerente General y se encargarán de las operaciones diarias de la AR, incluyendo la atención al cliente, la gestión financiera y el mantenimiento de los recursos.

16.1.1 Cifra de personas requeridas por rol.

La estructura interna generada por AUTHENTICSING se divide de la siguiente manera:

Gerente General (1)
Unidad de Asesoría Legal
Departamento Técnico - Legal
Abogado Junior
Abogado Semi Senior

Abogado Senior

Auditor (2)
Organización y Método

Coordinación de Administración (1)
Unidad de Talento Humano
Unidad de Comercialización

Coordinador de la Infraestructura de la clave Pública (1)
Operadores AC (1)
Operadores AR (1)

Coordinador de Seguridad de la Información y Plataforma (1)
Analista de Seguridad de la Información
Analista de Diseño y Desarrollo de Soluciones

Coordinación de Plataforma y Soporte a Usuarios (1)
Analista de Administración de la Plataforma
Analista de Soporte Técnico

16.1.2 Identidad y autenticación de cada rol.

La identidad y autenticación de cada rol, así como el establecimiento de nuevas responsabilidades corresponderá a la Alta Dirección del PSC AUTHENTICSING.

17. CONTROLES DE SEGURIDAD PERSONAL

17.1 Petición de antecedentes, calificación, experiencia y acreditación.

Para asegurar la calidad y confiabilidad de los servicios de la Infraestructura de

Clave Pública (ICP), PSC AUTHENTICSING somete a todo su personal operativo a rigurosos procesos de selección y verificación de antecedentes. La gestión de la ICP se encuentra bajo el control directo de la alta dirección.

El personal involucrado en el control y la operación de la Infraestructura de Clave Pública (ICP) estarán suficientemente entrenados para cumplir con cada una de las funciones asignadas a su rol y recibirá entrenamiento continuo para garantizar y asegurar los niveles sobre las políticas de seguridad. El proceso llevado a cabo de adiestramiento y desarrollo del personal se regulará por el documento de la política de adiestramiento y desarrollo del personal de AUTHENTICSING.

17.2 Requerimientos de formación para los miembros del personal.

Para garantizar la seguridad de la ICP, el acceso a sus componentes está estrictamente controlado y limitado al personal autorizado y capacitado. Todas las operaciones se llevan a cabo bajo supervisión y se documentan de manera detallada. Los procedimientos operativos son revisados regularmente para adaptarse a los nuevos requerimientos y mantener los más altos estándares de seguridad.

17.3 Sanciones por acciones no autorizadas.

Para garantizar el cumplimiento de las normas establecidas, todos los procedimientos deben ajustarse a lo dispuesto en la DPC y la PC. Cualquier desviación requiere autorización previa de la alta dirección. El incumplimiento de esta disposición será sancionado conforme a las normas internas.

18. PROCEDIMIENTOS DE CONTROL DE SEGURIDAD

18.1 Tipos de eventos registrados

EL PSC AUTHENTICSING, almacena cada registro electrónico de eventos (logs) referente a su actividad como PSC. Estos registros son almacenados de forma automática, electrónica y en los casos del acceso físico en formato papel y otros medios.

Todos los eventos registrados deben incluir, como mínimo, la fecha y hora de ocurrencia, un número de serie único, una descripción detallada del evento y la identificación del sistema o usuario que lo generó. Esta información es fundamental para cumplir con los requisitos mínimos de auditoría y aplican:

- Eventos de cada equipo que conforman la plataforma:
  - Instalación y configuración del sistema operativo.

- ❖ Instalación y configuración del módulo criptográfico.
- ❖ Accesos o intentos de acceso al equipo.
- ❖ Actualizaciones.
- ❖ Realización de copias de seguridad
- ❖ Instalación y configuración de cualquier aplicación instalada en el equipo.
- ❖ Instalación y configuración de la Autoridad de Certificación(AC).

➢ Eventos del software de certificación:

- ❖ Gestión de roles.
- ❖ Gestión de plantillas de certificados.
- ❖ Lista del control de acceso (LCA).
- ❖ Gestión de certificados (todo lo considerado en el periodo de dicho certificado).
- ❖ Gestión de usuarios.
- ❖ Eventos con relación al acceso físico.
- ❖ Acceso del personal a los equipos y sistemas.
- ❖ Acceso del personal al centro de datos.
- ❖ Eventos de acciones correctivas.
- ❖ Errores de hardware.
- ❖ Errores de software.

18.2 Regularidad de procesados de registros de logs.

Los registros de auditoría se ejecutan en cualquier momento que se realice una operación en la raíz de certificación de la Autoridad de Certificación (AC) del PSC AUTHENTICSING, de lo contrario la raíz de certificación de la Autoridad de Certificación (AC) se mantiene fuera de línea.

El equipo de operaciones comunica a su administrador de seguridad cuando un proceso o acción causa un incidente crítico de seguridad o discrepancia. A las entidades Infraestructura de Clave Pública (ICP) subordinadas (cuando aplique) también se les requiere comunicar cualquier tipo evento que pueda causar un incidente crítico de seguridad o discrepancia. En todo caso, la gerencia principal y el consultor de tecnología decidirán los pasos que se deban seguir.

18.3 Período de retención para los logs de auditoría.

Cada registro de Auditoría se retiene por un período de diez (10) años.

18.4 Protección de los logs de auditoría.

El sistema de auditoría de AUTHENTICSING es un conjunto de procedimientos que involucran tanto componentes tecnológicos (como la raíz de certificación y sistemas operativos) como recursos humanos (personal operacional) para verificar y validar la información relacionada con los certificados digitales.

Para garantizar la seguridad de los datos, el sistema cuenta con estrictos controles de acceso y separación de funciones en el software y hardware utilizados para la recolección automática. Además, los procedimientos operativos para el manejo de estos sistemas son altamente confidenciales y solo son conocidos por el equipo de la Autoridad de Certificación de PSC AUTHENTICSING. La integridad de las auditorías se verifica mediante la firma digital de cada evento, asegurando la trazabilidad de las acciones realizadas.

19. ARCHIVO DE INFORMACIONES Y REGISTROS

- Los records de la Infraestructura de Clave Pública (ICP) de la Autoridad de Certificación (AC) del PSC AUTHENTICSING relacionados a la operación de sus funciones y servicios de certificación son archivados y retenidos por un tiempo exacto o mínimo de veinte (20) años.

- La raíz de certificación de AUTHENTICSING cuenta con un sistema de seguridad robusto que incluye verificaciones diarias independientes de sus recursos. Todos los registros de actividad se almacenan con marca de tiempo y se mantienen bajo estricto control de acceso, sujetos a auditorías regulares.

- Cada uno de los archivos de records e información de identificación deberán ser archivados directamente por la Autoridad de Registro (AR) del PSC AUTHENTICSING.

- La Autoridad de Registro (AR) se compromete a conservar los registros e información relacionados con los certificados durante un mínimo de diez años a partir de su fecha de vencimiento. La AR empleará todos los medios a su alcance para garantizar el cumplimiento de esta obligación, ya sea a través de archivos físicos o electrónicos.

19.1 Tipo de informaciones y eventos registrados

El tipo de información y registro de eventos será el mismo contemplado en el punto “Tipos de eventos registrado (19.1)” del actual documento de Declaración de

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

19.2 Período de retención para el archivo.

El período de retención para archivo será el mismo contemplado en el punto "Protección de los logs de auditoría", del actual documento de Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC).

19.3 Protección del archivo.

Para cada uno de los métodos de protección de archivo será el mismo contemplado en el aparte "Protección de los logs de auditoría", del actual documento de Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC).

19.4 El Requerimiento para el estampado de tiempo para el registro.

Al no existir una regulación detallada por parte de SUSCERTE en cuanto a los procesos de estampado de tiempo, PSC AUTHENTICSING cuenta con la flexibilidad para diseñar y desarrollar sus propios procedimientos. Esto le permite adaptar los procesos a las necesidades específicas del servicio y a los estándares de seguridad más actualizados.

19.5 Sistema de repositorio de archivos de auditoría (interno vs externo).

Los equipos presentes en la plataforma de certificación poseen un módulo para almacenar los logs de eventos, específicamente eventos de las aplicaciones, de los sistemas y de seguridad, incluyendo el aplicativo de certificación.

Este registro de eventos facilita la auditoría y verificación de todas las acciones realizadas en el sistema, incluyendo intentos de acceso no autorizados y operaciones que puedan comprometer la seguridad de los datos. Además, se mantiene una copia de seguridad de estos registros en la nube para garantizar su integridad y disponibilidad.

20. CAMBIO DE CLAVE

El esquema de operación del PSC AUTHENTICSING y su plataforma tecnológica de certificación se encuentran completamente configurados para que el cliente produzca su par de claves (pública y privada). Siempre y en todo caso el compromiso de clave derivará del mismo cliente, AUTHENTICSING no producirá el par de claves (pública y privada).

En caso de pérdida de la clave privada, el cliente deberá solicitar un nuevo

certificado, cumpliendo nuevamente con el proceso de contratación establecido por el PSC. La clave pública, por su parte, permanecerá almacenada en el repositorio, según lo indicado en el punto 15.2 de la DPC y PC.

21. PLAN DE RECUPERACIÓN EN CASO DE DESASTRES

21.1 Procedimientos de Gestión de Incidentes y Vulnerabilidades

El Plan de Recuperación ante Desastres (PRD) de PSC AUTHENTICSING tiene como objetivo garantizar la continuidad del servicio en caso de emergencias. El Comité de Continuidad del Negocio evaluará y clasificará cualquier incidente que afecte las operaciones, activando el Plan de Contingencia correspondiente.

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

PSC AUTHENTICSING ha establecido un protocolo de contingencia y recuperación ante desastres para garantizar la continuidad de sus servicios en caso de afectaciones a su Infraestructura de Clave Pública (ICP). Este plan es evaluado regularmente para adaptarse a los cambios en el entorno de riesgo.

- Desastres naturales y terminación.
- Fallas/corrupción de recursos de computación;
- Compromiso de la Integridad de la Clave (Pública y Privada).

La alta dirección, representada por un director, el Gerente general, el consultor de tecnología y los equipos de operadores de informática, deben tomar en consideración los correctivos y emprender con cada una de las actividades requeridas y necesarias para restaurar o mejorar la plataforma tecnológica de certificación en el momento de presentarse un incidente o evento de desastre. En el plan de continuidad de negocio y recuperación ante desastre o accidentes, se especificará cada procedimiento y ejecución a realizar en cada uno de los escenarios considerados como desastre y a continuación se mencionan los principales compromisos de cada uno de los cargos a la hora de ejecutarse el plan de recuperación:

- Un director junto al gerente general declara el escenario de desastre y aprueban la activación del plan de contingencia.
- El consultor de tecnología gestiona, supervisa y apoya la ejecución de todas las actividades de recuperación del desastre
- Los operadores ejecutan las actividades de restauración del servicio.

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

AUTHENTICSING ha establecido un protocolo de seguridad para activar el HSM (Hardware Security Module) de forma local, únicamente en presencia del consultor de tecnología y el Gerente general. Este procedimiento, considerado un escenario de desastre, se activará en caso de un posible compromiso de la clave privada.

Una vez confirmado el riesgo, se procederá a implementar las siguientes acciones correctivas:

- Comunicar a la compañía aseguradora que mantiene la fianza de operación del PSC.
- Examinar el motivo del compromiso, y realizar un informe técnico detallando cada una de las razones por las que se vio comprometida la clave privada del PSC AUTHENTICSING.
- Determinar junto con SUSCERTE las acciones que se deben tomar para la reactivación del servicio de emisión de certificados.
- Declaración de PSC AUTHENTICSING del escenario de desastre.
- Comunicado a SUSCERTE del compromiso de la clave, para la inmediata revocación del certificado de AUTHENTICSING.
- Publicación del evento en la Página Web de AUTHENTICSING.
- Comunicar a los clientes del PSC AUTHENTICSING vía correo electrónico

21.4 Seguridad de las instalaciones tras un desastre natural o de otro tipo.

El centro de datos desde donde opera la Autoridad de Certificación (AC) mantiene las pólizas o instrumentos emitidos por empresas de seguros solventes y reconocidos, a los efectos de mantener un respaldo en caso de alguna ocurrencia de contingencia que afecte la integridad física de la referida sede administrativa y pueda ofrecer una seguridad y garantía de su continuidad operacional.

Aun así, AUTHENTICSING ha previsto medidas para asegurar la continuidad de sus operaciones, como la contratación de un centro de datos alternativo con el que tiene un convenio, en caso de que el centro de datos principal de Daycohost sufra daños irreparables o se vea afectado por algún desastre.

22. CESE DE LAS ACTIVIDADES DEL PSC.

El PSC AUTHENTICSING ha establecido un plan de contingencia que incluye las siguientes medidas en caso de una suspensión temporal o definitiva de sus actividades:

- Finalidad por vencimiento de acreditación.
- Finalidad por cese de operaciones.
- Finalidad por revocación de acreditación. En este caso, y solo por razones comprobadas de incumplimiento, llevará a cabo la ejecución de la garantía y seguridad solicitada por SUSCERTE al momento de la acreditación
- Finalidad derivada de aspectos tecnológicos.

En el tal caso de alguna ocurrencia de cualquier de las premisas antes mencionados el PCS AUTHENTICSING, estará en toda la obligación de colocar a disposición de SUSCERTE el repositorio de todos los certificados emitidos durante su gestión, incluyendo la condición de cada uno de ellos.

23. CONTROLES DE SEGURIDAD TÉCNICA

23.1 Entrega de la clave privada.

El proceso de generación de pares de claves en AUTHENTICSING se realiza mediante un dispositivo de seguridad de hardware (HSM) certificado bajo el estándar FIPS 140-2 Nivel 3. Si bien AUTHENTICSING cuenta con esta infraestructura para generar sus propias claves, el diseño de la plataforma está configurado para que el cliente sea el encargado de generar su par de claves, asegurando así la independencia y control del proceso por parte del usuario final.

En caso de pérdida de la clave privada por parte del cliente, se emitirá un nuevo certificado, supeditado al cumplimiento de los procedimientos contractuales establecidos con el Prestador de Servicios de Certificación (PSC). La clave pública, por su parte, permanecerá almacenada en el repositorio, conforme a lo dispuesto en la Declaración de Prácticas de Certificación (DPC) y la Política de Certificados (PC).

23.2 Entrega de la clave pública

El modelo operativo de PSC AUTHENTICSING establece que el cliente es el único responsable de generar su par de claves criptográficas. En consecuencia, en caso de pérdida o compromiso de la clave privada, el cliente deberá solicitar un nuevo certificado, cumpliendo nuevamente con los procedimientos de contratación establecidos.

23.3 Disponibilidad de la clave pública

AUTHENTICSING se encuentra en la obligación de mantener en su repositorio y disponible su clave pública, la cual cualquier cliente o parte interesada puede

acceder a través de la página Web de AUTHENTICSING https://www.authenology.com.ve

23.4 Tamaño de las claves.

La Autoridad de Certificación emplea módulos raíz que utilizan claves de 384 bits basadas en el algoritmo de curva elíptica.

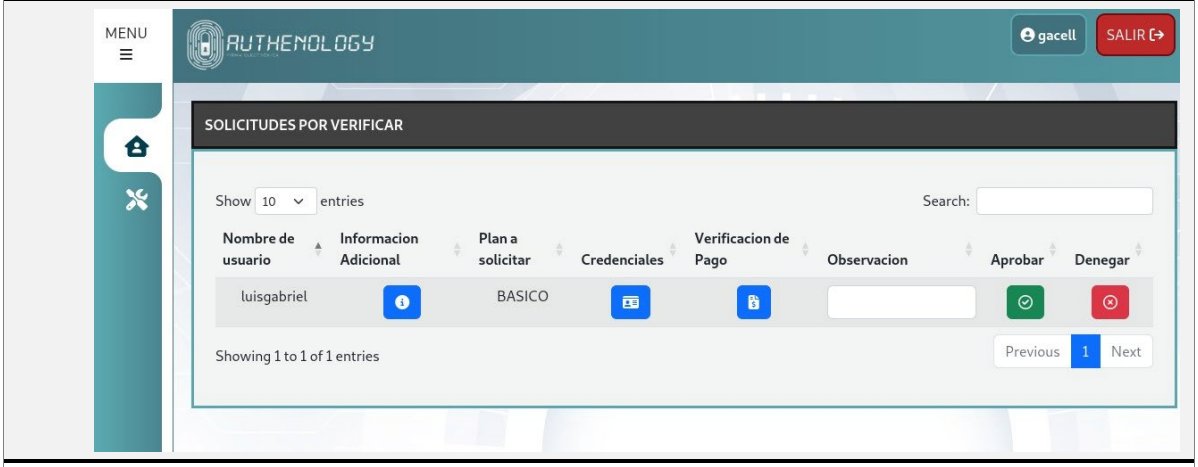
23.5 Parámetros de generación de la clave pública y verificación de la calidad.

Las claves públicas que se generan cumplen con los estándares de seguridad más altos (FIPS 140-2 Nivel 3). Aunque el proceso es sencillo, requiere seguir medidas de seguridad específicas.

A continuación, se detallan los procedimientos para generar el par de claves criptográficas, así como las medidas de seguridad indispensables para salvaguardar la clave privada:

- El usuario final debe ingresar a la página web del PSC AUTHENTICSING www.authenology.com.ve y presionar clic sobre el enlace sistema de certificación https://app.authenology.com.ve y de esta manera podrá ingresar al sistema de certificación.
- Allí debe de verificar que los datos contenidos están correctos, esta solicitud está compuesta en cuatro (04) partes:

Imagen # 3



Esquema de Operación

- Información del Usuario: Este punto contiene el nombre y apellido del usuario que fue proporcionado al PSC AUTHENTICSING.
- Subject: Información general del usuario que dependiendo del tipo de certificado algunos puntos serán obligatorios. A continuación, se nombrara en lista los puntos, y cuáles son los obligatorios por certificados:

Tipo de Certificado	Nombre	Organización	SerialNum-ber(DN)	dNSName	Titulo	Email	País	Identificador de documento
Representante legal de la empresa privada	✓	✓			✓		✓	
Representante legal de la empresa publica	✓	✓			✓		✓	
Empleados de empresa (Privada y público)	✓	✓	✓		✓	✓	✓	✓
Profesional titulado	✓	✓	✓		✓	✓	✓	✓
Persona natural	✓					✓	✓	✓
Funcionario Publico	✓	✓	✓		✓	✓	✓	✓
Factura Electrónica	✓	✓	✓				✓	
OCSP	✓	✓					✓	
SSL	✓	✓					✓	
VPN	✓	✓					✓	
Firma de software	✓	✓	✓				✓	
Firma de transacción	✓	✓	✓				✓	
Control de acceso lógico	✓	✓		✓			✓	
Dispositivos móviles	✓		✓				✓	
Servidor	✓	✓	✓			✓	✓	
Cédula electrónica	✓		✓				✓	
Banca Electrónica	✓	✓					✓	

De acuerdo con la Norma SUSCERTE N° 032, los campos obligatorios seleccionados varían en función del tipo de estructura de certificación elegida.

- Información del nombre alternativo: En esta sección debe de contener el número de RIF o C.I. del signatario.
- Opciones de clave: En esta sección es requerido escoger el Proveedor de Servicios Criptográfico (CSP), es importante tomar en

cuenta que, si el certificado se va a instalar en un Etoken criptográfico, los drivers del dispositivo deben de estar instalados previamente en el equipo que se va a utilizar para generar el par de claves (Pública y Privada) del usuario. Seguidamente, el usuario debe aceptar los términos y condiciones para habilitar el botón "Generar". Luego de presionar el botón "Generar", el usuario tendrá la opción de proteger su clave privada con un nivel de seguridad alto utilizando una contraseña segura. Seguido a la aprobación de la solicitud por la Autoridad de Certificación (AC) del PSC AUTHENTICSING enviará al correo del usuario un link donde logrará descargar el certificado. El procedimiento de generación de par de claves mencionado, asegura y garantiza la privacidad de la clave privada del usuario, ya que el usuario es quien la genera, el PSC AUTHENTICSING solo garantiza la vinculación del individuo con la clave pública, dicha clave pública está asociada a su vez a la clave privada.

23.6 Hardware/software de generación de claves.

PSC AUTHENTICSING emplea una solución híbrida para la generación de pares de claves y certificados. Esta solución combina la Autoridad de Certificación (AC) de Microsoft con software especializado. La seguridad de la clave privada de la AC se garantiza mediante un módulo de seguridad de hardware (HSM) YUBIHSM2 con certificación FIPS 140-2. Las especificaciones técnicas detalladas de este dispositivo se adjuntan:

23.6.1 Algoritmos Criptográficos soportados.

- Cryptographic interfaces (APIs):
  - XVII. Microsoft CNG (KSP)
  - XVIII. PKCS#11 (Windows, Linux, macOS)
  - XIX. Native YubiHSM Core Libraries (C, python)

- Cryptographic capabilities:
  - XX. Hashing (used with HMAC and asymmetric signatures)
  - XXI. SHA-1, SHA-256, SHA-384, SHA-512

- RSA:
  - XXII. 2048, 3072, and 4096 bit keys
  - XXIII. Signing using PKCS#1v1.5 and PSS
  - XXIV. Decryption using PKCS#1v1.5 and OAEP

- Elliptic Curve Cryptography (ECC):
  - XXV. Curves: secp224r1, secp256r1, secp256k1, secp384r1, secp521r, bp256r1, bp384r1, bp512r1, curve25519
  - XXVI. Signing: ECDSA (all except curve25519), EdDSA (curve25519 only)
  - XXVII. Decryption: ECDH (all except curve25519)

- Key wrap:
  - XXVIII. Import and export using NIST AES-CCM Wrap at 128, 196, and 256 bits

- Random numbers:
  - XXIX. On-chip True Random Number Generator (TRNG) used to seed NIST SP 800-90 AES 256 CTR_DRBG

- Attestation:
  - XXX. Asymmetric key pairs generated on-device may be attested using a factory certified attestation key and certificate, or using your own key and certificate imported into the HSM

23.6.2 Referencias.

Para proteger la información de nuestros usuarios, la Autoridad de Certificación utiliza un dispositivo de seguridad especial (módulo criptográfico Yubico https://www.yubico.com/products/hardware-security-module/) capaz de generar claves muy seguras y de proteger los datos mediante firmas digitales y cifrado.

23.7 Propósitos de utilización de claves:

La Clave de privada del PSC AUTHENTICSING puede ser utilizada para:

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

24. PROTECCIÓN DE LA CLAVE PRIVADA.

24.1 Estándares para los módulos criptográficos.

La infraestructura de clave pública (ICP) de PSC AUTHENTICSING emplea un módulo criptográfico con certificación FIPS nivel 3. Este módulo, especialmente el que protege la raíz de certificación, se mantiene en un entorno aislado para garantizar la seguridad.

24.2 Control "N" de "M" de la clave privada:

La clave privada de PSC AUTHENTICSING se encuentra protegida bajo un sistema de custodia compartida. Para su habilitación, es necesario ejecutar un procedimiento de inicialización del software de la AC que involucra la participación conjunta de operadores de la AC, administradores del HSM y usuarios del sistema operativo. Este es el único método autorizado para activar dicha clave.

24.3 Custodia de la clave privada.

La seguridad de la clave privada de la Autoridad de Certificación está garantizada mediante su almacenamiento en un HSM. El proceso de instalación de este dispositivo ha sido establecido por la AC y se describe a continuación:

- Instalación de los drivers: Se necesitará instalar los drivers respectivos al HSM en el servidor de certificación (CA).
- Instalación física
- Creación del Mundo de Seguridad. Se creará el Mundo de Seguridad bajo los comandos establecidos.
- Se crearán los perfiles y roles dentro del mundo de seguridad.

24.4 Copia de seguridad de la clave privada.

El respaldo de la clave privada se realiza en dos (2) unidades de CD/DVD (la principal y la de respaldo) selladas con un precinto y almacenadas en una caja de seguridad. La clave de cifrado de la raíz de certificación del PSC AUTHENTICSING solamente se respalda para los fines de recuperación ante Desastres.

24.5 Archivo de la clave privada.

La clave privada de la Autoridad de Certificación (AC) está protegida en un dispositivo de seguridad de hardware (HSM). Este dispositivo no solo almacena la clave, sino que también la cifra y crea copias de seguridad. Para garantizar su máxima protección, estas copias de seguridad se guardan en cintas magnéticas y se almacenan en una ubicación externa y segura, fuera del centro de datos.

24.6 Inserción de la clave privada en el módulo criptográfico.

Se han establecido los parámetros de generación de claves, según lo dispuesto por la Autoridad de Certificación, los cuales son los siguientes:

- Se generará el nuevo mundo de seguridad.
- Se instalará la autoridad de certificación bajo la modalidad de Subordinada y se generará la petición de certificado.
- SUSCERTE firmará la solicitud del certificado del PSC AUTHENTICSING.
- Se instalará y activará el certificado del PSC AUTHENTICSING.

24.7 Método de activación de la clave privada.

Para la activación de la clave privada es requerido y necesario utilizar tarjetas inteligentes, requiere dos de cuatro tarjetas de administrador y una de dos tarjetas de operador, es necesario el acceso al sistema operativo del servidor de certificación.

24.8 Método de destrucción de la clave privada.

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.

24.9 Ranking del módulo criptográfico.

La AC emplea un HSM YUBIHSM2 con certificación FIPS 140-2 para el almacenamiento seguro de su clave privada, garantizando así la integridad y confidencialidad de las operaciones criptográficas.

Estos dispositivos son equipos de máxima seguridad, utilizados por bancos y agencias gubernamentales de todo el mundo gracias a su eficacia y confiabilidad demostrada.

25. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES.

25.1 Archivo de la clave pública.

La clave pública del PSC AUTHENTICSING es archivada según el formato PKCS#7, por un tiempo de diez (10) años.

25.2 Períodos operativos de los certificados y período de uso del par de claves.

El certificado emitido por PSC AUTHENTICSING tendrá una vigencia máxima de diez (10) años. Las firmas digitales y los certificados electrónicos generados bajo

este certificado tendrán una validez de un año a partir de su activación, siendo el mismo plazo de vigencia aplicable al par de claves criptográficas asociado.

26. DATOS DE ACTIVACIÓN.

26.1 Generación e instalación de datos de activación.

La seguridad de los certificados digitales de la AC de AUTHENTICSING comienza con la generación segura del par de claves, un proceso que requiere seguir protocolos específicos.

A continuación, se describirá el proceso de generación de claves y se destacarán las medidas de seguridad esenciales para proteger la clave privada:

- La Autoridad de Registro verifica la identidad del usuario y envía los datos a la Autoridad de Certificación para que esta vincule la identidad con la clave pública del usuario en el sistema.

- El proceso de obtención de un certificado electrónico inicia al acceder a la página web de AUTHENTICSING (https://www.authenology.com.ve/). Allí, el usuario debe seguir estos pasos: hacer clic en 'Certificados Electrónicos', seleccionar el sistema de certificación correspondiente y completar el registro.

- Tras completar el registro, deberá autenticarse en el sistema de solicitudes con su nombre de usuario y contraseña, y confirmar su correo electrónico.

- Tras validar tu correo electrónico, deberás acceder al módulo de certificados para iniciar la solicitud. Selecciona la opción de "certificado de firma electrónica", proporciona la información personal requerida y elige el proveedor de servicios de cifrado que prefieras. Finalmente, pulsa el botón "Generar" para iniciar el proceso de emisión.

Importante: Es fundamental garantizar la seguridad del equipo o dispositivo donde se genera la solicitud del certificado, ya que este será el lugar donde se almacene.

Al hacer clic en "Generar", se produce un par de claves criptográficas (pública y privada) y se inicia automáticamente la solicitud de certificación, la cual requiere la confirmación presencial de la identidad del solicitante ante la autoridad de registro.

AUTHENTICSING se encarga de vincular la identidad del usuario con su clave pública, sin tener acceso a la clave privada generada por el usuario, lo que garantiza

la privacidad de esta última.

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

26.2 Protección de datos de la activación.

La activación del certificado emitido, es realizado mediante el sistema de certificación del PSC AUTHENTICSING, limitándose en el equipo o el dispositivo donde se hayan generado el par de claves (Pública y Privada).

27. CONTROLES DE SEGURIDAD DEL COMPUTADOR.

27.1 Requisitos técnicos específicos.

A fin de garantizar la seguridad de la información, PSC AUTHENTICSING ha implementado controles de seguridad en los equipos informáticos, tales como políticas de uso, controles de acceso, auditorías, mecanismos de autenticación multifactor, pruebas de intrusión y planes de recuperación ante desastres.

27.2 Calificaciones de seguridad computacional.

Con el fin de asegurar la integridad de las operaciones criptográficas, se utilizan equipos certificados y se aplican los controles de seguridad definidos en la norma ISO 27002:2013."

28. CONTROLES DE SEGURIDAD DE LA RED

- El control de acceso a la red está restringido a personal autorizado.
- Los componentes de red se encuentran localizados en instalaciones seguras con monitoreo permanente.
- La red es protegida por cortafuegos configurados con políticas de acceso y sistemas de alertas para evitar el acceso no autorizado.
- La comunicación de información sensible entre AC y las AR del PSC AUTHENTICSING, es realizada vía VPN incluyendo el uso de firmas electrónicas

29. PERFILES DE CERTIFICADOS LCR / OCSP

29.1 Perfil del certificado

Los certificados del PSC AUTHENTICSING son emitidos conforme a los siguientes estándares:

- RFC 6818: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, January 2013.
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile, March2004 (prevaleciendo en caso de conflicto la TS 101 862).
- 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.

29.2 Número de versión.

Tal como se especificó previamente en la sección "Perfil de certificado", la versión del certificado es la V3 para **Políticas** y V2 para **LCR**.

29.3 Extensiones del certificado.

Las extensiones de los certificados del PSC AUTHENTICSING autorizan codificar información adicional en los certificados. Las extensiones estándar X.509 definen los siguientes puntos:

- SubjectKeyIdentifier.
- AuthorityKeyIdentifier.
- BasicConstraints.
- Certificate Policies.
- KeyUsage.
- LCRDistribucionPoint.
- SubjectAlternativeName.
- AuthorityInformationAccess.

29.4 Identificadores de objeto (OID) de los algoritmos.

La CA debe indicar una clave ECDSA utilizando el identificador de algoritmo:

- id-ecPublicKey (OID: 1.2.840.10045.2.1).

El OID del algoritmo criptográfico usado por AUTHENTICSING es:

- ECDSA-whit- SHA-384 con curva elíptica (OID: 1.3.132.0.34)

29.5 Formatos de nombres.

En el punto 12.1.3 de la Declaración de Prácticas de Certificación y Política de

Certificados se encuentra una descripción exhaustiva del formato y la interpretación de los nombres asignados a las firmas y certificados electrónicos generados por AUTHENTICSING

29.6 Identificador de objeto (OID) de la PC.

AUTHENTICSING, usará 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).

29.7 Perfil de LCR:

La lista de Certificados Revocados (LCR) es una lista de firmas y certificados electrónicos, en el que concretamente, se muestran cada uno de 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, por ese motivo el usuario no debe confiar en ningún certificado incluido en la LCR del sistema. Una (LCR) es un archivo que contiene lo siguiente:

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

Dicha lista está firmada electrónicamente por la propia Autoridad de Certificación (AC) que la emitió.

La Lista de Revocación de Certificados (LCR) es esencial para verificar la validez de un certificado digital. Al descargar la LCR más reciente de la Autoridad de Certificación (AC), el usuario puede comprobar si un certificado específico sigue siendo válido o si ha sido revocado. Esta verificación se realiza automáticamente al comparar los datos del certificado con la información contenida en la LCR. La autenticidad de la LCR está respaldada por la firma electrónica de la AC.

La estructura de datos de la LCR se presenta de la siguiente manera:

ESTRUCTURA DE DATOS DE LAS LISTA DE CERTIFICADOS REVOCADOS	
NOMBRE DEL PUNTO	**VALOR**
Versión	V2 (Número de versión del certificado)

Algoritmo de firma (signatureAlgorithm)	ecdsa-with-SHA512
DATOS DEL EMISOR	
Nombre común (commonName)	AUTHENTICSING
Organización (organizationName)	Sistema Nacional de Certificación Electrónica
OU (organizationName)	PROVEEDOR DE CERTIFICADOS AUTHENTICSING
C (countryName)	VE
PERIODO DE VALIDEZ	
Válido desde:	Fecha (UTC)
Válido hasta:	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)	
Punto distribución LCR	https://www.authenology.com.ve/ac-raiz/authenologycrl.crl
CERTIFICADOS REVOCADOS	
Certificados revocados (Revoked Certificates)	
Serial del Certificado (Serial Number)	Entero Hexadecimal (Serial de certificado revocado)
Fecha de revocación (RevocatiónDate	fecha y hora en formato UTC
Razón de Revocación (CRL ReasonCode)	Razón de Revocación (Anexo G de la Norma 32)
Firma	
Algoritmo de Firma (signatureAlgorithm)	sha512WithECDSAEncryption
Firma(signature)	<Contenido de la Firma>

30. AUDITORIA 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.

Para el auditor externo se debe cumplir lo establecido en la Norma N°047 de SUSCERTE. En el caso de los auditores internos, estos no podrán tener relación Funcional con el área objeto de la auditoría.

30.1 Relación entre el auditor y la autoridad auditada:

Entre el PSC AUTHENTICSING y el auditor seleccionado, solamente existe una relación comercial que no causa dependencia. El PSC AUTHENTICSING 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 AUTHENTICSING y a SUSCERTE, y de mantener en todo momento la confidencialidad de la información a la cual tuvo acceso durante el proceso de auditoría.

30.2 Tópicos cubiertos por el control de conformidad.

Los tópicos cubiertos por la auditoria de cumplimiento incluyen:

- Seguridad física.
- Evaluación de tecnología.
- Administración de servicios CA.
- Investigación de personal.
- Documento de la Declaración de Prácticas de Certificación (DPC) y Políticas de Certificados (PC) y la política de certificados (PC) y otras políticas y documentos aplicables.
- Contractos.
- Protección de datos y consideraciones sobre privacidad.
- Planificación de recuperación ante desastres.

31. REQUISITOS COMERCIALES Y LEGALES

31.1 Aranceles

Los certificados electrónicos emitidos por el PSC ATHENTICSING tienen un costo variable que depende del tipo de certificado y del perfil del suscriptor. Los factores que influyen en la tarifa incluyen el volumen anual de firmas electrónicas y el modelo de suscripción seleccionado.

AUTHENTICSING contrata a un auditor externo para verificar el cumplimiento de los requisitos establecidos por SUSCERTE. Esta relación es de carácter comercial y no genera ninguna dependencia entre las partes. El auditor emitirá un informe confidencial sobre los resultados de la auditoría, tanto a AUTHENTICSING como a SUSCERTE.

31.2 Responsabilidad financiera del PSC

. La responsabilidad de PSC AUTHENTICSING hacia sus clientes se encuentra estrictamente delimitada por los acuerdos contractuales suscritos. Esta limitación abarca cualquier tipo de reclamo, incluyendo aquellos de naturaleza contractual, extracontractual o delictiva, relacionados con el uso de los certificados electrónicos emitidos.

AUTHENTICSING limita su responsabilidad a 15.000 unidades tributarias por certificado emitido, cubriendo cualquier reclamo relacionado con el certificado y la infraestructura de clave pública, siempre y cuando el certificado esté vigente. Esta limitación aplica a todos los usuarios del certificado, sin importar quién haya causado el daño.

La AC declina cualquier responsabilidad que vaya más allá de los límites previamente definidos.

31.3 Políticas de confidencialidad

31.3.1 Información Confidencial

Toda la información recopilada por la Autoridad de Certificación (AC) de PSC AUTHENTICSING se maneja de acuerdo con las leyes venezolanas y los estándares establecidos en nuestra Política y Declaración de Prácticas de Certificación. Respetamos la privacidad de los usuarios y diferenciamos entre información resumida e información de identificación personal. En caso de suspensión de operaciones, transferiremos los datos personales a SUSCERTE, como ente regulador.

La prestación continua de los servicios de certificación requiere el almacenamiento y la disponibilidad de los datos de los usuarios. la política de operación de la AR detalla los procesos de recopilación, procesamiento y almacenamiento de datos personales. La información de identificación, esencial para la prestación de los servicios, se considera confidencial y su tratamiento se rige por los principios de protección de datos.

31.3.2 Información no confidencial

La información accesible al público es:

- Resumen de la información.
- Lista de certificados revocados (LCR).
- Clave pública del PSC AUTHENTICSING.

- La política de AUTHENTICSING permite la divulgación de los datos de los certificados emitidos para uso público.
- Versión de la DPC y PC.
- Los certificados emitidos por AUTHENTICSING son de acceso público y pueden ser consultados por cualquier persona.
- Normativas y procedimientos institucionales.

31.3.3 Publicación de Información sobre la Revocación de un Certificado.

La LCR es un registro que incluye todos los certificados digitales que han dejado de ser válidos. Las razones para revocar un certificado pueden ser diversas, como la pérdida o robo de la clave privada, la solicitud del titular, el uso indebido del certificado o situaciones relacionadas con la Autoridad de Certificación. La LCR es publicada cada veinticuatro (24) horas en:

- https://www.authenology.com.ve/ac-raiz/

Cada uno de los procesos de revocación de certificado es informado por el PSC AUTHENTICSING vía correo electrónico al Cliente propietario del certificado electrónico. Dicha notificación es elaborada con copia a SUSCERTE y se incluye en el depósito digitalizado mantenido por el PSC AUTHENTICSING.

31.3.4 Divulgación de Información a Autoridades Judiciales

La publicación de los motivos por los cuales se suspende o revoca un certificado será determinada por la normativa legal aplicable y, en su defecto, por la decisión exclusiva de PSC AUTHENTICSING.

La divulgación de datos sobre la suspensión de certificados estará restringida al titular del certificado y a SUSCERTE, excepto cuando sea requerida por orden judicial. La AC y la AR de PSC AUTHENTICSING no entregarán documentación alguna a terceros, salvo en los casos previstos por la ley, salvo que ocurran algunos de los hechos señalados a continuación:

- Se produzca debidamente una orden
- Solicitud judicial
- El representante oficial de la ley esté debidamente identificado
- Se cumpla con los demás procedimientos legales.

Ningún documento confidencial o registro almacenado por la Autoridad de Certificación (AC) y Autoridad de Registro (AR) del PSC AUTHENTICSING es

entregado a ninguna persona excepto donde:

- La persona que requiere la información es una persona autorizada para hacerlo y está debidamente identificada.
- Se produzca una solicitud de información debidamente documentada (Ej. que haya cumplido con todos los procedimientos legales).

Cualquier tercero puede solicitar información sobre los servicios de certificación de AUTHENTICSING como prueba en un juicio, siempre y cuando se sigan los canales legales correspondientes en la jurisdicción donde se presente la solicitud.

32. PROTECCIÓN DE LA INFORMACIÓN PRIVADA/SECRETA

32.1 Información considerada privada

En AUTHENTICSING, de conformidad con lo establecido en la Constitución de la República Bolivariana de Venezuela, se considerará como información privada la siguiente:

- Nombres y apellidos.
- Número de cédula de identidad y RIF.
- Direcciones y datos telefónicos del suscriptor.
- Datos suministrados en el proceso de contratación de firma o certificado electrónico.

32.2 Información considerada no privada

Tipos de información no considerados confidenciales:

- Resumen de información
- Todos los certificados emitidos por la infraestructura de clave pública (ICP) para uso público pueden ser divulgados públicamente
- Todos los certificados emitidos por la autoridad de certificación (AC) en su condición servicios de certificación a terceros también pueden ser divulgados públicamente.

32.3 Responsabilidad de proteger la información privada/secreta

El PSC AUTHENTICSING tiene la obligación de mantener a resguardo la información suministrada por los clientes contratantes de firmas o certificados electrónicos generados por el PSC AUTHENTICSING. A tales fines, se mantendrán los datos bajo archivo electrónico con certificados de seguridad asociados al acceso de la misma. El acceso a la información de los clientes solo estará limitado al representante de la Autoridad de Registro (AR) y al Gerente general del PSC

AUTHENTICSING.

32.4 Consentimiento previo para el uso de información privada/secreto

La información contenida en los archivos de PSC AUTHENTICSING se tratará de forma estrictamente confidencial y no será compartida con terceros sin el consentimiento expreso y verificable del cliente. Este consentimiento puede ser otorgado por escrito, de manera electrónica (con firma digital) o mediante orden judicial.

32.5 Comunicación de la información a autoridades administrativas y/o judiciales

Respecto a la comunicación de la información, serán seguidos y aplicables los principios y requerimientos señalados en el presente documento de la Declaración de Prácticas de Certificación (DPC) y la Política de Certificados (PC).

33. PROTECCIÓN DE LA INFORMACIÓN PRIVADA/SECRETA

33.1 Información considerada privada

En PSC AUTHENTICSING considerará información privada, a tenor de lo dispuesto en la Constitución de la República Bolivariana de Venezuela, la siguiente:

- Nombres y apellidos.
- Número de cédula de identidad y RIF.
- Direcciones y datos telefónicos del cliente.
- Datos suministrados en el proceso de contratación de firma o certificado electrónico.

33.2 Información considerada no privada

Tipos de información no considerados confidenciales:

- Resumen de información
- Todos los certificados emitidos por la infraestructura de clave pública (ICP) para uso público pueden ser divulgados públicamente
- Todos los certificados emitidos por la autoridad de certificación (AC) en su condición servicios de certificación a terceros también pueden ser divulgados públicamente

33.3 Responsabilidad de proteger la información privada/secreta

El PSC AUTHENTICSING tiene la obligación de mantener a resguardo la información suministrada por los clientes contratantes de firmas o certificados

electrónicos generados por el PSC AUTHENTICSING. A tales fines, se mantendrán los datos bajo archivo electrónico con certificados de seguridad asociados al acceso de la misma. El acceso a la información de los clientes solo estará limitado al representante de la Autoridad de Registro (AR) y al Gerente general del PSC AUTHENTICSING.

33.4 Consentimiento previo para el uso de información privada/secreta

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

33.5 Comunicación de la información a autoridades administrativas y/o judiciales

Respecto a la comunicación de la información, serán seguidos y aplicables los principios y requerimientos señalados en el presente Documento de la Declaración de Prácticas de Certificación (DPC) y la Política de Certificados (PC).

34. DERECHO DE PROPIEDAD INTELECTUAL

Los componentes de la infraestructura de clave pública (ICP) de PSC AUTHENTICSING, incluyendo certificados, listas de revocación y documentación asociada, están protegidos por derechos de propiedad intelectual. El uso de estos elementos por parte de terceros está restringido y requiere autorización expresa de PSC AUTHENTICSING.

34.1 Claves pública y privada.

La entidad generadora o su designada conservará todos los derechos de propiedad intelectual sobre las claves criptográficas. Los certificados emitidos bajo la autoridad de clientes finales no confieren ningún derecho sobre su contenido o formato a los servicios de certificación.

34.2 Certificado.

En constante momento el PSC AUTHENTICSING se reserva el derecho de suspender o revocar cualquier tipo certificado de acuerdo con los procedimientos y las políticas establecidas en el actual documento de la Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC).

34.3 Nombres distinguidos.

Los derechos de propiedad intelectual, en nombres distinguidos y números de identificación de clientes, no son responsabilidad del PSC AUTHENTICSING, a menos que se especifique todo lo contrario a través de en un contrato o acuerdo.

34.4 Propiedad intelectual.

La propiedad intelectual del actual 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 AUTHENTICSING y contenidos o no dentro de su página web www.authenology.com.ve son propiedad exclusiva del PSC AUTHENTICSING.

35. REPRESENTACIONES Y GARANTIAS

PSC AUTHENTICSING opera de forma autónoma en el mercado, gestionando sus activos intelectuales y estableciendo alianzas estratégicas con empresas líderes en el sector. Además de sus servicios de certificación electrónica, ofrece una amplia gama de productos y soluciones tecnológicas, respaldados por su compromiso con la calidad y la satisfacción del cliente.

36. LIMITACIONES DE RESPONSABILIDAD

36.1 Límites de responsabilidad y garantía limitada:

La Autoridad de Certificación (AC) tiene como objetivo principal facilitar la adopción de tecnologías de firma electrónica y clave pública por parte de todos los usuarios, tanto personas como organizaciones, independientemente de su tamaño.

Con el fin de cumplir con lo establecido, AUTHENTICSING ofrece una amplia gama de servicios de certificación, detallados en esta Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC). Estos documentos describen las rigurosas medidas de seguridad y los procedimientos que garantizan un manejo del riesgo óptimo, adaptándose a las necesidades de cada cliente.

La Autoridad de Certificación (AC) sigue los procedimientos establecidos en las referidas garantías y al hacerlo no pretende suministrar un cien por ciento de seguridad, lo que resulta imposible, con las condiciones de operación de los servicios de certificación. Al hacerlo, la Autoridad de Certificación (AC) simplemente busca incrementar el nivel general de cada seguridad. Por lo tanto, AUTHENTICSING asume la responsabilidad del cumplimiento de los

procedimientos y las medidas de seguridad descritas en las garantías.

36.2 Limitación de responsabilidades

AUTHENTICSING no se responsabilizará por aquellos datos o procedimientos que no estén explícitamente regulados en la Ley de Mensaje de Datos y Firmas Electrónicas, su reglamento y las normas de SUSCERTE, dentro de esos procedimientos se describe lo siguiente:

- Alcanzar resultados específicos.
- Apto para el uso previsto
- Con relación a la exactitud o confiabilidad de la información contenida en los Certificados que no sean suministrados y/o verificados por la Autoridad de Registro (AR).
- Que no están relacionadas con los temas cubiertos por este Documento de la Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC).
- Respecto a la fiabilidad y solvencia financiera de entidades externas que proporcionen servicios de certificación bajo su propia autoridad o que colaboren en procesos de doble certificación.
- Sobre la validez jurídica, la capacidad de satisfacer requerimientos formales o el estatus de prueba de las firmas electrónicas, certificados o claves criptográficas.
- Con relación a los asuntos fuera del control razonable de la Autoridad de Certificación (AC).
- Al utilizar los servicios de AUTHENTICSING, el usuario acepta que la empresa no se responsabiliza por daños que puedan surgir de un uso indebido de los certificados digitales, ni por aquellos que estén fuera de su control directo. La indemnización máxima estará determinada por la fianza establecida.
- Transacciones subyacentes entre los clientes y terceros, incluyendo las partes dependientes.
- Elementos externos (hardware y software) de terceros que se integran o utilizan en los procesos de certificación y firma electrónica.
- Si se producen retrasos, daños o pérdidas en los datos o documentos durante su gestión.
- Dependencia inaceptable de un Certificado, una firma electrónica, una clave criptográfica o par clave, o los servicios de certificación a los cuales se refiere esta política de certificación (PC) y Declaración de Prácticas de Certificación (DPC).
- La falta de cumplimiento por parte de terceros, entre ellos los miembros de la comunidad de Infraestructura de Clave Pública de AUTHENTICSING, de las disposiciones legales y reglamentarias locales en materia de protección de

datos, privacidad y derechos del consumidor.

- Daños colaterales, incluyendo pérdida de beneficios, de buena voluntad, de datos o interrupción de actividades comerciales.

A fin de mitigar los riesgos inherentes a la prestación de servicios de certificación y asegurar la sostenibilidad de la Infraestructura de Clave Pública, la responsabilidad civil de la empresa se encuentra limitada por los términos de la póliza de seguro exigida por la SUSCERTE.

36.3 Limitaciones de pérdidas.

La responsabilidad de AUTHENTICSING hacia sus clientes se encuentra estrictamente definida en los contratos individuales suscritos con cada uno. Estos contratos, junto con la Declaración de Prácticas de Certificación (DPC) y la Política de Certificados (PC), establecen los límites de responsabilidad en cada caso particular. Cualquier reclamo, independientemente de su naturaleza, estará sujeto a las condiciones establecidas en dichos acuerdos.

De acuerdo con los términos de este contrato, la responsabilidad por cualquier problema relacionado con las firmas electrónicas o certificados se limita a lo establecido en la declaración de prácticas de certificación (DPC).

De acuerdo con los términos del contrato, la responsabilidad máxima de AUTHENTICSING por cualquier daño relacionado con un certificado emitido se limita a 15.000 unidades tributarias. Este límite aplica de forma global y acumulada, sin importar la cantidad de reclamos o el tiempo que el certificado permanezca activo.

37. PLAZO Y FINALIZACIÓN

37.1 Plazo

Es fundamental que los clientes informen a AUTHENTICSING sobre cualquier inconveniente en un plazo máximo de dos semanas. Los reclamos presentados después del vencimiento del certificado no podrán ser procesados.

37.2 Finalización

PSC AUTHENTICSING documentará de manera exhaustiva todos los reclamos de sus clientes, asegurando así la trazabilidad de cada proceso.

El acuerdo o finalización de cada reclamo producirá un documento de acuerdo Al

finalizar cada reclamo, se emitirá un documento oficial que evidencie la solución adoptada, la fecha de resolución y la conformidad expresa del cliente, dando por cerrado el proceso.

38. MODIFICACIONES

Las modificaciones a los documentos definidos serán realizadas por el PSC AUTHENTICSING, pero solo entrarán en vigencia una vez obtenida la autorización correspondiente de SUSCERTE.

38.1 Procedimientos de publicación y notificación

A través de los procedimientos de publicación y notificación, AUTHENTICSING asegura que tanto usuarios como interesados estén siempre informados sobre nuestros certificados electrónicos, políticas y normas.

Con el fin de cumplir con los lineamientos de SUSCERTE, cualquier modificación a la documentación de políticas y normas del PSC AUTHENTICSING que deba publicarse en www.authenology.com, requerirá seguir un proceso establecido. Este proceso incluye la aprobación de SUSCERTE y la notificación a los clientes por correo electrónico. Internamente, se mantendrá un registro detallado de cada cambio.

38.2 Procedimientos de Cambio de Especificaciones

Los procedimientos de cambio son un conjunto de reglas y pasos establecidos para gestionar de manera controlada cualquier modificación en la DCP y PC, incluyendo políticas, normas y procesos técnicos. Estos procedimientos tienen como objetivo principal garantizar que los cambios se implementen sin afectar negativamente las operaciones del PSC AUTHENTICSING, sus clientes y socios comerciales.

Se establecerán procedimientos específicos para modificar las normas que regulan la DPC y la PC en los siguientes casos:

- Cambios estructurales de la organización.
- Cambios en los procesos.
- Actualización en la normativa por parte de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).
- Incorporación de un nuevo tipo de certificado electrónico a la cartera de productos, complementando las opciones actuales.
- Incorporación de un nuevo ente a la estructura jerárquica de confianza de AUTHENTICSING.

- Documentación con más de un (1) año, sin modificación o actualización, deberá imprimirse como una nueva versión.
- Cambios en la plataforma tecnológica del PSC AUTHENTICSIN, que impliquen una transformación de los modelos operativos.
- Toda modificación deberá ser notificada y aprobada previamente por la SUSCERTE.

38.3 Procedimientos de aprobación

La gestión de la documentación del PSC AUTHENTICSING estará regida por una política específica que establecerá los procedimientos para su aprobación, modificación y ajuste.

39. RESOLUCIÓN DE CONFLICTOS

39.1 Resolución extrajudicial de conflictos.

Ante cualquier controversia relacionada con la prestación del servicio, las partes acuerdan en primer lugar intentar resolverla de mutuo acuerdo. En caso de no llegar a un acuerdo en un plazo de quince (15) días hábiles, se someterá la controversia al mecanismo de resolución de conflictos establecido en SUSCERTE, conforme a lo dispuesto en el numeral 13 del artículo 22 del Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas. La decisión de SUSCERTE será definitiva y obligatoria.

39.2 Jurisdicción competente.

Si las partes no logran resolver sus diferencias a través del procedimiento de resolución extrajudicial descrito en el punto anterior, podrán acudir a la vía judicial ordinaria. En este caso, serán competentes los tribunales de la Circunscripción Judicial del Área Metropolitana de Caracas.

40. LEGISLACIÓN APLICABLE

Lo no especificado en esta Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC) se regirá por la normativa legal venezolana vigente. Esto implica que tanto el funcionamiento de PSC AUTHENTICSING como de las entidades de su jerarquía de confianza, así como este documento, están sujetos a las leyes y reglamentos aplicables en materia de certificados digitales en Venezuela. A continuación, se detallan las leyes aplicables al presente caso:

- Constitución Bolivariana de Venezuela.
- Decreto 1.204 con Fuerza de Ley Sobre Mensajes de Datos y Firmas electrónicas

(LSMDFE).

- Reglamento Parcial de la Ley Sobre Mensajes de Datos y Firmas Electrónicas LSMDFE).
- Ley Orgánica de Procedimientos Administrativos (LOPA).
- Ley Orgánica de Administración Pública (LOAP).
- Y cualesquiera otras normas complementarias dictada por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).

41. OBLIGACIONES Y RESPONSABILIDAD CIVIL.

41.1 Obligaciones de la Autoridad de Registro (AR):

La Autoridad de Registro (AR) del PSC AUTHENTICSING asume bajo el presente documento, el cumplimiento de una serie de requerimientos técnicos, legales y procedimentales, los cuales son nombrados a continuación:

- Acatar y cumplir estrictamente toda la normativa nacional vigente, incluyendo la Constitución, la Ley sobre Mensajes de Datos y Firmas Electrónicas y sus reglamentos, en lo que respecta a la materia de certificación electrónica y autoridades de certificación.

- Acatar las directrices y normativas técnicas emanadas de SUSCERTE.

- Mantener actualizada y cumplir en todo momento con la normativa vigente (LSMDFE, RLSMDFE o sus sucesores) que regula la actividad de los proveedores de servicios de certificación (PSC).

- Garantizar la integridad y actualización constante de la documentación del PSC AUTHENTICSING.

- Publicar en la página web (www.authenology.com.ve) el documento de la Declaración de Prácticas de Certificación (DPC) y la Política de Certificados (PC), la información sobre Lista de Certificados Revocados (LCR) y la política de vida de certificados del PSC AUTHENTICSING, así como toda la documentación que sea de obligatorio.

- Se respetará y asegurará los derechos de los clientes, incluyendo el derecho a la privacidad de sus datos. La información suministrada será tratada de forma confidencial, salvo en los casos en que AUTHENTICSING este obligado a revelarla por mandato judicial, siempre y cuando se respeten los procedimientos legales establecidos y se garantice la notificación al cliente.

- Mantener un registro y archivo de las contrataciones de servicios del PSC AUTHENTICSING por un lapso de diez (10) años contados a partir de la fecha de suscripción de cada uno de los contratos para la adquisición de certificados de certificación electrónica.

- Mantener y actualizar la documentación que sea de obligatorio cumplimiento a tenor de lo dispuesto en el Decreto Ley Sobre Mensajes De Datos y Firmas Electrónicas o la normativa SUSCERTE.

- Verificar que los clientes de AUTHENTICSING presenten toda la documentación exigida para cada tipo de certificado electrónico solicitado.

- Validar que la información entregada por el cliente sea correcta.

- Implementar mejoras continuas en el proceso de acreditación para brindar una experiencia más eficiente a los signatarios.

- Cumplir las políticas de empresa en materia de informática, administración y recursos humanos.

- Cumplir la normativa laboral y demás leyes de corte social que regulen la relación entre el PSC AUTHENTICSING y sus trabajadores.

- Cumplir las normas legales aplicables a la materia de certificación electrónica y el marco legal aplicable a la gestión regular del PSC AUTHENTICSING.

41.2 Obligaciones de la Autoridad de Certificación (AC).

La Autoridad de Certificación (AC) del PSC AUTHENTICSING asume bajo el presente documento, el cumplimiento de una serie de requerimientos técnicos, legales y procedimentales, los cuales son nombrados a continuación:

- Con el fin de garantizar la seguridad y confiabilidad de los servicios, la AC debe cumplir estrictamente con todas las leyes, reglamentos y normas técnicas aplicables en materia de certificación electrónica, incluyendo los establecidos en la Constitución, la LSMDFE y las directrices de SUSCERTE.

- Garantizar el cumplimiento estricto de todos los requisitos legales y técnicos establecidos para operar como proveedor de servicios de certificación electrónica, con el fin de ofrecer un servicio seguro y confiable a nuestros

clientes, en línea con lo establecido en el LSMDFE y demás normativas vigentes.

- Presentar, mantener y cumplir con la vigencia de la póliza de seguro requerida por SUSCERTE para operar una Autoridad de Certificación electrónica.

- Cumplir cada uno de los contratos de prestación de servicios de certificación mantenidos con los clientes de la Autoridad de Certificación.

- Mantener y actualizar la documentación del PSC AUTHENTICSING, en especial el documento de la Declaración de Prácticas de Certificación (DPC), la Política de Certificados (PC)y la Lista de Certificados Revocados (LCR).

- Conforme a los requisitos legales, se debe pública en la página web www.authenology.com.ve los siguientes documentos: Declaración de Prácticas de Certificación, Política de Certificados, Lista de Certificados Revocados y demás documentación exigida por el Decreto Ley sobre Mensajes de Datos y Firmas Electrónicas y la normativa de SUSCERTE.

- Cumplir y asegurar la ejecución de auditorías de cumplimiento anuales por parte de auditores acreditados ante SUSCERTE.

- Se debe mantener el derecho a la privacidad de los clientes y proteger la confidencialidad de la información que se confía a AUTHENTICSING. La única excepción a este principio será en caso de un requerimiento judicial válido y legalmente exigible, siempre y cuando se cumplan los procedimientos establecidos y se garantice la protección de los derechos del cliente.

- Mantener un registro y archivo de las contrataciones de servicios de certificación electrónica por un lapso de diez (10) años contados a partir de la fecha de suscripción de cada uno de los contratos para la adquisición de certificados de certificación electrónica.

- Gestionar el contrato de prestación de servicios con el centro de datos que alberga la plataforma de certificación de la AC AUTHENTICSING, incluyendo su custodia y renovación.

- Mantener y actualizar la documentación que sea de obligatorio cumplimiento a tenor de lo dispuesto en el decreto ley sobre mensajes de datos y firmas

electrónicas o la normativa emanada de SUSCERTE.

41.3 Obligaciones de los terceros de buena fe.

Los usuarios finales de certificados electrónicos emitidos por la Autoridad de Certificación (AC), así como los terceros de buena fe, están sujetos a los siguientes requisitos:

- Acceder a la página web del PSC AUTHENTICSING www.authenology.com.ve y activar los botones de compra de certificados electrónicos.
- Seleccionar el tipo de certificado que desea el cliente.
- Leer y aceptar el contenido del contrato de prestación de servicios de certificación.
- Leer y aceptar las prácticas de certificación del PSC AUTHENTICSING.
- Cumplir y completar bajo fe de juramento el ingreso de datos y contactos de personas jurídicas o naturales, según sea el caso.
- Cancelar electrónicamente el importe de costo del certificado electrónico.
- Generar sus claves criptográficas.
- Cumplir con la remisión de información soporte de sus datos y contactos, en original o copia certificada al casillero postal señalado en la página web del PSC AUTHENTICSING www.authenology.com.ve.
- Asistir a la entrevista fijada por la autoridad de registro (AR) para la validación de datos y contactos del cliente.
- Cumplir con el uso contratado y aceptado del certificado electrónico adquirido por el cliente.
- El cliente debe presentarse en las oficinas administrativas de PSC AUTHENTICSING dentro de las siguientes 48 horas hábiles a partir de la publicación de la revocación de su certificado en la Lista de Certificados Revocados (LCR) de la Autoridad de Certificación (AC) AUTHENTICSING.
- Verificar los costos asociados al registro y renovación de los certificados en la página web www.authenology.com.ve.
- En todos los casos, al aceptar o recibir el certificado emitido a éste, el cliente garantiza lo siguiente:
    - Que los datos contenidos en el certificado son exactos.
    - Confiar en el contenido y uso del certificado electrónico.
    - Que la clave criptográfica privada asociada con la clave pública contenida en el certificado no ha sido comprometida.
    - Que sólo usará el par de clave criptográfica y los certificados electrónicos de acuerdo con los usos autorizados para el tipo y/o clase correspondiente

- ❖ Que ejercerá el cuidado razonable para evitar el uso sin autorización de la clave criptográfica privada asociada a la clave pública contenida en el certificado;
- ❖ Que el cliente cumplirá con las obligaciones tributarias asociadas a la venta del certificado electrónico, fijada por la legislación que regula la materia de impuestos, tasas o contribuciones dentro de la República Bolivariana de Venezuela.
- ❖

➢ Antes de la expiración de un certificado, se notificará a todos los usuarios involucrados (clientes, Autoridad de Certificación, etc.) acerca de dicha situación:

- ❖ Que la clave privada ha sido extraviada, robada, o está potencialmente comprometida
- ❖ Que ha perdido el control de su clave privada debido a que su contraseña ha sido comprometida o por otra razón
- ❖ Inexactitud o cambios al contenido del certificado
- ❖ Que el cliente final desea suspender o revocar un certificado por cualquier razón que considere apropiada.

Todos los clientes que utilicen los servicios de PSC AUTHENTICSING, incluyendo la Infraestructura de Clave Pública (ICP), Listas de Certificados Revocados (LCR), y demás servicios relacionados, aceptan los términos y condiciones establecidos en los contratos de adquisición de firmas y certificados electrónicos, disponibles en www.authenology.com.

Asimismo, se comprometen a cumplir con las políticas y procedimientos de PSC AUTHENTICSING:

- ➢ Comprobar la validez, suspensión o revocación del certificado, utilizando información actualizada sobre el estado del certificado en la Lista de Certificados Revocados (LCR).
- ➢ Tomar en cuenta cualquier limitación sobre el uso y límites de responsabilidad del certificado.
- ➢ Confiar en las Firmas Electrónicas y Certificados solamente cuando dicha confianza sea razonable. Al considerar la viabilidad de la dependencia, los aspectos a tomar en cuenta incluirán si:
  - ❖ La Firma Electrónica fue creada durante el período de validez del certificado.
  - ❖ La Firma Electrónica puede verificarse exitosamente.
  - ❖ Todas las huellas digitales de la clave pública de los certificados dentro de las cadenas de certificados correspondientes son

verificadas exitosamente.

- ❖ Los certificados en la cadena de certificados son validados exitosamente.
- ❖ No existen circunstancias adicionales que puedan afectar la confiabilidad de la firma electrónica, certificado, cadena de certificado o Lista de Certificados Revocados (LCR).

42. CONFORMIDAD CON LEY APLICABLE.

Los procedimientos, información técnica y legal contenidos en esta Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC) cumplen íntegramente con los requisitos establecidos en el Decreto Ley Sobre Mensajes de Datos y Firmas Electrónicas y la normativa complementaria emitida por SUSCERTE.

43. AJUSTES AL DOCUMENTO.

La documentación requerida por SUSCERTE para la operación de un PSC se ajustará de manera periódica, en concordancia con las modificaciones en el marco normativo y legal, los avances tecnológicos o los requerimientos específicos de la Superintendencia, garantizando así el cumplimiento continuo de la regulación vigente.

43.1 Mecanismo de desarrollo del documento:

Esta Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC) se ha elaborado en estricto cumplimiento con los requisitos establecidos por SUSCERTE, la entidad de acreditación competente en nuestro país. Asimismo, se adhiere a los estándares internacionales aplicables en materia de certificación electrónica.

43.2 Mecanismo para ajuste del documento:

Ante modificaciones sustanciales en la normativa vigente (Decreto Ley de Mensajes de Datos y Firmas Electrónicas, reglamento, normas SUSCERTE o estándares internacionales), que afecten los procesos y medidas de seguridad de los Prestadores de Servicios de Certificación (PSC), AUTHENTICSING revisará y actualizará el presente documento para garantizar el cumplimiento de los nuevos requisitos. Los cambios propuestos serán evaluados y aprobados por la alta dirección, siguiendo los procedimientos establecidos en la política de gestión documental

43.3 Mecanismo para aprobación de los ajustes al documento:

Cualquier modificación a la Declaración de Prácticas de Certificación (DPC) y a la Política de Certificados (PC) requerirá la aprobación formal de la alta dirección de

PSC AUTHENTICSING. Todos los cambios deberán documentarse por escrito, indicando el número de versión, fecha de elaboración, aprobación y la firma del representante autorizado. Este proceso se ajustará a nuestra política de gestión documental.

44. MARCO LEGAL Y NORMATIVO.

- Decreto ley de mensaje de datos y firmas electrónicas y su reglamento.
- Normativa de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).
- Normativa AUTHENTICSING.
- Estándar internacional RFC 3647.
- Estándar internacional RFC 5280.
- Estándar internacional ITU- T X.509 V3.
- Estándar internacional ITU-T X.609.
- CA-Browser-Forum TLS BR.
- Norma ISO 9000:2015.
- Norma ISO/IEC 9594-8.
- Norma ISO/TR 10013:2001.
- Norma ISO/IEC 27001:2013.

45. ESQUEMA DE UN CONJUNTO DE DISPOSICIONES (RFC 3647, sección 6)

ESTRUCTURA DE DOCUMENTO	
RFC 3647 - sección 6	**Estructura Authenticsing**
1.INTRODUCCIÓN	CUMPLE/NO CUMPLE
1.1 Descripción general	CUMPLE
1.2 Nombre del documento e identificación	CUMPLE
1.3 participantes de PKI	CUMPLE
1.3.1 Autoridades de certificación	CUMPLE
1.3.2 Autoridades de registro	CUMPLE
1.3.3 Suscriptores	CUMPLE
1.3.4 Parte que confían	CUMPLE

1.3.5 Otros participantes	CUMPLE
1.4 Uso del certificado	CUMPLE
1.4.1 Usos apropiados del certificado	CUMPLE
1.4.2 Usos prohibidos del certificado	CUMPLE
1.5.1 Organización que administra el documento	CUMPLE
1.5.2 Persona de contacto	CUMPLE
1.5.3 Persona que determina la idoneidad del CPS para la poliza	CUMPLE
1.5.4 Procedimientos de aprobación de la CPS	CUMPLE
1.6 Definiciones y siglas	CUMPLE
2. RESPONSABILIDADES DE PUBLICACIÓN Y DEPÓSITO	CUMPLE/NO CUMPLE
2.1 Repositorios	CUMPLE
2.2 Publicación de información de certificación	CUMPLE
2.3 Hora o frecuencia de publicación	CUMPLE
2.4 Controles de acceso a los repositorios	CUMPLE
3. IDENTIFICACIÓN Y AUTENTICACIÓN (11)	CUMPLE/NO CUMPLE
3.1 Denominación	CUMPLE
3.1.1 Tipos de nombres	CUMPLE
3.1.2 Necesidad de que los nombres sean significativos	CUMPLE
3.1.3 Anonimato o seudónimo de los suscriptores	CUMPLE
3.1.4 Reglas para interpretar varias formas de nombres	CUMPLE
3.1.5 Unicidad de los nombres	CUMPLE
3.1.6 Reconocimiento, autenticación y función de las marcas	CUMPLE

3.2 Validación de identidad inicial	CUMPLE
3.2.1 Método para acreditar la posesión de clave privada	CUMPLE
3.2.2 Autenticación de la identidad de la organización	CUMPLE
3.2.3 Autenticación de identidad individual	CUMPLE
3.2.4 Información del abonado no verificada	CUMPLE
3.2.5 Validación de autoridad	CUMPLE
3.2.6 Criterios de interoperación	NO CUMPLE
3.3 Identificación y autenticación para solicitudes de nueva clave	CUMPLE
3.3.1 Identificación y autenticación para la renovación de claves de rutina	CUMPLE
3.3.2 Identificación y autenticación para nueva clave después de la revocación	CUMPLE
3.4 Identificación y autenticación para solicitud de revocación	CUMPLE
4. REQUISITOS OPERATIVOS DEL CICLO DE VIDA DEL CERTIFICADO (11)	CUMPLE/NO CUMPLE
4.1 Solicitud de Certificado	CUMPLE
4.1.1 ¿Quién puede presentar una solicitud de certificado?	CUMPLE
4.1.2 Proceso de inscripción y responsabilidades	CUMPLE
4.2 Tramitación de la solicitud de certificado	CUMPLE
4.2.1 Realizar funciones de identificación y autenticación	CUMPLE
4.2.2 Aprobación o rechazo de solicitudes de certificado	CUMPLE

4.2.3 Tiempo para procesar las solicitudes de certificado	CUMPLE
4.3 Emisión de certificados	CUMPLE
4.3.1 Acciones de CA durante la emisión de certificados	CUMPLE
4.3.2 Notificación al suscriptor por parte de la CA de la emisión de certificado	CUMPLE
4.4 Aceptación del certificado	CUMPLE
4.4.1 Conducta que constituye la aceptación del certificado	CUMPLE
4.4.2 Publicación del certificado por parte de la CA	CUMPLE
4.4.3 Notificación de emisión de certificado por parte de la CA a otras entidades	CUMPLE
4.5 Uso de par de claves y certificados	CUMPLE
4.5.1 Uso de certificado y clave privada del suscriptor	CUMPLE
4.5.2 Uso de certificado y clave pública del usuario de confianza	CUMPLE
4.6 Renovación de certificado	CUMPLE
4.6.1 Circunstancia para la renovación del certificado	CUMPLE
4.6.2 Quién puede solicitar la renovación	CUMPLE
4.6.3 Tramitación de solicitudes de renovación de certificados	CUMPLE
4.6.4 Notificación de nueva emisión de certificado al suscriptor	CUMPLE
4.6.5 Conducta que constituye la aceptación de un certificado de renovación	CUMPLE
4.6.6 Publicación del certificado de renovación por parte de la AC	CUMPLE

4.6.7 Notificación de la emisión del certificado por parte de la CA a otros	CUMPLE
4.7 Nueva clave del certificado	CUMPLE
4.7.1 Circunstancias para la nueva clave del certificado	CUMPLE
4.7.2 Quién puede solicitar la certificación de una nueva clave pública	CUMPLE
4.7.3 Procesamiento de solicitudes de nueva clave de certificado	CUMPLE
4.7.4 Notificación de nueva emisión de certificado al suscriptor	CUMPLE
4.7.5 Conducta que constituye la aceptación de un certificado con nueva clave	CUMPLE
4.7.6 Publicación del certificado con nueva clave por parte de la CA	CUMPLE
4.7.7 Notificación de la emisión del certificado por parte de la CA a otros	CUMPLE
4.8 Modificación del certificado	CUMPLE
4.8.1 Circunstancia de modificación del certificado	CUMPLE
4.8.2 Quién puede solicitar la modificación del certificado	CUMPLE
4.8.3 Tramitación de solicitudes de modificación de certificado	CUMPLE
4.8.4 Notificación de nueva emisión de certificado al suscriptor	CUMPLE
4.8.5 Conducta que constituye la aceptación del certificado modificado	CUMPLE
4.8.6 Publicación del certificado modificado por la CA	CUMPLE
4.8.7 Notificación de la emisión del certificado por parte de la CA a otros entidades	CUMPLE

4.9 Revocación y suspensión del certificado	CUMPLE
4.9.1 Circunstancias de revocación	CUMPLE
4.9.2 ¿Quién puede solicitar la revocación?	CUMPLE
4.9.3 Procedimiento de solicitud de revocación	CUMPLE
4.9.4 Período de gracia de solicitud de revocación	CUMPLE
4.9.5 Plazo dentro del cual la CA debe procesar la solicitud de revocación	CUMPLE
4.9.6 Requisito de verificación de revocación para partes que confían	CUMPLE
4.9.7 Frecuencia de emisión de CRL (si corresponde)	CUMPLE
4.9.8 Latencia máxima para CRL (si corresponde)	CUMPLE
4.9.9 Disponibilidad de verificación de estado/revocación en línea	CUMPLE
4.9.10 Requisitos de verificación de revocación en línea	CUMPLE
4.9.11 Otras formas de anuncios de revocación disponibles	CUMPLE
4.9.12 Requisitos especiales relacionados con compromisos clave	CUMPLE
4.9.13 Circunstancias de suspensión	CUMPLE
4.9.14 ¿Quién puede solicitar la suspensión?	CUMPLE
4.9.15 Procedimiento para solicitud de suspensión	CUMPLE
4.9.16 Límites del período de suspensión	CUMPLE
4.10 Servicios de estado de certificado	CUMPLE
4.10.1 Características operativas	CUMPLE

4.10.2 Disponibilidad del servicio	CUMPLE
4.10.3 Funciones opcionales	CUMPLE
4.11 Fin de suscripción	CUMPLE
4.12 Custodia y recuperación de claves	CUMPLE
4.12.1 Políticas y prácticas clave de custodia y recuperación	CUMPLE
5. INSTALACIONES, GESTIÓN Y CONTROLES OPERACIONALES (11)	CUMPLE/NO CUMPLE
5.1 Controles físicos	CUMPLE
5.1.1 Ubicación del sitio y construcción	CUMPLE
5.1.2 Acceso físico	CUMPLE
5.1.3 Energía y aire acondicionado	CUMPLE
5.1.4 Exposiciones al agua	CUMPLE
5.1.5 Prevención y protección contra incendios	CUMPLE
5.1.6 Almacenamiento de medios	CUMPLE
5.1.7 Eliminación de residuos	CUMPLE
5.1.8 Copia de seguridad externa	CUMPLE
5.2 Controles procesales	CUMPLE
5.2.1 Roles confiables	CUMPLE
5.2.2 Número de personas necesarias por tarea	CUMPLE
5.2.3 Identificación y autenticación para cada rol	CUMPLE
5.2.4 Funciones que requieren separación de funciones	CUMPLE
5.3 Controles de personal	CUMPLE
5.3.1 Requisitos de calificaciones, experiencia y autorización	CUMPLE
5.3.2 Procedimientos de verificación de antecedentes	CUMPLE

5.3.3 Requisitos de formación	CUMPLE
5.3.4 Frecuencia y requisitos de reentrenamiento	CUMPLE
5.3.5 Frecuencia y secuencia de rotación de puestos	CUMPLE
5.3.6 Sanciones por acciones no autorizadas	CUMPLE
5.3.7 Requisitos del contratista independiente	CUMPLE
5.3.8 Documentación suministrada al personal	CUMPLE
5.4 Procedimientos de registro de auditoría	CUMPLE
5.4.1 Tipos de eventos registrados	CUMPLE
5.4.2 Frecuencia del registro de procesamiento	CUMPLE
5.4.3 Período de retención del registro de auditoría	CUMPLE
5.4.4 Protección del registro de auditoría	CUMPLE
5.4.5 Procedimientos de copia de seguridad del registro de auditoría	CUMPLE
5.4.6 Sistema de recopilación de auditorías (interno versus externo)	CUMPLE
5.4.7 Notificación al sujeto causante del evento	CUMPLE
5.4.8 Evaluaciones de vulnerabilidad	CUMPLE
5.5 Archivo de registros	CUMPLE
5.5.1 Tipos de registros archivados	CUMPLE
5.5.2 Período de conservación del archivo	CUMPLE
5.5.3 Protección del archivo	CUMPLE
5.5.4 Procedimientos de copia de seguridad de archivos	CUMPLE

5.5.5 Requisitos para el sellado de tiempo de los registros	NO CUMPLE
5.5.6 Sistema de recopilación de archivos (interno o externo)	CUMPLE
5.5.7 Procedimientos para obtener y verificar información de archivo	CUMPLE
5.6 Cambio de clave	CUMPLE
5.7 Compromiso y recuperación ante desastres	CUMPLE
5.7.1 Procedimientos de manejo de incidentes y compromisos	CUMPLE
5.7.2 Los recursos informáticos, el software y/o los datos están dañados	CUMPLE
5.7.3 Procedimientos de compromiso de clave privada de la entidad	CUMPLE
5.7.4 Capacidades de continuidad del negocio después de un desastre	CUMPLE
5.8 Terminación de CA o RA	CUMPLE
6. CONTROLES TÉCNICOS DE SEGURIDAD (11)	CUMPLE/NO CUMPLE
6.1 Generación e instalación de pares de claves	CUMPLE
6.1.1 Generación de pares de claves	CUMPLE
6.1.2 Entrega de clave privada al suscriptor	CUMPLE
6.1.3 Entrega de clave pública al emisor del certificado	CUMPLE
6.1.4 Entrega de clave pública de CA a partes que confían	CUMPLE
6.1.5 Tamaños de clave	CUMPLE
6.1.6 Generación de parámetros de clave pública y control de calidad	CUMPLE
6.1.7 Propósitos de uso de claves (según el campo de uso de claves	CUMPLE

X.509 v3)	
6.2 Protección de clave privada e ingeniería de módulos criptográficos	CUMPLE
6.2.1 Estándares y controles del módulo criptográfico	CUMPLE
6.2.2 Control de varias personas con clave privada (n de m)	CUMPLE
6.2.3 Custodia de clave privada	CUMPLE
6.2.4 Copia de seguridad de clave privada	CUMPLE
6.2.5 Archivo de clave privada	CUMPLE
6.2.6 Transferencia de clave privada hacia o desde un módulo criptográfico	CUMPLE
6.2.7 Almacenamiento de clave privada en módulo criptográfico	CUMPLE
6.2.8 Método de activación de la clave privada	CUMPLE
6.2.9 Método de desactivación de la clave privada	CUMPLE
6.2.10 Método de destrucción de la clave privada	CUMPLE
6.2.11 Clasificación del módulo criptográfico	CUMPLE
6.3 Otros aspectos de la gestión de pares de claves	CUMPLE
6.3.1 Archivo de clave pública	CUMPLE
6.3.2 Períodos operativos del certificado y períodos de uso del par de claves	CUMPLE
6.4 Datos de activación	CUMPLE
6.4.1 Generación e instalación de datos de activación	CUMPLE
6.4.2 Protección de datos de activación	CUMPLE

6.4.3 Otros aspectos de los datos de activación	NO CUMPLE
6.5 Controles de seguridad informática	CUMPLE
6.5.1 Requisitos técnicos específicos de seguridad informática	CUMPLE
6.5.2 Calificación de seguridad informática	CUMPLE
6.6 Controles técnicos del ciclo de vida	CUMPLE
6.6.1 Controles de desarrollo del sistema	CUMPLE
6.6.2 Controles de gestión de seguridad	CUMPLE
6.6.3 Controles de seguridad del ciclo de vida	CUMPLE
6.7 Controles de seguridad de la red	CUMPLE
6.8 Sellado de tiempo	NO CUMPLE
7. PERFILES DE CERTIFICADO, CRL Y OCSP	CUMPLE/NO CUMPLE
7.1 Perfil de certificado	CUMPLE
7.1.1 Número(s) de versión	CUMPLE
7.1.2 Extensiones de certificado	CUMPLE
7.1.3 Identificadores de objetos de algoritmo	CUMPLE
7.1.4 Formas de nombre	CUMPLE
7.1.5 Restricciones de nombre	CUMPLE
7.1.6 Identificador de objeto de política de certificado	CUMPLE
7.1.8 Sintaxis y semántica de calificadores de políticas	CUMPLE
7.1.9 Semántica de procesamiento para las Políticas de Certificación críticas	CUMPLE
7.2 Perfil CRL	CUMPLE

7.2.1 Número(s) de versión	CUMPLE
7.2.2 CRL y extensiones de entrada CRL	CUMPLE
7.3 Perfil OCSP	CUMPLE
7.3.1 Número(s) de versión	CUMPLE
7.3.2 Extensiones OCSP	CUMPLE
8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES	CUMPLE/NO CUMPLE
8.1 Frecuencia o circunstancias de la evaluación	CUMPLE
8.2 Identidad/calificaciones del evaluador	CUMPLE
8.3 Relación del tasador con la entidad evaluada	NO CUMPLE
8.4 Temas cubiertos por la evaluación	CUMPLE
8.5 Acciones tomadas como resultado de la deficiencia	NO CUMPLE
8.6 Comunicación de resultados	CUMPLE
9. OTROS ASUNTOS LEGALES Y COMERCIALES	CUMPLE/NO CUMPLE
9.1 Tarifas	NO CUMPLE
9.1.1 Tarifas de emisión o renovación de certificados	NO CUMPLE
9.1.2 Tarifas de acceso al certificado	NO CUMPLE
9.1.3 Tarifas de acceso a la información de revocación o estado	NO CUMPLE
9.1.4 Tarifas por otros servicios	NO CUMPLE
9.1.5 Política de reembolso	NO CUMPLE
9.2 Responsabilidad financiera	NO CUMPLE
9.2.1 Cobertura de seguro	NO CUMPLE
9.2.2 Otros activos	NO CUMPLE
9.2.3 Cobertura de seguro o garantía para entidades finales	NO CUMPLE

9.3 Confidencialidad de la información comercial	CUMPLE
9.3.1 Alcance de la información confidencial	CUMPLE
9.3.2 Información que no está dentro del alcance de la información confidencial	CUMPLE
9.3.3 Responsabilidad de proteger la información confidencial	CUMPLE
9.4 Privacidad de la información personal	CUMPLE
9.4.1 Plan de privacidad	CUMPLE
9.4.2 Información tratada como privada	CUMPLE
9.4.3 Información no considerada privada	CUMPLE
9.4.4 Responsabilidad de proteger la información privada	CUMPLE
9.4.5 Aviso y consentimiento para utilizar información privada	CUMPLE
9.4.6 Divulgación conforme a proceso judicial o administrativo	CUMPLE
9.4.7 Otras circunstancias de divulgación de información	CUMPLE
9.5 Derechos de propiedad intelectual	CUMPLE
9.6 Declaraciones y garantías	CUMPLE
9.6.1 Declaraciones y garantías de CA	CUMPLE
9.6.2 Declaraciones y garantías de RA	CUMPLE
9.6.3 Declaraciones y garantías del suscriptor	CUMPLE
9.6.4 Declaraciones y garantías de la parte que confía	CUMPLE
9.6.5 Declaraciones y garantías de otros participantes	CUMPLE

9.7 Renuncias de garantías	NO CUMPLE
9.8 Limitaciones de responsabilidad	CUMPLE
9.9 Indemnizaciones	NO CUMPLE
9.10 Plazo y terminación	NO CUMPLE
9.10.1 Término	CUMPLE
9.10.2 Terminación	CUMPLE
9.10.3 Efecto de la terminación y supervivencia	CUMPLE
9.11 Avisos individuales y comunicaciones con los participantes	CUMPLE
9.12 Enmiendas	NO CUMPLE
9.12.1 Procedimiento de modificación	NO CUMPLE
9.12.2 Mecanismo y plazo de notificación	NO CUMPLE
9.12.3 Circunstancias bajo las cuales se debe cambiar el OID	NO CUMPLE
9.13 Disposiciones para la resolución de disputas	NO CUMPLE
9.14 Ley aplicable	CUMPLE
9.15 Cumplimiento de la legislación aplicable	CUMPLE
9.16 Disposiciones varias	CUMPLE
9.16.1 Acuerdo completo	CUMPLE
9.16.2 Asignación	CUMPLE
9.16.3 Divisibilidad	CUMPLE
9.16.4 Ejecución (honorarios de abogados y renuncia de derechos)	CUMPLE
9.16.5 Fuerza mayor	CUMPLE
9.17 Otras disposiciones	CUMPLE

SAMUEL SIMON GOMEZ GONZALEZ

Firmado digitalmente por SAMUEL SIMON GOMEZ GONZALEZ
Nombre de reconocimiento (DN): c=VE, st=MIRANDA, l=CALLE BOLIVAR EDIF DON DAVID PISO PB OF 001 URB CHACAO CARACAS (CHACAO), o=Authenticsing C.A, ou=Presidencia, title=Presidente Ejecutivo, serialNumber=J503240237, cn=SAMUEL SIMON GOMEZ GONZALEZ, email=sgomez@authenology.com.ve
Fecha: 2025.09.16 11:26:20 -04'00'

--- Fin de Documento ---