AUTHENTICSING C.A.

Política de Certificado de firma electrónica para Empleados de Empresa Privada.

2024

Resumen de Información.

-- -

Empresa	**AUTHENTICSING C.A**		
Documento	Política de Certificado de firma electrónica para Empleados de Empresa Privada.		
Tipo de Documento	Documentación sobre la Infraestructura de Clave Pública		
ID	DIF-006		
Autor	Ing. Carlos García.		
Colaboradores			
Revisado por	Samuel Gómez.	**Fecha de creación**	2024 agosto
Aprobado por	Abog. Zolange González.	**Fecha Aprobación**	29/02/2024
Versión/Edición	1.0v	**Nº Total de Páginas**	**- 36 -**
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

Índice....3
1. Control de versiones. 6
2. Título. 6
3. CÓDIGO DEL DOCUMENTO. 6
4. Introducción....6
5. Objetivo. 7
6. Alcance. 7
7. TÉRMINOS Y DEFINICIONES. 7
8. SÍMBOLOS Y ABREVIATURAS 14
9. Uso de LOS Certificado 14
9.1 Usos permitidos. 14
9.1.1 Certificado de firma electrónica para empleado de empresa privada....14
10. POLÍTICAS DE ADMINISTRACIÓN DEL PSC 17
11. PUBLICACIÓN DE INFORMACIÓN DEL PSC Y REPOSITORIOS DE LOS CERTIFICADOS....17
11.1 Repositorios....17
11.2 Frecuencia de publicación 18
11.1.1 Certificados del Proveedor de Servicio de Certificación (PSC). 18
11.1.2 Lista de Certificados Revocados (LCR) 18
11.1.3 Versiones y actualizaciones de la DPC y PC. 18
11.1.4 Controles de acceso al repositorio de certificados. 18
12. IDENTIFICACIÓN Y AUTENTICACIÓN....18
13. CONTROLES DE ACCESO AL REPOSITORIO DE CERTIFICADOS 19
14. TRAMITACIÓN DE SOLICITUD DE UN CERTIFICADO. 19
14.1 Realización de las funciones de identificación y autenticación 19
14.2 Aprobación o denegación de un certificado 19
14.3 Plazo para la tramitación de un certificado 20
14.4 Plazo para la tramitación de un certificado 20
15. EMISIÓN DE un CERTIFICADO....20
15.1 Acciones del PSC durante la emisión de un certificado....20
15.2 Notificación al solicitante por parte del PSC acerca de la emisión de su certificado electrónico....21

16. USO DEL PAR DE CLAVES Y DEL CERTIFICADO. 21
16.1 Uso de la clave privada del certificado....21
16.2 Uso de la clave pública y del certificado por los terceros de buena fe....21
17. RENOVACIÓN DEL CERTIFICADO....21
17.1 Causas para la renovación 21
17.2 Entidad que puede solicitar la renovación de un certificado 22
17.3 Procedimiento de solicitud para la renovación de un certificado 22
17.4 Notificación de la emisión de un nuevo certificado 22
17.5 Publicación del certificado renovado por el PSC 22
17.6 Notificación de la emisión del certificado a otras entidades....22
18. REVOCACIÓN Y SUSPENSIÓN DE UN CERTIFICADO. 22
18.1 Circunstancias para la Revocación del certificado del signatario 22
18.2 Entidad que puede solicitar la Revocación 23
18.3 Procedimientos de Solicitud de la Revocación 23
18.4 Límites del período de la Solicitud de Revocación....24
18.5 Circunstancias para la Suspensión....24
18.6 Entidad que puede solicitar la Suspensión 25
18.7 Procedimientos para la Solicitud de Suspensión 25
18.8 Límites del Período de Suspensión de un Certificado 25
18.9 Frecuencia de Emisión de Listas de Certificados Revocados 26
18.10 Requisitos para la comprobación de la Lista de Certificados Revocados....26
18.11 Disponibilidad de comprobación en Línea del Servicio de Revocación del Estado del Certificado 26
18.12 Requisitos de comprobación en Línea del Estado de Revocación 26
18.13 Otras Formas Disponibles para la Divulgación de la Revocación....26
18.14 Requisitos para la Verificación de Otras Formas de Divulgación de Revocación....26
18.15 Requisitos Específicos para Casos de Compromiso de Claves....26
19. Servicio de comprobación de estado de certificados. 27
19. 27
19.1 Servicio de comprobación de estado de certificados 27
1.1 27
19.1.1 Características operativas....27
19.1.2 Disponibilidad del servicio 27

19.1.3 Características adicionales 27
20. FINALIZACIÓN DE LA SUSCRIPCIÓN 27
21. CUSTODIA Y RECUPERACIÓN DE LA CLAVE. 27
22.1 Prácticas y políticas de recuperación de la clave 27
22. CAMBIO DE CLAVE 28
23. CONTROLES DE SEGURIDAD DEL COMPUTADOR 28
24. REQUISITOS COMERCIALES Y LEGALES 28
25. PERFILES DE CERTIFICADOS, LCR / OCSP. 29
25.1 Perfil del certificado 29
25.2 Número de versión 29
25.3 Extensiones del certificado. 29
25.4 Identificadores de objeto (OID) de los algoritmos. 29
25.5 Formatos de nombres. 30
25.6 Identificador de objeto (OID) de la PC. 30
25.7 Perfil de LCR: 30
26. Auditoría de conformidad 33
26.1 Relación entre el auditor y la autoridad auditada: 33
26.2 Tópicos cubiertos por el control de conformidad. 33
27. LEGISLACIÓN APLICABLE. 33
28. CONFORMIDAD CON LEY APLICABLE. 34
29. AJUSTES AL DOCUMENTO. 34
29.1 Mecanismo de desarrollo del documento: 34
29.2 Mecanismo para ajuste del documento: 35
29.3 Mecanismo para aprobación de los ajustes al documento: 35
32. MARCO LEGAL Y NORMATIVO. 35

1. CONTROL DE VERSIONES.

Control de Cambio			
Versión	**Revisión**	**Fecha**	**Observaciones**
1	0	2024Agos.20	Versión inicial

2. TÍTULO.

Política de Certificado de firma electrónica para Empleados de Empresa Privada.

3. CÓDIGO DEL DOCUMENTO.

DIF-006

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 **“Política de Certificado de firma electrónica para Empleados de Empresa Privada.” (DIF-006).** 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, 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 C.A.

- **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.

- ➢ **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

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. USO DE LOS CERTIFICADO

9.1 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:

9.1.1 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)	sha512WithECDSAEncryption
DATOS DEL EMISOR	
Nombre común (commonName)	AUTHENTICSING
Organización (organizationName)	Sistema Nacional de Certificación Electrónica
OU (organizationName)	PROVEEDOR DE CERTIFICADOS AUTHENTICSING
Correo Electrónico (emailAddress)	authenticsing2012@gmail.com
Localidad (localityName)	Caracas
Estado (stateOrProvinceName)	Miranda
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	P-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)	sha512WithECDSAEncryption
Firma(signature)	<Contenido de la Firma>

- El uso del Certificado de firma electrónica para Empleados 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. POLÍTICAS DE ADMINISTRACIÓN DEL PSC

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. PUBLICACIÓN DE INFORMACIÓN DEL PSC Y REPOSITORIOS DE LOS CERTIFICADOS

11.1 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.

11.2 Frecuencia de publicación

11.1.1 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.

11.1.2 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.

11.1.3 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.

11.1.4 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.

12. IDENTIFICACIÓN Y AUTENTICACIÓN

Las características de identificación y los procedimientos de validación detallados en el punto 16 se encuentran alineados con los criterios establecidos en el punto 13 de la Declaración de Prácticas de Certificación (DPC) (DIF-002).

13. 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.

14. TRAMITACIÓN DE SOLICITUD DE UN CERTIFICADO.

14.1 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 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.

14.3 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.

14.4 Plazo para la tramitación de un certificado

El plazo para la tramitación y proceso de compra de la firma o certificado electrónico seleccionado por el cliente, dependerá en gran medida de la información suministrada por el mismo cliente y de su asistencia a la entrevista de validación con la AR de AUTHENTICSING. Si producto de la entrevista la AR determina que el cliente cumple los requisitos establecidos por AUTHENTICSING, la AR informará a la AC para que proceda a la generación y firma de la firma o certificado electrónico, según corresponda.

15. EMISIÓN DE UN CERTIFICADO

15.1 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.

15.2 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 instalado y se le guiará en la generación de su par de claves y el uso del aplicativo para la firma de documentos.

16. USO DEL PAR DE CLAVES Y DEL CERTIFICADO.

16.1 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.

16.2 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.

17. RENOVACIÓN DEL CERTIFICADO

17.1 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.

17.2 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.

17.3 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.

17.4 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 notificara 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.

17.5 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.

17.6 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."

18. REVOCACIÓN Y SUSPENSIÓN DE UN CERTIFICADO.

18.1 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.

18.2 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.

18.3 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:** Para el caso del PSC AUTHENTICSING Se deben de seguir los siguientes pasos:

18.4 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.

18.5 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.

18.6 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.

18.7 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.

18.8 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

18.9 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.

18.10 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.

18.11 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.

18.12 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.

18.13 Otras Formas Disponibles para la Divulgación de la Revocación

No definidas.

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

No definidas.

18.15 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.

19. SERVICIO DE COMPROBACIÓN DE ESTADO DE CERTIFICADOS.

19.1 Servicio de comprobación de estado de certificados

19.1.1 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.

19.1.2 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.

19.1.3 Características adicionales

No definidas.

20. 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

21. CUSTODIA Y RECUPERACIÓN DE LA CLAVE.

22.1 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.

22. 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.

22. CONTROLES DE SEGURIDAD TÉCNICA

Los controles de seguridad física, tanto de gestión como operativos, se detallan en el punto 23 de la Declaración de Prácticas de Certificación (DPC) y Políticas de Certificados (DIF-002).

23. CONTROLES DE SEGURIDAD DEL COMPUTADOR

Los controles de seguridad del computador se detallan en el punto 27 de la Declaración de Prácticas de Certificación (DPC) y Políticas de Certificados (DIF-002

24. REQUISITOS COMERCIALES Y LEGALES

La Declaración de Prácticas de Certificación (DPC, DIF-002) incluye un apartado específico (punto 31) donde se detallan los requisitos comerciales y legales aplicables.

25. PERFILES DE CERTIFICADOS, LCR / OCSP.

25.1 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.

25.2 Número de versión.

Tal como se especificó previamente en la sección "Perfil de certificado", la versión del certificado es la V3.

25.3 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.

25.4 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)

25.5 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

25.6 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).

25.7 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	V3 (Número de versión del certificado)
Algoritmo de firma (signatureAlgorithm)	sha512WithECDSAEncryption
DATOS DEL EMISOR	
Nombre común (commonName)	AUTHENTICSING
Organización (organizationName)	Sistema Nacional de Certificación Electrónica
OU (organizationName)	PROVEEDOR DE CERTIFICADOS AUTHENTICSING
Correo Electrónico (emailAddress)	authenticsing2012@gmail.com
Localidad (localityName)	Caracas
Estado (stateOrProvinceName)	Miranda
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	sha512WithECDSAEncryption

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

26. AUDITORÍA DE CONFORMIDAD

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

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.

26.1 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.

26.2 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.

27. 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).

28. 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..

29. 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.

29.1 Mecanismo de desarrollo del documento:

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

29.2 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

29.3 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.

32. 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.

--- Fin de Documento ---