AUTHENOLOGY
FIRMA ELECTRÓNICA

PSC AUTHENTICSING

Política de Certificado de firma electrónica para Profesionales Titulados.

2024

Zolange Gonzalez Colon

Firmado digitalmente por Zolange Gonzalez Colon
Fecha: 2024.02.14 19:40:15 -04'00'

Resumen de Información.

Empresa	**AUTHENTICSING C.A**		
Documento	Política de Certificado de firma electrónica para Profesionales Titulados.		
Tipo de Documento	Documentación sobre la Infraestructura de Clave Pública		
ID	DIF-010		
Autor	Ing. Carlos García.		
Colaboradores			
Revisado por	Samuel Gómez.	**Fecha de creación**	2024 Enero
Aprobado por	Abog. Zolange González.	**Fecha Aprobación**	29/02/2024
Versión/Edición	1.0v	**Nº Total de Páginas**	**- 34 -**
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

Índice3
1. Control de versiones.6
2. Título.6
3. CÓDIGO DEL DOCUMENTO6
4. Introducción.6
5. Objetivo.7
6. Alcance.7
7. Términos y definiciones.7
8. Uso de lOS CertificadoS (DPC Y PC).14
   8.1 Usos permitidos.14
      8.1.1 Certificado de firma electrónica para profesionales titulados14
   8.2 Usos no permitidos16
9. POLÍTICAS DE ADMINISTRACIÓN DEL PSC (DPC Y PC)17
10. PUBLICACIÓN DE INFORMACIÓN DEL PSC Y REPOSITORIOS DE LOS CERTIFICADOS.17
   10.1 Repositorios17
   10.2 Publicación de información17
   10.3 Regularidad y constancia de publicación.18
11. IDENTIFICACIÓN Y AUTENTICACIÓN18
12. CONTROLES DE ACCESO AL REPOSITORIO DE CERTIFICADOS18
13. TRAMITACIÓN DE SOLICITUD DE UN CERTIFICADO.18
   13.1 Funciones de identificación y autenticación18
   13.2 Aceptación o denegación de un certificado19
   13.3 Plazo para la tramitación de un certificado19
14. EMISIÓN DE CERTIFICADO.19
   14.1 Acciones del PSC durante la emisión de un certificado20
   14.2 Notificación al solicitante por parte del PSC acerca de la emisión de su certificado electrónico20
15. USO DEL PAR DE CLAVES Y DEL CERTIFICADO.20
   15.1 Uso de la clave privada del certificado20
   15.2 Uso de la clave pública y del certificado por los terceros de buena fe21
16. RENOVACIÓN DEL CERTIFICADO21

16.1 Causas para la renovación21
16.2 Entidad que puede solicitar la renovación de un certificado21
16.3 Procedimiento de solicitud para renovación de un certificado21
16.4 Notificación de la emisión de un nuevo certificado21
16.5 Publicación del certificado renovado por el PSC22
16.6 Notificación de la emisión del certificado a otras entidades22
16.7 Nueva clave del certificado22
16.9 Modificación de certificados22
17. REVOCACIÓN Y SUSPENSIÓN DE UN CERTIFICADO.22
17.1 Circunstancias para la revocación de certificado del signatario22
17.2 Entidad que puede requerir y solicitar la revocación22
17.3 Procedimientos de Solicitud de la Revocación23
17.4 Límites del período de la Solicitud de Revocación23
17.5 Circunstancias para la Suspensión23
17.6 Entidad que puede solicitar la Suspensión23
17.7 Procedimientos para la solicitud de suspensión23
17.8 Límites del período de suspensión de un certificado23
17.9 Frecuencia de emisión de Lista de Certificados Revocados23
17.10 Requisitos para la comprobación de la lista de certificados revocados24
17.11 Disponibilidad de comprobación en línea del servicio de revocación del estado del certificado24
17.12 Requisitos de comprobación en Línea del Estado de Revocación24
17.13 Otras Formas Disponibles para la Divulgación de la Revocación24
17.14 Requisitos para la Verificación de Otras Formas de Divulgación de Revocación24
17.15 Otras Formas Disponibles para la Divulgación de la Revocación24
17.16 Requisitos para la Verificación de Otras Formas de Divulgación de Revocación24
17.17 Requisitos Específicos para Casos de Compromiso de Claves24
18. Servicio de comprobación de estado de certificados.25
18.1 Características operativas.25
18.2 Disponibilidad del servicio25
18.3 Características adicionales25
19. FINALIZACIÓN DE LA SUSCRIPCIÓN25

20. CUSTODIA Y RECUPERACIÓN DE LA CLAVE.25
20.1 Prácticas y políticas de recuperación de la clave25
21. CAMBIO DE CLAVE26
22. CONTROLES DE SEGURIDAD DEL COMPUTADOR.26
23. CONTROLES DE SEGURIDAD TÉCNICA (DPC).26
24. REQUISITOS COMERCIALES Y LEGALES (DPC Y PC).26
25. PERFILES DE CERTIFICADOS, LCR / OCSP.26
25.1 Perfil del certificado27
25.2 Número de Versión27
25.3 Extensiones del Certificado27
25.4 Identificadores de Objeto (OID) de los Algoritmos27
25.5 Formatos de Nombres28
25.6 Identificador de Objeto (OID) de la PC28
25.7 Perfil de LCR / OCSP:28
25.8 Auditoría de conformidad (DPC)29
25.8.1 Relación entre el auditor y la autoridad auditada30
25.8.2 Tópicos cubiertos por el control de conformidad.30
25.8.3 Acciones a tomar como resultado de una deficiencia30
25.8.4 Comunicación del resultado31
26. LEGISLACIÓN APLICABLE.31
27. CONFORMIDAD CON LEY APLICABLE.31
28. AJUSTES AL DOCUMENTO.32
28.1 Mecanismo de desarrollo del documento:32
28.2 Mecanismo para ajuste del documento:32
28.3 Mecanismo para aprobación de los ajustes al documento:32
29. MARCO LEGAL Y NORMATIVO.33

1. CONTROL DE VERSIONES.

Control de Cambio			
Versión	**Revisión**	**Fecha**	**Observaciones**
1	0	30/10/2023	Versión inicial

2. TÍTULO.

Política de Certificado de firma electrónica para profesionales titulados.

3. CÓDIGO DEL DOCUMENTO

DIF-010

4. INTRODUCCIÓN.

El Proveedor de Servicios de Certificación (PSC) "**AUTHENTICSING**", en su carácter de empresa de PSC y como parte de sus procesos y funciones presenta el siguiente documento **"Política de Certificado de firma electrónica para profesionales titulados."** a fines de comunicar, informar y documentar todo lo concerniente a los procesos de las Estructura del certificado de firma electrónica de la AC del solicitante. Todos los clientes, proveedores, partes interesadas que utilicen los certificados electrónicos emitido por **AUTHENTICSING** deberán dar fiel cumplimientos en la presente política de certificado, a fin de conocer las responsabilidades, obligaciones y la estructura del certificado correspondiente.

En la presente documento se mostrara la estructura del certificado, la capacidad generada del certificado, los datos del signatarios, la versión del certificado, el tiempo de validez del certificado, el uso asignado para el certificado, el tipo de algoritmo que usa el certificado, las extensiones así como las rutas de distribución de la LCR; también está presente en este documento las limitaciones del certificado y las políticas de administración de la AC.

5. OBJETIVO.

El presente documento **"Política de Certificado de firma electrónica para Profesionales titulados"** tiene como objetivo establecer las prácticas y políticas que lleva a cabo **AUTHENTICSING** para emitir, gestionar, revocar y renovar los certificados electrónicos.

6. ALCANCE.

El presente documento establece la Estructura del certificado de firma electrónica de la AC para profesionales titulados de **AUTHENTICSING,** cada Política de certificación está dirigida a un tipo de certificado en particular y da a conocer las condiciones, procedimientos y usos particulares para el tipo de certificado. Es Aplicada a la Alta dirección, Clientes, Proveedores, Personal y otros interesados de **AUTHENTICSING,** para el proceso de emisión de certificados y funcionamiento de la plataforma tecnológica de certificación de. **AUTHENTICSING**

7. TÉRMINOS Y DEFINICIONES.

A los efectos de este documento se aplican las siguientes definiciones:

- **Authenology:** Se define como la marca y es el signo distintivo de la empresa **AUTHENTICSING C.A**. Su función es la de diferenciar e individualizar en el mercado unos productos o servicios de otros productos o servicios idénticos o similares, así como identificar su origen empresarial y, en cierta manera, ser un indicador de calidad y un medio de promoción de ventas.

- **Activos de Información:** Son los 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, etc.
  - **Software:** Software de aplicaciones, software de sistemas, herramientas de desarrollo, etc.
  - **Activos físicos:** Computadoras, equipamiento de redes y comunicaciones, medios de almacenamiento, mobiliario, lugares de emplazamiento.

- **Administración de Riesgos:** Se entiende por 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:** Se refiere a un sistema informático, tanto desarrollado por Authenology 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):** Significa una autoridad en la cual confían los clientes para crear, emitir y manejar el ciclo de vida de los certificados, la cual a los efectos del decreto ley de mensajes de datos y firmas electrónicas debe contar con la acreditación otorgada por SUSCERTE.

- **Autoridad de Registro:** Significa la entidad cuyo propósito es suministrar apoyo local a la infraestructura de clave pública (ICP) de una Autoridad de Certificación (AC). La Autoridad de Registro desempeña un conjunto de funciones orientadas a la validación, comprobación y conformación de la documentación suministrada, así como la identidad física de un cliente que opte a la compra de una firma electrónica o certificado electrónico generado por **AUTHENTICSING.**

- **Certificado:** Significa una estructura de datos que utiliza el estándar CCITT ITU X.509, que contiene la clave pública de una entidad junto a información asociada y presentada como "un-forgettable" (inolvidable), mediante una firma electrónica de la autoridad de certificación que la generó.

- **Cifrado:** Significa el proceso mediante el cual los datos simples de un texto son transformados para ocultar su significado. El cifrado es un proceso reversible que se efectúa mediante el uso de un algoritmo criptográfico y una clave.

- **Clave Asimétrico:** Es el par de claves relacionadas, en el cual la clave privada define la modificaciones 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) de **AUTHENTICSING** . 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:** El 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** 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**.

- **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:** Es cuando se obtiene una información para identificar positivamente a una entidad y suministrarle los servicios de certificación que solicite.

- **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):** Significa la lista de certificados que han sido revocados o suspendidos por. AUTHENTICSING.

- **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:** Significa el par de claves relacionadas donde la clave privada define la transformación privada y la clave pública define la transformación pública.

- **Parte interesada:** Significa la organización o persona que tiene interés en el desempeño o éxito de **AUTHENTICSING**

- **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) de 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. Un registro de auditoría consiste de un conjunto de descripciones de auditoría, cada uno de los cuales tiene un conjunto de atributos de auditoría asociados a éste. Cada registro de auditoría tiene una descripción de auditora para el encabezamiento del registro y usualmente tiene descripciones de auditoría adicionales que describen la entidad(es) y objeto(s) involucrados en el evento.
- ➢ 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 la 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.

Adicionalmente, deberán considerarse los conceptos de:

- **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:** se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la **AUTHENTICSING.**
- **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.

A los efectos de una correcta interpretación de la presente Política, se realizan las siguientes definiciones:

- **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:** La tecnología de la información (TI) es el proceso de creación, almacenamiento, transmisión y percepción de la información y los métodos de aplicación de dichos procesos.
- ❖

- ➢ **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 de **AUTHENTICSING PSC.** 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. USO DE LOS CERTIFICADOS (DPC Y PC).

8.1 Usos permitidos.

El manejo del certificado subordinado del PSC AUTHENTICSING estará limitado para cada uno de los diferentes tipos de certificados electrónicos que son emitidos por el PSC AUTHENTICSING.

Es importante tener en cuenta que el uso de los certificados electrónicos generados y emitidos por el PSC AUTHENTICSING cumple con las leyes y regulaciones aplicables, y que el uso indebido de los certificados electrónicos puede tener consecuencias legales y financieras graves. Por lo tanto, se recomienda utilizar los certificados electrónicos de manera responsable y cumplir con los requisitos y restricciones aplicables.

A continuación, se presenta los diferentes tipos de certificados generados y emitidos por el PSC AUTHENTICSING

8.1.1 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 CAMPO	**VALOR**
Versión	V3 (Número de versión del certificado)
Número de serie	Serial Number Octet Size 20
Algoritmo	ECDSA-whit- SHA-384 (Algoritmo de Firma)
DATOS DEL EMISOR	
Nombre común (CN)	AUTHENTICSING
Organización (O)	Sistema Nacional de Certificación Electrónica
Empresa (OU)	PROVEEDOR DE CERTIFICADOS AUTHENTICSING <Opcional>
País (C)	VE
PERIODO DE VALIDEZ	
Valido desde:	Inicio vigencia del certificado
Válido hasta:	Expiración del periodo de validez
DATOS DEL TITULAR	
Nombre (CN)	(Nombre del profesional y el número de colegiado)
Organización (O)	(Nombre o dominación de la colegiatura que otorgó el título profesional) <Opcional>
Titulo (T)	(Nombre del titular registrado ante la colegiatura) <Opcional>
Correo (E)	(Correo electrónico del signatario)
País (C)	(País)
Estado (ST)	(Estado o región donde se encuentra el signatario)
Localidad (L)	Ciudad donde se encuentra el signatario <Opcional>
Serial Number (DN)	Registro Único de Información Fiscal (R.I.F) <Opcional>
INFORMACIÓN DE CLAVE PUBLICA	
Algoritmo clave publica	id-ecPublicKey (ALGORITMO EN QUE SE GENERO LA CLAVE PUBLICA)
Tamaño clave publica	(384 bit)
EXTENSIONES	
Restricciones básicas	CA: FALSE
Identificador clave titular	(Identificador clave titular)
Claves de usos (KeyUsage)	
Firma digital	digitalSignature (0)
Compromiso con el contenido(Anteriormente no repudio)	contentCommitment (Non Repudiation)
Cifrado de datos	DatdataEncipherment(3)

Nombre alternativo del titular (subjectAltNAme)	
Nombre RFC822 (rfc822name)	(Correo electrónico del colegio que otorgo el título profesional)
Nombre DNS (dNSName)	(Sitio web del colegio que otorgo el título profesional) <Opcional>
Identificador de clave de autoridad certificadora	
Clave de Autoridad (KeyIdentifier)	(ID de la Clave pública del AC-Raíz)
AIA Información de acceso de autoridad y política de información	
Punto de distribución LCR	URI:https://www.authenology.com.ve/ac-raiz/authenologycrl.crl <LCR del repositorio del PSC>
Dirección de Acceso	http://ocsp.authenology.com.ve/ <URL del servicio OSCP>
Política de Certificados	
Política de información de la PC	OID Autorizada por Suscerte CPS: https://www.authenology.com.ve/normativas/ <Link de repositorio>
Política de Información de la DPC	OID Autorizada por Suscerte CPS: https://www.authenology.com.ve/normativas/ <Link de repositorio>
FIRMA	
Algoritmo de firma (Signature Algorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo ECDSA-whit- SHA-384)
Firma (SignatureValue)	(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 profesionales titulados.	Firma digital, no repudio, cifrado de datos	Firma de Documentos

8.2 Usos no permitidos

El signatario de los certificados electrónicos o firmas electrónicas emitidas por AUTHENTICSING, se exige a utilizarlo conforme a los usos válidos permitidos y son todos aquellos que no están explícitamente permitidos en el apartado (9.1) del documento DIF-002.

Para el certificado electrónico cuyo signatario viole el uso acreditado y autorizado, será revocado. Además de eso, el signatario deberá encargarse y asumir la responsabilidad de indemnizar al AUTHENTICSING por daños y perjuicios causados a terceros procedentes de acciones, reclamos, pérdidas o daños (incluyendo multas legales) ocasionados por el uso indebido e incorrecto

del servicio contratado

9. POLÍTICAS DE ADMINISTRACIÓN DEL PSC (DPC Y PC)

Las políticas de administración del PSC, son las señaladas en el punto 10 de la Declaración de Prácticas de Certificación (DPC) y Políticas de Certificados (PC) (DIF-002).

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

10.1 Repositorios

Los certificados de la AC raíz subordinada y toda información de este documento de la Política de Certificados (PC) y Declaración de Prácticas de Certificación (DPC), y demás documentos importantes, están disponible en la página web www.authenology.com.ve durante los trecientos sesenta y cincos (365) días del año, las veinticuatro (24) horas del día y los siete (7) días de la semana.

- Certificado de la AC Subordinada AUTHENTICSING, los certificados emitidos por dicha AC y la DPC: https://www.authenology.com.ve/ac
- Lista de Certificados Revocados: https://www.authenology.com.ve/lrc
- Servicio de validación en línea (OCSP): https://www.authenology.com.ve/ocsp
- El repositorio público del PSC AUTHENTICSING, no incluye ninguna información confidencial o privada

10.2 Publicación de información

Es deber y obligatorio para AUTHENTICSING hacer pública y notorio la información relativa a sus procedimientos, sus certificados y el estado recientemente actualizado de dichos certificados. Las publicaciones que realice AUTHENTICSING, de toda la información reservado o clasificada como pública, se informará en su correspondiente página web de la forma siguiente:

- Lista de Certificados Revocados (LCR), se encuentra útil y apto en formato CRL en: https://www.authenology.com.ve/lrc
- El actual documento se encuentra útil y disponible en: https://www.authenology.com.ve/normativas/
- El certificado de la AC Subordinada AUTHENTICSING se encuentra útil y disponible en: https://www.authenology.com.ve/ac

- Los certificados emitidos por la AC Subordinada AUTHENTICSING se encuentran en: https://www.authenology.com.ve/ac
- La información de contacto del PSC AUTHENTICSING en la dirección: https://www.authenology.com.ve La acreditación y documentación técnica del PSC AUTHENTICSING en la dirección: https://www.authenology.com.ve

10.3 Regularidad y constancia de publicación.

- **Certificados del Proveedor de Servicio de Certificación (PSC):** La publicación de los certificados se ejecutará una vez conseguido la identificación y acreditación por parte de SUSCERTE. La vigencia es de diez (10) años.
- **Lista de certificados revocados (LCR):** La publicación de la lista de certificados revocados se actualizara y ejecutará cada veinticuatro (24) horas.
- **Declaración de prácticas de certificación:** A menos que explícitamente se indique lo contrario en este documento de la política de certificado de firma electrónica para empleado de empresa, se publicarán en la página web de AUTHENTICSING (www.authenology.com.ve), las nuevas versiones de este documento, cuando las mismas sean revisadas y validadas por la alta dirección de AUTHENTICSING y SUSCERTE.

11. IDENTIFICACIÓN Y AUTENTICACIÓN

Las características de la identificación mencionados en el punto 16 y procedimientos para la validación son las señaladas en los puntos 13 y 14 de la declaración de prácticas de certificación (DPC) (DIF-002).

12. CONTROLES DE ACCESO AL REPOSITORIO DE CERTIFICADOS

El acceso a la información publicada por el PSC AUTHENTICSING será de consulta y no podrá ser modificada por personas no autorizadas. La información pública solo será actualizada por el personal encargado de esa función que labora en el PSC AUTHENTICSING; además se garantiza la consulta de la LCR y al OCSP.

13. TRAMITACIÓN DE SOLICITUD DE UN CERTIFICADO.

13.1 Funciones de identificación y autenticación

Las funciones de identificación y autenticación de los clientes que optan a la compra de una firma o certificado, está asignada a la autoridad de registro AR de AUTHENTICSING. La explicación detallada de las funciones y atribuciones de la AR de AUTHENTICSING se encuentran detallados en los puntos 14 y

15.1.6 de la declaración de prácticas de certificación (DPC) (DIF-002).

13.2 Aceptación o denegación de un certificado

La aprobación o denegación de una firma o certificado electrónico se encuentra asignada a la AC de AUTHENTICSING. Toda solicitud de firma o certificado electrónico que no sea validada por la AR de AUTHENTICSING automáticamente será rechazada y en consecuencia denegada. La autoridad de certificación antes del proceso de aprobación de una firma o certificado electrónico validará el cumplimiento de las condiciones siguientes:

- Validar el pago efectuado por el cliente.
- Validar el informe emitido por la AR.
- Validar el tipo de certificado solicitado y tramitar ante la Universal Register Authority (URA), el cual es el módulo de generación de certificados.

Una vez verificados y cumplidos a satisfacción los pasos mencionados, la AC de AUTHENTICSING procederá a generar la firma o certificado electrónico y según sea el caso. Las circunstancias para la revocación del certificado son las señaladas en el punto 15.1.5 de la declaración de prácticas de certificación (DPC) (DIF-002).

13.3 Plazo para la tramitación de un certificado

El plazo para la tramitación y proceso de compra de la firma o certificado electrónico seleccionado por el cliente, dependerá en gran medida de la información suministrada por el mismo cliente y de su asistencia a la entrevista de validación con la AR 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.

El lapso establecido por AUTHENTICSING para la aprobación y firma de los certificados, es de quince (15) días continuos luego de la entrevista de validación de identidad y datos con la AR de AUTHENTICSING. La AC de AUTHENTICSING generará y firmará los certificados dentro del referido lapso y notificará al cliente, para que este proceda a la descarga e instalación de la firma o certificado electrónico.

14. EMISIÓN DE CERTIFICADO.

14.1 Acciones del PSC durante la emisión de un certificado

La emisión de los certificados implica la autorización de la solicitud por parte del PSC AUTHENTICSING. Después de la aprobación de la solicitud se procederá a la emisión de los certificados de forma segura y se pondrán los certificados electrónicos a disposición signatario.

El PSC AUTHENTICSING es el representante de producir y generar los certificados obtenidos por los clientes. Seguido a la validación en nombre de la Autoridad de Registro (AR) del PSC AUTHENTICSING, el administrador del módulo de la Autoridad de Certificación (AC) procede a la admisión y aprobación de la emisión del certificado; en ese momento el software de certificación informará por vía https con la Autoridad de Certificación (AC) y solicita la firma de la clave pública del certificado.

La Autoridad de Certificación (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

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

La AC del PSC AUTHENTICSING es el representante de comunicar por vía de correo electrónico al cliente contratante referente a la cita para que acuda a las oficinas de Authenticsing para retirar su certificado y generar su par de clave; para así hacer entrega del certificado correspondiente en un dispositivo y del aplicativo para la firma de documentos.

15. USO DEL PAR DE CLAVES Y DEL CERTIFICADO.

15.1 Uso de la clave privada del certificado

La entrega de clave a los clientes no es realizada y en consecuencia no será suministrada, ya que cada cliente generará su propio par de claves (pública y privada). El titular solo puede utilizar la clave privada y el certificado para usos autorizados en este documento de la política de certificado de firma electrónica para empleado de empresa.

El cliente es el único responsable de la custodia y cuido de su clave privada y deberá reportar a AUTHENTICSING acerca del compromiso de la clave privada del cliente, sin menoscabo de responder personalmente por las acciones y consecuencias derivadas del uso indebido de sus firmas o certificados electrónicos por parte de terceras personas.

15.2 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 la Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC). 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 la DIF-002.

16. RENOVACIÓN DEL CERTIFICADO

16.1 Causas para la renovación

La causa de la renovación de un certificado electrónico por parte del PSC AUTHENTICSING, es por la caducidad.

Bajo el documento de Políticas de Certificación (PC), el PSC AUTHENTICSIG no renueva Certificados electrónicos, esto quiere decir, que todas las renovaciones de certificados realizadas en el ámbito del documento DPC-PC se realizarán con cambio de claves. 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, de la Declaración de Prácticas de Certificación (DPC) y Políticas de Certificados (PC) y política de certificados (PC) de AUTHENTICSING.

16.2 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.

16.3 Procedimiento de solicitud para 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 de la Declaración de Prácticas de Certificación (DPC) y Políticas de Certificados (PC) y política de certificados (PC) de AUTHENTICSING.

16.4 Notificación de la emisión de un nuevo certificado

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

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 de la Declaración de Prácticas de Certificación (DPC) y Políticas de Certificados (PC) y política de certificados (PC) de AUTHENTICSING.

16.5 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.

16.6 Notificación de la emisión del certificado a otras entidades

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

16.7 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.

16.9 Modificación de certificados

Los Certificados Electrónicos generados y emitidos por la AC de Authenticsing del PSC AUTHENTICSING, durante su período de vigencia mantendrán su integridad y no podrán ser objeto de modificación o cambio alguno. Por tanto, cualquier necesidad de modificación conlleva la expedición de un nuevo Certificado Electrónico.

17. REVOCACIÓN Y SUSPENSIÓN DE UN CERTIFICADO.

17.1 Circunstancias para la revocación de certificado del signatario

Las circunstancias para la revocación del certificado son las mencionadas en el campo (13.9.1) de la declaración de prácticas de certificación (DPC) y Políticas de Certificado (PC) (DF-002).

17.2 Entidad que puede requerir y solicitar la revocación

La entidad que puede solicitar la revocación de la firma o certificado electrónico según corresponda se encuentra señalada en el campo 13.9.2 de la declaración de prácticas de certificación (DPC) (DIF-002).

17.3 Procedimientos de Solicitud de la Revocación

El procedimiento de solicitud de la revocación de la firma o certificado electrónico según corresponda, mencionado en el campo 13.9.3 de la declaración de prácticas de certificación (DPC) (DIF-002).

17.4 Límites del período de la Solicitud de Revocación

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

17.5 Circunstancias para la Suspensión

Las circunstancias para la suspensión de firma o certificado electrónico según corresponda, es el mencionado en el campo 13.9.5 de la declaración de prácticas de certificación (DPC) (DIF-002).

17.6 Entidad que puede solicitar la Suspensión

La entidad para la suspensión de firma o certificado electrónico según corresponda, es el señalado en el campo 13.9.6 de la declaración de prácticas de certificación (DPC) (DIF-002).

17.7 Procedimientos para la solicitud de suspensión

El procedimientos para la solicitud de suspensión de firma o certificado electrónico según corresponda, es mencionado en el punto 13.9.7 de la declaración de prácticas de certificación (DPC) (DIF-002).

17.8 Límites del período de suspensión de un certificado

La publicación de la Lista de Certificados Revocados (LCR) se emiten cada veinticuatro (24) horas o cuando se produce una revocación y será publicada o anunciada en una ruta de la página web de AUTHENTICSING (https://www.authenology.com.ve), con la finalidad de que esté disponible y actualizada las veinticuatro (24) horas al día. Adicionalmente, estará disponible un servicio OCSP que permita determinar en línea el estado de los certificados

17.9 Frecuencia de emisión de Lista de Certificados Revocados

La publicación de la Lista de Certificados Revocados (LCR) se emiten cada veinticuatro (24) horas o cuando se produce una revocación y será publicada o anunciada en una ruta de la página web de AUTHENTICSING

(https://www.authenology.com.ve), con la finalidad de que esté disponible y actualizada las veinticuatro (24) horas al día. Adicionalmente, estará disponible un servicio OCSP que permita determinar en línea el estado de los certificados

17.10 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.

17.11 Disponibilidad de comprobación en línea del servicio de revocación del estado del certificado

La información relativa al estado de los certificados estará disponible en línea las 24 horas del día, los 7 días de la semana. En caso de fallo del sistema se pondrá en marcha el Plan de continuidad de negocio para solventar el incidente a la mayor brevedad posible.

17.12 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.

17.13 Otras Formas Disponibles para la Divulgación de la Revocación

No definidas.

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

No definidas.

17.15 Otras Formas Disponibles para la Divulgación de la Revocación

No definidas.

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

No definidas.

17.17 Requisitos Específicos para Casos de Compromiso de Claves

El PSC AUTHENTICSING utilizará medios de comunicación razonables para informar a los Suscriptores que su clave privada puede haber sido

comprometida. Siempre que se confirme un compromiso de la clave, el PSC AUTHENTICSING revocará los Certificados afectados conforme a lo descrito en el apartado 13.9.1 de la declaración de prácticas de certificación (DPC) (DIF-002).

18. SERVICIO DE COMPROBACIÓN DE ESTADO DE CERTIFICADOS.

18.1 Características operativas

El servicio de comprobación se realiza mediante el protocolo OCSP y/o la LCR, el cual proporciona la información más reciente acerca del estado de un Certificado Electrónico determinado.

18.2 Disponibilidad del servicio

El servicio de comprobación, para el estado de los Certificado Electrónico, está disponible de forma continua, manteniendo las siguientes excepciones: los períodos de mantenimiento no excederán más de 4 horas continuas y no más de 36 horas al año.

18.3 Características adicionales

No definidas.

19. FINALIZACIÓN DE LA SUSCRIPCIÓN

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

- Revocación del Certificado Electrónico por cualquiera de las causas mencionadas en el apartado 13.9.1 de la declaración de prácticas de certificación (DPC) (DIF-002).
- CIRCUNSTANCIAS PARA LA REVOCACIÓN DE UN CERTIFICADO”,
- Caducidad de la vigencia del Certificado Electrónico CE.

20. CUSTODIA Y RECUPERACIÓN DE LA CLAVE.

20.1 Prácticas y políticas de recuperación de la clave

La clave privada de la AC de Authenticsing se encuentra bajo control multipersonal, divididas en varios fragmentos y es necesario un mínimo de tres (3) de cinco (5) fragmentos para poder volver a recuperar la clave de la AC de Authenticsing.

EL PSC AUTHENTICSING mantienen las copias de backup de la clave

privada de la AC Authenticsing, almacenadas y cifradas en dispositivo criptográfico, que a su vez maneja diversos mecanismos de seguridad adicionales.

Por otro lado, el signatario del Certificado Electrónico CE emitido por el PSC AUTHENTICSING es el responsable de generar el par de claves (pública y privada), por lo tanto tiene la obligación de resguardar la clave privada y en caso de que tuviera conocimiento o sospecha del compromiso de la misma o de cualquier otro hecho determinante debe solicitar la revocación inmediata del Certificado Electrónico CE.

21. 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 pues el AUTHENTICSING no produzca el par de claves (pública y privada).

A consecuencia de si el cliente extravía su clave privada, se necesitará proceder a la emisión de un nuevo certificado y deberá cumplir el proceso de contratación del PSC a tales efectos. La clave pública siempre estará en el repositorio, de conformidad con lo señalado en el punto 15.2 del documento de Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC)

22. CONTROLES DE SEGURIDAD DEL COMPUTADOR.

Los controles de seguridad física de gestión y de operaciones son los señalados en el punto 26 de la Declaración de Prácticas de Certificación (DPC) y Políticas de Certificados (PC) (DIF-002).

23. CONTROLES DE SEGURIDAD TÉCNICA (DPC).

Los controles de seguridad técnica son los mencionados en el punto 22 de la declaración de prácticas de certificación (DPC) (DIF-002).

24. REQUISITOS COMERCIALES Y LEGALES (DPC Y PC).

Los requisitos comerciales y legales se encuentran mencionados en el punto 30 de la declaración de prácticas de certificación (DPC) (DIF-002).

25. PERFILES DE CERTIFICADOS, LCR / OCSP.

25.1 Perfil del certificado

Los certificados del AUTHENTICSING son emitidos conforme a las siguientes normas:

- 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

Como se indicó en el punto "Perfil de certificado", que precede, el número de versión del certificado es V3.

25.3 Extensiones del Certificado

Las extensiones de los certificados del 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 el AUTHENTICSING es:

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

25.5 Formatos de Nombres

El formato y significado asignado a los nombres en cada uno de las firmas y certificados electrónicos generados por AUTHENTICSING se encuentran detallados en los puntos 12.1.3 y 28.5 de la declaración de prácticas de certificación (DPC) (DIF-002).

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 / OCSP:

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

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

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

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

ESTRUCTURA DE DATOS DE LAS LISTA DE CERTIFICADOS REVOCADOS.	
Nombre del punto	**Valor**
Versión	V3 (Número de versión de la LCR)
Algoritmo	ECDSA-WHITH-SHA384 (Algoritmo de Firma)
DATOS DEL EMISOR	
CN	AUTHENTICSING
O	Sistema Nacional de Certificación Electrónica
C	VE (VENEZUELA)
PERIODO DE VALIDEZ	
Última Actualización	Contiene la fecha y hora en que fue emitida la LCR
Próxima Actualización	Fecha en que se emitirá la próxima LCR
Lista de certificados revocados	
Certificados Revocados	Contiene la lista de certificados revocados indicados por su número de serie y su fecha de revocación.
Extensiones	
Identificación de clave de la AC	Proporciona un medio para identificar la clave pública que corresponde a la clave privada utilizada para firmar una LCR (ID DE CLAVE)
Nombre alternativo del emisor	
DNS Name	www.authenology.com.ve
Otro nombre	
Punto de distribución del emisor	https://www.authenology.com.ve/ac-raiz/authenologycrl.crl https://www.authenology.com.ve/ac-raiz/

El perfil correspondiente al OCSP se encuentra detallado en el presente documento de la Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC).

25.8 Auditoría de conformidad (DPC)

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.

25.8.1 Relación entre el auditor y la autoridad auditada

Entre AUTHENTICSING y el auditor seleccionado, solamente existe una relación comercial que no causa dependencia. AUTHENTICSING contratará la auditoría de seguimiento ordenada por SUSCERTE y el auditor prestará el servicio con la obligación de generar un informe de cumplimiento, el cual entregará a 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.

25.8.2 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.

25.8.3 Acciones a tomar como resultado de una deficiencia

Todo punto u observación generado por el auditor acreditado ante la SUSCERTE respecto a la operación y generación de certificados del

PSC AUTHENTICSING y que sea considerado como “disconformidad”, será sometido a plan de remediación y cumplimiento, el cual deberá establecer el cronograma y tiempo fijado para superar la “disconformidad”, en el supuesto que la misma sea declarada. Si el PSC AUTHENTICSING no supera o cumple con el proceso de remediación de la “disconformidad”, no podrá optar a la renovación de su acreditación como PSC y cesará operación.

25.8.4 Comunicación del resultado

Los resultados de las auditorias se consideran información comercial sensitiva. A menos que esté estipulado en el contrato, serán protegidos como información confidencial de acuerdo con el punto 38. de la Declaración de Prácticas de Certificación (DPC) y Políticas de Certificados (PC) (DIF-002).

26. LEGISLACIÓN APLICABLE.

Lo no predicho en el presente documento de la Declaración de Prácticas de Certificación (DPC) y la Política de Certificados (PC), será regulado de conformidad con lo establecido en la normativa legal vigente y aplicable a la materia dentro de la República Bolivariana de Venezuela, esto quiere decir que el funcionamiento y operación de las entidades pertenecientes a la jerarquía de confianza del PSC AUTHENTICSING, sí como el presente documento está regido por la legislación venezolana vigente en cada momento. Se toman como de aplicación las siguientes leyes:

- 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 cualquier otras normas complementarias dictada por la Superintendencia de Servicios de Certificación Electrónica.

27. CONFORMIDAD CON LEY APLICABLE.

Cada uno de los procedimientos, información técnica y legal contenida en el presente documento de la Declaración de Prácticas de Certificación (DPC) y La Política de Certificados (PC), se encuentra íntegramente elaborada y de conformidad con lo establecido en el Decreto Ley Sobre Mensajes De Datos y Firmas Electrónicas y las normas de rango sub-legal derivadas de SUSCERTE.

28. AJUSTES AL DOCUMENTO.

Los ajustes a la documentación requerida por SUSCERTE para la operación de un PSC, serán realizados en cada oportunidad que ocurra un cambio en el marco normativo y legal aplicable a los PSC, cuando suceda un cambio técnico que justifique el ajuste o cambio, cuando sea requerido y solicitado por SUSCERTE o en su revisión anual.

28.1 Mecanismo de desarrollo del documento:

El presente documento de la Declaración de Prácticas de Certificación (DPC) y la Política de Certificados (PC) se encuentra desarrollado sobre la base de la normativa de acreditación aplicable a los interesados a convertirse en PSC. Dicha norma de acreditación es dictada y emitida por SUSCERTE. También, el presente documento de la Declaración de Prácticas de Certificación (DPC) y la Política de Certificados (PC) cumple con los requerimientos de la normativa internacional aplicable al área de certificación electrónica.

28.2 Mecanismo para ajuste del documento:

Los cambios en el decreto ley de mensajes de datos y firmas electrónicas, su reglamento, la normativa de SUSCERTE o de la norma internacional vinculante y exigida para la operación de los PSC, que contemplen cambios sustanciales en los procesos y métodos de seguridad y operación, los cuales incluyan variación de los procedimientos y actividades de los PSC producirán una revisión del presente Documento, con el objetivo de ajustar los procesos y procedimientos a los estándares y normativa aplicable y validadas por SUSCERTE para la operación de los PSC.

28.3 Mecanismo para aprobación de los ajustes al documento:

Cada ajuste o modificación del documento de la Declaración de Prácticas de Certificación (DPC) y la Política de Certificados (PC), tendrá que contar con la aprobación de la alta dirección del AUTHENTICSING, ser documentada y constar por escrito, nombrando el número de edición y revisión, fecha de elaboración, fecha de aprobación y la firma del representante de la alta dirección que aprueba el ajuste o modificación. Se documentará el ajuste o modificación y su aprobación conforme al documento de la política de documentación y gestión documental.

29. 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 ITU- T X.509 V3.
- Estándar Internacional ITU-T X.609.
- Norma ISO 9000:2015.
- Norma ISO/IEC 9594-8.
- Norma ISO/TR 10013:2001.
- Norma ISO/IEC 27001:2013.

--- Fin de Documento ---