AUTHENTICSING C.A

Modelo de Confianza

2024

Zolange Gonzalez Colon

Firmado digitalmente por Zolange Gonzalez Colon
Fecha: 2024.02.14 19:12:15 -04'00'

Resumen de Información.

--

Empresa	**AUTHENTICSING C.A**		
Documento	Modelo de Confianza		
Tipo de Documento	Documentación sobre la Infraestructura de Clave Pública		
ID	DIF-001		
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**	**- 21 -**
Tipo de Uso	**Uso Interno** ☐ **Uso Público** ☒		

CONTROL DE DISTRIBUCIÓN

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

ÍNDICE

1. CONTROL DE VERSIONES.

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

2. TÍTULO.

Modelo de confianza.

3. CÓDIGO DEL DOCUMENTO.

DIF-001

4. INTRODUCCIÓN.

AUTHENTICSING ha creado e implementado un sistema automatizado para emitir y gestionar de forma adecuada certificados DIGITALES o ELECTRONICOS así como la gestión de los procesos correspondiente a la solicitud y compra de certificados electrónicos; basado en el marco legal y las normativas dada por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) en fecha del (**COLOCAR FECHA DE APROBACION POR PARTE DE SUSCERTE**) y en cumplimiento con las normas, términos condiciones dadas por "**AUTHENTICSING C.A**".

AUTHENTICSING , en su carácter de empresa y como parte de sus procesos y funciones presenta el siguiente documento "Modelos de Confianza" cuya finalidad es documentar e informar a todos sus clientes, proveedores y servidores de AUTHENOLY, el esquema y el proceso por el cual se sustenta la validez del CERTIFICADO ELECTRONICO y de los entes que respaldan la cadena de confianza de los certificados; todo esto con la finalidad de generar la confianza en el cliente final y en todos los usuarios de los certificados electrónicos emitido por **AUTHENTICSING** y dar cumplimiento a los requisitos y requerimientos que estipula

la ley.

Los clientes, proveedores o parte interesada que utilice los certificados electrónicos emitidos por **AUTHENTICSING** , deberán dar cumplimiento al uso adecuado del certificado electrónico, confiando en los certificados, validando su vigencia a través de la Lista de Certificados Revocados (LCR) y constatando el origen de los certificados electrónicos a través del examen del contenido del certificado.

5. OBJETIVO.

El presente manual Modelo de Confianza tiene como objetivo mostrar, documentar e informar a los usuarios, clientes y proveedores el esquema y proceso por el cual se sustenta la validez del CERTIFICADO ELECTRONICO.

6. ALCANCE.

El alcance del Modelo de Confianza se centra en permitir verificar a los signatarios de certificados de firma electrónica un mecanismo de confianza que permitan comprobar la validez de cualquier certificado emitido por **AUTHENTICSING** en cumplimiento del marco legal y las normativas dadas por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).

7. 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 **AUTHENTICSING** 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.

- **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:** Director del departamento de Informática.

- **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.** 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. AMBITO DE APLICACIÓN

El presente documento es de aplicación en relación a:

8.1. Concerniente al Modelo de Confianza.

El presente manual Modelo de Confianza representa una guía técnica para el cliente o signatario, el cual constituyen un documento que da a conocer el proceso y procedimiento de operación, gestión y valides legal de los certificados electrónicos que son generados por de **AUTHENTICSING,** esto permite que el cliente o signatario pueda verificar la validez de los certificados electrónicos y de esta manera poder confiar en el modelo del proceso operacional de **AUTHENTICSING.**

El modelo de confianza permite hacer saber al cliente y signatario acerca de la raíz de certificación o autoridad que firma a **AUTHENTICSING.**

8.2. Concerniente al Modelo de Confianza para la acreditación.

Con base a las leyes, modelos y normativas legales que rigen en Venezuela entre ellas el Decreto Ley de Mensajes de Datos y Firmas Electrónicas (LSMDFE), se contempla que todo interesado, ya sea público o privado, cumpla con un proceso de acreditación ante la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), lo cual supone el cumplimiento de los pasos siguientes:

8.3.1. Auditoria.

Previa a la solicitud de acreditación ante SUSCERTE, la cual debe ser realizada por un Auditor Informático acreditado por dicho despacho. El auditor acreditado emitirá un informe de auditoría técnica de cumplimiento de la norma y estándares aplicables y exigibles para la operación. Dicho informe de auditoría técnica se constituye en uno de los requisitos para realizar la solicitud de acreditación o de renovación de acreditación ante SUSCERTE.

Los auditores autorizados para el proceso de acreditación o renovación son los pertenecientes al registro de auditores de SUSCERTE, información disponible en el sitio web www.suscerte.gob.ve.

8.3.2. Solicitud de acreditación o renovación.

Presentación de solicitud para acreditación o renovación de acreditación ante SUSCERTE, lo cual supone un conjunto de recaudos legales y técnicos que se debe cumplir, además del cumplimiento de los requisitos y estándares financieros solicitados por SUCERTE.

Para la solicitud de acreditación los recaudos que deben ser presentados ante SUSCERTE el cual son de tipo:

- **a.** Legal.
- **b.** Económicos-financieros.
- **c.** Técnicos.
- **d.** De auditoría.

Los recaudos deben consignarse en archivos digitalizados en formato PDF y firmados electrónicamente por el Representante legal del solicitante o una persona debidamente autorizada por éste. En caso de no contar con la firma electrónica, pueden presentarse en digital a la vista del documento físico original, con su respectiva firma autógrafa.

8.3.3. Auditoria por parte de SUSCERTE.

Una vez realizado la solicitud, SUSCERTE revisara y auditora toda la documentación requerida por el estado para el proceso correspondiente (Acreditación o Renovación) que le permita operar.

8.3. Concerniente al Modelo de Confianza de la Autoridad de Certificación (AC) Raíz con base a las leyes de la República Bolivariana de Venezuela.

La Autoridad de Certificación (AC) Raíz, señalan una autoridad de confianza, responsable de emitir y revocar los certificados utilizando en ellos las firmas electrónicas, La AC Raíz dispone de un certificado autoafirmado con su clave privada, con el que firma los certificados de clave pública de los acreditado; bajo dicho esquema la Autoridad de Certificación (AC) raíz no se encuentra subordinada a una cadena de certificación o entidad de certificación extranjera, y auto firma un certificado raíz único para la certificación de firmas electrónicas o emisión de certificados electrónicos.

La AC Raíz es la primera autoridad en la jerarquía de la Infraestructura Nacional de Certificación Electrónica, operada y administrada por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), quien se encarga del ciclo de vida de los certificados electrónicos a:

1) La propia Autoridad de Certificación Raíz del Estado Venezolano.

2) Las Autoridades de certificación de los Proveedores de Servicios de Certificación Acreditados.
3) Las Autoridades de Certificación para casos especiales en proyectos de interés nacional.

En Venezuela el ente rector de la materia es SUSCERTE el cual cumple con estándares tecnológicos y legales internacionalmente reconocidos y aplicables en la materia de certificación electrónica y es la encargada de realizar la custodia del certificado raíz al cual se encontrarán subordinados todos los PSC públicos o privados que se encuentren legalmente acreditados para operar en la República Bolivariana de Venezuela.

8.3.4. Emisión de la acreditación.

Una vez cumplidos todos los requisitos de Ley, SUSCERTE, emitirá la acreditación y número de operación asignado en caso de ser la primera solicitud se procederá a la emisión de una providencia administrativa, donde SUSCERTE junto a Authenticsing procederán al proceso de ceremonia de claves e instalarán en la plataforma tecnológica, el certificado raíz emitido y firmado por SUSCERTE; para el caso de una renovación SUSCERTE procederá emitir una publicación con respecto a la providencia administrativa de renovación en gaceta oficial.

8.4. Concerniente al Modelo de Confianza aplicado por AUTHENTICSING.

AUTHENTICSING es una sociedad mercantil, empresa de iniciativa privada, con la finalidad de constituirse como un proveedor seguro y fiable de servicios de certificación electrónica con base a lo establecido en el Decreto Ley de Mensaje de Datos y Firmas Electrónicas, con sus reglamentos y normativas que puedan sustituir a estos; donde sus servicios es ofrecer firmas y certificados electrónicos a personas naturales o jurídicas, públicas y privadas, prestar el servicio técnico y de soporte a las aplicaciones para firmas y certificados electrónicos; realizar acciones de adiestramiento en materia de firmas y certificados electrónicos, comercio electrónico y demás aplicaciones que involucren el uso de certificados electrónicos; desarrollar, mantener y ofrecer aplicaciones para tramites en línea con entes de la administración pública centralizada y descentralizada, gobernaciones y municipios de la República Bolivariana de Venezuela; compra, venta, distribución, importación y/o exportación de productos, bienes y servicios, software y hardware, así como la realización de toda clase de actividades comerciales, mercantiles e industriales lícitas, representación de empresas nacionales y extranjeras y todos aquellos actos de lícito comercio que permita la Ley, estén o no comprendidos en la enumeración de actividades que antecede.

AUTHENTICSING tiene su sede principal en la ciudad de Caracas Distrito Capital, República Bolivariana de Venezuela; por el cual cumple con todos los requisitos legales, financieros y técnicos solicitados por SUSCERTE, a través de la exhaustiva normativa dictada a tales efectos por dicho ente regulador de la actividad.

AUTHENTICSING opera bajo estándar tecnológico y claves criptográficas de autoridad subordinada, lo cual facilita la instalación del certificado raíz emitida por SUSCERTE y la independencia y seguridad de la base de datos de certificados emitidos por el **AUTHENTICSING**.

La plataforma de certificación de **AUTHENTICSING** deriva de un hardware y software criptográfico, los cuales se denominan en el caso del hardware "HSM" y en el caso del software criptográfico "Plataforma de Servicios de Certificación", el cual es propiedad de la empresa **AUTHENTICSING** está en capacidad de emitir certificados electrónicos para distintos usos.

Las claves criptográficas se mantienen fuera de línea en el Centro de Datos desde el cual opera el **AUTHENTICSING**. **AUTHENTICSING** publica la Lista de Certificados Revocados (LCR), la cual se constituye en un registro de todos aquellos certificados que, habiendo cumplido su proceso de generación y asignación de Ley, son revocados cuando se encuentra comprometida su clave, por solicitud del usuario, por uso indebido del certificado, por causa imputable al usuario o por cese de operación de **AUTHENTICSING**.

La LCR es actualizada cada veinticuatro (24) horas en la página web de **AUTHENTICSING** (**www.authenology.com.ve**), durante los trescientos sesenta y cinco (365) días de cada año calendario, mientras se encuentre en operación el **AUTHENTICSING.**

Adicionalmente el **AUTHENTICSING** cuenta con un enlace OCSP, el cual permite validar en línea el estado de los certificados. Todo proceso de vencimiento o revocación de certificado es notificado de forma automática por correo electrónico al signatario propietario del certificado.

8.5. Concerniente al Modelo de Confianza aplicado para la autoridad de registro (AR) de AUTHENTICSING.

La AR es una entidad encargada de validar y comprobar la identificación de las personas jurídicas o naturales que optan a la compra o renovación de certificados electrónicos; esto con el fin de poder dar fe pública acerca de la identidad del cliente y en consecuencia, ofrecer la prueba legal de la responsabilidad y obligaciones derivadas del uso del certificado electrónico de que se trate bajo los

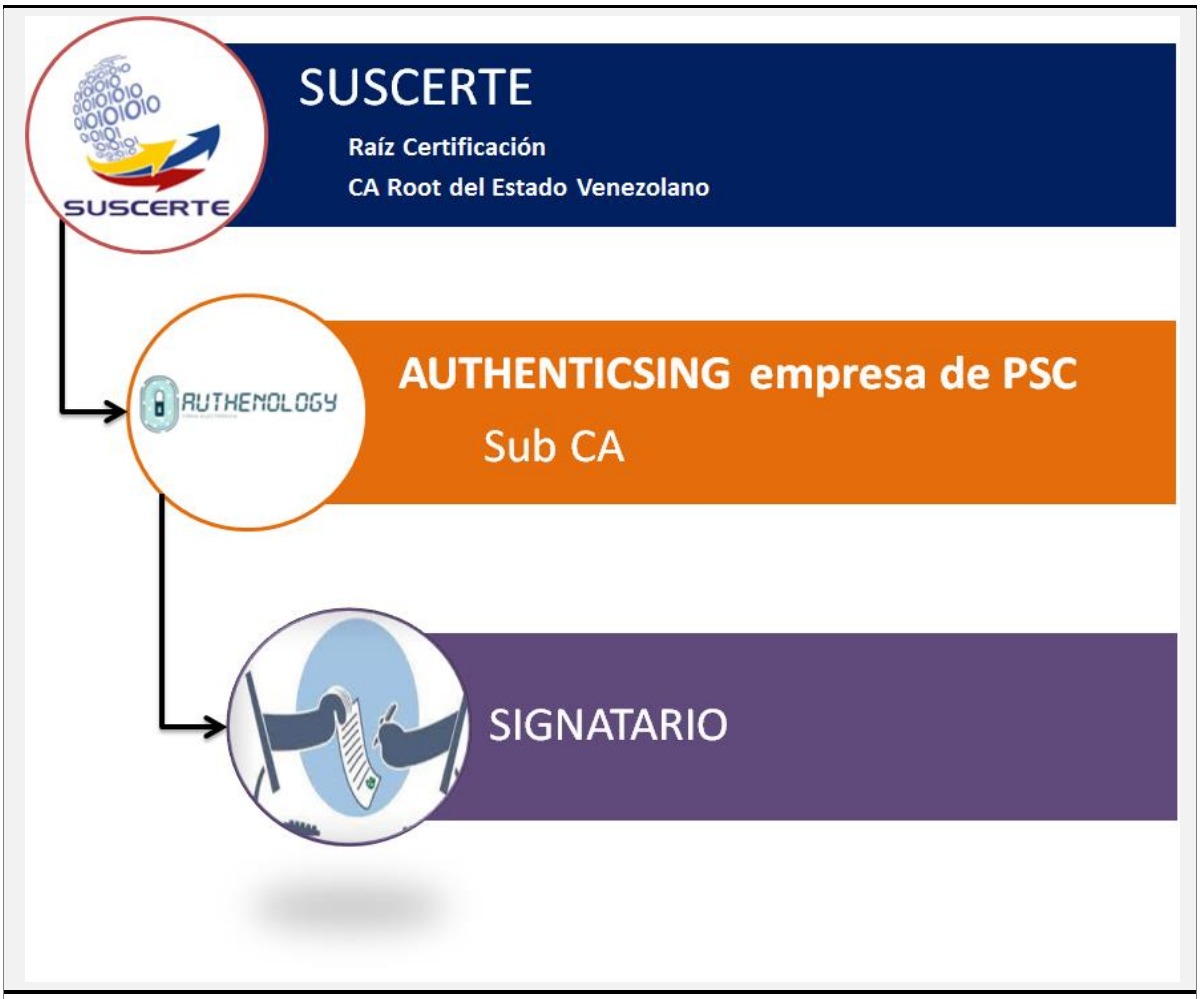
supuestos del Decreto Ley de Mensajes de Datos y Firmas Electrónicas y su Reglamento. Conforme a la normativa internacional, las autoridades de registro pueden operar por separado o integradas a las autoridades de certificación.

Para el caso del **AUTHENTICSING,** la AR se encuentra integrada dentro del sistema de validación y certificación de clientes. Todos los interesados en obtener un certificado electrónico bajo el Decreto Ley de Mensajes de Datos y Firmas Electrónicas, su Reglamento y la normativa SUSCERTE, deberán acceder a la página web de **AUTHENTICSING (www.authenology.com.ve)**, incluir su datos e información solicitada y remitir la documentación soporte de sus datos en original o copia certificada y atender la cita fijada por la AR a los efectos de realizar la verificación y registro de los soportes y demás documentos que acreditan la identidad y/o representación de los representantes de personas jurídicas que opten por un certificado electrónico bajo el Decreto Ley de Mensajes de Datos y Firmas Electrónicas y su Reglamento, así como para dejar constancia de su validación de identidad.

Si el interesado no acude a la entrevista pautada por la AR a los efectos de validar su identidad, sin causa justificada, se procederá a establecer una nueva cita; si el interesado no atiende la nueva cita, quedará anulada su solicitud o petición de registro y se le aplicará una retención por penalidad equivalente al 100% del costo del certificado.

La documentación soporte utilizada para validar a los clientes que solicitan certificados electrónicos será almacenada por el **AUTHENTICSING** durante el período de vigencia del certificado o de cualquiera de sus renovaciones, de ser ese el caso. Los registros de archivo digital de certificados en todo caso tendrán una vigencia de diez (10) años antes de proceder a su desincorporación y disposición.

Imagen



Esquema del Modelo de Confianza

8.6. Concerniente al Modelo de Confianza del Certificado Electrónico de AUTHENTICSING.

Por normativa y como parte del proceso de emisión de certificados electrónicos, todo cliente o signatario, usuario de firmas electrónicas y certificados electrónicas, debe y tiene que proceder al recibir un certificado emitido por un acreditado ante SUSCERTE proceder a verificar la validez y vigencia de dicho certificado electrónico. En el caso de **AUTHENTICSING** el cliente deberá cumplir los pasos siguientes:

8.6.1. Acceder al Contenido.

Acceder al contenido de detalle del certificado electrónico y validar la cadena de confianza, partiendo desde SUSCERTE, luego **AUTHENTICSING** y por último el cliente propietario del certificado

electrónico.

8.6.2. Validez del Certificado.

Revisar la validez o vigencia del Certificado electrónico emitido por **AUTHENTICSING.**

8.6.3. Consultar la lista de Certificados Revocados LCR.

Si el sistema no acepta de forma automática el certificado o firma electrónica, el cliente deberá consultar la Lista de Certificados Revocados publicada por el **AUTHENTICSING** en su página web www.authenology.com.ve

8.6.4. Verificación.

Verificar que el sistema no genere un mensaje de firma o certificado corrupto. En caso de ser generado dicho mensaje no se debe confiar en el mensaje.

9. Distribución de claves públicas.

9.1. Generación y distribución de los certificados

La AC de AUTHENTICSING se asegurará la verificación de la integridad y la autenticidad de la clave pública, la AC la firma asegurando de esta forma lo anterior, así como cualquier parámetro asociado que se mantenga durante su distribución a las partes que confían.

La AC de AUTHENTICSING verifica y firma las claves públicas poniéndola de esta forma a disposición de las partes que confían. De esta manera se asegura la integridad de las mismas y se autentica su origen a los efectos de garantizar su distribución confiable.

10. ACTORES SUJETOS AL CUMPLIMIENTO DE LA POLÍTICA.

El presente documento del modelo de confianza del de **AUTHENTICSING**, emitido conforme a los lineamientos de SUSCERTE, se constituye en norma de obligatorio cumplimiento y sujeción por parte de los actores que se indican a continuación:

- Alta Dirección del **AUTHENTICSING**.

- Empleados de **AUTHENTICSING**.
- Clientes usuarios de certificados electrónicos emitidos por el de **AUTHENTICSING**.
- Parte Interesada de los certificados electrónicos emitidos por el de **AUTHENTICSING.**

11. MECANISMO PARA EL DESARROLLO, AJUSTE Y APROBACIÓN.

11.1 Desarrollo del documento

El presente documento de modelo de confianza de **AUTHENTICSING** cumple con bases a las normativas de acreditación estipulada y aplicada por SUSCERTE ente rector en la materia en Venezuela, a los interesados a convertirse en Proveedores de Servicios de Certificación.

11.2 Ajuste.

Los cambios que se puedan dar en la legislación de la República Bolivariana de Venezuela con respecto al Decreto Ley de Mensajes de Datos y Firmas Electrónicas, su reglamento, Normativas en SUSCERTE o algún ajuste o cambio en la normativas internacionales vinculada y obligatoria para las operaciones y prestación de servicios exigida, conllevaran a realizar cambios o ajuste sustanciales o parciales en los procesos de seguridad, operación y procedimientos de las actividades de **AUTHENTICSING** esto con el fin de ajustar los procesos y procedimientos a los estándar y normativas aplicable por SUSCERTE para operadores en la República Bolivariana de Venezuela.

Todo ajuste que se le realicen al presente documento Modelo de Confianza se basara en el trabajo mancomunado entre el personal del área técnico y legal de **AUTHENTICSING** el cual deberá contar con la aprobación de la directiva de la **AUTHENTICSING** para su posterior implementación de cambio.

11.3 Aprobación.

Los procesos asociados a la revisión, modificación o ajuste y aprobación con respecto a la documentación de **AUTHENTICSING** serán regulados por el formato del Modelo de la Política de Documentación y Gestión Documental.

11.4 Funciones y Responsabilidades dentro de AUTHENTICSING.

Las funciones y las responsabilidades de los distintos niveles dentro de **AUTHENTICSING**, respecto al manejo, control y resguardo del presente documento, se encuentran definidos en el Documento de la Política para el Establecimiento de Funciones y Responsabilidades.

12. MARCO LEGAL Y NORMATIVO.

- 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 27001:2022

--- Fin de Documento ---