AUTHENOLOGY
FIRMA ELECTRÓNICA

AUTHENTICSING C.A.

Políticas y Plan de Administración de Claves Criptográficas.

2024

Zolange Gonzalez Colon

Firmado digitalmente por Zolange Gonzalez Colon
Fecha: 2024.02.14 19:52:02 -04'00'

Resumen de Información.

Empresa	**AUTHENTICSING C.A.**		
Documento	Política y Plan de Administración de Claves Criptográficas (Implementación y Mantenimiento).		
Tipo de Documento	Documentación Técnica sobre Planes de Seguridad.		
ID	DIF-003		
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**	**- 27 -**
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.

Política y plan de administración de claves criptográficas.

3. CÓDIGO DEL DOCUMENTO

DPL-003

4. INTRODUCCIÓN.

El presente documento constituye la Política y Plan de Administración de Claves Criptográficas (Implementación y Mantenimiento) parte de los Proveedores de Certificados AUTHENTICSING a fines de comunicar, informar y documentar cada uno de los procesos de certificación, para ofrecer una mejor y sencilla comprensión e entendimiento por parte de la Alta dirección, Clientes, Proveedores, Personal y otros interesados en AUTHENTICSING.

Política y Plan de Administración de Claves Criptográficas (Implementación y Mantenimiento), permite a la Alta dirección, Clientes, Proveedores, Personal, y otros interesados del PSC, dar a entender cada uno de los desarrollos y subdesarrollos involucrados en las etapas de vida de los certificados electrónicos; documentar los procesos de recuperación ante accidentes, uso de claves criptográficas y proporcionar una perspectiva general de los equipos e infraestructura que sostiene el esquema de seguridad de AUTHENTICSING .

5. 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.
- **Continuidad del negocio:** Es la "capacidad estratégica y táctica de la organización para planificar y responder ante los incidentes e interrupciones del negocio con el fin de permitir la continuidad de las actividades operativas y comerciales en un nivel aceptable previamente definido"
- **Recuperación ante desastres:** se refiere "al proceso, políticas y procedimientos relacionados con preparar la recuperación o continuación de la infraestructura tecnológica crítica de una organización después de un desastre natural o producido por el hombre".

- **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.
- **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 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).

6. OBJETIVO.

El presente documento de Política y Plan de Administración de Claves Criptográficas (Implementación y Mantenimiento), tiene como objetivo mostrar e informar a los usuarios cada proceso que debe cumplir con la finalidad de proceder a gestionar el proceso de solicitud de certificado de firma electrónica y así poder garantizar el cumplimiento del marco legal y las normativas dadas por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).

7. ALCANCE.

El presente documento de Política y Plan de Administración de Claves Criptográficas (Implementación y Mantenimiento) 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 revocación o renovación y de emisión de certificados y funcionamiento de la plataforma tecnológica de certificación de AUTHENTICSING.

8. ÁMBITO DE APLICACIÓN.

Relativas al Personal: El equipo de trabajo de AUTHENTICSING tendrá que cumplir con cada uno de los pasos descritos en el actual documento Contentivo de la Política y del Plan de Administración de Claves Criptográficas (Implementación y Mantenimiento) de AUTHENTICSING. Cada procedimiento no contemplado en el actual documento deberá contar con la aprobación formulada y de forma escrita de la alta dirección de la Autoridad de Certificación (AC) de AUTHENTICSING y de

SUSCERTE, y de lo contrario será considerado como una acción de sabotaje para fines internos de AUTHENTICSING y será sancionado y penalizado con despido justificado, por infracción e incumplimiento de las obligaciones requeridas que es aplicada a la relación de trabajo.

8.1 Referente al personal.

El Personal de la Autoridad de Certificación (AC) y la Autoridad de Registro (AR) de AUTHENTICSING, deberá cumplir con todos y cada uno de los pasos puntualizados en el actual documento **"Política y del Plan de Administración de Claves Criptográficas (Implementación y Mantenimiento"** de AUTHENTICSING. Los procedimientos no contemplado en el actual documento, deberá contar con la aprobación formulada y de forma escrita de la alta dirección de la Autoridad de Certificación (AC) de AUTHENTICSING y de SUSCERTE, y de lo contrario será considerado como una acción de sabotaje para fines internos de AUTHENTICSING y será sancionado y penalizado con despido justificado, por infracción e incumplimiento de las obligaciones requeridas que es aplicada a la relación de trabajo.

Cada alteración o cambio del actual documento procedente de la actualización de normas y procedimientos así como por alguna renovación tecnológica, deberá ser documentada y contar con la aceptación de la alta dirección de la Autoridad de Certificación (AC) de AUTHENTICSING y de SUSCERTE, para su publicación.

8.2 Referente a las claves.

La clave privada de AUTHENTICSING, con el objetivo de poder generar los certificados electrónicos subordinados de dicha raíz, requiere para su creación, el establecimiento de un protocolo de acceso mediante tarjetas de seguridad (smart card), este activará la plataforma de creación del par de claves (pública y privada), el certificado raíz igualmente servirá con los efectos de instalar, desinstalar, activar o desactivar el certificado raíz de la Autoridad de Certificación (AC). El certificado Raíz y sus subordinados son generados con algoritmo de firma ECDSA-WITH-SHA 384 y la longitud de curva eliptica; la Raíz es de 512 bits y la longitud de clave de los usuarios finales es de 384 bits. El certificado Raíz de AUTHENTICSING es almacenado y resguardado en un dispositivo Hardware Security Module (HSM) el cual cumple con el estándar FIPS 140-2. Únicamente las llaves de la Raíz de AUTHENTICSING se mantienen en el dispositivo HSM. Las llaves de los usuarios son generadas por ellos mismos en el proceso de generación del certificado. AUTHENTICSING no mantiene repositorio de las claves privadas de los signatarios.

La gestión, manejo y ciclo de vida de las claves criptográficas de AUTHENTICSING, debe ser establecido con el objetivo de contemplar cada uno de los niveles de seguridad, acceso, reposición y creación de dichas claves. De igual forma, la Autoridad de Certificación (AC) AUTHENTICSING debe asegurar que los certificados electrónicos subordinados al certificado electrónico raíz emitido por SUSCERTE, cuenten con los niveles de seguridad requeridos, acceso, reposición y creación conveniente, con la finalidad de garantizar la integridad y uso de los mismos.

8.3 Referente a los Roles

El manejo del ciclo de vida de las claves criptográficas tanto de la Autoridad de Certificación (AC) AUTHENTICSING, como de las claves criptográficas generadas por los signatarios, la Autoridad de Certificación (AC) AUTHENTICSING debe documentar y definir todas las actividades y roles que serán realizados por cada uno de los representantes involucrados en el uso de los certificados y de las claves. La presente política, contempla el establecimiento y descripción de los distintos roles involucrados en el manejo del ciclo de vida de la clave criptográficas, además, contempla los aspectos mencionados a la administración del ciclo de vida del hardware criptográfico utilizado por la Autoridad de Certificación (AC) AUTHENTICSING.

A continuación se hace mención de los roles definidos a los efectos de la presente política:

- Rol de Infraestructura de Clave Pública (ICP),
- Rol de Modulo de Seguridad de Hardware (HSM) y Rol de Seguridad.

La presente política contempla y analiza la descripción por separado de cada rol, los cuales pueden ser realizados por grupos separados de trabajo o por un mismo trabajador en caso de ser requerido por razones de Causa Extraña de algún incumplimiento o Fuerza Mayor.

8.1.1 Rol de Infraestructura de Clave Pública (ICP)

El concepto del rol ICP, es necesario definir como tal, al encargado de gestionar la infraestructura de clave pública utilizada por la Autoridad de Certificación (AC) AUTHENTICSIN, para la generación del par de claves requerida por la Autoridad de Certificación (AC) AUTHENTICSING para generar a su vez el certificado raíz del cual dependerán los certificados subordinados usados por diferentes usuarios de la plataforma de certificación de AUTHENTICSING. El rol ICP limitará cuatro roles

principales para su manejo. Más de un rol puede ser efectuado por una persona, siempre y cuando no exista ninguna dificultad o conflicto de interés. Dichos roles son los siguientes:

8.1.1.1 Administrador de la Autoridad de Certificación (AC) AUTHENTICSING.

El Administrador de la Autoridad de Certificación (AC) AUTHENTICSING es consciente y responsable de la administración de la cuenta y de la generación del par de claves (pública y privada) de la Autoridad de Certificación (AC) AUTHENTICSING. Por definición y entendimiento, el cargo de Administrador de la Autoridad de Certificación (AC) AUTHENTICSING será ocupado y ejercido por un (1) solo representante de la Alta Dirección de AUTHENTICSING El Administrador mantiene y configura la Autoridad de Certificación (AC) AUTHENTICSING Un usuario al que se le haya asignado el rol de Administrador de la AC AUTHENTICSING puede denominar o nombrar otros Administradores de Autoridad de Certificación (AC), Gerente de Certificados, previa autorización de la Alta Dirección de AUTHENTICSING, para llevar a cabo las tareas son las siguientes:

- **Configuración de extensione**s: Definir el Localizador Uniforme de Recursos (LUR) o en su denominación en inglés Uniform Resource Locator (URL) para los Puntos de Distribución de la lista de certificados revocados (LCR) y Acceso de Autoridad de Información (AAI).
- **Configurar los módulos de política y salida:** Los módulos de política y salida establecen la acción que toma una Autoridad de Certificación (AC) en el transcurso de la emisión del certificado. Por ejemplo, el módulo de política le permite al Administrador de la AC AUTHENTICSING configurar si cada una de las solicitudes de certificados se mantiene en estado pendiente o se aprobaran de manera automática apoyándose en las credenciales del usuario. Un módulo de salida le permite definir si la información del certificado es publicada en una base de datos redundante.
- **Designar al gerente de certificados:** Designar al Gerente de Certificados para emitir y negar solicitudes de certificados y para extraer claves privadas cifradas de la base de datos de la AC AUTHENTICSING para la recuperación de claves en caso de una contingencia mayor. Por definición y diseño, el puesto de Gerente de Certificados será ocupado.
- **Determinar las restricciones del gerente de certificado:** Establecer y documentar todas funciones y atribuciones del Gerente de Certificado al momento de administrar las claves criptográficas de

la Autoridad de Certificación (AC) AUTHENTICSING o de administrar la gestión de los certificados electrónicos subordinados y emitidos por la Autoridad de Certificación (AC) AUTHENTICSING.

- **Limitar al gerente de certificados:** Limitar al Gerente de Certificados para emitir y negar solicitudes de certificados y para retirar o sustraer las claves privadas cifradas de la base de datos de la Autoridad de Certificación (AC) AUTHENTICSING para la recuperación de claves en caso de una contingencia mayor. Por definición y entendimiento, el cargo de Gerente de Certificados será ocupado y ejercido por el Gerente de Informática de AUTHENTICSING.
- **Limitar el agente de recuperación de clave:** Limitar al agente de recuperación de clave de certificados en la Autoridad de Certificación (AC) AUTHENTICSING para el archivo y la recuperación de clave privada de la Autoridad de Certificación (AC) AUTHENTICSING. En caso de no existir nombramiento del cargo, las actividades fundamentales al mismo serán realizadas de manera conjunta por un (1) representante de la Alta Dirección y el Gerente de Informática de AUTHENTICSING.
- **Manejo de la Autoridad de Certificación (AC)** AUTHENTICSING: Llevar a cabo cada una de las tareas y actividades asociadas y necesarias para la correcta operación, administración y manejo de la Autoridad de Certificación (AC) AUTHENTICSING.
- **Configurar la Lista de Certificados Revocados (LCR): Determinar**: y establecer de forma conjunta con el Gerente de Certificados, todos los aspectos relacionados con la publicación de la LCR y revocación de la LCR dentro de la plataforma de certificación de la AC AUTHENTICSING.
- **Configurar la lectura de información de Autoridad de Certificación (AC):** Configurar la Autoridad de Certificación (AC) AUTHENTICSING y capacitar únicamente las áreas de la Autoridad de Certificación (AC) AUTHENTICSING susceptibles de ser modificadas por el Administrador de la AC AUTHENTICSING y el resto del personal de operaciones de AUTHENTICSING.
- **Detener y arrancar los Servicios de Certificados**: Detener y arrancar junto al Gerente de Certificados y un (1) operador los Servicios de Certificados para emplear cambios de registro, sujetos al cumplimiento y desempeño realizado de la normativa contenida en la Ley de Mensajes de Datos y Firmas Electrónicas y su reglamento, la norma de SUSCERTE y la normativa de la Autoridad de Certificación (AC) AUTHENTICSING aplicable.
- **Configurar parámetros de auditoría:** Definir la frecuencia de las

auditorías informáticas de cumplimiento de la plataforma AUTHENTICSING, sujetas al acatamiento de la normativa contenida en la Ley de Mensajes de Datos y Firmas Electrónicas y su reglamento, la norma de SUSCERTE y la normativa de la Autoridad de Certificación (AC) AUTHENTICSING aplicable.

8.1.1.2 Gerente de Certificado.

El Gerente de Certificado es consciente y responsable de la utilización del certificado incluyendo la emisión y revocación de certificados. Por definición y entendimiento, el puesto de Gerente de Certificados será ocupado y ejercido por el Gerente de Informática de AUTHENTICSING. Este rol aprueba o niega las solicitudes de inscripción para certificado, también revoca certificados emitidos. Concretamente, un usuario al que se le asigne el rol de Gerente de Certificado puede:

- **Emitir o negar solicitudes de certificados pendientes**: En una Autoridad de Certificación (AC) independiente de todas las solicitudes de certificados se encuentran pendientes predeterminada hasta que el Gerente de Certificado valide las solicitudes de certificado. Igualmente, se puede definir una plantilla de certificado de forma que el Gerente de Certificado deba validad la solicitud de certificado antes que la Autoridad de Certificación (AC) emita el certificado.
- **Revocar certificados emitidos**: El Gerente de Certificado puede revocar un certificado pero solo si la política de revocación de certificados de la Autoridad de Certificación (AC) AUTHENTICSING requiere de la revocación del certificado. Establecer y determinar los agentes de recuperación de clave. El Gerente de Certificado establece que un agente de recuperación de clave definido puede descifrar una clave privada archivada en la base de datos de la Autoridad de Certificación (AC) AUTHENTICSING.

8.1.1.3 Auditor: El Auditor es responsable de mantener, conservar y supervisar las entradas de los registros de auditoría de la Autoridad de Certificación (AC) en el registro de "Windows Security".

- En el caso de no existir nombramiento del cargo, las actividades fundamentales al Auditor serán efectuadas de manera conjunta por el Gerente de Informática y un (1) solo Operador de AUTHENTICSING, reportado en funciones al Administrador de la Autoridad de Certificación (AC) AUTHENTICSING.

- El auditor puede determinar los controles internos de auditoría de la Autoridad de Certificación (AC) AUTHENTICSING para los servicios de certificación. Incluyendo la definición de eventos específicos y el control de los registros de eventos de seguridad para la verificación de los sucesos relacionados con los servicios de Certificación. El auditor puede habilitar desde la consola de la Autoridad de Certificación (AC) AUTHENTICSING ubicada en el centro de datos AUTHENTICSING , con las funciones siguientes:
  - Respaldo y restablecimiento de la base de datos de la Autoridad de Certificación (AC) AUTHENTICSING. Registra todos los intentos para respaldar o restablecer la base de datos de la Autoridad de Certificación (AC) AUTHENTICSING en el “Windows Security log”.
  - Cambio de configuraciones de la Autoridad de Certificación (AC) AUTHENTICSING. Registra cada uno de los intentos para modificar la configuración de la Autoridad de Certificación (AC) . AUTHENTICSING Puede incluir la definición de la AAI y las URLs, CDP y/o la definición de un Agente de Recuperación de Clave.
  - Cambio de los controles de seguridad de la Autoridad de Certificación (AC) AUTHENTICSING. Registra todo intento de modificar los permisos de la Autoridad de Certificación (AC) AUTHENTICSING. Puede incluir; agregar Administradores de AC o Gerentes de Certificados.
  - Manejo y emisión de solicitudes de certificados. Registra todos los intentos realizados por un Gerente de Certificado para validar o negar solicitudes de certificados que están pendientes por aprobación.
  - Revocación de certificados y publicación de la LCR. Registra todos y cada uno de los intentos realizados por un Gerente de Certificado para revocar o emitir certificado por el Administrador de la Autoridad de Certificación (AC) AUTHENTICSING para publicar una LCR actualizada.
  - Almacenamiento y recuperación de claves archivadas. Registra todos y cada uno de los intentos en el transcurso de proceso de inscripción para archivar claves privadas en la base de datos de la Autoridad de Certificación (AC) AUTHENTICSING o realizados por el Gerente de Certificados para retirar o extraer claves privadas archivadas de la base de datos de la Autoridad de Certificación (AC) AUTHENTICSING.
  - Arranque y cierre de los Servicios de certificado. Registra todos y cada uno de los intentos realizados por el

Administrador de la Autoridad de Certificación (AC) AUTHENTICSING para arrancar o cerrar los servicios de certificación.

8.1.1.4 Operador de respaldo.

El Operador de Respaldo es el administrador responsable de efectuar los respaldos de la información de la ICP, y realizar respaldos bajo la supervisión del Gerente de Informática de AUTHENTICSING, a continuación se mencionan las actividades:

- Programar los respaldos automáticos de la base de datos de la Autoridad de Certificación (AC) AUTHENTICSING.
- Comprobar el debido funcionamiento de la combinación de hardware y software de respaldo.
- Realizar el respaldo semanal acatando la política de respaldo de la Autoridad de Certificación (AC) AUTHENTICSING.
- Realizar la configuración del par clave privado y público de la Autoridad de Certificación (AC) AUTHENTICSING Si el par clave privado y público de la Autoridad de Certificación (AC) está almacenado en un Módulo de Seguridad de hardware (MSH), el Operador de Respaldos solo podrá respaldar el par clave si el contexto de seguridad del MSH permite esta acción.

8.1.2 Rol de módulo de seguridad de hardware (HSM)

La definición del rol HSM, es necesario definir al Módulo de Seguridad de Hardware (HSM) usando, almacenar y proteger la clave privada solicitada por la Autoridad de Certificación (AC) AUTHENTICSING por lo que dependerán los certificados subordinados utilizados por los distintos usuarios de la plataforma de certificación de AUTHENTICSING . El rol HSM comprende la descripción del manejo, funcionalidades y las opciones proporcionada por el dispositivo o hardware criptográfico utilizado por la Autoridad de Certificación (AC) AUTHENTICSING, con la finalidad de proteger su clave privada. El hardware de cifrado usado por la Autoridad de Certificación (AC) AUTHENTICSING se denomina “nShield PCI 500 TPS, F3”. El referido dispositivo permite ejecutar operaciones sobre él mismo, mediante el empleo de una o más tarjetas de seguridad (smart card).

8.1.2.1 Rol de seguridad: La definición del rol de seguridad, es necesario definir el Modulo encargado de administrar y gestionar la seguridad de las tarjetas de seguridad de la Autoridad de Certificación (AC) AUTHENTICSING, requerida para mantener y conservar la integridad de la clave privada solicitada por la Autoridad de Certificación (AC) AUTHENTICSING. Las tarjetas de seguridad son duplicadas o divididas. Adicionalmente, estas copias y las partes divididas no se almacenan en la misma ubicación. El acceso a la ubicación de las tarjetas de seguridad se encuentra dividido en función del rol desempeñado y establecido en la presente política. El referido acceso es el siguiente:

- **Grupo de Acceso A:** El Acceso A tiene la combinación del On-site, es decir, en una caja de seguridad localizada en la Autoridad de Certificación (AC) AUTHENTICSING y del Off-site, es decir, de la bóveda designada y contratada por AUTHENTICSING por el motivo antes mencionado.
- **Grupo de Acceso B:** El Acceso B tiene acceso autorizado Off-site, es decir, en una bóveda externa contratada por AUTHENTICSING por el motivo antes mencionado.

9. CICLO DE VIDA DE LAS CLAVES DE LA AUTORIDAD DE CERTIFICACIÓN (AC) AUTHENTICSING.

9.1 Generación de las claves de la Autoridad de Certificación de firma electrónica del PSC o CE.

La generación de la clave de pública y privada para la Autoridad de Certificación (AC) AUTHENTICSING, se realiza mediante la activación de la ceremonia de generación de clave en FECHA -- DE --- DE 20--. La Autoridad de Certificación (AC) AUTHENTICSING, ha decretado los parámetros y lineamientos bajo los cuales se realizará la generación de claves, las mismas se describen a continuación:

- Asignación de las tarjetas a Administradores y custodios.
- Activación del nuevo Mundo de Seguridad en el módulo criptográfico.
- Se instalará la Autoridad de Certificación bajo el modo de Subordinada, y se generará la petición de certificado.
- Se generará el respectivo certificado por parte de SUSCERTE.
- Se instalará y activará el certificado de la Autoridad de Certificación (AC) AUTHENTICSING.

9.2 Almacenamiento, respaldo y recuperación de la clave.

9.1.1 Recuperación de clave.

Después de establecer las claves públicas y privadas en hardware criptográfico (HSM), se crearan dos símbolos (duplicados) de respaldo para efectos de recuperación, uno es almacenado en sitio (“Onsite”) y el otro externamente (“Offsite”). La clave privada solo puede ser recuperada utilizando un símbolo de respaldo y las llaves 1, 3 y 5 o sus respectivas tarjetas de respaldo. Cada uno de los detalles técnicos y operacionales sobre el respaldo y la recuperación de la clave privada de la Autoridad de Certificación (AC) AUTHENTICSING se encuentran detalladamente en el Manual de Operación de la Autoridad de Certificación (AC) AUTHENTICSING.

9.1.2 Respaldo de la Clave.

El respaldo de la clave privada es realizada en dos (2) unidades de CD/DVD (principal y respaldo), son selladas con un precinto y almacenadas en una caja de seguridad. Los roles necesarios para realizar los procedimientos de respaldo se representan mediante la utilidad de una tarjeta de seguridad específica. Los pasos requeridos para llevar cabo un respaldo completo de la clave privada de la Autoridad de Certificación (AC) AUTHENTICSING y para obtener un símbolo de respaldo se describen en la tabla siguiente:

Descripción del Procedimiento.
1. Ingresar como administrador al servidor de certificación donde está instalado YuviHSM_2.
2. Se detienen todos los Servicios de la entidad de certificación.
3. tener a disposición al menos 2 unidades de CD/DVD, precinto y la caja de seguridad.
4. Insertar el CD/DVD en la unidad copiadora de CD/DVD.
5. Generar una copia de la carpeta nFast ubicada en el disco C del servidor de certificación en el primer CD/DVD.
6. Generar una copia de la carpeta nFast ubicada en el disco C del servidor de certificación en el segundo CD/DVD.
7. Verificar que la carpeta nFast\local se haya copiado satisfactoriamente en ambas unidades de CD/DVD.
8. Colocar el CD/DVD en su respectiva caja, colocar los precintos e introducirlo en la caja de seguridad.

9.1.3 Recuperación de Clave

Si se desea efectuar una operación de recuperación de la clave privada de la "Root AUTHENTICSING", se debe aplicar el siguiente procedimiento:

Descripción del Procedimiento.
1. Colocar el HSM en modo "Initialization"
2. Copiar la carpeta de backup "nfast\local" en "c:\nfast\local"
3. Ejecutar el comando: "C:\nfast\bin>new-world -l"
4. Introducir las tarjetas de seguridad 3 (permisos de administración) y la passphrase
5. Introducir las tarjetas de seguridad 5 (permisos de administración) y la passphrase
6. Introducir las tarjetas de seguridad 1 (permisos de operación) y la passphrase
7. Colocar el HSM en modo operacional

9.3 Distribución de la clave pública de la AC de firma electrónica.

La clave pública de la Autoridad de Certificación (AC) AUTHENTICSING está distribuida a través de su certificado raíz que es emitido pro SUCERTE y la publicación es realizada por medio la página web de AUTHENTICSING (www.authenology.com.ve) utilizando su canal seguro SSL.

De igual manera, cumpliendo con lo establecido en la ley de mensajes de datos y firmas electrónicas (LSMDFE), se publica en la página web de AUTHENTICSING toda la información relativa a la declaración de prácticas DPC, Políticas de Certificados PC, Lista de Certificados Revocados LCR y del respondedor OCSP.

9.4 Uso de la clave privada de la AC de firma electrónica.

El uso de la clave privada de la Autoridad de Certificación (AC) AUTHENTICSING, estará contemplado para la firma de certificados electrónicos para Autoridades Subordinadas, certificados establecidos en las Políticas de Certificados y la firma de las listas de Certificados Revocados (LCR) correspondientes.

9.5 Termino del ciclo de vida de la AC de firma electrónica.

La vigencia de la acreditación es de diez (10) años, una vez espirado este plazo, se debe realizar la renovación de la certificación mediante el cumplimiento de los procedimientos operativos establecidos por la SUSCERTE.

9.6 Revocación del certificado del PSC o CE.

La clave privada de origen de la Autoridad de Certificación (AC) AUTHENTICSING puede ser destruida retornando al HSM a su estado original de fábrica y borrando cada uno de los símbolos de respaldo. Para la destrucción completamente de la clave privada originaria de la Autoridad de Certificación (AC) AUTHENTICSING, se deben seguir los pasos siguientes:

- **Inicializar el HSM:** Al reinicializar el HSM se borra toda información existente de dicho HSM y esto implica también para sus datos. Luego, se deben inicializar el HSM ejecutando el Security World.
- **Destrucción física de las tarjetas:** La Autoridad de Certificación (AC) AUTHENTICSING creó dos (2) unidades de respaldo para los procedimientos de Recuperación de Clave. Para neutralizar la clave privada de origen de la Autoridad de Certificación (AC) AUTHENTICSING, se deben destruir dichas unidades.

10. ADMINISTRACION DEL CICLO DE VIDA DEL HARDWARE CRIPTOGRAFICO UTILIZADO POR LA AC.

10.1 Asignación de tarjetas criptográficas.

Se activa el mundo de seguridad de la HSM y se asignan 3 tarjetas criptográficas para administradores, las cuales estarán bajo la custodia de los siguientes responsables:

- Gerente general de Authenticsing.
- Gerente de la infraestructura de clave pública.
- Gerente de seguridad de la información y plataforma.

10.2 Roles de los Administradores de tarjetas criptográficas.

- Creación de claves de custodios.
- Administrador de la lista de control de acceso.
- Asignación de tarjetas criptográficas.
- Definición de roles en el HSM.

- Definición de parámetros de seguridad.
- Generación y restauración del par de claves.
- Cambiar y eliminar claves de acceso.
- Formatear criptográficas.

10.3 Longitud de las claves criptográficas.

AUTHENTICSING se encuentra en posibilidad de producir certificados de firma electrónica con clave ECDSA-WITH-SHA 384 y la longitud de curva elíptica. El estándar valido por SUSCERTE para los certificados nacionales es de 256 bit de longitud de tamaño mínimo de clave

11. SERVICIOS DE ADMINISTRACIÓN DE LAS CLAVES DE LOS SIGNATARIOS SUMINISTRADAS POR LA AC (GENERACIÓN DE CLAVE, RENOVACIÓN DESPUÉS DE VENCIMIENTO Y REVOCACIÓN DE LA CLAVE).

{{ñdhfñksdñfksñaldhfñlashkflñashñfljashñdjfhñasdjfhñasljdfhñslad { asdhñgñljhasñdjfhñsdjhfñsa

11.1 Generación de clave.

Con base al modelo de negocio de AUTHENTICSING y su plataforma de servicio de certificación, se encuentra configurado para que el signatario sea el responsable de generar el par de clave pública y privada desde las oficinas de AUTHENTICSING. Una vez sea generado el certificado electrónico, se le hará entrega al signatario en una unida externa (pendrive) el certificado electrónico junto con el aplicativo para poder firmar.

11.2 Renovación después de vencida.

Para el proceso de renovación de una clave para certificado electrónico después de vencida, este será igual al procedimiento como si fuera a solicitar un certificado por primera vez, documento de Política de Certificados (PC) y Declaración de Prácticas de Certificación (DPC) (DIF-002) punto 15.2, 16.1.3. Y 20.3.

11.3 Revocación de clave.

Con base a las políticas, normas y procedimientos con el cual opera el AUTHENTICSING bajo el diseño de su plataforma tecnológica de certificación el cliente envía la solicitud de suspensión o revocación de su certificado por el aplicativo web en la siguiente dirección www.authenology.com.ve, de acuerdo con los métodos y procedimientos específicos descritos en el siguiente apartado

(15.1.1) del documento de Política de Certificados (PC) y Declaración de Prácticas de Certificación (DPC) (DIF-002)

12. PREPARACIÓN DE LOS DISPOSITIVOS SEGUROS DE LOS SIGNATARIOS.

La Autoridad de Certificación (AC) AUTHENTICSING, le ofrece al signatario la posibilidad de proteger su clave privada usando un dispositivo de seguridad (eToken). Dicho dispositivo es organizado de la manera siguiente

- La Autoridad de Certificación (AC) obtiene el dispositivo desde un proveedor autorizado por el fabricante.
- Posteriormente la recepción verifica y valida la correcta operatividad y funcionamiento de los dispositivos adquiridos.
- Antes de hacer la entrega al signatario de dicho dispositivo, la Autoridad de Certificación (AC) AUTHENTICSING lo inicializa (borra todo su contenido) y configura la opción de exigir al signatario crear una nueva contraseña para activar el dispositivo.

13. REPRESENTANTES SUJETOS AL CUMPLIMIENTO DE LA POLÍTICA

El actual documento de la Política y del Plan de Administración de Claves Criptográficas (Implementación y Mantenimiento) de PSC AUTHENTICSING, emitido de acuerdo a los lineamientos de AUTHENTICSING, se establece en reglamento de obligatorio cumplimiento y obediencia por parte de los representantes que se indican a continuación:

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

14. MECANISMO PARA EL AJUSTE, DESARROLLO Y APROBACIÓN.

14.1 Mecanismo para ajuste del documento

Los cambios en la Ley de Mensajes de Datos y Firmas Electrónicas, su Reglamento, la normativa de SUSCERTE o la norma internacional obligatoria

y exigida para la operación de los PSC, que contemplen los cambios fundamentales en los procedimientos de seguridad y operación, los cuales incluyen variación de los procesos y actividades de los PSC, producirán una revisión del actual documento, con el objetivo de cambiar los procesos y procedimientos a los estándares y normativas aplicable y validada por SUSCERTE para la operación de los PSC. Cada cambio al presente documento de la Política y del Plan de Administración de Claves Criptográficas (Implementación y Mantenimiento) de AUTHENTICSING, será producto del trabajo del equipo técnico y legal de AUTHENTICSING y deberá contar para su implantación, con la aprobación de Alta Dirección.

14.2 Mecanismo de desarrollo del documento

El actual documento de la Política y del Plan de Administración de Claves Criptográficas (Implementación y Mantenimiento) de AUTHENTICSING, se encuentra desarrollado sobre la base de la normativa de acreditación aplicable a los interesados a convertirse en Proveedores de Servicios de Certificación. Referida normativa de acreditación es dictada y emitida por SUSCERTE, ente rector de la materia dentro de la República Bolivariana de Venezuela.

El actual documento de la Política y del Plan de Administración de Claves Criptográficas (Implementación y Mantenimiento) de AUTHENTICSING cumple con cada uno de los requerimientos de la normativa internacional aplicable al área de certificación electrónica.

14.3 Mecanismo para la aprobación de los cambios al documento

Cada cambio o modificación del documento de la Política y del Plan de Administración de Claves Criptográficas (Implementación y Mantenimiento) de PSC AUTHENTICSING tendrá que contar con la aprobación de la Alta Dirección de AUTHENTICSING ser documentada y por escrito, indicando el número de edición y revisión, fecha de elaboración, fecha de aprobación y la firma del representante de la Alta Dirección que valide el ajuste o modificación al Manual. Posteriormente se documentará el ajuste o modificación y su aprobación.

15. MARCO LEGAL Y NORMATIVO.

- Decreto Ley de Mensaje de Datos y Firmas Electrónicas y su Reglamento.
- Normativa de SUSCERTE.
- Normativa. AUTHENTICSING
- Estándar Internacional ETSI TS 102 042

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

16. FUNCIONES Y RESPONSABILIDADES DENTRO DE LA AUTORIDAD DE CERTIFICACIÓN (AC) AUTHENTICSING.

Las funciones y responsabilidades de los diferentes niveles del PSC AUTHENTICSING, respecto al uso, control y resguardo del actual documento, están detalladas y especificadas en el documento de la Política para el Establecimiento de Funciones y Responsabilidades.

17. REVISIÓN, APROBACIÓN Y MODIFICACIÓN

Los procedimientos asociados a la revisión, aprobación, modificación o ajuste de la documentación de AUTHENTICSING, serán reglamentados por el Documento de la Política de Documentación y Gestión Documental.

--- Fin de Documento ---