AUTHENTICSING C.A.

Evaluación de la Plataforma Tecnológica

2024

Zolange Gonzalez Colon

Firmado digitalmente por Zolange Gonzalez Colon
Fecha: 2024.02.14 20:01:03 -04'00'

Resumen de Información.

Empresa	**AUTHENTICSING C.A.**		
Documento	Evaluación de la plataforma Tecnológica.		
Tipo de Documento	Documentación Técnica sobre las Políticas		
ID	DPO-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**	**- 26 -**
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.

Evaluación de la plataforma Tecnológica.

3. CÓDIGO DEL DOCUMENTO.

DPO-001

4. INTRODUCCIÓN.

El presente documento constituye la Evaluación de la plataforma Tecnológica 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 PSC **AUTHENTICSING** .

5. OBJETIVO.

El objetivo principal del actual documento de la Evaluación de la plataforma Tecnológica de AUTHENTICSING , se establece en la instauración de una mejora continua del certificado electrónico usado por los clientes, proveedores o parte interesada mediante la confirmación o verificación de las condiciones de seguridad asociadas y existentes a la plataforma tecnológica de certificación de AUTHENTICSING , permitiendo de esta manera presentar y ofrecer más y mejores

disposiciones o condiciones de generación de los certificados electrónicos y de publicación de la LCR, con el objetivo de dar cumplimiento a la normativa impuesta por SUSCERTE.

6. ALCANCE.

El actual documento de la Evaluación de la plataforma Tecnológica de AUTHENTICSING es aplicado para el proceso de verificación y comprobación de la seguridad ofrecida y garantizada por la Plataforma Tecnológica de Certificación de AUTHENTICSING durante el desarrollo y proceso de generación de certificados, de la LCR y operatividad del OCSP, de acuerdo a los lineamientos impuestos por SUSCERTE para la generación del certificado.

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

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 el PSC **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 PSC** 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 el PSC **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 PSC.

- ❖ 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 UNC 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 alegueante 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 PSC.**
- **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. Área de aplicación

7.1 Referente al personal

El personal de AUTHENTICSING**,** deberá cumplir con cada uno de los pasos especificados en el actual documento de la Evaluación de la plataforma Tecnológica.

Los procedimientos no contemplado en el presente documento, deberá contar con la aprobación expresada y por escrito de la Alta Dirección de AUTHENTICSING y de SUSCERTE, de lo contrario, se considerará como acto de sabotaje a los fines internos de **AUTHENTICSING** y será penalizado con despido comprobado y justificado, por infracción o incumplimiento con las obligaciones que impone la relación de trabajo. Cada alteración o modificación del actual documento procedente de la actualización tecnológica o de procedimientos, será justificada y posteriormente documentada, y deberá contar con la aprobación de la Alta Dirección de AUTHENTICSING y de SUSCERTE.

7.2 Módulo criptográfico.

Imagen gráfica del módulo criptográfico.

Imagen # 1

Módulo criptográfico.

7.3 Funcionamiento y operatividad

7.3.1 Generación de pares de claves (privada y pública).

El módulo criptográfico usado por el PSC AUTHENTICSING, soporta la generación de claves de 4096 bits y tiene la capacidad de cifrar y firmar. A continuación, se describen los siguientes algoritmos criptográficos soportados:

- Cifrado simétrico:
  - CAST.
  - DES.
  - Triple-DES.
  - AES – Rijndael.
  - ArcFour (compatible con RC4).
- Cifrado de clave pública
  - El Gamal.
  - RSA.
  - DSA.
- Mecanismos de intercambio de claves
  - MD2.
  - MD5.
  - RIPEMD 160.
  - SHA-2.
  - SHA-1.
  - DH.
  - DES / DES3 XOR.
  - Funciones HASH y HMAC.
- Referencias.

  Con la finalidad de documentar y suministrar información del hardware criptográfico utilizado por el PSC AUTHENTICSING, se menciona la dirección web que se indica a continuación:

  https://resources.yubico.com/53ZDUYE6/at/q4bsft-z2wi8-fo7agg/YubiHSM2_Product_Brief.pdf?format=pdf

7.3.2 Seguridad

- **Método de precaución de acceso a la clave privada de AUTHENOLOGY:** En la instalación y configuración del HSM son preparadas y habilitadas seis (6) tarjetas de seguridad; dos (2) tarjetas con autorización de operación y cuatro (4) tarjetas con autorización de administración, para poder acceder a la clave privada de AUTHENTICSING**.** Es necesario contar con al menos una (1) tarjeta con autorización de operador y dos (2) tarjetas con autorización de administrador, siendo la división (ubicación física) y niveles de seguridad (contraseñas de acceso) de las tarjetas, garantizando de que solo en presencia y disposición de un director, del gerente general o del consultor de tecnología, son los que podrán acceder a la clave privada del PSC. **AUTHENTICSING**

- **Método de control de acceso para acceder a los funcionamientos de firma y cifrado:** Para poder acceder a los funcionamientos de firma y de cifrado, es importante acceder al software (software) de certificación, usando de esta manera un certificado de autenticación con autorización de administrador. Para este tipo de certificado solo es asignado al director encargado o gerente general y al consultor de tecnología.

7.3.3 Duración

- **Respaldo de la Clave Privada de AUTHENTICSING:** La clave privada de AUTHENTICSING es almacenada en un hardware criptográfico y es respaldada a través de una carpeta cifrada usando una unidad de cinta, el cual está almacenada en una bóveda situada en un sitio alterno al centro de datos.

- **Restauración de la Clave Privada de AUTHENTICSING :** El hardware criptográfico permite restablecer la clave privada de AUTHENTICSING , ubicando el respaldo de la carpeta cifrada (cinta situada en sitio alterno al centro de datos) y utilizando al menos una (1) tarjeta con autorización de administrador y dos (2) tarjetas con autorización de operador.

7.3.4 Auditoría

- **Generación de log:** El hardware de encriptación tienen la capacidad de generar log de eventos verificables y comprobables para la gestión y administración de contingencias y efectos nada convenientes (maliciosos), dicha información de eventos es almacenada en el directorio del disco duro de la máquina y adicional a la descripción del evento, especifica los diferentes niveles de riesgos: fatal, severe, error, warning y notification.

7.3.5 Documentación

Se encuentra referida y señalada la "Documentación" de del actual documento.

7.4 Modulo autoridad de certificación (AC)

7.4.1 Funcionamiento y operatividad

- El PSC **AUTHENTICSING** puede generar certificados de firma electrónica con clave hasta 384, de acuerdo con el tipo de certificado a emitir.

- El software de certificación permite al administrador (director encargado, gerente general o consultor de tecnología) suspender o revocar cualquier certificado que sea emitido por el PSC **AUTHENTICSING**, solamente buscando dicho certificado y presionando el botón revocar o suspender, es necesario describir la razón de la modificación del estatus.

- El software de certificación tiene capacidad de generar y publicar de manera automática la lista de certificados revocados que son emitido por el PSC **AUTHENTICSING**, en un enlace de acceso público, ubicado específicamente en **https://ura.authenology.com.ve**

- La lista de Certificados Revocados (LCR) específica y comunica detalladamente tanto su fecha de publicación (campo fecha) como la fecha de la siguiente renovación (campo próxima actualización), esta actualización y publicación es llevada a cabo cada veinticuatro (24) horas.

- El PSC AUTHENTICSING tiene la capacidad de entregar certificados y la Lista de Certificados Revocados (LCR) a directorios públicos X500.

- El PSC AUTHENTICSING tiene la capacidad de entregar la Lista de Certificados Revocados (LCR) usando el OCSP mediante el enlace siguiente: **http://ura.AUTHENOLOGY.net.ve/ocsp**.

- El PSC AUTHENTICSING está en capacidad de generar tantas firmas electrónicas como certificados electrónicos sean contratados y requeridos por los clientes. La cantidad inicial de emisión de certificados se calcula sobre la capacidad de disco disponible (130 GB) entre el espacio que será ocupado por cada certificado o firma electrónica generada por el PSC **AUTHENTICSING,** lo cual es considerado en 10KB cada uno. Estableciendo la cantidad, se determina una capacidad inicial de generación de firmas electrónicas y certificados electrónicos de hasta trece millones (13.000.000), siendo incrementada en función del espacio de memoria que sea adicionado a dicha plataforma.

7.4.2 Seguridad

- Para acceder a la generación/aprobación de certificados de AUTHENTICSING es necesario contar con un certificado que contenga autorización de administrador. El software de certificación posee un sistema de control de acceso para acceder al módulo de generación de certificados.

- El software de certificación contiene un módulo de seguridad para acceder a los log de eventos ocurridos en la Autoridad de Certificación (AC) de AUTHENTICSING**,** dicho log detalla el tipo de recurso, tipo de operación, hora, fecha, operador, y una referida descripción del mensaje. Para el ingreso al módulo, es necesario contar con un certificado con autorización de administrador.

7.4.3 Periodo de vida.

- El software de certificación le permite al PSC **AUTHENTICSING** gestionar y manejar los certificados, inspeccionado y controlando desde la emisión hasta la suspensión y revocación del mismo.

- El software de certificación tiene la capacidad de revocar el certificado raíz de AUTHENTICSING y generar uno nuevo.

7.4.4 Auditoría

El software de certificación genera los log de eventos que le permite al PSC **AUTHENTICSING** auditar, gestionar y administrar las actividades del personal autorizado y los accesos maliciosos.

De manera específica permite auditar los acontecimientos o eventos siguientes:

- Inicio y detención del servicio de certificación.
- Respaldo y restauración de la base de datos de AUTHENTICSING.
- Certificados revocados y publicación de la Lista de Certificados Revocados (LCR).
- Almacenamiento y recuperación de las claves almacenadas.
- **Todos los eventos del sistema operativo Windows Server 2003, y Windows Server 2008**.
- Cambios en la configuración de AUTHENTICSING.
- Cambios en la configuración de seguridad de AUTHENTICSING.
- Generación y administración de la solicitud de certificados.

7.4.5 Documentación

Se encuentra referida y señalada en el punto 7.10 “Documentación” de del actual documento.

7.5 Módulo Autoridad de Registro (AR).

7.5.1 Funcionamiento y operatividad

- El software de certificación le permite a los clientes efectuar las solicitudes y requerimientos en línea, desde la página web del PSC AUTHENOLOGY “www.authenology.com.ve” detallando toda la información requerida según el tipo de certificado que se quiera emitir.

- La Autoridad de Registro (AR) tiene la capacidad de recibir las solicitudes de certificados por parte del cliente, y luego de la validación de la información, poder enviar a la Autoridad de certificación (AC) la solicitud de validación del certificado.

- La Autoridad de Registro (AR) se encuentra apoyada en su

operación por el grupo de operadores asignados a tales efectos por el Coordinador de Tecnología de AUTHENTICSING**.**

- La Autoridad de Registro (AR) creará los expedientes y registros electrónicos de los clientes usuarios de certificados electrónicos.

- La Autoridad de Registro (AR) luego de efectuar la validación y conformación de los datos e identidad de los clientes usuarios de certificados electrónicos, enviará una notificación electrónica por vía correo al gerente general y al consultor de tecnología, quienes tendrán la obligación de seguir el procedimiento de generación y aprobación de las firmas electrónicas y certificados electrónicos.

7.5.2 Seguridad

- Para acceder al módulo de generación de peticiones, el cliente debe registrarse en el software de certificación, ingresando sus datos como; nombre, apellido, cédula, correo electrónico y la información de acceso requerida. Seguidamente de ser validada la cuenta de correo electrónico, el cliente podrá generar una petición de certificado.

- Para acceder al módulo de la Autoridad de Registro (AR) y enviar una solicitud de comprobación y aprobación de certificado a la Autoridad de Certificación (AC), es importante contar con un certificado de operador, dicho certificado es asignado por el administrador de la plataforma (director encargado o coordinador de tecnología) a los operadores de **AUTHENTICSING**.

- El software de certificación posee un módulo de seguridad para ingresar a los log de eventos ocurridos en la Autoridad de Registro (AR). Para el acceso a este módulo, es importante contar con un certificado autorizado por el administrador.

7.5.3 Duración

La Autoridad de Registro (AR) a través del software de certificación tiene la capacidad de enviar solicitudes de certificados a la Autoridad de Certificación (AC), luego de la recepción de la solicitud y aprobación de los datos del cliente.

7.5.4 Auditoría

El software de certificación posee un módulo de seguridad para ingresar a los log de eventos ocurridos en la Autoridad de Registro (AR), dicho log detalla el tipo de recurso, tipo de operación, operador, fecha y hora, y una detallada descripción del mensaje. Para acceder a este módulo es necesario contar con un certificado con autorización de administrador.

7.5.5 Documentación

Se encuentra referida y señalada en el punto 7.10 “Documentación” de del actual documento.

7.6 Módulo de almacenamiento y publicación de certificados

El software de certificación permite el almacenamiento de certificados en base de datos X500 y permite la publicación mediante los protocolos OCSP V1.0.

7.7 Protocolo de comunicaciones entre la Autoridad de Certificación (AC) y la Autoridad de Registro (AR).

La Autoridad de Registro (AR) luego de comprobar y validar personalmente la identidad del signatario y los datos proporcionado por este, posteriormente se procede a enviar la solicitud a la Autoridad de Certificación (AC), para este envío están involucrados dos (2) procedimientos de comunicación y se describen a continuación:

- El primero es efectuado internamente por el software de certificación.
- El segundo es ejecutado mediante un túnel seguro SSL sobre el puerto 443 entre el software de certificación y el servidor de certificación.

7.8 Componentes de administración de auditoría y log.

Todos y cada uno de los equipos presentes en la plataforma de certificación posee un módulo para almacenar los log de eventos, detalladamente eventos de las aplicaciones, los sistemas y de seguridad, esto incluye el software de certificación. Para este registro de eventos se autoriza auditar y verificar los intentos de accesos, los accesos y los procedimientos que puedan dañar, sean intencionales o no.

7.9 Plataforma tecnológica.

7.9.1 Interconexión de sistemas y cableado de datos.

Los servidores de la plataforma de certificación de AUTHENTICSING se encuentran separados en dos (2) zonas; una Pública o DMZ y otra Privada. En la zona pública o DMZ se encuentra el servidor virtual Web en clúster activo/activo y Monitoreo, en la zona Privada se encuentra el servidor de certificación que alberga la Autoridad de Certificación (CA) y un servidor de base de dato. El servicio de internet es proporcionado por la empresa Daycohost.

7.9.2 Cableado de poder principal y auxiliar.

El Rack donde se encuentran instalados los servidores de la plataforma de certificación de AUTHENTICSING dispone de dos (2) líneas de tensión distintas, una principal y otra auxiliar, dichas líneas de tensión están conectadas a dos (2) fuentes de energía ininterrumpida (UPS), entre ellos a su vez están conectadas a dos (2) plantas generadoras de energía. A continuación, se presenta una imagen con gráfico referencial de la conexión del suministro de energía:

Imagen # 2

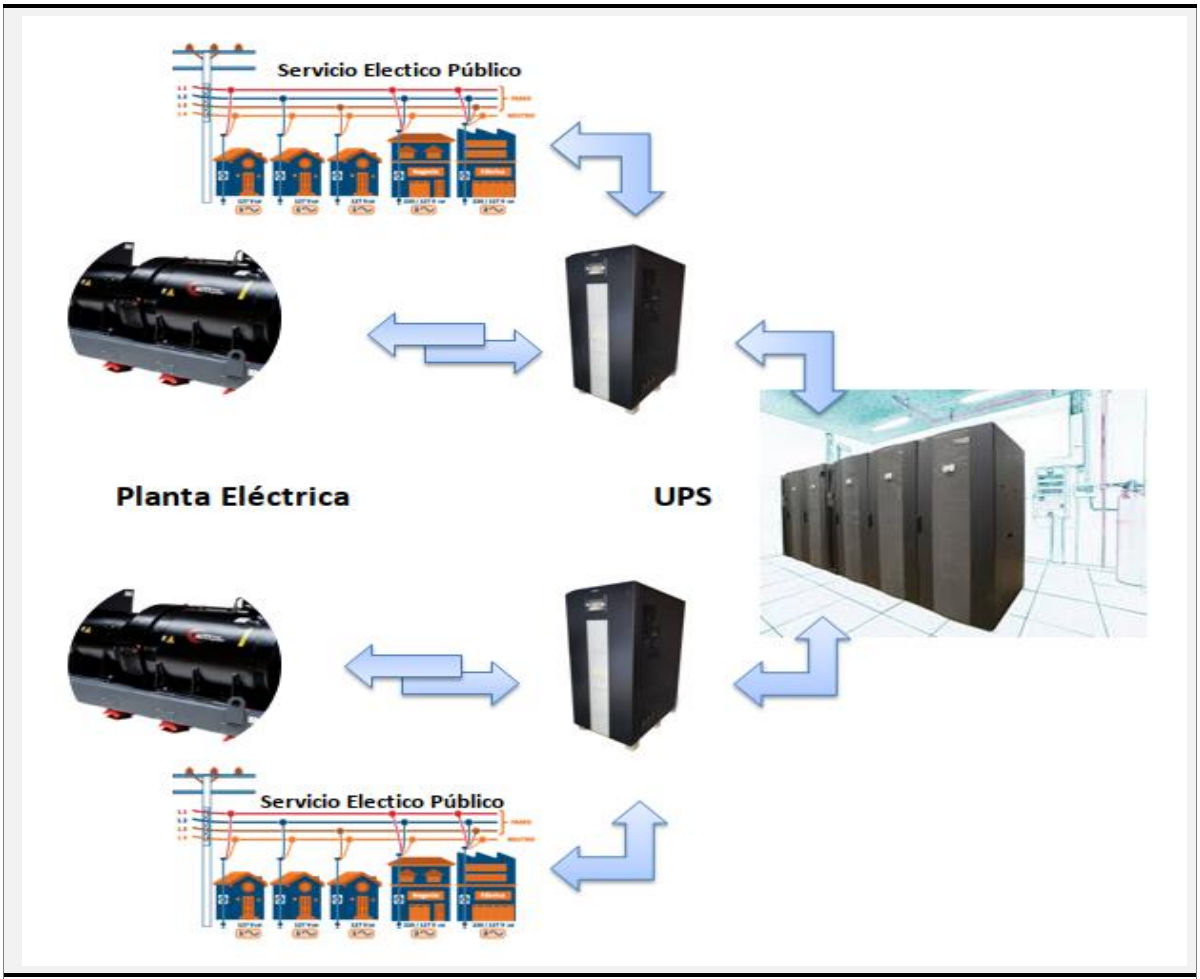

Diagrama del sistema de alimentación eléctrica.

7.9.3 Mecanismo de seguridad y control de acceso

Para poder acceder al área de servidores del centro de datos donde se encuentran ubicados los servidores que conforman la plataforma tecnológica de AUTHENTICSING**,** complementario a los puestos de vigilancia acorde a las primeras capas de seguridad física, hay solo tres (3) dispositivos calificados y configurados para que solo el personal autorizado pueda ingresar:

- Identificador biométrico de mano que apruebe el tamaño, forma, lectura biométrica y calor de la mano antes de habilitar la entrada al pasillo de ingreso al área de servidores; adicionalmente solicita una contraseña.
- Lector de banda magnética, permite solo el ingreso a los operadores de Daycohost, al área donde se encuentra situado el centro de control

y acceso al área de servidores del centro de datos.

- Control de acceso con identificación biométrica por huella dactilar para ingresar finalmente a la sala de servidores del centro de datos.

7.10 Documentación

7.10.1 Manual de procedimiento, configuración y puesta en marcha

Cada información o documentación referida al hardware criptográfico usado por el PSC **AUTHENTICSING C.A** , es mencionada en la siguiente dirección web que se indica a continuación:

- https://www.thalesesecurity.com/about-us/newsroom/news-releases/ncipher-enhances-line-industry-leading-hardware-security-modules.

7.10.2 Método de recuperación ante eventualidad.

El método de recuperación ante eventualidad abarca los pasos siguientes:

- **Primer paso:** Instalación de un nuevo HSM, en acontecimiento de algún problema de hardware del equipo principal. El PSC **AUTHENTICSING** posee en su stock de equipos, un HSM de respaldo.
- **Segundo paso**: Instalación física y configuración lógica (creación del Security World) del HSM.
- **Tercer paso**: Búsqueda del respaldo de la clave privada almacenada en bóveda.
- **Cuarto pasó**: Restauración de la clave privada usando las dos (2) tarjetas de administrador usadas para cifrar la información y una (1) tarjeta de operador para ingresar al módulo criptográfico.
- **Quinto paso:** Reactivación de la Autoridad de Certificación (AC).
- **Sexto paso:** Sincronización de todos y cada uno de los elementos que conforman la plataforma de certificación.

9. Mecanismo para el ajuste, desarrollo, y aprobación.

8.1 Mecanismo para el ajuste del documento

Las modificaciones o cambios en el Decreto Ley de Mensajes de Datos y Firmas Electrónicas, su Reglamento, la Normativa de SUSCERTE o de la normativa internacional obligatoria y requerida para la operación de los PSC, que contemplen cambios fundamentales en los desarrollos y procesos de seguridad y operación, los cuales impliquen alteración de los procedimientos y

actividades de los PSC, producirán una revisión del actual documento, con el objetivo de ajustar los procesos y procedimientos a los estándares y normativa aplicada y aprobada por SUSCERTE para la operación de AUTHENTICSING Cada ajuste o modificación del actual documento de la Evaluación de la plataforma Tecnológica de AUTHENTICSING**,** será producto del trabajo del equipo técnico y legal de AUTHENTICSING y necesitará contar para su implantación, la aprobación de Alta Dirección, conforme a lo especificado en el campo "Funcionamiento y operatividad" de la página 4 del actual documento.

8.2 Mecanismo de desarrollo del documento

El actual documento de la Evaluación de la plataforma Tecnológica de **AUTHENTICSING**, está desarrollado sobre la base de la normativa de acreditación aplicable a los interesados en convertirse en PSC. Referida normativa de acreditación es dictada y emitida por SUSCERTE, ente rector de la materia dentro de la República Bolivariana de Venezuela. Asimismo, el actual documento de la Evaluación de la plataforma Tecnológica de AUTHENTICSING cumple con cada uno de los requisitos de la normativa internacional aplicado al área de certificación electrónica.

8.3 Mecanismo para la aprobación de los ajustes al documento

Cada ajuste o modificación del documento de la Evaluación de la plataforma Tecnológica de AUTHENTICSING deberá contar con la autorización de la Alta Dirección de AUTHENTICSING ser documentada y constar por escrito, especificando el número de revisión y edición, fecha de elaboración, fecha de aprobación y la firma del representante de la alta dirección que valide el ajuste o modificación. Adicionalmente, se documentará el ajuste o modificación y su aprobación de acuerdo al contenido en el documento de la política de documentación y gestión documental. Además, será sometido a la aprobación por parte de SUSCERTE antes de ser publicada definitivamente.

10. Marco legal y normativo.

- Normativa de la Superintendencia de Servicios de Certificación Electrónica
- (SUSCERTE).
- Ley de Mensaje de Datos y Firmas Electrónicas y su Reglamento.
- Normativa AUTHENTICSING.
- Estándar internacional ITU- T X.509 V3.
- Estándar Internacional ITU-T X.609.
- Norma ISO/TR 10013:2001.
- Norma ISO 9000:2015.

- Norma ISO/IEC 27001:2022.
- Norma ISO/IEC 9594-8.

11. Funciones y responsabilidades dentro del PSC AUTHENTICSIN.

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

12. Revisión, aprobación y modificación

Los desarrollos y procesos asociados a la revisión, aprobación, modificación o ajuste de la documentación de AUTHENTICSING**,** serán regulados por el documento de la política de documentación y administración documental.

--- Fin de Documento ---