



PSC AUTHENTICISING

**Política para el Establecimiento
de Funciones y
Responsabilidades.**

2024

	INFRAESTRUCTURA DE CLAVE PÚBLICA Política para el Establecimiento de Funciones y Responsabilidades DPO-003	Edición: 1 Revisión: N° 1 Fecha: 29/02/2024
---	--	--

Resumen de Información.

Empresa	AUTHENTICSING C.A.		
Documento	Política para el Establecimiento de Funciones y Responsabilidades		
Tipo de Documento	Política para el Establecimiento de Funciones y Responsabilidades		
ID	DPO-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	N° Total de Páginas	- 16 -
Tipo de Uso	Uso Interno ☒ Uso Público ☐		

CONTROL DE DISTRIBUCIÓN

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

ÍNDICE

Índice.....	3
1. CONTROL DE VERSIONES.	3
2. TÍTULO.	4
3. CÓDIGO DEL DOCUMENTO.	4
4. INTRODUCCIÓN.	4
5. OBJETIVO.	4
6. ALCANCE.	5
7. TÉRMINOS Y DEFINICIONES.	5
8. PRINCIPIOS.....	8
8.1 Principio de claridad.....	8
8.2 Principio de coherencia.....	8
8.3 Principio de eficiencia	8
8.4 Principio de responsabilidad	8
8.5 Principio de rendición de cuentas	8
9. PROCESOS	8
10. Revisión	10
11. definición de las funciones y responsabilidades	11
11.1 Título y Descripción	11
12. AJUSTES AL DOCUMENTO.	14
12.1 Mecanismo de desarrollo del documento:	14
12.2 Mecanismo para ajuste del documento:	14
12.3 Mecanismo para aprobación de los ajustes al documento:	14
13. MARCO LEGAL Y NORMATIVO.	15

1. CONTROL DE VERSIONES.

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

2. TÍTULO.

Política para el establecimiento de funciones y responsabilidades.

3. CÓDIGO DEL DOCUMENTO.

ID: DPO-003

4. INTRODUCCIÓN.

La presente documentación hace referencia a **AUTHENTICSING C.A.**, y a su marca comercial **AUTHENOLOGY**, como una empresa de PSC “Proveedor de Servicios de Certificación” registrado, acreditado y autorizado por **SUSCERTE** para tal fin.

Como parte de sus procesos y funciones presenta el siguiente documento de la **“Política para el establecimiento de funciones y responsabilidades” “DPO-003”** esto con la finalidad de presentar, orientar, documentar y establecer las especificaciones de los requisitos para cada uno de los procesos empleados por la AC del PSC **AUTHENTICSING** para la generación, publicación y administración de los certificados electrónicos emitidos por **AUTHENTICSING**, y de esta manera ofrecer una mejor y sencilla comprensión e entendimiento por parte de la Junta directiva, Clientes, Proveedores, Personal y otros interesados en **AUTHENTICSING**.

5. OBJETIVO.

El presente documento tiene por objetivo presentar la “Política para el

establecimiento de funciones y responsabilidades” establecidas por el PSC **AUTHENTICSING C.A.**, con las condiciones y características para emitir, gestionar, revocar y renovar los certificados electrónicos.

6. ALCANCE.

El siguiente documento de “Política para el establecimiento de funciones y responsabilidades” tiene como alcance orientar a las autoridades, clientes, sobre los procesos para generación, emisión de los diferentes certificados que serán generados y emitidos por **AUTHENTICSING C.A.**, definir la autoridad de certificación y la autoridad de registro, el modelo de confianza, así como los diferentes tipos de certificados que serán emitidos por **AUTHENTICSING C.A.**

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.
- **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 (AR):** 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 C.A.**
- **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.
- **Cliente:** Es la entidad que ha solicitado la emisión de un certificado dentro de la Infraestructura de Clave Pública (ICP) del PSC **AUTHENTICSING C.A.** A los

fin del Decreto Ley de Mensajes de Datos y Firmas Electrónicas y su Reglamento el Cliente será entendido como el Signatario y viceversa.

- **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.
- **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).
- **Lista de Certificados Revocados (LCR):** Significa la lista de certificados que han sido revocados o suspendidos por el PSC AUTHENTICSING C.A.
- **Alta Dirección:** Son los responsables de establecer la estrategia y los objetivos de la empresa, y de garantizar que se cumplan. También son responsables de la gestión de los recursos de la organización, como el personal, el capital y los activos.
- **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.
- **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.
- **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: válido, 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 PSC AUTHENTICSING.
 - ❖ **Registros Personales:** Son los relacionados con las personas físicas o jurídicas.
 - ❖ **Registros de Producción:** Son los asociados a las actividades de Authenticsing o de alguno de sus miembros.
- **Registro de Auditoría:** Es la unidad de dato discreta para el rastro de auditoría cuando ocurre un evento que es examinado y registrado. 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.
- **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.
- 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.
- **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.
- **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. PRINCIPIOS

La política del PSC Authenticsing establecerá cada uno de los principios fundamentales que guiarán el establecimiento de funciones y responsabilidades. A continuación, se detallan los siguientes principios establecidos:

8.1 Principio de claridad

Las funciones y responsabilidades son claras y precisas para que todo el personal de Authenticsing pueda comprenderlas. La política deberá definir claramente las funciones y responsabilidades de cada persona o grupo.

8.2 Principio de coherencia

Las funciones y responsabilidades estarán alineadas con los objetivos y estrategias del PSC Authenticsing.

8.3 Principio de eficiencia

La política debe asignar las funciones y responsabilidades que serán suficientes para garantizar que las tareas y actividades sean realizadas de manera eficaz y eficiente.

8.4 Principio de responsabilidad

Las funciones y responsabilidades serán asignadas a personas o grupos que tengan las habilidades y los recursos necesarios para realizarlas de manera efectiva.

8.5 Principio de rendición de cuentas

Se establecerá un proceso para que las personas y los grupos responsables tengan que rendir cuentas de su desempeño laboral.

9. PROCESOS

La política de Authenticsing tiene detalladamente el proceso para establecer funciones y responsabilidades. Este proceso es claro y conciso, y se garantiza que se tenga en cuenta a todas las partes interesadas.

Se describen a continuación los siguientes procesos:

- **Paso 1: Identificación de las funciones y responsabilidades**
El Gerente de Documentación y Gestión Documental de Authenticsing identificará las funciones y responsabilidades que necesitan establecerse. Esto se hará mediante un análisis de los procesos y procedimientos del PSC Authenticsing.
- **Paso 2: Revisión de las políticas y procedimientos existentes**
El Gerente de Documentación y Gestión Documental de Authenticsing deberá revisar las políticas y procedimientos existentes para identificar cualquier función o responsabilidad que ya esté establecida. Esto ayudará a evitar la duplicación de funciones y responsabilidades.
- **Paso 3: Desarrollo de un borrador de funciones y responsabilidades**
El Gerente de Documentación y Gestión Documental desarrollará un borrador de funciones y responsabilidades que incluya la siguiente información:
 - ❖ **Título de la función o responsabilidad:** El título debe ser claro y conciso.
 - ❖ **Descripción de la función o responsabilidad:** La descripción debe ser detallada y precisa. Debe indicar qué tareas y actividades son responsables de realizar la persona o el grupo.
 - ❖ **Persona o grupo responsable:** La persona o el grupo responsable debe ser claramente identificado.
- **Paso 4: Revisión del borrador de funciones y responsabilidades**
El borrador de funciones y responsabilidades será revisado por las partes interesadas relevantes, como la Alta Dirección, los gerentes de departamento y los empleados. Esto garantiza que el borrador sea completo y preciso.
- **Paso 5: Aprobación de las funciones y responsabilidades**
Las funciones y responsabilidades deberán ser aprobadas por la Alta Dirección. Esto ayudará a garantizar que las funciones y responsabilidades sean apoyadas por la dirección.
- **Paso 6: Comunicación de las funciones y responsabilidades**
Las funciones y responsabilidades serán comunicadas a todos los empleados. Esto ayudará a garantizar que todos los empleados conozcan sus responsabilidades.

10. REVISIÓN

La revisión de las funciones y responsabilidades de Authenticsing será realizada periódicamente para garantizar que sigan siendo relevantes y eficaces. La revisión será realizada por un equipo de personas con experiencia en diferentes áreas de la organización. A continuación se nombran los siguientes pasos de Revisión:

➤ **Paso 1: Identificación de los criterios de revisión**

El equipo de revisión deberá identificar los criterios que se utilizarán para evaluar las funciones y responsabilidades. Los criterios serán claros y concisos, y deben ser relevantes para los objetivos y estrategias del PSC Authenticsing. Los criterios pueden incluir:

- ❖ Coherencia con los objetivos y estrategias de Authenticsing.
- ❖ Eficiencia y eficacia de las tareas y actividades.
- ❖ Adecuación de las habilidades y recursos de las personas o grupos responsables.

➤ **Paso 2: Revisión de las funciones y responsabilidades**

El equipo de revisión deberá revisar las funciones y responsabilidades para evaluar si cumplen con los criterios de revisión. Se hará mediante una serie de métodos, como entrevistas, encuestas y análisis de documentos.

➤ **Paso 3: Recomendaciones de mejora**

El equipo de revisión deberá preparar un informe que contenga las recomendaciones de mejora. Las recomendaciones deben ser específicas y factibles.

➤ **Paso 4: Implementación de las recomendaciones**

Las recomendaciones de mejora deberán ser implementadas por la organización. Esto puede requerir la participación de la Alta Dirección, los gerentes de departamento y los empleados de Authenticsing.

Adicionalmente se deberá cumplir los siguientes puntos para la revisión de funciones y responsabilidades:

- Revisar las funciones y responsabilidades al menos una vez al año.
- Reunir a un equipo de personas con experiencia en diferentes áreas de la organización para ayudar a revisar las funciones y responsabilidades.
- Involucrar a los empleados en el proceso de revisión.

11. DEFINICIÓN DE LAS FUNCIONES Y RESPONSABILIDADES

Estas definiciones de las funciones y responsabilidades deben ser claras y concisas. En este campo se indicará quién es responsable de qué tareas y de qué actividades es responsable.

11.1 Título y Descripción

➤ Gerente de Documentación y Gestión Documental:

El Gerente de Documentación y Gestión Documental es responsable de la implementación y el mantenimiento de la política de documentación y gestión documental. Las tareas y actividades específicas incluyen lo siguiente:

- ❖ Desarrollar y mantener un sistema de gestión documental.
- ❖ Gestionar el proceso de creación, revisión, aprobación y publicación de documentos.
- ❖ Garantizar que los documentos sean accesibles a los empleados.
- ❖ Mantener un sistema periódico de investigación de normativas y estándares internacionales referentes a las actividades realizadas por el PSC, para la posterior actualización de la documentación de Authenticsing.
- ❖ Estudiar, desarrollar y documentar métodos que permitan la ejecución de las tareas de la forma más eficiente posible.

➤ Gerente del PSC

El Gerente del PSC es responsable de llevar la dirección y administración del PSC; así como la generación de las líneas estratégicas para la promoción, desarrollo y masificación del uso de las tecnologías de Infraestructura de Clave Pública (PKI)

Las tareas y actividades específicas incluyen lo siguiente:

- ❖ Garantizar una gestión y planificación estratégica de proyectos.
- ❖ Manejo del personal.
- ❖ Desarrollo de estrategias que permitan el crecimiento de empresa Authenticsing en el mercado de la PKI.
- ❖ Velar por el mantenimiento óptimo de los recursos humano, material y monetario de la empresa Authenticsing para el desarrollo de sus funciones como PSC.
- ❖ Realizar de forma mensual informes que reflejen la productividad

del PSC (actividades, logros, pendientes, finanzas, entre otros), el mismo será presentado ante la Alta Dirección.

- ❖ Participación activa en el establecimiento y afianzamiento de relaciones de negocio que incentiven la productividad del PSC.

➤ **Gerente de Auditoría Interna**

El Gerente de Auditoría Interna se encargará de la ejecución de las auditorías internas al PSC. Debe contar con autonomía para la realización de sus tareas y así evitar conflicto de intereses. Presentar informe de actividades y proponer soluciones técnicas de carácter preventivo y correctivo. Autorizado para ver los archivos y registros de auditoría de los sistemas de confianza de PSC.

Las tareas y actividades específicas incluyen lo siguiente:

- ❖ Realizar de forma periódica y aleatoria auditorías a las distintas gerencias que funcionan en la empresa Authenticsing.
- ❖ En caso de existir alguna incidencia con alguna gerencia o personal de Authenticsing Este deberá liderar los procesos de auditoría y presentar un informe con los resultados de las mismas ante la Alta Dirección.
- ❖ Velar por el mantenimiento de la imparcialidad y autonomía de la gerencia para el desarrollo óptimo de sus actividades.
- ❖ Publicar informes de interés general para los integrantes de la empresa Authenticsing, de carácter informativo que promuevan las buenas prácticas para la ejecución de las actividades programadas.
- ❖ Organizar evaluaciones aleatorias e individuales al personal sustantivo de la empresa.

➤ **Coordinador de la Infraestructura De La Clave Pública**

Se encargará la coordinación de proyectos y actividades inherentes al área de ICP del PSC. Asigna y distribuye actividades según las fortalezas del personal bajo su coordinación. Es el responsable de diseñar y presentar soluciones complejas a requerimientos del cliente y vigilar la materialización de los proyectos de su unidad. Así mismo presenta informes técnicos detallados para la toma de decisiones de nivel medio.

Las tareas y actividades específicas incluyen lo siguiente:

- ❖ Coordinar y supervisar el desarrollo de las actividades del PSC inherentes a la PKI.
- ❖ Supervisar las interacciones directas entre el cliente y el personal del PSC.
- ❖ Velar por el mantenimiento óptimo de la PKI del PSC.

- ❖ Brindar soluciones de forma rápida y eficiente a cualquier inconveniente que pueda surgir en los procesos del PSC.
- ❖ Realizar informes diarios y semanales para el Gerente del PSC.
- ❖ Coordinar y supervisar el desarrollo de las estrategias realizadas por el Gerente del PSC para el desarrollo de los objetivos del PSC.
- ❖ Supervisar el rendimiento de los equipos y el personal que operan la PKI.

➤ **Operador AC**

Se encargará de la ejecución de las actividades técnicas-operativas de la operación de la AC. Opera y administra la autoridad de certificación. Presenta informe de actividades. Ejecuta las actividades de mantenimiento de la plataforma vinculada con la AC. Conoce las Políticas de Seguridad de la Información de la AC. Responsable de la aprobación, generación, revocación y suspensión de certificados electrónicos.

Las tareas y actividades específicas incluyen lo siguiente:

- ❖ Ejecución de las actividades operativas asignadas por el coordinador de Infraestructura de Clave Pública.
- ❖ Operar la Autoridad de Certificación del PSC Authenticsing.
- ❖ Ejecutar el mantenimiento preventivo y/o correctivo de la Infraestructura de Clave Pública.
- ❖ Mantener los sistemas de la Autoridad de Certificación en estado óptimo para su desempeño pleno en las actividades de certificación.

➤ **Operador AR**

Opera y administra la autoridad de registro. Se encargará de la gestión de las solicitudes de los certificados electrónicos. Presenta informes sobre las actividades asignadas. Conoce las políticas de certificado de la AC. Lleva a cabo la provisión de los dispositivos criptográficos de los signatarios y presta atención de la revocación.

Las tareas y actividades específicas incluyen lo siguiente:

- ❖ Ejecución de las actividades operativas asignadas por el coordinador de Infraestructura de Clave Pública.
- ❖ Operar la Autoridad de Registro del PSC Authenticsing.
- ❖ Ejecutar el mantenimiento preventivo y/o correctivo de la Infraestructura de Clave Pública.
- ❖ Mantener los sistemas de la Autoridad de Registro en estado óptimo para su desempeño pleno en las actividades de

certificación.

- ❖ Realizar las labores de Atención al Cliente.

12. AJUSTES AL DOCUMENTO.

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

12.1 Mecanismo de desarrollo del documento:

Política para el Establecimiento de Funciones y Responsabilidad se encuentra desarrollada sobre la base de la normativa de acreditación aplicable a los interesados a convertirse en PSC. Dicha norma de acreditación es dictada y emitida por SUSCERTE.

12.2 Mecanismo para ajuste del documento:

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

Todo ajuste al presente Política para el Establecimiento de Funciones y Responsabilidad, será producto del trabajo del personal técnico y legal del PSC AUTHENTICSING y exigirá contar para su implementación, con la aprobación y validación de alta dirección, de acuerdo a lo descrito en el punto de "Mecanismo para aprobación de los ajustes al documento" del presente documento. El proceso llevado a cabo para el ajuste será documentado y realizado conforme al documento de la política de documentación y gestión documental.

12.3 Mecanismo para aprobación de los ajustes al documento:

Cada ajuste o modificación del documento de la Política para el Establecimiento de Funciones y Responsabilidad tendrá que contar con la aprobación de la alta dirección del PSC AUTHENTICSING, ser documentada y constar por escrito, nombrando el número de edición y revisión, fecha de

elaboración, fecha de aprobación y la firma del representante de la alta dirección que aprueba el ajuste o modificación.

Se documentará el ajuste o modificación y su aprobación conforme al documento de la política de documentación y gestión documental.

13.MARCO LEGAL Y NORMATIVO.

- Decreto ley de mensaje de datos y firmas electrónicas y su reglamento.
- Normativa de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).
- Normativa AUTHENTICSING.
- Estándar internacional ITU- T X.509 V3.
- Estándar Internacional ITU-T X.609.
- Norma ISO 9000:2015.
- Norma ISO/IEC 9594-8.
- Norma ISO/TR 10013:2001.
- Norma ISO/IEC 27001:2013.



--- Fin de Documento ---