AUTHENOLOGY
FIRMA ELECTRÓNICA

AUTHENTICSING C.A.

Declaración de Prácticas de Certificación (DPC) y Política de Certificados.

Zolange Gonzalez Colon

Firmado digitalmente por Zolange Gonzalez Colon
Fecha: 2024.03.18 21:13:45 -04'00'

2024

Resumen de Información.

Empresa	**AUTHENTICSING C.A.**		
Documento	Declaración de Prácticas de Certificación (DPC) y Política de Certificados.		
Tipo de Documento	Documentación sobre la Infraestructura de Clave Pública		
ID	DIF-002		
Autor	Ing. Carlos García.		
Colaboradores			
Revisado por	Abog. Samuel Gómez.	**Fecha de creación**	2024 Enero
Aprobado por	Abog. Zolangel González.	**Fecha Aprobación**	29/02/2024
Versión/Edición	1.0v	**Nº Total de Páginas**	**- 133 -**
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.....12
2. TÍTULO.....12
3. CÓDIGO DEL DOCUMENTO.....12
4. INTRODUCCIÓN.....12
5. OBJETIVO.....13
6. ALCANCE.....13
7. TÉRMINOS Y DEFINICIONES.....13
8. COMUNIDAD DE USUARIOS Y APLICABILIDAD.....19
8.1 Autoridad de certificación (AC).....20
8.1.1 Modelo de operación del PSC AUTHENTICSING.....20
8.1.2 Certificado raíz del PSC AUTHENTICSING.....21
8.1.3 Raíz de certificación del PSC AUTHENTICSING.....23
8.2 Autoridad de Registro (AR).....25
8.2.1 Modelo de Operación de la AR.....27
8.3 Signatario.....30
8.4 Tercero de buena fe.....31
9. USO DE LOS CERTIFICADOS (DPC y PC).....31
9.1 Usos permitidos.....31
9.1.1 Certificado de firma electrónica para empleado de empresa privada.....31
9.1.2 Certificado de firma electrónica para representante de empresa pública.....34
9.1.3 Certificado de firma electrónica para funcionario público.....36
9.1.4 Certificado de firma electrónica para representante legal de empresa privada.....38
9.1.5 Certificado de firma electrónica para profesionales titulados.....41
9.1.6 Certificado electrónico de firma para persona natural.....44
9.1.7 Estructura del Certificado de Servidor de OCSP.....46
9.2 Usos no permitidos.....47
10. POLÍTICAS DE ADMINISTRACIÓN DEL PSC (DPC y PC).....48
10.1 Especificaciones de la organización administrativa.....48
10.2 Persona Contacto.....48

10.3 Competencia para determinar la adecuación de la DPC y las políticas.....49
11. PUBLICACIÓN DE INFORMACIÓN DEL PSC Y REPOSITORIOS DE LOS CERTIFICADOS (DPC)..... .49
11.1 Repositorios..... .49
11.2 Publicación..... .49
11.3 Frecuencia de publicación..... .50
11.3.1 Certificados del Proveedor de Servicio de Certificación (PSC).....50
11.3.2 Lista de Certificados Revocados (LCR).....50
11.3.3 Declaración de Prácticas de Certificación..... .50
11.3.4 Controles de acceso al repositorio de certificados..... .50
12. IDENTIFICACION Y AUTENTICACIÓN (DPC y PC).....51
12.1 Registro de nombres.....51
12.1.1 Tipo de nombres.....51
12.1.2 Necesidad de que los nombres sean significativos..... .52
12.1.3 Interpretación de formatos de nombres.....52
12.1.4 Unicidad de nombres.....52
12.1.5 Resolución de Conflictos relativos a nombres.....53
12.2 Validación inicial de la identidad..... .53
12.2.1 Método de prueba de posesión de la clave privada..... .53
12.2.2 Autenticación de la identidad de la organización.....53
12.2.3 Autenticación de la identidad de Personas Naturales.....55
12.2.4 Comprobación de las facultades de representación.....55
12.3 Identificación y autenticación de las solicitudes de renovación de la clave.....56
12.3.1 Generación de nuevo Par de Claves.....56
12.3.2 Generación de Nuevo Certificado (Posterior a Revocación).....56
12.4 Identificación y autenticación de las solicitudes de revocación de la clave.....57
13. EL CICLO DE VIDA DE LOS CERTIFICADOS (REQUERIMIENTOS OPERATIVOS) (DPC y PC)..... .57
13.1 Solicitud de certificados..... .57
13.1.1 Proceso de generación de la solicitud de certificados y responsabilidades.. 58
13.1.2 Proceso de firma del certificado..... .60
13.1.3 Proceso de generación de la solicitud de renovación de las claves del certificado..... .61

13.1.4 Procedimiento para realizar una solicitud de renovación de un certificado.. .62
13.1.5 Procedimiento para realizar una solicitud de suspensión de un certificado...62
13.2 Tramitación de solicitud de un certificado..... .63
13.2.1 Realización de las funciones de identificación y autenticación.....63
13.2.2 Aprobación o denegación de un certificado.....64
13.2.3 Plazo para la tramitación de un certificado..... .65
13.3 Emisión de certificados..... .65
13.3.1 Acciones del PSC durante la emisión de un certificado.....65
13.3.2 Notificación al solicitante por parte del PSC acerca de la emisión de su certificado electrónico..... .65
13.4 Aceptación de certificados..... .66
13.4.1 Forma en la que se acepta el certificado..... .66
13.4.2 Publicación del certificado..... .66
13.4.3 Notificación de la emisión del certificado a otras autoridades.....66
13.5 Uso de par de claves y del certificado..... .66
13.5.1 Uso de la clave privada del certificado..... .66
13.5.2 Uso de la clave pública y del certificado por los terceros de buena fe.....67
13.6 Renovación del certificado..... .67
13.6.1 Causas para la renovación..... .67
13.6.2 Entidad que puede solicitar la renovación de un certificado.....67
13.6.3 Procedimiento de solicitud para la renovación de un certificado.....67
13.6.4 Notificación de la emisión de un nuevo certificado..... .68
13.6.5 Publicación del certificado renovado por el PSC..... .68
13.6.6 Notificación de la emisión del certificado a otras entidades.....68
13.7 Nueva clave del certificado..... .68
13.8 Modificación de certificados..... .68
13.9 Revocación y suspensión de un certificado..... .68
13.9.1 Circunstancias para la Revocación del certificado del signatario.....68
13.9.2 Entidad que puede solicitar la Revocación..... .69
13.9.3 Procedimientos de Solicitud de la Revocación..... .70
13.9.4 Límites del período de la Solicitud de Revocación..... .71
13.9.5 Circunstancias para la Suspensión..... .71

13.9.6 Entidad que puede solicitar la Suspensión..... .72
13.9.7 Procedimientos para la Solicitud de Suspensión..... .73
13.9.8 Límites del Período de Suspensión de un Certificado..... .73
13.9.9 Frecuencia de Emisión de Listas de Certificados Revocados..... .73
13.9.10 Requisitos para la comprobación de la Lista de Certificados Revocados. . .73
13.9.11 Disponibilidad de comprobación en Línea del Servicio de Revocación del Estado del Certificado..... .74
13.9.12 Requisitos de comprobación en Línea del Estado de Revocación.....74
13.9.13 Otras Formas Disponibles para la Divulgación de la Revocación..... .74
13.9.14 Requisitos para la Verificación de Otras Formas de Divulgación de Revocación..... .74
13.9.15 Requisitos Específicos para Casos de Compromiso de Claves.....74
13.10 Servicio de comprobación de estado de certificados..... .74
13.10.1 Características operativas..... .74
13.10.2 Disponibilidad del servicio..... .75
13.10.3 Características adicionales..... .75
13.11 FINALIZACIÓN DE LA SUSCRIPCIÓN..... .75
13.12 Custodia y recuperación de la clave..... .75
13.12.1 Prácticas y políticas de recuperación de la clave..... .75
14. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES (DPC) ..... .76
14.1 Controles de seguridad física.....76
14.1.1 Controles de la garantía y seguridad física y construcción del PSC.....76
14.1.2 Acceso físico..... .77
14.1.3 Suministro de electricidad y acondicionador de aire.....79
14.1.7 Exposición de agua..... .80
14.1.8 Protección y prevención de incendios..... .81
14.1.9 Sistemas y técnicas de almacenamiento.....81
14.1.10 Sistemas de almacenamiento.....81
14.1.11 Eliminación de residuos.....81
14.1.12 Almacenamiento de copias de seguridad.....81
15. CONTROLES DE PROCEDIMIENTOS..... .82
15.1 Definición de roles confiables..... .82

15.1.1 Cifra de personas requeridas por rol..... .82
15.1.2 Identidad y autenticación de cada rol..... .83
16. CONTROLES DE SEGURIDAD PERSONAL..... .84
16.1 Petición de antecedentes, calificación, experiencia y acreditación.....84
16.2 Requerimientos de formación para los miembros del personal..... .84
16.3 Sanciones por acciones no autorizadas..... .84
18. PROCEDIMIENTOS DE CONTROL DE SEGURIDAD.....85
18.1 Tipos de eventos registrados..... .85
18.2 Regularidad de procesados de registros de logs.....86
18.3 Período de retención para los logs de auditoría..... .86
18.4 Protección de los logs de auditoría..... .86
19. ARCHIVO DE INFORMACIONES Y REGISTROS..... .86
19.1 Tipo de informaciones y eventos registrados.....87
19.2 Período de retención para el archivo..... .87
19.3 Protección del archivo.....87
19.4 El Requerimiento para el estampado de tiempo para el registro.....87
19.5 Sistema de repositorio de archivos de auditoría (interno vs externo).....88
20. CAMBIO DE CLAVE..... .88
21. PLAN DE RECUPERACIÓN EN CASO DE DESASTRES..... .88
21.1 El procedimiento y desarrollo de gestión de incidentes y vulnerabilidades.....88
21.2 Alteración de los recursos, hardware, software y/o datos.....89
21.3 Procedimiento de actuación ante la vulnerabilidad de la clave privada de una autoridad..... .89
21.4 Seguridad de las instalaciones tras un desastre natural o de otro tipo.....90
22. CESE DE LAS ACTIVIDADES DEL PSC..... .90
23. CONTROLES DE SEGURIDAD TÉCNICA (DPC).....91
23.1 Entrega de la clave privada.....91
23.2 Entrega de la clave pública..... .91
23.3 Disponibilidad de la clave pública..... .91
23.4 Tamaño de las claves..... .92
23.5 Parámetros de generación de la clave pública y verificación de la calidad.....92
23.6 Hardware/software de generación de claves..... .94

23.6.1 Algoritmos Criptográficos soportados..... .95
23.6.2 Referencias..... .96
23.7 Propósitos de utilización de claves:..... .96
24. PROTECCIÓN DE LA CLAVE PRIVADA..... .96
24.1 Estándares para los módulos criptográficos..... .96
24.2 Control “N” de “M” de la clave privada:..... .96
24.3 Custodia de la clave privada..... .96
24.4 Copia de seguridad de la clave privada..... .97
24.5 Archivo de la clave privada..... .97
24.6 Inserción de la clave privada en el módulo criptográfico.....97
24.7 Método de activación de la clave privada..... .97
24.8 Método de destrucción de la clave privada.....98
24.9 Ranking del módulo criptográfico.....98
25. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES.....98
25.1 Archivo de la clave pública.....98
25.2 Períodos operativos de los certificados y período de uso del par de claves.....98
26. DATOS DE ACTIVACIÓN.....98
26.1 Generación e instalación de datos de activación.....98
26.2 Protección de datos de la activación.....99
27. CONTROLES DE SEGURIDAD DEL COMPUTADOR.....100
27.1 Requisitos técnicos específicos..... .100
27.2 Calificaciones de seguridad computacional..... .100
28. CONTROLES DE SEGURIDAD DE LA RED.....100
29. PERFILES DE CERTIFICADOS LCR / OCSP.....100
29.1 Perfil del certificado.....100
29.2 Número de versión.....101
29.3 Extensiones del certificado..... .101
29.4 Identificadores de objeto (OID) de los algoritmos..... .101
29.5 Formatos de nombres..... .101
29.6 Identificador de objeto (OID) de la PC..... .102
29.7 Perfil de LCR / OCSP:..... .102
30. AUDITORIA DE CONFORMIDAD (DPC).....103

30.1 Relación entre el auditor y la autoridad auditada:.....104
30.2 Tópicos cubiertos por el control de conformidad.....104
31. REQUISITOS COMERCIALES Y LEGALES (DPC y PC).....104
31.1 Aranceles.....104
31.2 Responsabilidad financiera del PSC.....105
31.3 Políticas de confidencialidad.....106
31.3.1 Información Confidencial.....106
31.3.2 Información No Confidencial.....107
31.3.3 Publicación de Información sobre la Revocación o Suspensión de un Certificado.....107
31.3.4 Divulgación de Información a Autoridades Judiciales.....107
32. PROTECCIÓN DE LA INFORMACIÓN PRIVADA/SECRETA.....108
32.1 Información considerada privada.....108
32.2 Información considerada no privada.....109
32.3 Responsabilidad de proteger la información privada/secreta.....109
32.4 Consentimiento previo para el uso de información privada/secreta.....109
32.5 9.4.5 Comunicación de la información a autoridades administrativas y/o judiciales.....109
33. PROTECCIÓN DE LA INFORMACIÓN PRIVADA/SECRETA.....110
33.1 Información considerada privada.....110
33.2 Información considerada no privada.....110
33.3 Responsabilidad de proteger la información privada/secreta.....110
33.4 Consentimiento previo para el uso de información privada/secreta.....110
33.5 Comunicación de la información a autoridades administrativas y/o judiciales.....111
34. DERECHO DE PROPIEDAD INTELECTUAL.....111
34.1 Condición general.....111
34.2 Claves pública y privada.....111
34.3 Certificado.....111
34.4 Nombres distinguidos.....112
34.5 Propiedad intelectual.....112
35. REPRESENTACIONES Y GARANTIAS.....112
36. LIMITACIONES DE RESPONSABILIDAD.....112

36.1 Límites de responsabilidad y garantía limitada:..... .112
36.2 Deslinde de responsabilidades:..... .113
36.3 Limitaciones de pérdidas..... .114
37. PLAZO Y FINALIZACIÓN..... .115
37.1 Plazo..... .115
37.2 Terminación..... .116
38. MODIFICACIONES..... .116
38.1 Procedimientos de Publicación y Notificación..... .116
38.2 Procedimientos de Cambio de Especificaciones..... .117
38.3 Procedimientos de Aprobación..... .117
39. RESOLUCIÓN DE CONFLICTOS..... .117
39.1 Resolución extrajudicial de conflictos..... .117
39.2 Jurisdicción competente..... .118
40. LEGISLACIÓN APLICABLE..... .118
41. OBLIGACIONES Y RESPONSABILIDAD CIVIL (DPC y PC)..... .119
41.1 Obligaciones y responsabilidad civil..... .119
41.1.1 Obligaciones de la Autoridad de Registro (AR):..... .119
41.1.2 Obligaciones de la Autoridad de Certificación (AC)..... .120
41.2 Obligaciones de los terceros de buena fe:..... .122
42. CONFORMIDAD CON LEY APLICABLE..... .124
43. AJUSTES AL DOCUMENTO..... .124
43.1 Mecanismo de desarrollo del documento:..... .124
43.2 Mecanismo para ajuste del documento:..... .125
43.3 Mecanismo para aprobación de los ajustes al documento:..... .125
44. MARCO LEGAL Y NORMATIVO..... .125
45. ESQUEMA DE UN CONJUNTO DE DISPOSICIONES (RFC 3647, Sección 6)..... .126

1. CONTROL DE VERSIONES.

Control de Cambio			
Versión	**Revisión**	**Fecha**	**Observaciones**
1	0	2023Ene.20	Versión inicial

2. TÍTULO.

Declaración de Prácticas de Certificación (DPC) y Política de Certificados.

3. CÓDIGO DEL DOCUMENTO.

ID: DIF-002

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 ***"Declaración de Prácticas de Certificación (DPC) y Política de Certificados" "DIF-002"*** 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**.

En el presente documento se utiliza la estructura de documento de la AC Raíz de Venezuela (SUSCERTE), la cual difiere de la estructura planteada en la RFC 3647 de la Sección 6. La estructura de SUSCERTE es la estructura recomendada por el Gobierno de Venezuela para los documentos relacionados con la seguridad de la información. La estructura de SUSCERTE contiene lo siguiente: Cuerpo, encabezado y apéndice.

5. OBJETIVO.

El presente documento tiene por objetivo presentar la "Declaración de Prácticas de Certificación (DPC) y Política de Certificados" establecidas por el PSC AUTHENTICSING C.A., de las condiciones y características para emitir, gestionar, revocar y renovar los certificados electrónicos.

6. ALCANCE.

La siguiente Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC) tiene como alcance suministrar a las autoridades, clientes, 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.
- **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, entre otros.
  - Software: Software de aplicaciones, software de sistemas, herramientas de desarrollo, entre otros.
  - 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 C.A 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 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.
- **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) del PSC AUTHENTICSING C.A. 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 C.A 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 C.A.
- **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 C.A.
- **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 del PSC AUTHENTICSING C.A.
- **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) del 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.
- 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 Authenticsing que así lo requieran.
- **Responsable de un Sistema de Información:** Encargado de velar por la puesta

en marcha y el correcto funcionamiento del Sistema de Información o en su defecto el Responsable de la Unidad Organizativa.

- **Revocación:** Es el cambio de estatus de un certificado válido o suspendido a "revocado" a partir de una fecha específica en adelante.
- **Revocación de Certificado:** Son los procesos que consisten en cambiar el estatus de un certificado válido o suspendido o revocado. Cuando un certificado tiene un estado revocado, esto significa que una entidad ya no es confiable para ningún objetivo.
- **Seguridad de la Información:** La seguridad de la información se entiende como la preservación de las siguientes características:
  - Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
  - Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
  - Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, deberán considerarse los conceptos de:

- Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegueante terceros que no la envió o recibió.
- Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta al PSC AUTHENTICSING C.A.
- 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: Se refiere al hardware y software operados por la PSC AUTHENTICSING o por un tercero que procese información en su nombre, para llevar a cabo una función propia del PSC AUTHENTICSING, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo

- ➢ **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 del PSC **AUTHENTICSING.** son las Unidades y las áreas de la administración central que dependen directamente del Director o Gerente General. Las Unidades Organizativas se detallarán en la estructura organizativa de la empresa.
- ➢ **Uso del Certificado:** Conjunto de reglas que indican la aplicabilidad del certificado de una comunidad en particular y/o la clase de aplicación con requerimientos de seguridad comunes.

- **Validación:** Es un proceso que lleva a cabo la verificación de validez de un Certificado en términos de su estatus o condición (Ej. si es suspendido o revocado).

8. COMUNIDAD DE USUARIOS Y APLICABILIDAD.

Está incluye las distintas entidades que cumplen roles con relación al certificado y cuya integración se encuentre prevista para el cumplimiento de la actividad de certificación.

8.1 Autoridad de certificación (AC)

El PSC AUTHENTICSING C.A., es una Sociedad de Capital o Sociedad Mercantil, disciplinada y de estricta iniciativa o determinación privada, establecidas y diseñada para los efectos de establecerse como un PSC, cumpliendo lo establecido en el decreto ley de mensaje de datos y firmas electrónicas (LMDFE), su reglamentación o los cuerpos normativos que sustituyan a estos; tiene como objetivo ofrecer certificados electrónicos y firmas electrónicas a personas privadas y públicas, jurídicas o naturales, prestar el servicio técnico y de soporte a las aplicaciones para firmas y certificados electrónicos; realizar acciones de adiestramiento en materia de firmas y certificados electrónicos, comercio electrónico, y demás aplicaciones y usos que involucren su uso; desarrollo, mantenimiento, y ofrecer aplicaciones para tramites en línea con entes de la administración pública, gobernaciones y municipios de la República Bolivariana de Venezuela.

8.1.1 Modelo de operación del PSC AUTHENTICSING.

8.1.1.1 Sede Administrativa.

En la sede administrativa de Authenticsing, se gestionara los procesos financieros, administrativos, fiscales, de recursos humanos y operacional para la completa operatividad de AUTHENTICSING, esto quiere decir que desde la sede administrativa operara la Autoridad de Registro (AR) la cual es el representante de gestionar la validación de la documentación e identidad de los Clientes y/o Usuarios contratantes y dar seguridad y afirmación pública de la revisación y conformación de los datos aportados por cada uno de los Clientes y/o Usuarios contratantes de certificados electrónicos. Así como la Autoridad de Certificación (AC),

La dirección física de la sede administrativa es la siguiente:

DATOS DE LA EMPRESA DIRECCIÓN FÍSICA.	
Nombre	**Proveedor de Certificados AUTHENTICSING**
Dirección	Calle Bolívar, Edificio Don David, PB – Ofic. 001, Municipio Chacao del estado Miranda de la República Bolivariana de Venezuela
Código Postal	1060
Correo electrónico	contacto@authenology.com.ve
Número de teléfono	+58 – 0212 - 2647658
Numero de Fax	+58 – 0212 - 2647658
Página web-*-	www.authenology.com.ve
Horario de atención al publico	8:00 a.m. a 12:00 m y de 1:00 p.m. a 5:00 p.m. de Lunes a Viernes.
	AUTHENTICSING proporcionará certificados electrónicos de firma a todas las personas naturales y/o jurídicas que si cumplan con los requisitos contemplados en el decreto ley de mensaje de datos y firmas electrónicas y reglamento y que finalicen y completen exitosamente el proceso de contratación y aprobación de términos contractuales; fijándose un plazo de vigencia para los certificados que sean emitidos, de un (1) año.

8.1.2 Certificado raíz del PSC AUTHENTICSING.

El PSC AUTHENTICSING es una autoridad de certificación de nivel superior y se encuentra subordinada a la autoridad de certificación raíz del estado venezolano y solamente estará en funcionamiento durante la realización de las operaciones para las que se establece. La estructura del certificado raíz del PSC AUTHENTICSING es la siguiente:

ESTRUCTURA DE DATOS DEL CERTIFICADO RAIZ.	
NOMBRE DEL PUNTO	**VALOR**
Versión	**V3 (Número de versión del certificado)**
Número de serie	**Serial Number Octet Size 20**
Algoritmo	**ECDSA-whit- SHA-512 (Algoritmo de Firma)**
DATOS DEL EMISOR	
CN	Autoridad de Certificación Raíz del Estado Venezolano
O	Sistema Nacional de Certificación Electrónica
C	VE (VENEZUELA)
PERIODO DE VALIDEZ	
Valido desde:	Inicio vigencia del certificado
Válido hasta:	Expiración del periodo de validez
DATOS DEL TITULAR	
CN	AUTHENTICSING
O	Sistema Nacional de Certificación Electrónica
OU	PROVEEDOR DE CERTIFICADOS AUTHENTICSING
C	VE
INFORMACIÓN DE CLAVE PUBLICA	
Algoritmo clave publica	**ECDSA (Algoritmo en que se generó la clave pública).**
Tamaño clave publica	(VALOR)
Extensiones	
Restricciones básicas	CA: TRUE Y LONGITUD DEL PATH = 1
IDENTIFICADOR DE CLAVE DE AUTORIDAD CERTIFICADORA	
Id. De clave	Identificador de la clave
Emisor de certificado	Datos del emisor
Numero serie certificado	Numero de serial
Uso de la clave	Firma electrónica del certificado y firma de LCR
NOMBRE ALTERNATIVO DEL TITULAR	
DNS Name	www.authenology.com.ve
OID 2.16.862.2.1	PSC-NUMERO ASIGNADO
OID 2.16.862.2.2	**RIF J-503240237**
Punto de distribución LCR	https://www.suscerte.gob.ve/lcr/CERTIFICADO-RAIZ-SHA384CRLDER.crl
Información del emisor	https://ocsp.suscerte.gob.ve
Política de Certificados	https://www.authenology.com.ve/normativas/

8.1.3 Raíz de certificación del PSC AUTHENTICSING.

El PSC AUTHENTICSING contiene una plataforma de certificación revisada y autorizada por SUSCERTE, la cual cumple con los estándares internacionales para la operación de una infraestructura de clave pública bajo un estándar X-509 V3. El PSC AUTHENTICSING se encuentra en capacidades de emitir certificados electrónicos para distintos usos.

Las claves criptográficas son generadas por el usuario a través de los OCSP contenidos en los browsers. SUSCERTE procede una evaluación

de cumplimiento de los requisitos de Ley, y luego firma una petición de certificado con la plataforma del certificado raíz del estado venezolano. Una vez ya firmado el certificado, el PSC AUTHENTICSING se establece en una autoridad de certificación de nivel y se encuentra subordinada por SUSCERTE.

El certificado raíz generado por SUSCERTE, debe ser incorporado por Authenticsing , dentro de su plataforma de certificación a los efectos de poder así generar y asignar los certificados electrónicos bajo los parámetros del decreto ley sobre mensajes de datos y firmas electrónicas (LSMDFE) y su reglamento (RLSMDFE). El PSC AUTHENTICSING, deberá producir cada veinticuatro (24) horas una lista de certificados revocados (LCR), el cual se constituirá en un mecanismo de validación y aprobación del estado de los certificados electrónicos y verificar cuales son los que se encuentran revocados.

Todo este proceso y transcurso de revocación de certificado es informado por el PSC AUTHENTICSING, por vía de correo electrónico al Cliente o Usuario propietario del certificado electrónico. Dicha notificación se informará mensualmente a SUSCERTE y se ajustará en el depósito digitalizado y mantenido por AUTHENTICSING.

8.1.3.1 **Relación con proveedores de tecnología y demás compañías relacionadas.**

El PSC AUTHENTICSING mantiene asociaciones estratégicas y relaciones comerciales con las siguientes empresas que se indican a continuación:

- DAYCOHOST

8.1.3.2 **Página y Aplicativo Web.**

AUTHENTICSING mantiene en operación un aplicativo web (**https://app.authenology.com.ve**) con una excelente disponibilidad. El aplicativo web der AUTHENTICSING en su página de inicio mantiene los siguientes vínculos: (NAVEGACION DEL APLICATIVO WEB)

i. Información de contacto AUTHENTICSING.
ii. Firma de documentos.
iii. Tipos de certificados.
iv. Firmas electrónicas
v. Planes y Servicios.
vi. Inicio de Sección.

vii. Registros.

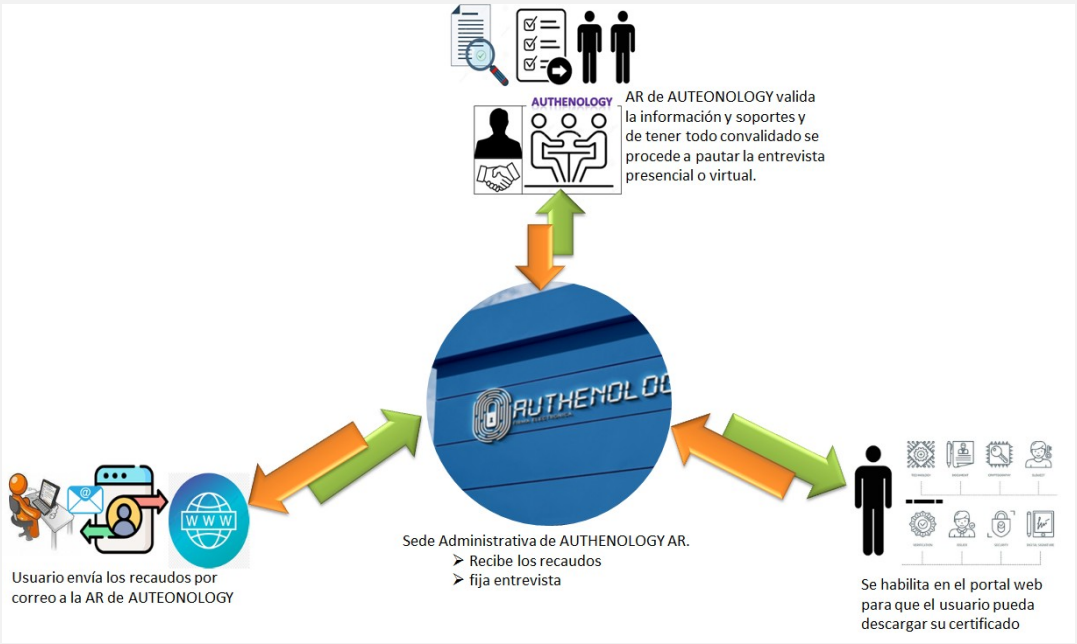
Authenticsing a su vez también cuenta

8.1.3.3 **Centro de datos.**

AUTHENTICSING provee un esquema operativo orientado a garantizar una constancia funcional y prestación de servicios con estándares de calidad, oportunidad y seguridad. El centro de datos se constituye en la sede de Daycohost. Opera las veinticuatro (24) horas del día, los trescientos sesenta y cinco (365) días del año y mantiene una autonomía y/o independencia operacional superior a los dos (2) meses. Adicionalmente, el centro de datos reúne condiciones y características de construcción antisísmica y de prevención de incendio e inundaciones, mantiene un perímetro de seguridad y cuenta con siete (7) niveles de seguridad de acceso. El centro de datos donde opera el PSC AUTHENTICSING mantiene las pólizas o instrumentos emitidos por empresas de seguros solventes y reconocidos, a los efectos de mantener un respaldo en caso de ocurrencia de una contingencia que afecta la integridad física de la referida sede administrativa y pueda ofrecer de esa manera una garantía de su continuidad operacional. La autoridad de certificación (AC) mantiene contrato de operación de centro alterno en caso de daño permanente que imposibilite y restrinja la operación regular del centro de datos.

8.1.3.4 **Esquema del modelo operacional de AUTHENTICSING**

Imagen #1



Esquema de Operación

La Autoridad de Registro (AR) es una entidad o persona responsable de verificar y registrar la información de identificación del solicitante para un certificado electrónico antes de que se emita el certificado. La AR actúa como intermediario entre el solicitante y la entidad emisora del certificado, Autoridad Certificado (AC), verificando la identidad del solicitante y proporcionando la información necesaria a la AC para emitir el certificado.

La función de la AR es fundamental para garantizar la autenticidad y la integridad de los certificados digitales emitidos, ya que la AC se basa en la información proporcionada por la AR para emitir el certificado. La AR también puede ser responsable de comprobar la validez de los documentos de identificación presentados por el solicitante y de garantizar que se cumplan los requisitos de seguridad y privacidad aplicables.

En el caso del PSC AUTHENTICSING su función es de identificar y validar los datos proporcionados por los signatarios y/o personas jurídicas y naturales que desean o han adquirido un certificado electrónico emitido por AUTHENTICSING, es la encargada de garantizar la identidad del signatario en un certificado

electrónico y en consecuencia dar validez de las responsabilidades y obligaciones procedentes del manejo y uso de la firma electrónica bajo los decreto de la ley sobre mensajes de datos y firmas electrónicas y su normativa.

Los interesados en obtener un certificado electrónico bajo el decreto ley sobre mensajes de datos y firmas electrónicas, deberán enviar una copia de la documentación, soporte de sus datos y apelar a la cita fijada por la Autoridad de Registro (AR) del PSC AUTHENTICSING a los efectos de realizar la comprobación, la validación presencial y documental de los registros, soportes y demás comprobantes que autentiquen su identidad y/o autoridad de los representantes de personas jurídicas que opten por un certificado electrónico.

Si el interesado no consideré y/o atiende la entrevista pautada por la Autoridad de Registro (AR) del PSC AUTHENTICSING quedará totalmente revocada y anulada su solicitud o petición de registro y se aplicará la retención por sanción o penalidad; como consecuencia de esto, el cliente tendrá que realizar una nueva solicitud de proceso de registro, este proceso lo podrá tramitar por medio de la pagina web (www.authenology.com.ve) o dirigiéndose a las oficinas del PSC AUTHENTICSING.

La documentación de soporte utilizada para la autenticación de los Clientes que solicitan certificados electrónicos, será almacenada por el PSC AUTHENTICSING, durante el período de diez (10) años determinados a partir de la vigencia del certificado o de cualquiera de sus renovaciones. Durante la solicitud de conexión un primer mensaje firmado digitalmente por la clave privada del operador RA es enviado a la AC quien verifica la identidad y autorización de la persona

De ser aprobada la conexión por parte de la AC en adelante todos los datos que viajen desde la AR a la AC serán firmados digitalmente por el operador AR, incluidas las solicitudes de generación y revocación.

8.2.1 Modelo de Operación de la AR

La AR del PSC AUTHENTICSING conserva un esquema de gestión orientado a asegurar y garantizar la constancia funcional y servicios con amplios estándares de seguridad y calidad. La AR elabora desde la ubicación administrativa del PSC AUTHENTICSING y es el encargado de dar consentimiento, conformidad y validación acerca de la autenticidad de los clientes contratantes de certificados electrónicos, y

una vez verificada la información e identidad de los clientes, se procederá con el registro de los clientes y posterior generación de los certificados electrónicos.

El proceso para validar la identidad de los clientes, es necesario para los procesos llevados a cabo por el PSC AUTHINTICSING, ya que permite conocer e identificar la validez de identificación de los clientes y potenciales signatarios. Este proceso es muy importante sobre todo cuando están involucrados temas sensibles como la seguridad de usuarios, aplica tanto para cliente jurídico o natural; a personas individuales así como integrantes en una organización y/o instituciones públicas o privadas.

De manera general, la autoridad de registro AR del PSC AUTHENTICSING puede validar para el caso de personas naturales identificación oficial (por ejemplo, cedula de identidad) comprobar que es vigente, genuina y extraer todos sus datos. Ahí mismo, se puede convalidar esta identificación con el sistema del consejo electoral nacional el cual están registrada en el padrón electoral. Para el caso de una persona jurídica, esta se podrá consultar su identificación con el sistema del SENIAT. Todo esto con base a la información que le solicita AUTHENTICSING para la solicitud y tramitación de un certificado electrónico correspondiente del caso.

Cuando sea cumplido el proceso de la contratación de certificados electrónicos a través del portal web de AUTHENTICSING **(www.authenology.com.ve)**, el cliente contratante tendrá que atender la entrevista programada por el sistema de contratación de AUTHENTICSING, con el propósito de ser efectuada la verificación de sus datos e identidad por parte de los operadores de la Autoridad de Registro (AR) del PSC AUTHENTICSING. La Autoridad de Registro (AR) del PSC AUTHENTICSING opera desde la oficina administrativa y es encargada de verificar y validar la identidad de los clientes que contratan certificados electrónicos, de manera que la información de los clientes y la identidad sea verificada, la información se hace llegar a la Autoridad de certificación (AC) del PSC AUTHENTICSING, con la finalidad de continuar con el proceso de expedición de los certificados electrónicos.

Sin la documentación correcta y registro, el PSC AUTHENTICSING se detendrá a continuar con el proceso de cualquier tipo de solicitud.

Para la comprobación mediante la dirección de correo electrónico, la Autoridad de Registro (AR) del PSC AUTHENTICSING envía un correo electrónico solicitando información al cliente. Todos los correos electrónicos desde la Autoridad de Registro (AR) del PSC AUTHENTICSING están firmados con firma electrónica. Los mensajes de correo electrónico exigirán la autorización del titular de la cuenta de correo electrónico. Cada e-mail del PSC AUTHENTICSING debe solicitar requisitos diferentes asociados con el proceso de validación en cada caso. Estos mensajes de correo electrónico del PSC AUTHENTICSING no son predecibles, ya que se requiere información que sólo el cliente conoce. Adicionalmente, el personal del PSC AUTHENTICSING debe verificar cada información (declaraciones juradas, las facturas de servicios públicos, estatutos, el RIF, la identificación de las empresas, entre otros).

La Autoridad de Registro (AR) del PSC AUTHENTICSING usa el número de teléfono proporcionados por el cliente en la declaración jurada debidamente firmada. Esta información tendrá que ser verificada y validada con los registros oficiales y públicos de la página Web de la Compañía Telefónica Nacional. Cuando un cliente solicita información para comprar un certificado, recibirá un correo electrónico de la Autoridad de Registro (AR) del PSC AUTHENTICSING con información completa. Por lo que ofrece la garantía de suministrar en cada momento toda la información que el cliente desee.

AUTHENTICSING mantiene los documentos que se solicitan al cliente. Estos documentos pueden variar y los clientes son informados por correo electrónico firmado en cada oportunidad. Con el propósito de disponer cada prevención de los constantes cambios en la DPC del PSC AUTHENTICSING derivados de cambios en los requisitos (inclusión o exclusión de cualquiera de ellos).

La integridad de AUTHENTICSING se asegurará y protegerá de cualquier cambio innecesario. Los clientes contratantes de firmas o certificados electrónicos deberán asistir a la Oficina Administrativa de AUTHENTICSING ubicada en **la calle Bolívar, edificio Don David, planta baja, oficina 001 en el municipio Chacao del estado Miranda** de la República Bolivariana de Venezuela, en la fecha y hora establecidos por el sistema de contratación **AUTHENTICSING** dentro del horario de trabajo de 8:00 am a 12:00 m y de 1:00 pm a 5:00 pm, de lunes a viernes de cada semana del mes.

El cliente contratante deberá comunicar e informar las condiciones o imposibilidad de asistir a la cita fijada por correo electrónico a la dirección de contacto@authenology.com.ve, no debe ser menos de cuarenta y ocho (48) horas antes de la fecha fijada para dicha cita.

La Autoridad de registro (AR) del PSC AUTHENTICSING aplazará y programará una nueva cita para una sola oportunidad y comunicará al usuario contratante por correo electrónico. Si el cliente contratante no informa su imposibilidad de poder asistir a una nueva cita programada, y no asiste a dicha cita, la Autoridad de Registro (AR) del PSC AUTHENTICSING procederá a la anulación de la cita e impondrá una sanción establecida en el proceso de contratación, por lo que el cliente acepta en el momento de la compra de un certificado electrónico.

Con relación a la verificación y validación de certificados extranjeros, prevista en el Decreto Ley de Mensajes de Datos y Firmas Electrónicas (LSMDFE) y su Reglamento, la Autoridad de Registro (AR) del PSC AUTHENTICSING, mantendrá actualizada la data con los cuales mantenga relación de reconocimiento y validación de certificados electrónicos, evitando en todo momento el uso de certificados revocados.

Se planificará anualmente auditorías de control y validación de la documentación e identidad de los clientes contratantes de certificados electrónicos. La documentación se mantendrá en soporte electrónico almacenado en repositorios de bóvedas.

1.1.1.3 **Diagrama del modelo de la AR.**

Imagen #1

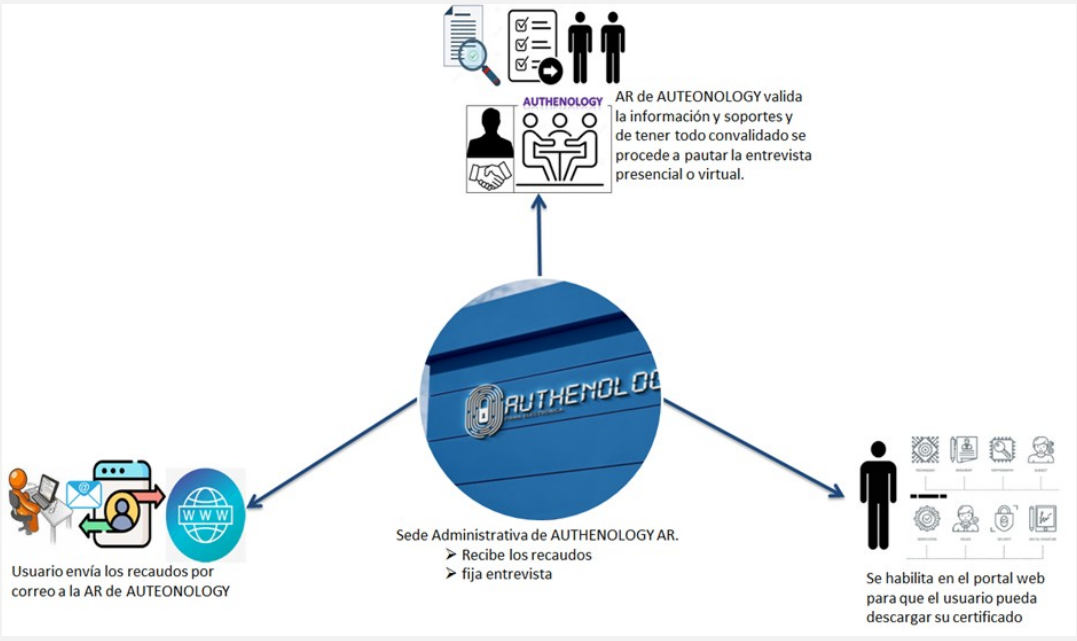


Diagrama de la AR

8.3 Signatario

En el contexto de la firma y certificados electrónico, un signatario puede ser una persona natural o jurídica que firma un documento digitalmente utilizando una firma electrónica. En este caso, la firma electrónica se considera equivalente a una firma manuscrita y es legalmente vinculante de acuerdo con las leyes y regulaciones aplicables.

Para el caso del PSC AUTHENTICSING, es toda aquella persona física o jurídica, equipamientos u aplicaciones que recibirán certificados electrónicos emitidos por el PSC Authenticsing.

8.4 Tercero de buena fe.

Los terceros de buena fe, son entidades jurídicas que confían en una firma electrónica, certificado electrónico, registro de certificados revocados o información generada por el PSC AUTHENTICSING y sobre las cuales pueden depositar su seguridad y confianza de acuerdo con el actual documento de la la Política de Certificados (PC) y Declaración de Prácticas de Certificación (DPC).

La Infraestructura de Clave Pública (ICP) del PSC AUTHENTICSING, está reconocida y obligada, directa o indirectamente (mediante cadena de contratos) con todos los proveedores, clientes y/o parte interesada, usuarios de firmas electrónicas y certificados electrónicos generados por el PSC AUTHENTICSING. De esta manera corresponder a una comunidad cerrada y depositar su confianza en sus servicios, se requiere precisamente de la aprobación de los clientes (terceros de buena Fe), a las condiciones del contrato de adquisición de firmas electrónicas o certificados electrónicos generados por el PSC AUTHENTICSING

9. USO DE LOS CERTIFICADOS (DPC y PC).

9.1 Usos permitidos.

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

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

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

9.1.1 Certificado de firma electrónica para empleado de empresa privada.

El uso asignado para este tipo de certificado son los siguientes puntos:

- Comunicaciones electrónicas sin representación de empresas privadas o públicas.
- Transacciones en línea.
- Identificar en línea a empleados o trabajadores de empresas públicas o privadas.
- Comunicaciones electrónicas sin representación de empresas públicas o privadas.
- No confiere representación legal de empresas públicas o privadas.

ESTRUCTURA DEL CERTIFICADO ELECTRÓNICO DE FIRMA PARA EMPLEADO DE EMPRESA PRIVADA.	
NOMBRE DEL CAMPO	**VALOR**
Versión	V3 (Número de versión del certificado)
Número de serie	Serial Number Octet Size 20
Algoritmo	ECDSA-whit- SHA-384 (Algoritmo de Firma)
DATOS DEL EMISOR	
Nombre común (CN)	AUTHENTICSING
Organización (O)	Sistema Nacional de Certificación Electrónica
Empresa (OU)	PROVEEDOR DE CERTIFICADOS AUTHENTICSING <Opcional>
País (C)	VE
PERIODO DE VALIDEZ	
Valido desde:	Inicio vigencia del certificado
Válido hasta:	Expiración del periodo de validez
DATOS DEL TITULAR	
Nombre común (CN)	(Nombre del empleado o signatario <Nombres y Apellidos>)
Organización (O)	(Nombre de la empresa u organización)
Titulo (T)	(Título o cargo del empleado o signatario)
Departamento (OU)	(Nombre del departamento o unidad administrativa de la organización)
País (C)	(País)
Estado (ST)	(Estado o región donde se encuentra la empresa u organización suscriptora)
Correo (E)	(Correo electrónico del empleado o signatario)
Localidad (L)	Ciudad donde se ubica la organización propietaria de la organización <Opcional>
Serial Number (DN)	Registro Único de Información Fiscal (R.I.F) <Opcional>
INFORMACIÓN DE CLAVE PUBLICA	
Algoritmo clave publica	id-ecPublicKey (ALGORITMO EN QUE SE GENERO LA CLAVE PUBLICA)
Tamaño clave publica	(384 bit)
EXTENSIONES	
Restricciones básicas	CA: FALSE
Identificador clave titular	(Identificador clave titular)
Claves de usos (KeyUsage)	
Firma digital	digitalSignature (0)
Compromiso con el contenido(Anteriormente no repudio)	contentCommitment (Non Repudiation)

Cifrado de datos	DatdataEncipherment(3)
Nombre alternativo del titular (subjectAltNAme)	
Nombre RFC822 (rfc822name)	(Correo electrónico de la Empresa)
Nombre DNS (dNSName)	(Sitio web de la empresa) <Opcional>
Identificador de clave de autoridad certificadora	
Clave de Autoridad (KeyIdentifier)	(ID de la Clave pública del AC-Raíz)
AIA Información de acceso de autoridad y política de información	
Punto de distribución LCR	URI:https://www.authenology.com.ve/ac-raiz/authenologycrl.crl <LCR del repositorio del PSC>
Dirección de Acceso	http://ocsp.authenology.com.ve/ <URL del servicio OSCP>
Política de Certificados	
Política de información de la PC	OID Autorizada por Suscerte CPS: https://www.authenology.com.ve/normativas/ <Link de repositorio>
Política de Información de la DPC	OID Autorizada por Suscerte CPS: https://www.authenology.com.ve/normativas/ <Link del repositorio>
FIRMA	
Algoritmo de firma (SignatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo ECDSA-whit-SHA-384)
Firma (SignatureValue)	(contenido de la firma)

- El uso del certificado de firma electrónica para empleado de empresa privada emitido por el PSC **AUTHENTICSING** estará limitado según el tipo de certificado, y a continuación se menciona el uso del mismo:

Tipo de certificado	Uso	Uso mejorado
Certificado de firma electrónica para empleado de empresa privada.	Firma digital, no repudio, cifrado de datos	Firma de Documentos

9.1.2 Certificado de firma electrónica para representante de empresa pública.

El uso asignado para este tipo de certificado es el siguiente:

- Transacciones en línea públicas o privadas, en representación de Entidades de Derecho Público o Empresas.
- Comercio electrónico en representación de Entidades de Derecho Público o Empresas.

- Certificar a una persona como representante legal de una entidad jurídica publica
- Comunicaciones privadas o públicas en representación de Entidades de Derecho Público o Empresas.
- Declaraciones o trámites en línea ante gobierno en representación de Entidades de Derecho Público o Empresas.

ESTRUCTURA DEL CERTIFICADO ELECTRÓNICO DE REPRESENTANTES DE EMPRESA PÚBLICA	
NOMBRE DEL CAMPO	**VALOR**
Versión	V3 (Número de versión del certificado)
Número de serie	Serial Number Octet Size 20
Algoritmo	ECDSA-whit- SHA-384 (Algoritmo de Firma)
DATOS DEL EMISOR	
Nombre común (CN)	AUTHENTICSING
Organización (O)	Sistema Nacional de Certificación Electrónica
Empresa (OU)	PROVEEDOR DE CERTIFICADOS AUTHENTICSING <Opcional>
País (C)	VE
PERIODO DE VALIDEZ	
Valido desde:	Inicio vigencia del certificado
Válido hasta:	Expiración del periodo de validez
DATOS DEL TITULAR	
Nombre (CN)	(Nombre del empleado o signatario <Nombres y Apellidos>)
Organización (O)	(Nombre de la empresa u organización)
Titulo (T)	(Título y/o cargo o funciones del titular del certificado)
Departamento (OU)	(Nombre del departamento o unidad de trabajo al cual pertenece el titular)
País (C)	(País)
Estado (ST)	(Estado o región donde se ubica la organización propietaria del certificado)
Correo (E)	(Correo electrónico del empleado o signatario) <Opcional>
Localidad (L)	Ciudad donde se ubica la organización <Opcional>
Serial Number (DN)	Registro Único de Información Fiscal (R.I.F) <Opcional>
INFORMACIÓN DE CLAVE PUBLICA	
Algoritmo clave publica	id-ecPublicKey (ALGORITMO EN QUE SE GENERO LA CLAVE PUBLICA)
Tamaño clave publica	(384 bit)
EXTENSIONES	
Restricciones básicas	CA: FALSE

Identificador clave titular	(Identificador clave titular)
Claves de usos (KeyUsage)	
Firma digital	digitalSignature (0)
Compromiso con el contenido(Anteriorment e no repudio)	contentCommitment (Non Repudiation)
Cifrado de datos	DatdataEncipherment(3)
Nombre alternativo del titular (subjectAltNAme)	
Nombre RFC822 (rfc822name)	(Correo electrónico del ente Suscriptor)
Nombre DNS (dNSName)	(Sitio web de la empresa) <Opcional>
Identificador de clave de autoridad certificadora	
Clave de Autoridad (KeyIdentifier)	(ID de la Clave pública del AC-Raíz)
AIA Información de acceso de autoridad y política de información	
Punto de distribución LCR	URI:https://www.authenology.com.ve/ac-raiz/authenologycrl.crl <LCR del repositorio del PSC>
Dirección de Acceso	http://ocsp.authenology.com.ve/ <URL del servicio OSCP>
Política de Certificados	
Política de información de la PC	OID Autorizada por Suscerte CPS: https://www.authenology.com.ve/normativas/ <Link de repositorio>
Política de Información de la DPC	OID Autorizada por Suscerte CPS: https://www.authenology.com.ve/normativas/ <Link del repositorio>
FIRMA	
Algoritmo de firma (SignatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo ECDSA-whit-SHA-384)
Firma (SignatureValue)	(contenido de la firma)

- El uso del certificado de firma electrónica para representante de empresas públicas emitido por el PSC AUTHENTICSING estará limitado según el tipo de certificado, y a continuación se menciona el uso del mismo:

Tipo de certificado	Uso	Uso mejorado
Certificado de firma electrónica para representante de empresa pública.	Firma digital, no repudio, cifrado de datos	Firma de Documentos

9.1.3 Certificado de firma electrónica para funcionario público.

El uso asignado para este tipo de certificado es el siguiente:

- Transacciones en línea públicas o privadas, en representación de Entidades de Derecho Público o Empresas.
- Comercio electrónico en representación de Entidades de Derecho Público o Empresas.
- Certificar a una persona como representante legal de una entidad jurídica publica
- Comunicaciones privadas o públicas en representación de Entidades de Derecho Público o Empresas.
- Declaraciones o trámites en línea ante gobierno en representación de Entidades de Derecho Público o Empresas.

ESTRUCTURA DEL CERTIFICADO ELECTRÓNICO PARA FUNCIONARIO PÚBLICO.	
NOMBRE DEL CAMPO	**VALOR**
Versión	V3 (Número de versión del certificado)
Número de serie	Serial Number Octet Size 20
Algoritmo	ECDSA-whit- SHA-384 (Algoritmo de Firma)
DATOS DEL EMISOR	
Nombre común (CN)	AUTHENTICSING
Organización (O)	Sistema Nacional de Certificación Electrónica
Empresa (OU)	PROVEEDOR DE CERTIFICADOS AUTHENTICSING <Opcional>
País (C)	VE
PERIODO DE VALIDEZ	
Valido desde:	Inicio vigencia del certificado
Válido hasta:	Expiración del periodo de validez
DATOS DEL TITULAR	
Nombre (CN)	(Nombre del empleado o signatario <Nombres y Apellidos>)
Organización (O)	(Opcional)
Titulo (T)	(Título y/o cargo o funciones del titular del certificado)
Correo (E)	(Correo electrónico del empleado o signatario) <Opcional>
Departamento (OU)	(Nombre del departamento o unidad de trabajo al cual pertenece el titular)
País (C)	(País)
Estado (ST)	(Estado o región donde se ubica la organización propietaria del certificado)
Localidad (L)	Ciudad donde se ubica el signatario <Opcional>
Serial Number (DN)	Registro Único de Información Fiscal (R.I.F) <Opcional>

INFORMACIÓN DE CLAVE PUBLICA	
Algoritmo clave publica	id-ecPublicKey (ALGORITMO EN QUE SE GENERO LA CLAVE PUBLICA)
Tamaño clave publica	(384 bit)
EXTENSIONES	
Restricciones básicas	CA: FALSE
Identificador clave titular	(Identificador clave titular)
Claves de usos (KeyUsage)	
Firma digital	digitalSignature (0)
Compromiso con el contenido(Anteriorment e no repudio)	contentCommitment (Non Repudiation)
Cifrado de datos	DatdataEncipherment(3)
Nombre alternativo del titular (subjectAltNAme)	
Nombre RFC822 (rfc822name)	(Correo electrónico del ente Suscriptor)
Nombre DNS (dNSName)	(Sitio web de la empresa) <Opcional>
Identificador de clave de autoridad certificadora	
Clave de Autoridad (KeyIdentifier)	(ID de la Clave pública del AC-Raíz)
AIA Información de acceso de autoridad y política de información	
Punto de distribución LCR	URI:https://www.authenology.com.ve/ac-raiz/authenologycrl.crl <LCR del repositorio del PSC>
Dirección de Acceso	http://ocsp.authenology.com.ve/ <URL del servicio OSCP>
Política de Certificados	
Política de información de la PC	OID Autorizada por Suscerte CPS: https://www.authenology.com.ve/normativas/ <Link de repositorio>
Política de Información de la DPC	OID Autorizada por Suscerte CPS: https://www.authenology.com.ve/normativas/ <Link del repositorio>
FIRMA	
Algoritmo de firma (SignatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo ECDSA-whit-SHA-384)
Firma (SignatureValue)	(contenido de la firma)

- El uso del certificado de firma electrónica para funcionario público emitido por el PSC **AUTHENTICSING** estará limitado según el tipo de certificado, y a continuación se menciona el uso del mismo:

Tipo de certificado	Uso	Uso mejorado
Certificado de firma electrónica para funcionario público.	Firma digital, no repudio, cifrado de datos	Firma de documentos

9.1.4 Certificado de firma electrónica para representante legal de empresa privada.

El uso asignado para este tipo de certificado es el siguiente:

- Transacciones en línea públicas o privadas, en representación de Entidades de Derecho Público o Empresas.
- Comercio electrónico en representación de Entidades de Derecho Público o Empresas.
- Certificar a una persona como representante legal de una entidad jurídica publica
- Comunicaciones privadas o públicas en representación de Entidades de Derecho Público o Empresas.
- Declaraciones o trámites en línea ante gobierno en representación de Entidades de Derecho Público o Empresas.

ESTRUCTURA DEL CERTIFICADO ELECTRÓNICO DE FIRMA PARA REPRESENTANTE LEGAL DE EMPRESA PRIVADA.	
NOMBRE DEL CAMPO	**VALOR**
Versión	V3 (Número de versión del certificado)
Número de serie	Serial Number Octet Size 20
Algoritmo	ECDSA-whit- SHA-384 (Algoritmo de Firma)
DATOS DEL EMISOR	
Nombre común (CN)	AUTHENTICSING
Organización (O)	Sistema Nacional de Certificación Electrónica
Empresa (OU)	PROVEEDOR DE CERTIFICADOS AUTHENTICSING <Opcional>
País (C)	VE
PERIODO DE VALIDEZ	
Valido desde:	Inicio vigencia del certificado
Válido hasta:	Expiración del periodo de validez
DATOS DEL TITULAR	
Nombre (CN)	(Nombre del empleado o signatario <Nombres y Apellidos>)
Organización (O)	(Nombre de la empresa u organización)

Titulo (T)	(Título o cargo del empleado o signatario)
Correo (E)	(Correo electrónico del empleado o signatario) <Opcional>
Departamento (OU)	(Nombre del departamento o unidad administrativa de la organización) <Opcional>
País (C)	(País)
Estado (ST)	(Estado o región donde se encuentra la empresa u organización)
Localidad (L)	(Ciudad donde se ubica la organización) <Opcional>
Serial Number (DN)	Registro Único de Información Fiscal (R.I.F) <Opcional>
INFORMACIÓN DE CLAVE PUBLICA	
Algoritmo clave publica	id-ecPublicKey (ALGORITMO EN QUE SE GENERO LA CLAVE PUBLICA)
Tamaño clave publica	(384 bit)
EXTENSIONES	
Restricciones básicas	CA: FALSE
Identificador clave titular	(Identificador clave titular)
Claves de usos (KeyUsage)	
Firma digital	digitalSignature (0)
Compromiso con el contenido(Anteriorment e no repudio)	contentCommitment (Non Repudiation)
Cifrado de datos	DatdataEncipherment(3)
Nombre alternativo del titular (subjectAltNAme)	
Nombre RFC822 (rfc822name)	(Correo electrónico de la Empresa)
Nombre DNS (dNSName)	(Sitio web de la empresa) <Opcional>
Identificador de clave de autoridad certificadora	
Clave de Autoridad (KeyIdentifier)	(ID de la Clave pública del AC-Raíz)
AIA Información de acceso de autoridad y política de información	
Punto de distribución LCR	URI:https://www.authenology.com.ve/ac-raiz/authenologycrl.crl <LCR del repositorio del PSC>
Dirección de Acceso	http://ocsp.authenology.com.ve/ <URL del servicio OSCP>
Política de Certificados	
Política de información de la PC	OID Autorizada por Suscerte CPS: https://www.authenology.com.ve/normativas/ <Link de repositorio>
Política de Información de la DPC	OID Autorizada por Suscerte CPS: https://www.authenology.com.ve/normativas/ <Link del repositorio>
FIRMA	
Algoritmo de firma	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo ECDSA-whit-

(Signatare Algorithm)	SHA-384)
Firma (Signature Value)	(contenido de la firma)

- El uso del certificado de firma electrónica para representante legal de empresas privadas emitido por el PSC AUTHENTICSING estará limitado según el tipo de certificado, y a continuación se menciona el uso del mismo:

Tipo de certificado	Uso	Uso mejorado
Certificado de firma electrónica para representante de empresa privada.	Firma digital, no repudio, cifrado de datos	Firma de Documentos

9.1.5 Certificado de firma electrónica para profesionales titulados

El uso asignado para este tipo de certificado es el siguiente:

- Transacciones en línea asociadas al ejercicio de profesión u oficio con colegiatura y reconocimiento legal dentro de la República Bolivariana de Venezuela.
- Comunicaciones privadas o públicas asociadas al ejercicio de profesión u oficio con colegiatura y reconocimiento dentro de la República Bolivariana de Venezuela.
- Comercio electrónico asociadas al ejercicio de profesión u oficio con colegiatura y reconocimiento dentro de la República Bolivariana de Venezuela.
- Certificar a una persona como representante legal de una entidad jurídica publica
- Comunicaciones privadas o públicas en representación de Entidades de Derecho Público o Empresas.
- Declaraciones o trámites en línea ante gobierno asociadas al ejercicio de profesión u oficio con colegiatura y reconocimiento dentro de la República Bolivariana de Venezuela.

ESTRUCTURA DEL CERTIFICADO ELECTRÓNICO DE FIRMA PARA PROFESIONALES TITULADOS.	
NOMBRE DEL CAMPO	**VALOR**
Versión	V3 (Número de versión del certificado)
Número de serie	Serial Number Octet Size 20
Algoritmo	ECDSA-whit- SHA-384 (Algoritmo de Firma)
DATOS DEL EMISOR	

Nombre común (CN)	AUTHENTICSING
Organización (O)	Sistema Nacional de Certificación Electrónica
Empresa (OU)	PROVEEDOR DE CERTIFICADOS AUTHENTICSING <Opcional>
País (C)	VE
PERIODO DE VALIDEZ	
Valido desde:	Inicio vigencia del certificado
Válido hasta:	Expiración del periodo de validez
DATOS DEL TITULAR	
Nombre (CN)	(Nombre del profesional y el número de colegiado)
Organización (O)	(Nombre o dominación de la colegiatura que otorgó el título profesional) <Opcional>
Titulo (T)	(Nombre del titular registrado ante la colegiatura) <Opcional>
Correo (E)	(Correo electrónico del signatario)
País (C)	(País)
Estado (ST)	(Estado o región donde se encuentra el signatario)
Localidad (L)	Ciudad donde se encuentra el signatario <Opcional>
Serial Number (DN)	Registro Único de Información Fiscal (R.I.F) <Opcional>
INFORMACIÓN DE CLAVE PUBLICA	
Algoritmo clave publica	id-ecPublicKey (ALGORITMO EN QUE SE GENERO LA CLAVE PUBLICA)
Tamaño clave publica	(384 bit)
EXTENSIONES	
Restricciones básicas	CA: FALSE
Identificador clave titular	(Identificador clave titular)
Claves de usos (KeyUsage)	
Firma digital	digitalSignature (0)
Compromiso con el contenido(Anteriormente no repudio)	contentCommitment (Non Repudiation)
Cifrado de datos	DatdataEncipherment(3)
Nombre alternativo del titular (subjectAltNAme)	
Nombre RFC822 (rfc822name)	(Correo electrónico del colegio que otorgo el título profesional)
Nombre DNS (dNSName)	(Sitio web del colegio que otorgo el título profesional) <Opcional>
Identificador de clave de autoridad certificadora	

Clave de Autoridad (KeyIdentifier)	(ID de la Clave pública del AC-Raíz)
AIA Información de acceso de autoridad y política de información	
Punto de distribución LCR	URI:https://www.authenology.com.ve/ac-raiz/authenologycrl.crl <LCR del repositorio del PSC>
Dirección de Acceso	http://ocsp.authenology.com.ve/ <URL del servicio OSCP>
Política de Certificados	
Política de información de la PC	OID Autorizada por Suscerte CPS: https://www.authenology.com.ve/normativas/ <Link de repositorio>
Política de Información de la DPC	OID Autorizada por Suscerte CPS: https://www.authenology.com.ve/normativas/ <Link del repositorio>
FIRMA	
Algoritmo de firma (Signature Algorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo ECDSA-whit- SHA-384)
Firma (SignatureValue)	(contenido de la firma)

- El uso del certificado de firma electrónica para profesionales titulados emitido por el PSC **AUTHENTICSING** estará limitado según el tipo de certificado, y a continuación se menciona el uso del mismo:

Tipo de certificado	Uso	Uso mejorado
Certificado de firma electrónica para profesionales titulados.	Firma digital, no repudio, cifrado de datos	Firma de Documentos

9.1.6 Certificado electrónico de firma para persona natural

El uso asignado para este tipo de certificado es el siguiente:

- Transacciones privadas, distintas a prestación de servicios profesionales.
- Comunicaciones privadas o públicas a título personal.
- Compras electrónicas para personas naturales.
- Declaración o trámites en línea ante el gobierno para personas naturales.

ESTRUCTURA DEL CERTIFICADO ELECTRÓNICO DE FIRMA PARA PERSONA NATURAL.	
NOMBRE DEL CAMPO	**VALOR**
Versión	V3 (Número de versión del certificado)
Número de serie	Serial Number Octet Size 20
Algoritmo	ECDSA-whit- SHA-384 (Algoritmo de Firma)

DATOS DEL EMISOR	
Nombre común (CN)	AUTHENTICSING
Organización (O)	Sistema Nacional de Certificación Electrónica
Empresa (OU)	PROVEEDOR DE CERTIFICADOS AUTHENTICSING <Opcional>
País (C)	VE
PERIODO DE VALIDEZ	
Valido desde:	Inicio vigencia del certificado
Válido hasta:	Expiración del periodo de validez
DATOS DEL TITULAR	
Nombre (CN)	(Nombre1, Nombre2, Apellido1 Apellido2)
Organización (O)	(Opcional)
Correo (E)	(Correo electrónico del signatario)
País (C)	(País)
Estado (ST)	(Estado o región donde se encuentra el signatario) <opcional>
Localidad (L)	Ciudad donde se ubica la organización <Opcional>
Serial Number (DN)	Registro Único de Información Fiscal (R.I.F) <Opcional>
INFORMACIÓN DE CLAVE PUBLICA	
Algoritmo clave publica	id-ecPublicKey (ALGORITMO EN QUE SE GENERO LA CLAVE PUBLICA)
Tamaño clave publica	(384 bit)
EXTENSIONES	
Restricciones básicas	CA: FALSE
Identificador clave titular	(Identificador clave titular)
Claves de usos (KeyUsage)	
Firma digital	digitalSignature (0)
Compromiso con el contenido(Anteriorment e no repudio)	contentCommitment (Non Repudiation)
Cifrado de datos	DatdataEncipherment(3)
Nombre alternativo del titular (subjectAltNAme)	
Nombre RFC822 (rfc822name)	(Correo electrónico de la Empresa)
Identificador de clave de autoridad certificadora	
Clave de Autoridad (KeyIdentifier)	(ID de la Clave pública del AC-Raíz)
AIA Información de acceso de autoridad y política de información	
Punto de distribución LCR	URI: https://www.authenology.com.ve/ac-raiz/authenologycrl.crl <LCR del repositorio del PSC>

Dirección de Acceso	http://ocsp.authenology.com.ve/ <URL del servicio OSCP>
Política de Certificados	
Política de información de la PC	OID Autorizada por Suscerte CPS: https://www.authenology.com.ve/normativas/ <Link de repositorio>
Política de Información de la DPC	OID Autorizada por Suscerte CPS: https://www.authenology.com.ve/normativas/ <Link del repositorio>
FIRMA	
Algoritmo de firma signatareAlgorimo)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo ECDSA-whit-SHA-384)
Firma (signature)	(contenido de la firma)

- El uso del certificado de firma electrónica para persona natural emitido por el PSC AUTHENTICSING estará limitado según el tipo de certificado, y a continuación se menciona el uso del mismo:

Tipo de certificado	Uso	Uso mejorado
Certificado de firma electrónica para persona natural.	Firma digital, no repudio, cifrado de datos	Firma de Documentos

9.1.7 Estructura del Certificado de Servidor de OCSP

- Se debe colocar una estructura de Certificado de servidor OCSP para firmar respuestas generadas del servicio OCSP de una AC.
- Las restricciones básicas debe ser la AC= [false]

ESTRUCTURA DEL CERTIFICADO DE SERVIDOR OCSP	
NOMBRE DEL CAMPO	**VALOR**
Versión	V3 (Número de versión del certificado)
Número de serie	Serial Number Octet Size 20
Algoritmo	ECDSA-whit- SHA-384 (Algoritmo de Firma)
DATOS DEL EMISOR	
CN	PSC AUTHENTICSING
O	Sistema Nacional de Certificación Electrónica
C	VE
PERIODO DE VALIDEZ	

Valido desde:	Inicio vigencia del certificado
Válido hasta:	Expiración del periodo de validez
DATOS DEL TITULAR	
CN	(Nombre del representante legal a certificar).
O	(Nombre de la organización)
C	PAIS
INFORMACIÓN DE CLAVE PÚBLICA	
Algoritmo clave publica	ECDSA (ALGORITMO EN QUE SE GENERO LA CLAVE PUBLICA)
Tamaño clave publica	(384 bit)
EXTENSIONES	
Restricciones básicas	CA: [false]
Uso de la llave (KeyUsage)	Firma digital: ocsp-Signing[1] (Requerido)
Identificador clave titular	(Identificador de clave del titular)
IDENTIFICADOR DE CLAVE DE AUTORIDAD CERTIFICADORA	
Id. De clave	(Identificador de la clave)
Emisor de certificado	(Datos del emisor)
Numero serie certificado	(Número de serial)
Uso	Firma digital, Compromiso del contenido (No repudio), solo Encriptar, solo Descifrado
Mejorado	
NOMBRE ALTERNATIVO DEL TITULAR	
Other name	
OID 2.16.862.2.2	(Número de cédula o de pasaporte del signatario)
Punto de distribución LCR	https://www.authenology.com.ve/ac-raiz/authenologycrl.crl
Política de Certificados	https://www.authenology.com.ve/normativas/

- El uso del certificado de firma electrónica para servidor OCSP emitido por el PSC AUTHENTICSING estará limitado según el tipo de certificado, y a continuación se menciona el uso del mismo:

Tipo de certificado	Uso	Uso mejorado

Certificado de firma electrónica para persona natural.	Firma digital, Compromiso del contenido, solo Encriptar, solo Descifrado	N/A

9.2 Usos no permitidos

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

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

10. POLÍTICAS DE ADMINISTRACIÓN DEL PSC (DPC y PC)

Como parte de las políticas implementadas por el PSC AUTHENTICSING de establecer el conjunto de normas y criterios que se deben de implementar para la ejecución de las políticas de administración como Proveedor de Servicio de Certificación; es por eso que el PSC AUTHENTICSING estable, documenta, expone e informa a los clientes la información sobre la generación de certificados electrónicos sus usos y obligaciones.

10.1 Especificaciones de la organización administrativa

Esta sección incluye información correspondiente a la autoridad responsable dentro del PSC Authenticsing por el registro, mantenimiento y actualización de la DPC y PC.

DATOS DE LA EMPRESA	
Nombre	JUNTA DIRECTIVA DE AUTHENTICSING.
Correo electrónico	admin-pki@authenology.com.ve
Número de teléfono	+58 – 0212 - 2647658

Numero de Fax	+58 – 0212 - 2647658
Página web	www.authenology.com.ve

10.2 Persona Contacto.

DATOS DEL CONTACTO	
Nombre	PSC AUTHENTICSING.
Correo electrónico	admin-pki@authenology.com.ve
Número de teléfono	+58 – 0212 - 2647658
Numero de Fax	+58 – 0212 - 2647658
Página web	www.authenology.com.ve

10.3 Competencia para determinar la adecuación de la DPC y las políticas

El presente documento de la Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC), emitido por el PSC AUTHENTICSING conforme a los lineamientos de la SUSCERTE; su aplicabilidad es responsabilidad de la Alta gerencia del PSC AUTHENTICSING y es de uso de obligatorio cumplimiento y sujeción por parte de los actores que conforma esta organización.

11. PUBLICACIÓN DE INFORMACIÓN DEL PSC Y REPOSITORIOS DE LOS CERTIFICADOS (DPC)

11.1 Repositorios

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

- Certificado de la AC Subordinada AUTHENTICSING, los certificados emitidos por dicha AC y la DPC: https://www.authenology.com.ve/ac

- Lista de Certificados Revocados: https://www.authenology.com.ve/lrc
- Servicio de validación en línea (OCSP): https://www.authenology.com.ve/ocsp
- El repositorio público del PSC AUTHENTICSING, no incluye ninguna información confidencial o privada

11.2 Publicación

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

- Lista de Certificados Revocados (LCR), se encuentra útil y apto en formato CRL en: https://www.authenology.com.ve/lrc
- El actual documento se encuentra útil y disponible en: https://www.authenology.com.ve/dpc
- El certificado de la AC Subordinada AUTHENTICSING se encuentra útil y disponible en: https://www.authenology.com.ve/ac
- Los certificados emitidos por la AC Subordinada AUTHENTICSING se encuentran en: https://www.authenology.com.ve/ac
- La información de contacto del PSC AUTHENTICSING en la dirección: https://www.authenology.com.ve La acreditación y documentación técnica del PSC AUTHENTICSING en la dirección: https://www.authenology.com.ve

11.3 Frecuencia de publicación

La publicación de los certificados se ejecutará una vez conseguido la identificación y acreditación por parte de SUSCERTE. La vigencia es de diez (10) años.

11.3.2 Lista de Certificados Revocados (LCR)

La publicación de la Lista de Certificados Revocados se actualizara y ejecutará cada veinticuatro (24) horas.

11.3.3 Declaración de Prácticas de Certificación.

Aparte de que explícitamente se indique todo lo contrario del presente documento de la Política de Certificación (PC) y Declaración de Prácticas de Certificación (DPC), se hará público en el sitio web del PCS AUTHENTICSING https://www.authenology.com.ve las nuevas versiones de este documento, cuando las mismas sean revisadas y validadas por la alta dirección del PSC AUTHENTICSING y SUSCERTE.

11.3.4 Controles de acceso al repositorio de certificados.

El ingreso a la información publicada por el PSC AUTHENTICSING será de asesoramiento y consulta y no podrá ser cambiada o modificada por personal no autorizada. La información patente y pública solo será actualizada por el personal encargado de esa función que labora en AUTHENTICSING. Se asegurara el asesoramiento y la consulta a la Lista de Certificados Revocados (LCR) a los certificados emitidos, al servidor de Protocolo de Estado de Certificado en Línea (OCSP) y el actual documento.

12. IDENTIFICACION Y AUTENTICACIÓN (DPC y PC).

12.1 Registro de nombres.

La AC del PSC AUTHENTICSING solo genera y emite firmas certificadas con tipos de nombres acordes al estándar X.509 V3. A continuación los nombres de los datos del titular y del nombre alternativo del titular del certificado de la AC del PSC AUTHENTICSING.

- **AUTHENTICSING:** El Nombre Distintivo (DN) del PSC AUTHENTICSING está compuesto y conformado por los siguientes punto s:

- CN: AUTHENTICSING.
- O: Sistema Nacional de Certificación Electrónica.
- C: VE.
- E: [contacto@authenology.com.ve]

- El Nombre Alternativo (AN) del PSC AUTHENTICSING está compuesto y conformado por los siguientes puntos:

- DNSName: https://www.authenology.com.ve
- OtherName:
- OID 2.16.862.2.1. (Código de identificación del PSC AUTHENTICSING acreditado)
- OID 2.16.862.2.2.: RIF J-503240237

- **Para los Signatarios**: El Nombre Distintivo (DN) del signatario está conformado por los siguientes puntos:

- CN: (NOMBRE DEL TITULAR)
- O: (NOMBRE DE LA ORGANIZACIÓN).

- C: VE.
- E: [CORREO ELECTRONICO]
- S: [ESTADO]

  - El Nombre Alternativo (AN) del signatario está conformado por los siguientes punto s:

- OtherName: OID 2.16.862.2.2.: (Numero de Cedula de Identidad o Pasaporte)

12.1.2 Necesidad de que los nombres sean significativos.

El PSC AUTHENTICSING requerirá de los clientes contratantes de firmas o certificados electrónicos de sus nombres y apellidos completos y conformen estén presentados en la cédula de identidad laminada que presenta el aspirante y solicitante de certificado digitales o firmas. No serán recibidos o procesados por la Autoridad de Registro (AR), los documentos referentes a la disminución de nombres, reputación, seudónimos o alias con los cuales se solicite y pretenda identificar el cliente. Para el caso de las poblaciones indígenas será estimado y considerado los nombres que emita su cédula de identidad o pasaporte. En todo caso el PSC AUTHENTICSING asegura que los datos contenidos y argumentados en el punto s de los certificados son lo suficientemente significativos y distintivos para poder vincular la identidad de un cliente a su firma o certificado electrónico.

12.1.3 Interpretación de formatos de nombres.

Los reglamentos llevados a cabo para la interpretación y sentido de los nombres distinguidos en los certificados emitidos están descritos en la Organización ISO/IEC 9595 (X.509 - V3) Dintinguish Name (DN). Además, los certificados emitidos por AUTHENTICSING disponen codificación UTF8 para todos los atributos, según la RFC 6818 Actualizaciones del perfil de la lista de (CRL) y el certificado de infraestructura de clave pública X.509 de Internet, enero de 2013 (Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, January 2013).

12.1.4 Unicidad de nombres.

La Autoridad de Certificación de SUSCERTE precisa como el punto DN del Certificado de Autoridad (CA) como único y exclusivamente sin ambigüedad. Para esto se comprenderá e incluirá como parte del DN, concretamente en el punto OU, la razón o el nombre social del PSC

AUTHENTICSING, por consiguiente lo irrepetible se asegura mediante la franqueza y confianza sobre la unicidad de las marcas comerciales o nombres mercantiles en el registro nacional. Asimismo, con respecto a los clientes; si existe un cliente que conserva contrato y consiga más de un tipo de firma o certificado electrónico, el fundamento de datos del PSC AUTHENTICSING mantendrá un esquema parejo e igualitario de datos del cliente contratante y no será autorizado, legal o procesado por la Autoridad de Registro (AR) del PSC, datos personales diferentes y que pertenezcan a un mismo cliente.

12.1.5 Resolución de Conflictos relativos a nombres.

En el suceso de una contingencia de oposición y conflicto de nombre entre clientes y que pertenezca a nombre y apellidos iguales, la autoridad de registro (AR) del PSC AUTHENTICSING iniciará y procederá a ejecutar la selección y distinción de equivalencia y autenticidad de la misma por medio del uso del número de cédula de identidad y RIF personal de cada cliente del PSC AUTHENTICSING con las cuales se produzca el oposición y conflicto de nombre.

12.2 Validación inicial de la identidad

El esquema de operación del PSC AUTHENTICSING y su organización y plataforma tecnológica de certificación se encuentran formados Y configurados para que el cliente genere su par de claves (pública y privada) y firme la clave del CE.

En capacidad de lo anterior, una vez emitido cada certificado, es el cliente quien posee la custodia, garantía y resguardo de su clave privada, presuponiendo que el mismo la tiene y resguarda con todo el deber y obligándose conforme a la ley, salvo denuncia de el mismo cliente de compromiso de su clave privada, caso en el cual se procederá a la revocación de la firma o certificado electrónico que corresponda.

12.2.2 Autenticación de la identidad de la organización.

La Autoridad de Registro (AR) del PSC AUTHENTICSING en el momento de que se trate de firmas electrónicas que autentiquen y acrediten empresas o entes públicos se ejecutará de la siguiente manera:

1.1.1.4 Entidad público.

La Autoridad de Registro (AR) procederá a validar y comprobar el

anuncio o publicación en la gaceta oficial de la República Bolivariana de Venezuela de la determinación que establece a la entidad o empresa pública. Todo certificado electrónico de planificación y organización deberá estar agregado a un encargado y responsable ente por dicho certificado. La Autoridad de Registro (AR) del PSC AUTHENTICSING cumplirá los pasos de verificación, validación y comprobación de identidad y autoridad.

Una vez verificada la autenticidad de la organización y las facultades de representación, se procederá a validar el resto de la documentación e información requerida por el método de contratación del PSC AUTHENTICSING y cumpliendo los procedimientos exitosamente, la Autoridad de Registro (AR) informará a la Autoridad de Certificación (AC) del PSC AUTHENTICSING, su aprobación o conformidad respecto a los datos para que corresponda a la formación del certificado electrónico contratado por el cliente.

1.1.1.5 **Entidad privada.**

La Autoridad de Registro (AR) procederá a confirmar la existencia y validez de la empresa privada mediante la consulta de su documento constitutivo-legislativo, precisamente alistado en la oficina del registro mercantil correspondiente a la delimitación judicial de la dirección de la empresa privada, como la publicación del registro de empresa en un diario mercantil. Todo certificado electrónico de organización necesitará estar asociado a un responsable ente por dicho certificado. La Autoridad de Registro (AR) del PSC AUTHENTICSING cumplirá los pasos de verificación, confirmación y comprobación de identidad y autoridad.

Una vez revisado y verificada la identidad de la organización y las facultades que representa, se procederá a validar el resto de la información solicitada por el sistema de contratación del PSC AUTHENTICSING y cumpliendo el procedimiento exitosamente, la Autoridad de Registro (AR) informará a la Autoridad de Certificación (AC) del PSC AUTHENTICSING, su aprobación o conformidad respecto a los datos para que se proceda a la formación del certificado electrónico contratado por el cliente.

12.2.3 Autenticación de la identidad de Personas Naturales.

El proceso de validación de identidad es un conjunto de procedimientos

para verificar la identidad de una persona antes de emitir un certificado digital u otro tipo de documento de identificación. El objetivo del proceso es asegurarse de que la persona que solicita el certificado es realmente quien dice ser y que cumple con los requisitos necesarios para obtener el certificado.

La autentificación puede darse por los siguientes pasos:

- **Recopilación de información de identificación:** La persona interesada en obtener un certificado electrónico CE debe proporcionar información de identificación, como su nombre completo, dirección, fecha de nacimiento, número de cedula de identificación, etc.
- **Verificación de la información de identificación:** La autoridad de registro AR del PSC AUTHENTICSING del certificado debe verificar la información de identificación proporcionada por la persona interesada, utilizando diferentes métodos de verificación, como la comparación con bases de datos gubernamentales (SENIAT, SAIME, CNE), la verificación mediante documentos de identificación físicos, la verificación mediante videoconferencia o la verificación mediante terceros de confianza.
- **Verificación de la identidad en persona:** En algunos casos La autoridad de registro AR del PSC AUTHENTICSING requerirá que la persona interesada se presente en persona en la sede administrativa de Authenticsing para verificar su identidad. Esto puede incluir la verificación de documentos de identificación físicos o la toma de fotografías.
- **Verificación de la autenticidad de los documentos:** Si se requieren documentos adicionales para verificar la identidad, la AR del PSC AUTHENTICSING puede verificar la autenticidad de los documentos presentados, como pasaportes, licencias de conducir o tarjetas de identificación.

12.2.4 Comprobación de las facultades de representación.

La comprobación de las facultades de representación es realiza mediante la presentación de los documentos originales del signatario ante el operador AR del PSC AUTHENTICSING si la comprobación es en la sede administrativa del PSC AUTHENTICSING, en caso contrario también puede ser validada por el operador AC.

Así mismo la aplicación de la AR, valida la identidad del signatario a través de su serial de validación y correo electrónico, para la autenticación en la AR, previa a la emisión del CE por parte de la AC de

AUTHENTICSING.

12.3 Identificación y autenticación de las solicitudes de renovación de la clave.

La generación de un nuevo par de claves es un proceso importante para garantizar la seguridad y la integridad de las comunicaciones y transacciones electrónicas. Un par de claves es un conjunto de dos claves criptográficas, una clave pública y una clave privada, que se utilizan en la criptografía de clave pública para cifrar y descifrar datos y para proporcionar una firma electrónica segura y legalmente vinculante.

Para el PSC AUTHENTICSING la renovación del CE debe ser efectuada por el signatario con su clave de revocación desde el Sitio Web de la AR en la sede administrativa de Authenticsing.

En el caso de que el signatario no recuerde la clave de revocación debe presentarse con sus documentos para el tipo de CE, en la sede administrativa del PSC Authenticsing con los operadores AR.

12.3.2 Generación de Nuevo Certificado (Posterior a Revocación).

El PSC AUTHENTICSING no realiza la renovación del CE con la misma clave. Por tanto el signatario aunque no tenga su clave comprometida y deba de realizar la renovación del CE, este debe realizar el cambio de clave. Esta se da en la sede administrativa del PSC AUTHENTICSING con los operadores de la AR y AC. El diseño y esquema operacional del PSC AUTHENTICSING y su plataforma tecnológica de certificación, se encuentran conformadas y configuradas para que el cliente genere su par de claves (pública y privada). Continuamente y en el integro caso, la obligación y el compromiso de la clave procederá del mismo cliente, puesto que AUTHENTICSING no genera el par de claves (pública y privada).

La identidad y autenticidad para la renovación de un certificado luego de una revocación o revocación sin compromiso y no obligatorio de la clave será la igual para el registro principal e inicial. Seguidamente el signatario tendrá que demostrar satisfactoriamente al PSC AUTHENOLOHY que los motivos de la revocación anterior ya no están en disponibilidad o no se encuentran presentes.

12.4 Identificación y autenticación de las solicitudes de revocación de la clave.

En general la revocación es realizada por el signatario realizando la solicitud a AR por correo y previa solicitud de cita con su clave de revocación, en los casos que difiera se indica en la respectiva PC.

En el caso de que el signatario no recuerde la clave de revocación debe presentarse con sus documentos para el tipo de CE en:

- Sede Administrativa del PSC AUTHENTICSING con los operadores AR.

No se habilita por tanto ningún procedimiento para generar de forma telemática la renovación de los certificados siendo necesaria realizar la solicitud via correo electrónico y previa programación de cita por parte del AR de Authenticsing el caul se requerirá en todos los casos la presencia física del titular o signatario.

13. EL CICLO DE VIDA DE LOS CERTIFICADOS (REQUERIMIENTOS OPERATIVOS) (DPC y PC)

En este capítulo se recogen los requisitos operacionales para el ciclo de vida de los certificados generados y emitidos por el PSC AUTHENTICSING.

13.1 Solicitud de certificados.

Los requerimientos y procedimientos operacionales que establece la Autoridad de Certificación (AC) del PSC AUTHENTICSING para recibir los requerimientos y requisitos necesarios para generar y emitir un certificado.

La solicitud de certificado no está limitado para ningún tipo de ciudadano nacional o extranjero, jurídico o natural; siempre y cuando cumpla con los requerimientos, procedimientos y normas establecidos por el PSC AUTHENTICSING.

Los procedimientos que deben establecer para los requerimientos solo podrán ser iniciados por el suscriptor o por el representante autorizado de la persona jurídica solicitante.

El proceso de solicitud de Certificados Electrónicos lo pueden realizar de la siguiente manera:

Forma física, es decir, dirigiéndose directamente a las oficinas

administrativas de AUTHENTICSING ubicadas en la siguiente dirección:

- Calle Bolívar, Edificio Don David, PB – Ofic. 001, Municipio Chacao del estado Miranda de la República Bolivariana de Venezuela.
- +58 – 0212 – 2647658
- Solicitando toda la información referente a los certificados generados y emitidos por el PSC AUTHENTICSING.
- Tipos de Certificados:

❖ Certificado de firma electrónica para empleado de empresa privada
❖ Certificado de firma electrónica para representante de empresas pública
❖ Certificado de firma electrónica para funcionario público
❖ Certificado de firma electrónica para representante legal de empresa privada
❖ Certificado de firma electrónica para profesionales titulados
❖ Certificado electrónico de firma para persona natural
❖ Certificado de Servidor OCSP

O de forma electrónica en los siguientes medios:

1.) Portal web de AUTHENTICSING

2.) Correo electrónico a la siguiente dirección:

- Página web**:** www.authenology.com.ve

❖ Leer las condiciones y ofertas de los paquetes más acordes a su requerimiento.
❖ Escoger el o los certificados:
❖ Certificado de firma electrónica para empleado de empresa privada
❖ Certificado de firma electrónica para representante de empresas pública
❖ Certificado de firma electrónica para funcionario público
❖ Certificado de firma electrónica para representante legal de empresa privada
❖ Certificado de firma electrónica para profesionales titulados
❖ Certificado electrónico de firma para persona natural
❖ Certificado de Servidor OCSP
✓ Realizar la solicitud del tipo de certificado por el cual está realizando la tramitación.
✓ Enviar los requisitos solicitados para el tipo específico del certificado a tramitar.
✓ Aceptar los términos de contrato para la adquisición de certificados.
✓ Confirmar correo de solicitud y pautar cita.

- Correo Electrónico: contacto@authenology.com.ve

- Por medio del correo podrá realizar una solicitud y consulta de información con respecto a las ofertas de los paquetes económicos.
- La Autoridad de Registro (AR) responderá a la solicitud por medios electrónicos enviando la información solicitada.
- Realizar la solicitud del tipo de certificado por el cual está realizando la tramitación (,(Certificado de firma electrónica para empleado de empresa, Certificado de firma electrónica para representante de empresas Certificado de firma electrónica para funcionario público, Certificado de firma electrónica para representante legal de empresas, Certificado de firma electrónica para profesionales titulados, Certificado electrónico de firma para persona natural Certificado de firma electrónica para funcionario público.
- Enviar los requisitos solicitados para el tipo específico del certificado a tramitar.
- Aceptar los términos de contrato para la adquisición de certificados.
- Confirmar correo de solicitud y pautar cita.

Una vez revisado la solicitud del Certificado Electrónico por el cual está tramitando, se le pautara una cita con fecha y hora para que se dirija a las oficinas de AUTHENTICSING. Una vez aprobada la solicitud del Certificado Electrónico, se procederá a generar y emitir las claves y certificados correspondientes y el cliente pasa a ser un signatario de la cadena de confianza.

La acreditación del signatario, establece que opera en conformidad con las políticas y procedimientos establecido por el PSC AUTHENTICSING.

AUTHENTICSING se reserva el derecho a solicitar requisitos adicionales a los establecidos en el Manual de Operaciones, cuando lo considere necesario, para comprobar la identidad del solicitante de certificados electrónicos.

AUTHENTICSING se reserva el derecho de negar la emisión de un certificado electrónico a un solicitante, a su propia descripción, sin que ello implique responsabilidad alguna por este motivo.

13.1.2 Proceso de firma del certificado.

Para el PSC AUTHENTICSING, el proceso de firma del certificado

electrónico sigue el siguiente proceso de firma del certificado:

- **Identificación y autenticación:** El solicitante debe proporcionar información de identificación personal y/o institución, en algunos casos, y cuando Authenticsing lo considere se solicitara una prueba de identidad adicionales a los requerido para ser verificado y autenticado por la AR.

- **Solicitud de certificado:** Una vez que el solicitante ha sido identificado y autenticado, se procede a la solicitud del certificado electrónico. La solicitud puede realizarse a través de la plataforma en línea authenology o mediante procesos físicos en las oficinas administrativas del PSC AUTHENTICSING.

- **Verificación de la solicitud:** El AR verifica la solicitud y realiza las validaciones necesarias para asegurarse de que la solicitud sea válida.

- **Generación de la clave privada y pública:** El AR genera una clave privada y una clave pública para el solicitante. La clave privada es utilizada por el titular del certificado para firmar documentos electrónicos y la clave pública es utilizada por las partes que desean verificar la autenticidad de la firma digital del titular.

- **Firma del certificado:** El signatario firma digitalmente el certificado utilizando su propia clave privada para garantizar la autenticidad del certificado.

- **Entrega del certificado:** Una vez que el certificado ha sido firmado digitalmente, el AR y el AC harán entrega al titular del certificado, esto se hace desde las oficinas administrativas del PSC AUTHENTICSING donde se entrega en un dispositivo USB, el certificado Electrónico, el aplicativo para las firmas electrónicas y el manual de usuario del aplicativo.

13.1.3 Proceso de generación de la solicitud de renovación de las claves del certificado.

En el ámbito del PSC AUTHENTICSING, todas las renovaciones, con independencia de su causa, se realizarán con cambio de claves. Para el PSC AUTHENTICSING el proceso de renovación de las claves de

certificados sigue el siguiente proceso,

La solicitud de renovación de un Certificado Electrónico CE debe ser efectuado por el signatario, dentro de un lapso de 20 días antes del vencimiento del certificado correspondiente y seguir el mismo proceso como si cuando lo realizo por primera vez, o seguir los siguiente paso:

Forma física, es decir, dirigiéndose directamente a las oficinas administrativas de AUTHENTICSING: para la renovación del certificado electrónico, el signatario deberá dirigirse a la oficina administrativa de AUTHENTICSING y notificar su interés de renovar el certificado electrónico, el cual seguirá el mismo proceso como si estuviera realizando por primera vez el proceso. Para este caso la autoridad de registro AR le notificara o pautara una cita para realizar el proceso de generación de certificado electrónico.

- **De forma electrónica por medio del correo electrónico *contacto@authenology.com.ve*:** El signatario podrá enviar un correo con la intención e interés de renovar el certificado electrónico, el cual la autoridad de registro AR le notificara o pautara una cita para realizar el proceso de generación de certificado electrónico.

Proporcionar información de identificación: En el proceso de renovación, se requerirá que se proporcione nuevamente la información de identificación y demás requerimientos solicitados por el PSC AUTHENTICSING, dependiendo del tipo de certificado a renovar.

Verificar la información y envió de solicitud: Antes de enviar la solicitud de renovación, el signatario debe verificar que toda la información proporcionada sea correcta. Esto es importante para evitar errores y retrasos en el proceso de renovación. Una vez que se ha completado la solicitud de renovación y se ha verificado la información, se debe enviar la solicitud al proveedor de servicios de certificación.

Confirmación de cita: Después de enviar la solicitud de renovación, se debe esperar la confirmación de cita por parte del PSC AUTHENTICSING. En algunos casos, se puede requerir que se proporcione más información o se realice un proceso de verificación adicional antes de otorgar la renovación.

Generación del nuevo certificado: Si la renovación es aprobada, el PSC AUTHENTICSING proporcionará un nuevo certificado con las claves renovadas, cumpliendo con el proceso y protocolo de generación de par de claves.

13.1.4 Procedimiento para realizar una solicitud de renovación de un certificado.

El procedimiento para realizar una solicitud de renovación de un certificado, será el mismo procedimiento que se realiza cuando se procede por primera vez a realizar una solicitud de certificación electrónica.

13.1.5 Procedimiento para realizar una solicitud de suspensión de un certificado.

El procedimiento para realizar una solicitud de suspensión de un certificado puede variar dependiendo del contexto y circunstancia del mismo.

La suspensión es una invalidación temporal de un certificado.

Para la suspensión de un certificado puede ser a solicitud del signatario del certificado o la alta gerencia del PSC AUTHENTICSING y solo la puede efectuar el administrador de AUTHENTICSING.

La solicitud de suspensión del certificado electrónico, se pueden utilizar alguno de los siguientes medios:

Forma física, es decir, dirigiéndose directamente a las oficinas administrativas de AUTHENTICSING: para la suspensión del certificado electrónico, el signatario deberá dirigirse a la oficina administrativa de AUTHENTICSING y notificar su interés de suspender el certificado electrónico; para esto es necesario que presente la documentación requerida que lo identifique como signatario a los fines de su validación. . Para este caso la autoridad de registro AR convalidara la identificación presentada por el signatario.

- **De forma electrónica por medio del correo electrónico *contacto@authenology.com.ve*:** El signatario podrá enviar un correo con la intención e interés de suspender el certificado electrónico, el cual la

autoridad de registro AR le notificara o pautara una cita para realizar el proceso de suspensión del certificado electrónico.

13.2 Tramitación de solicitud de un certificado

Especifica las funciones de identificación y autenticación que realizan los funcionarios y personal encargado de las Autoridades de Registro del PSC de AUTHENTICSING.

Para el PSC de Authenticsing, esta hace énfasis en la comprobación de los datos del Signatario, identifica la entidad legal, esta función es efectuada por los operadores AR en la sede administrativa de la Authenticsing.

Estos funcionarios que desempeñan el rol de operador de registro, deben disponer de un dispositivo seguro de creación de firma (tarjeta de funcionario) para el control de acceso a la aplicación de expedición y control de integridad y no repudio de las operaciones y transacciones realizadas.

Para los Certificados de Firma Electrónica, el Solicitante (Jurídico o Natural) aportará los datos requeridos y acreditará su identidad personal o autorización según sea el caso. Los operadores de Authenticsing, a través de la Autoridad de Registro AR del PSC de AUTHENTICSING, constatarán la identidad del solicitante, la personalidad jurídica de la Entidad representada y la extensión y vigencia de las facultades de representación del Representante y conservará la documentación que la acredite. El PSC de AUTHENTICSING admitirá, en todo caso, la función e informe que realice la Autoridad de Registro AR.

13.2.2 Aprobación o denegación de un certificado

Se aprobará las solicitudes de certificación a aquellos solicitantes de carácter jurídico o natural, que cumplan con todos los requisitos y lineamientos técnicos, económicos y legales exigidos por el PSC AUTHENTICSING en la presente DPC-PC. El sistema garantiza que el certificado emitido este dentro de la cadena de confianza de la Infraestructura Nacional de Certificación Electrónica.

La confirmación o rechazo de una firma o certificado electrónico se encuentra estipulada por la Autoridad de Certificación (AC) del PSC AUTHENTICSING. Todo conjunto de solicitud de firma o certificado

electrónico que no sea homologada y aprobado por la Autoridad de Registro (AR) del PSC AUTHENTICSING, de forma automática y necesariamente será rechazada, incluyendo también en consecuencia denegada. La Autoridad de Certificación (AC), antes de dar el comienzo al desarrollo de aceptación de una firma o certificado electrónico se deberá validar el cumplimiento de lo estipulado y es lo siguiente:

- Aprobar el pago realizado por el Cliente.
- Verificar la información emitido por la Autoridad de Registro (AR)
- Hacer valido cual es el tipo de certificado requerido y gestionar o tramitar ante la Universal Register Authority (URA), por tanto es el módulo de posterioridad y generación de certificados.

Luego de estar comprobados y logrado con los pasos mencionados con anterioridad, la Autoridad de Certificación (AC) del PSC AUTHENTICSING se procederá a la firma o certificado electrónico y según sea el caso.

13.2.3 Plazo para la tramitación de un certificado

EL PSC AUTHENTICSING, previa verificación de los documentos de solicitud para la tramitación de un certificado electrónico, tendrá un plazo de veinte (20) días hábiles siguientes a la fecha de presentación de la solicitud en conjunto con todos los requisitos.

13.3 Emisión de certificados

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

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

La Autoridad de Certificación (AC) firma el certificado y lo envía al software de certificación usando igualmente la comunicación del https.

Posteriormente después de emitir el certificado el suscriptor tendrá que proceder a descargar e instalar.

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

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

13.4 Aceptación de certificados

Los certificados Electrónicos generados y emitido por el PSC AUTENTICSING se consideran aceptados por el signatario al momento de hacer entrega por parte de la AC de Authenticsing del certificado electrónico junto con el Aplicativo para firmas electrónicas y el manual de usuario y luego de su publicación en el repositorio de Infraestructura del PSC AUTENTICSING.

13.4.2 Publicación del certificado

El PSC AUTHENTICSING mantiene disponible, con acceso público, el repositorio de publicación de los Certificados Electrónicos el cual podrán ser consultados en la lista de certificados electrónicos y la LCR en el portal web de Authenology (www. Authenology.com.ve)

13.4.3 Notificación de la emisión del certificado a otras autoridades

Está sujeto a lo dispuesto por la normativa Legal y Sub-legal emitida por SUSCERTE y los acuerdos suscritos entre el PSC AUTHENTICSING y sus usuarios.

13.5 Uso de par de claves y del certificado

El PSC AUTHENTICSING no genera ni almacena las Claves Privadas asociadas a los Certificados expedidos bajo la presente Política de Certificación. Corresponde la condición de custodio, signatario y responsable sobre el control de las claves privadas del Certificado electrónico, al signatario del Certificado Electrónico.

El titular sólo puede utilizar la clave privada y el certificado para lo cual fue adquirido los usos autorizados y estipulado en la presente DPC.

13.5.2 Uso de la clave pública y del certificado por los terceros de buena fe

Los terceros de buena fe sólo pueden depositar su confianza en los certificados electrónicos para aquello que establece esta DPC. Los terceros de buena fe pueden realizar operaciones de clave pública de manera satisfactoria confiando en el certificado emitido por la cadena de confianza. Así mismo, deben asumir la responsabilidad de verificar el estado del certificado utilizando los medios que se establecen en esta DPC.

13.6 Renovación del certificado

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

Bajo las presentes Políticas de Certificación, el PSC AUTHENTICSIG no renueva Certificados electrónicos, esto quiere decir, que todas las renovaciones de certificados realizadas en el ámbito de esta DPC-PC se realizarán con cambio de claves. Por tal motivo, el procedimiento es el mismo cuando se realiza por primera vez el proceso de un certificado nuevo, el cual se describe en el apartado 13.1.

13.6.2 Entidad que puede solicitar la renovación de un certificado

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

13.6.3 Procedimiento de solicitud para la renovación de un certificado

Los signatarios deben cumplir nuevamente con el proceso de solicitud de Certificado Electrónicos para solicitar la renovación de un certificado electrónico. Por tal motivo, el procedimiento es el mismo cuando se realiza por primera vez el proceso de un certificado nuevo, el cual se describe en el apartado 13.1.

13.6.4 Notificación de la emisión de un nuevo certificado

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

Authenticsing notificara por medio de un correo electrónico al signatario la pronta caducidad del certificado electrónico y que requerirá realizar el mismo procedimiento cuando realizo por primera vez el proceso de un certificado nuevo, el cual se describe en el apartado 13.1.

13.6.5 Publicación del certificado renovado por el PSC

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

13.6.6 Notificación de la emisión del certificado a otras entidades

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

13.7 Nueva clave del certificado

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

13.8 Modificación de certificados

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

13.9 Revocación y suspensión de un certificado

Existen varias circunstancias en las que puede ser necesario revocar un certificado electrónico para garantizar la seguridad y la integridad de la información protegida por el certificado. Algunas de las circunstancias comunes en que los Certificados Electrónica expedidos por la PSC AUTHENTICSING quedarán sin efecto en los siguientes casos:

- **Compromiso del certificado:** Si se sospecha que el certificado ha sido comprometido o se ha visto comprometido de alguna manera, es importante revocar el certificado para evitar su uso fraudulento y proteger la información protegida por el certificado.
- **Cambio de circunstancias:** Si las circunstancias que rodearon la

emisión del certificado han cambiado de alguna manera, como la terminación de la relación laboral con la organización para la cual se emitió el certificado, puede ser necesario revocar el certificado para garantizar que la información protegida por el certificado no se utilice de manera inapropiada.

- **Pérdida o robo del dispositivo de seguridad:** Si el dispositivo de seguridad que almacena el certificado se ha perdido o ha sido robado, es importante revocar el certificado para evitar su uso fraudulento y proteger la información protegida por el certificado.
- **Caducidad del certificado:** Si el certificado ha caducado, es importante revocarlo para evitar su uso fraudulento después de su fecha de vencimiento.
- **Clave privada comprometida:** Si el signatario considera que su clave privada esta comprometida, es importante revocar el certificado para evitar su uso fraudulento y proteger la información protegida por el certificado.
- **Error en los datos del certificado:** Si se ha detectado un error en los datos del certificado, como información incorrecta del titular o la organización, puede ser necesario revocar el certificado para garantizar que la información protegida por el certificado sea precisa y confiable.
- **Incapacidad sobrevenida o fallecimiento del signatario:** En caso de que el signatario de un documento electrónico fallezca o se vuelva incapaz de firmar por cualquier razón.

13.9.2 Entidad que puede solicitar la Revocación

Al verse comprometida la clave del Certificado Electrónico, se rompe la cadena de confianza, en esos casos, las entidades autorizadas para solicitar la revocación del certificado electrónico son:

- La autoridad competente a la conformidad con la LSMDFE
- Un encargado del PSC AUTHENTICSING a quién expresadamente tenga lugar como autoridad para ejecutar la solicitud de suspensión o revocación.
- La decisión de un tribunal por medio el cual se proclame aplicablemente una decisión preventiva o ejecutoria solicitando la suspensión o revocación de una firma electrónica o certificado electrónico emitido por AUTHENTICSING.

13.9.3 Procedimientos de Solicitud de la Revocación

Para el procedimiento de solicitud en la que es necesario revocar un certificado electrónico para garantizar la seguridad y la integridad de la

información protegida por el certificado. Se deben de seguir los siguientes casos:

- **Proporcionar información de identificación:** Es necesario proporcionar información de identificación adecuada para identificar al titular del certificado y demostrar que se tiene la autoridad para solicitar la revocación del certificado. Esto puede incluir el nombre completo del titular del certificado, la organización a la que pertenece (si corresponde), la dirección de correo electrónico y la información de contacto del solicitante.
- **Proporcionar una justificación para la revocación:** Es importante proporcionar una justificación para la solicitud de revocación del certificado, como la sospecha de compromiso del certificado, la pérdida o el robo del dispositivo de seguridad que almacena el certificado, o un cambio en las circunstancias que rodean la emisión del certificado.
- **Proporcionar documentación de soporte:** Es posible que se requiera documentación de soporte para demostrar la justificación de la solicitud de revocación. Esto puede incluir copias de una denuncia de robo o pérdida, una declaración jurada, o cualquier otra documentación relevante.
- **Realizar la solicitud de revocación:** Para el caso del PSC AUTHENTICSING Se deben de seguir los siguientes pasos:

- SIGNATARIO:
- Debe realizar la solicitud de petición de revocación de su certificado electrónico por medio del envío de un correo electrónico al PSC AUTHENTICSING (**contacto@authenology.com.ve**)
- Agregar los siguientes datos en el envío de la solicitud: Ingresar cualquiera de los siguientes datos: Serial del Certificado, Nombre del Signatario y/o correo electrónico del signatario.
- Para el caso de No Recordar su clave de revocación, debe comunicarse telefónicamente con un operador de la AR del PSC AUTHENTICSING (+58 – 0212 – 2647658).
- El operador AR efectúa preguntas de seguridad al signatario para obtener la información necesaria del CE; procede a revocar y le indica al signatario que debe pasar a las oficinas administrativas del PSC AUTHENTICSING para continuar con el proceso.
- La alta gerencia determina la suspensión de certificado electrónico.
- El operador AR o el AC aprueba la solicitud de revocación del certificado electrónico.
- El Operador AC aprueba la petición, firma y publica el Certificado Electrónico

e la LCR.

- AUTHENTICSING:
- El PSC AUTHENTICSING o cualquiera de las entidades que la componen pueden solicitar la revocación de un Certificado Electrónico si tuviera conocimiento o sospecha del compromiso de la clave privada del signatario o cualquier otro hecho determinante que requiera proceder a revocar el Certificado Electrónico.
- En este caso, el operador AR vía telefónica, le notifica al signatario que le será enviado un correo electrónico que describe las circunstancias de la revocación de su Certificado Electrónico.
- Adicionalmente se documenta la actividad realizada para tal fin.
- Una vez revocado el Certificado Electrónico la AC de Authenticsing, pública la LCR con el fin de notificar a terceros de buena fe, que el Certificado Electrónico ha sido revocado, en el momento en que se solicite la verificación del mismo. Este servicio está disponible 24 horas / 7 días a la semana.

13.9.4 Límites del período de la Solicitud de Revocación

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

13.9.5 Circunstancias para la Suspensión

La suspensión de un certificado electrónico puede ser necesaria en ciertas circunstancias para garantizar la seguridad y la integridad de la información protegida por el certificado. Algunas de las circunstancias comunes para la suspensión de un certificado electrónico son:

- **Compromiso del certificado:** Si se sospecha que el certificado ha sido comprometido o se ha visto comprometido de alguna manera, es importante revocar el certificado para evitar su uso fraudulento y proteger la información protegida por el certificado.
- **Cambio de circunstancias:** Si las circunstancias que rodearon la emisión del certificado han cambiado de alguna manera, como la terminación de la relación laboral con la organización para la cual se emitió el certificado, puede ser necesario revocar el certificado para garantizar que la información protegida por el certificado no se utilice de manera inapropiada.

- **Pérdida o robo del dispositivo de seguridad:** Si el dispositivo de seguridad que almacena el certificado se ha perdido o ha sido robado, es importante revocar el certificado para evitar su uso fraudulento y proteger la información protegida por el certificado.
- **Caducidad del certificado:** Si el certificado ha caducado, es importante revocarlo para evitar su uso fraudulento después de su fecha de vencimiento.
- **Clave privada comprometida:** Si el signatario considera que su clave privada está comprometida, es importante revocar el certificado para evitar su uso fraudulento y proteger la información protegida por el certificado.
- **Error en los datos del certificado:** Si se ha detectado un error en los datos del certificado, como información incorrecta del titular o la organización, puede ser necesario revocar el certificado para garantizar que la información protegida por el certificado sea precisa y confiable.
- **Incapacidad sobrevenida del signatario:** En caso de que el signatario de un documento electrónico se encuentra incapacitado temporalmente y le sea incapaz de firmar por cualquier razón.

13.9.6 Entidad que puede solicitar la Suspensión

La suspensión de un Certificado Electrónico emitido por el PSC AUTHENTICSING, podrá ser solicitada por el signatario, o por la Alta dirección de Authenticsing o por los operadores de la AR y/o AC si tuviera conocimiento o sospecha del compromiso de la clave privada del signatario o la circunstancia que se indica en el apartado 13.9.5 así como cualquier otro hecho determinante que requiera proceder a revocar el CE según lo especificado en su correspondiente PC.

13.9.7 Procedimientos para la Solicitud de Suspensión

La suspensión es la pérdida de fiabilidad temporal del certificado impidiendo el uso por parte del signatario.

Cuando el signatario requiere la suspensión del Certificado Electrónico deberá solicitarlo vía telefónica (+58 – 0212 – 2647658), en el horario comprendido de 8:30 AM a 12:00 pm y de 1:00 PM a 4:30 pm; con la salvedad que el estado del certificado permanecerá suspendido, no permitiendo el uso del mismo para ningún fin durante veinte (20) días continuos, en este periodo el signatario debe presentarse en la sede administrativa de Authenticsing y entregar al operador AR u operador AV un formato predefinido para revocar el certificado o continuar activo el

Certificado Electrónico.

13.9.8 Límites del Período de Suspensión de un Certificado

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

13.9.9 Frecuencia de Emisión de Listas de Certificados Revocados

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

13.9.10 Requisitos para la comprobación de la Lista de Certificados Revocados

La publicación de las Listas de Revocación se realiza en el momento de generación de dichas Listas, por lo que el periodo de latencia o comprobación entre la generación de la LCR y su publicación es prácticamente nulo.

13.9.11 Disponibilidad de comprobación en Línea del Servicio de Revocación del Estado del Certificado

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

13.9.12 Requisitos de comprobación en Línea del Estado de Revocación

La comprobación en línea del estado de revocación de los Certificados AC subordinadas o de entidad final puede realizarse mediante el Servicio de información del estado de los certificados, ofrecido a través de OCSP.

13.9.13 Otras Formas Disponibles para la Divulgación de la Revocación

No definidas.

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

No definidas.

13.9.15 Requisitos Específicos para Casos de Compromiso de Claves

El PSC AUTHENTICSING utilizará medios de comunicación razonables para informar a los Suscriptores que su clave privada puede haber sido comprometida. Siempre que se confirme un compromiso de la clave, el PSC AUTHENTICSING revocará los Certificados afectados conforme a lo descrito en el apartado 13.9.1

13.10 Servicio de comprobación de estado de certificados

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

13.10.2 Disponibilidad del servicio

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

13.10.3 Características adicionales

No definidas.

13.11 FINALIZACIÓN DE LA SUSCRIPCIÓN

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

- Revocación del Certificado Electrónico por cualquiera de las causas mencionadas en el apartado 13.9.1 *CIRCUNSTANCIAS PARA LA REVOCACIÓN DE UN CERTIFICADO"*,
- Caducidad de la vigencia del Certificado Electrónico CE.

13.12 Custodia y recuperación de la clave

13.12.1 Prácticas y políticas de recuperación de la clave

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

EL PSC AUTHENTICSING mantienen las copias de backup de la clave privada de la AC Authenticsing, almacenadas y cifradas en dispositivo criptográfico, que a su vez maneja diversos mecanismos de seguridad adicionales.

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

14. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES (DPC)

14.1 Controles de seguridad física

14.1.1 Controles de la garantía y seguridad física y construcción del PSC.

Para el PSC AUTHENTICSING, como un proveedor de servicios de confianza, mantienen todos los sistemas que son críticos en una o más zona segura, tanto física como funcional y lógicamente.

La Autoridad de Certificación (AC) del PSC AUTHENTICSING conserva un diseño o esquema operacional orientado a garantizar la continuidad operacional y prestación de sus servicios con los altos estándares de calidad, oportunidad y seguridad.

El centro de datos se dispone en la sede operacional de la Autoridad de Certificación (AC) AUTHENTICSING y por consiguiente en donde opera la plataforma de emisión de certificados.

El centro de datos junta y mantiene cada uno de los requisitos de operación para este tipo de facilidades aplica para la normativa internacional en materia de seguridad asociada a la tecnología de información, la legislación de la república bolivariana de Venezuela y las normativas impuesta por SUSCERTE.

El equipo de operaciones del PSC AUTHENTICSING es el representante, en conjunto con el Gerente general y el asesor de tecnología de Informática de gestionar, tramitar y mantener la operación de la plataforma tecnológica de generación de certificados instalada en el Centro de Datos Daycohost, Calle Londres, entre Caroní y Nueva York, Torre Dayco, Las Mercedes, Caracas, Venezuela.

El centro de datos está disponible las veinticuatro (24) horas del día, los trescientos sesenta y cinco (365) días del año y mantiene una independencia operacional superior a los dos (2) meses. Además el centro de datos reúne cada una de las restricciones, condiciones y características de construcción anti sísmica y de la seguridad de prevención para incendio e inundaciones, mantiene un perímetro de seguridad y cuenta con siete (7) niveles de seguridad de acceso.

El centro de datos, en el lugar donde opera la Autoridad de Certificación (AC), mantiene las pólizas o instrumentos emitidos por empresas de seguros solventes y destacables, a los efectos de mantener un respaldo en casos de alguna ocurrencia y contingencia que pueda afectar la integridad física de la referida sede administrativa y pueda ofrecer de esa manera una garantía de su continuidad operacional.

La Autoridad de Certificación (AC) AUTHENTICSING conserva contrato de operación de centro alterno en caso de algún daño que perjudique permanente y que imposibilite y restrinja la operación regular del centro de datos.

14.1.2 Acceso físico.

AUTHENTICSING garantiza que cumple con las normativas aplicable en todos los aspectos de la seguridad física el cual se describe a lo largo del presente capitulo.

Se han establecido diferentes perímetros de seguridad, donde son ejecutadas las actividades críticas o sensibles, con barreras de seguridad y con controles de entrada, dotándose de mecanismo de control de seguridad para reducir el riesgo de acceso no autorizado o de daños a los recursos informáticos.

La Autoridad de Certificación (AC) del PSC AUTHENTICSING dentro de

su soporte tecnológica de certificación electrónica, mantiene las medidas del control de acceso, tanto lógicas (software de certificación) como físicas (equipos) asegurando la integridad de los servicios prestados.

En AUTHENTICSING se han establecido medidas físicas de control de accesos oportunas, sin olvidar que el recinto donde se encuentra alojada la AC de AUTHENTICSING, el cual se encuentra en la sede de DAYCOHOST dispone de un avanzado sistema perimetral de seguridad física compuesto por diversos anillos con los adecuados medios técnicos y humanos, contando con la protección y vigilancia de las fuerzas y cuerpos de seguridad privada y del Estado, así como de seguridad especializada.

Además de los diversos controles de acceso se dispone de diversos medios de control interior en las salas e instalaciones como son los controles de accesos basados en lectores de tarjetas, cámaras de video vigilancia, detectores de intrusismo, detectores de incendios, etc., además de los medios humanos dedicados a su atención tanto en el exterior como en el interior del recinto.

El acceso físico para el interior del rack (apertura) debe estar permitido solo al personal del PSC AUTHENTICSING. Con las siguientes Características del centro de datos:

- Se dispone de un exhaustivo sistema de controles físicos de personas a la entrada y salida que conforman diversos anillos de seguridad.
- Todas las operaciones críticas del Prestador de Servicios de Confianza se realizan dentro de un recinto físicamente seguro con diversos niveles de seguridad para acceder a las máquinas y aplicaciones críticas.
- Los sistemas AUTHENTICSING están físicamente separados de otros sistemas, de forma que exclusivamente el personal autorizado del PSC AUTHENTICSING pueda acceder a ellos, y se garantice la independencia de otras redes de propósito general.
- La cerca perimetral fija y determina el ingreso físico a la sede del centro de datos.
- La inspección y vigilancia con el personal de seguridad y cámaras digitales en servicio 7X24X365 días. En este nivel de seguridad se señalan y registran los equipos portátiles de computación.
- .El control de ingreso al corredor o pasillo del acceso al área de servidores se establece en un triple mecanismo de aseguramiento de acceso al área pública del centro de datos y al área de servidores. En este control se válida cada identidad de las personas autorizadas por AUTHENTICSING para poder

ingresar al área de servidores.

- El control de ingreso a la entrada del área interna del centro de datos se establece en un mecanismo de doble aseguramiento de acceso del personal autorizado.
- El dispositivo biométrico sensible al calor y autenticidad tiene como motivo bloquear el acceso al área de servidores para el personal no autorizado y acompañado por personal técnico y de operaciones.
- El carnet de magnético de seguridad para puerta de acceso al área interna de control del área de servidores valida, en efecto sólo el equipo autorizado y poseedor de la tarjeta cuente con acceso al área de control de servidores.
- El control de acceso al cuarto de servidores es ejecutado por los operadores de área de control externa del área de los servidores. Los operadores verifican y validan la identidad de la persona que ingresará al área de servidores, posteriormente registran sus datos y la hora de ingreso y egreso.
- La llave del acceso al rack de servidores de AUTHENTICSING está en posesión del personal de AUTHENTICSING para garantizar la seguridad y custodia de cada uno de los servidores y de la Autoridad de Certificación (AC).
- El dispositivo o mecanismo de seguridad del acceso a la puerta rack de los servidores de AUTHENTICSING se establece en un sistema de seguridad autorizado que sólo los operadores de AUTHENTICSING podrán acceder a los servidores de la plataforma de certificación.

14.1.3 Suministro de electricidad y acondicionador de aire.

El rack donde se encuentra instalados los servidores de la plataforma de certificación de la Autoridad de Certificación (AC) AUTHENTICSING cuenta con dos (2) líneas de tensión diferentes, una general o principal y otra auxiliar, las líneas de tensión están unidas a dos (2) sistemas de alimentación ininterrumpida (UPS “Uninterruptable Power Supply”), por lo tanto a su vez están unidas a dos (2) plantas productoras y generadoras de energía eléctrica.

La distribución garantiza y asegura el suministro de energía eléctrica, incluyendo la de aire acondicionado seguidamente. Posteriormente se mostrará un gráfico referencial de la conexión del suministro de electricidad:

Imagen #2

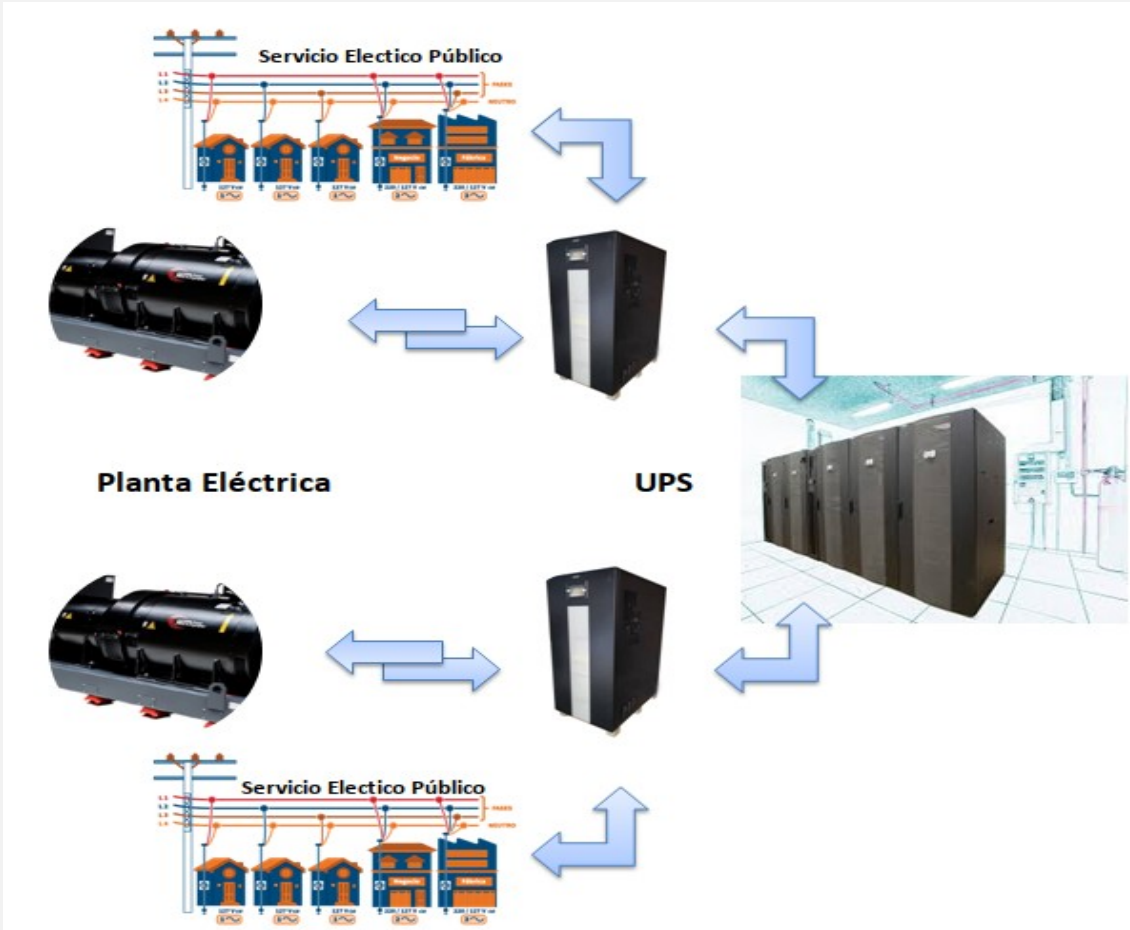


Diagrama del sistema de alimentación eléctrica.

El centro de datos reúne y mantiene cada uno de los requisitos de operación, para este tipo de compresibilidad informa la normativa internacional en tema de seguridad asociada a la tecnología de información, la ley de la república bolivariana de Venezuela y las normas impuesta por SUSCERTE.

14.1.5 Protección y prevención de incendios

El centro de datos reúne y mantiene cada uno de los requisitos de operación, para este tipo de compresibilidad informa la normativa internacional en tema de seguridad asociada a la tecnología de información, la ley de la república bolivariana de Venezuela y las normas

impuesta por SUSCERTE.

14.1.6 Sistemas y técnicas de almacenamiento.

El centro de datos reúne y mantiene cada uno de los requisitos de operación, para este tipo de compresibilidad informa la normativa internacional en tema de seguridad asociada a la tecnología de información, la ley de la república bolivariana de Venezuela y las normas impuesta por SUSCERTE.

14.1.7 Sistemas de almacenamiento

El centro de datos reúne y mantiene cada uno de los requisitos de operación, para este tipo de compresibilidad informa la normativa internacional en tema de seguridad asociada a la tecnología de información, la ley de la república bolivariana de Venezuela y las normas impuesta por SUSCERTE.

14.1.8 Eliminación de residuos

El centro de datos reúne y mantiene cada uno de los requisitos de operación, para este tipo de compresibilidad informa la normativa internacional en tema de seguridad asociada a la tecnología de información, la ley de la república bolivariana de Venezuela y las normas impuesta por SUSCERTE.

14.1.9 Almacenamiento de copias de seguridad

El centro de datos reúne y mantiene cada uno de los requisitos de operación, para este tipo de compresibilidad informa la normativa internacional en tema de seguridad asociada a la tecnología de información, la ley de la república bolivariana de Venezuela y las normas impuesta por SUSCERTE.

15. CONTROLES DE PROCEDIMIENTOS

15.1 Definición de roles confiables

La Autoridad de Certificación (AC) y Autoridad de Registro (AR) mantendrán y guardarán un esquema o diseño de administración y operación apoyado en una estructura plana, respaldada y reforzada sobre la interrelación e interdependencia del equipo en sus diversos roles y funciones. La operación regular del PSC AUTHENTICSING será dividida en funciones del procedimiento y administración.

La alta dirección se establece en el nivel con mayor poder de decisión y mando dentro de la organización. Las actividades de operación y administración serán coordinadas por el Gerente general y el asesor de tecnología del PSC AUTHENTICSING, lo cual comunicaran directamente a la alta dirección.

El control, monitoreo y seguimiento continuo de la administración de la plataforma tecnológica de certificación será realizada por cada uno de los operadores de informática. El equipo de operadores de informática contará con un encargado de operadores, y será designado por el Gerente general y el consultor de tecnología y necesitará contar con la confirmación y seguidamente con la aprobación de la alta dirección.

El equipo de operadores de informática estará incorporado por un total de hasta cuatro (4) operadores, por lo cual estarán en capacidades de atender y solucionar cada uno de los requerimientos operacionales de la plataforma tecnológica de certificación.

La gestión regular de la Autoridad de Registro (AR) será asignada a un encargado o administrador de acreditación de información de identidad y datos. La administración regular del Gerente general estará apoyado por un asistente administrativo, quien ejecutará las gestiones de oficinistas y recepcionista, trasferirá pagos y coordinará cada una de las relaciones con los servicios de subcontratación y mantendrá cada uno de los inventario del material administrativo y logístico requerido por el personal del PSC AUTHENTICSING.

La estructura interna y emitida por AUTHENTICSING se encuentra apartado de la siguiente manera:

Gerente General (1)

- Unidad de Asesoría Legal
- Departamento Técnico - Legal
- Abogado Junior
- Abogado Semi Senior
- Abogado Senior

Auditor (2)

- Organización y Método

Coordinación de Administración (1)

- Unidad de Talento Humano
- Unidad de Comercialización

Coordinador de la Infraestructura de la clave Pública (1)

- Operadores AC (1)
- Operadores RC (1)

Coordinador de Seguridad de la Información y Plataforma (1)

- Analista de Seguridad de la Información
- Analista de Diseño y Desarrollo de Soluciones

Coordinación de Plataforma y Soporte a Usuarios (1)

- Analista de Administración de la Plataforma
- Analista de Soporte Técnico

15.1.2 Identidad y autenticación de cada rol.

La identidad y autenticación de cada rol, así como el establecimiento de nuevas responsabilidades corresponderá a la Alta Dirección del PSC AUTHENTICSING.

16. CONTROLES DE SEGURIDAD PERSONAL

16.1 Petición de antecedentes, calificación, experiencia y acreditación.

El personal del PSC que está involucrado en la operación de la Infraestructura de clave pública (ICP) está sujeto a la investigación y verificación de antecedentes. Las referencias son rigurosamente investigadas en el caso del personal operacional. Toda la operación de la Infraestructura de Clave Pública (ICP) del PSC AUTHENTICSING está bajo la responsabilidad directa de la alta dirección.

El personal involucrado en el control y la operación de la Infraestructura de Clave Pública (ICP) estarán suficientemente entrenados para cumplir con cada una de las funciones asignadas a su rol y recibirá entrenamiento continuo para garantizar y asegurar los niveles sobre las políticas de seguridad y los procedimientos. El proceso llevado a cabo de adiestramiento y desarrollo del personal se regulará por el documento de la política de adiestramiento y desarrollo

del personal de AUTHENTICSING.

16.2 Requerimientos de formación para los miembros del personal.

Ningún miembro del personal del PSC AUTHENTICSING puede tener acceso físico u operar cualquier componente de la Infraestructura de Clave Pública (ICP) sin preparación previa y sin contar con la presencia de otros miembros designados del personal que tengan las destrezas que son requeridas para confirmar que no se lleven a cabo acciones inapropiadas o sin ninguna autorización o sin contar con la debida preparación y formación. Los procedimientos son definidos y documentados para todas las operaciones relacionadas con la Infraestructura de Clave Pública (ICP). Los procedimientos operacionales son revisados regularmente al surgir nuevos requerimientos operacionales.

16.3 Sanciones por acciones no autorizadas.

17. PROCEDIMIENTOS DE CONTROL DE SEGURIDAD

17.1 Tipos de eventos registrados

EL PSC AUTHENTICSING, almacena cada registros electrónicos de eventos (logs) referente a su actividad como PSC. Estos registros son almacenados de forma automática y electrónica y en los casos del acceso físico en formato papel y otros medios.

Cada registro de eventos incluye datos referentes a la fecha y hora en que se produjo, número de serie, descripción del evento y el sistema o persona que lo origino. Los records mínimos de auditoría que deben tener mantenimiento, aplican:

- Eventos de cada equipo que conforman la plataforma:
  - Instalación y configuración del sistema operativo.
  - Instalación y configuración del módulo criptográfico.
  - Accesos o intentos de acceso al equipo.
  - Actualizaciones.
  - Realización de copias de seguridad
  - Instalación y configuración de cualquier aplicación instalada en el equipo.
  - Instalación y configuración de la Autoridad de Certificación(AC)

- Eventos del software de certificación:

- ❖ Gestión de roles.
- ❖ Gestión de plantillas de certificados.
- ❖ Lista del control de acceso (LCA).
- ❖ Gestión de certificados (todo lo considerado en el periodo de dicho certificado)
- ❖ Gestión de usuarios.
- ❖ Eventos con relación al acceso físico:
- ❖ Acceso del personal a los equipos y sistemas.
- ❖ Acceso del personal al centro de datos.
- ❖ Eventos de acciones correctivas:
- ❖ Errores de hardware.
- ❖ Errores de software.

17.2 Regularidad de procesados de registros de logs.

Los registros de auditoría se ejecutan en cualquier momento que se realice una operación en la raíz de certificación de la Autoridad de Certificación (AC) del PSC AUTHENTICSING, de lo contrario la raíz de certificación de la Autoridad de Certificación (AC) se mantiene fuera de línea. El equipo de operaciones comunica a su administrador de seguridad cuando un proceso o acción causa un incidente crítico de seguridad o discrepancia. A las entidades Infraestructura de Clave Pública (ICP) subordinadas (cuando aplique) también se les requiere comunicar cualquier tipo evento que pueda causar un incidente crítico de seguridad o discrepancia. En todo caso, la gerencia principal y el consultor de tecnología decidirán los pasos que se deban seguir.

17.3 Período de retención para los logs de auditoría.

Cada registro de Auditoría se retiene por un período de diez (10) años.

17.4 Protección de los logs de auditoría.

El sistema de recolección de auditoría del PSC AUTHENTICSING es una combinación de procesos automáticos y técnicas manuales ejecutados por la raíz de Certificación de la Autoridad de Certificación (AC) de AUTHENTICSING, los sistemas operativos y por el personal operacional. Por consiguiente, el sistema es mantenido mediante unos mecanismos de control de acceso y separación de roles con relación al software y el hardware que manejan la recolección automática y mediante procedimientos operacionales confidencialmente y reservadamente documentados, conocidos y seguidos por el equipo de la Autoridad de Certificación (AC) del PSC AUTHENTICSING. De la misma manera, la integridad y

responsabilidad de los eventos de auditoría son protegidos mediante la firma de cada evento con la clave privada de la persona que realiza dicha acción.

18. ARCHIVO DE INFORMACIONES Y REGISTROS

Los records de la Infraestructura de Clave Pública (ICP) de la Autoridad de Certificación (AC) del PSC AUTHENTICSING relacionados a la operación de sus funciones y servicios de certificación son archivados y retenidos por un tiempo exacto o mínimo de veinte (20) años.

Los recursos de etapa para la raíz de certificación de la Autoridad de Certificación (AC) del PSC AUTHENTICSING es verificado y confirmado diariamente de manera independiente y todos los records automatizados de la raíz de certificación de AUTHENTICSING, están asociados a la hora y fecha de su ocurrencia. Los archivos de records se mantienen bajo preciso control de acceso y están sujetos a la inspección y comprobación de auditores.

Cada uno de los archivos de records e información de identificación deberán ser archivados directamente por la Autoridad de Registro (AR) del PSC AUTHENTICSING y requerirá a la

Autoridad de Registro (AR) que archive los records e información por un período de diez (10) años a partir de la fecha de vencimiento del certificado y hará sus mejores esfuerzos para que dicha cadena cumplan con sus obligaciones en esta tema. Los records pueden ser archivados en papel o en forma electrónica.

18.1 Tipo de informaciones y eventos registrados

El tipo de información y registro de eventos será el mismo contemplado en el punto “Tipos de eventos registrado” del actual documento de Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC).

18.2 Período de retención para el archivo.

El período de retención para archivo será el mismo contemplado en el punto “Protección de los logs de auditoría”, del actual documento de Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC).

18.3 Protección del archivo.

Para cada uno de los método de protección de archivo será el mismo

contemplado en el aparte “Protección de los logs de auditoría”, del actual documento de Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC).

18.4 El Requerimiento para el estampado de tiempo para el registro.

Cada uno de los procesos y pasos llevados a cabo, necesitarán ser cumplidos por el PSC AUTHENTICSING para prestar el servicio de estampado de tiempo no se encuentran reglamentados o desarrollados por SUSCERTE. Sistema de repositorio de archivos de auditoría (interno vs uno de los equipos presentes en la plataforma de certificación posee un módulo para almacenar los log de eventos, específicamente eventos de las aplicaciones, de los sistemas y de seguridad, incluyendo el aplicativo de certificación.

18.5 Sistema de repositorio de archivos de auditoría (interno vs externo).

Los equipos presentes en la plataforma de certificación poseen un módulo para almacenar los log de eventos, específicamente eventos de las aplicaciones, de los sistemas y de seguridad, incluyendo el aplicativo de certificación.

Para este registro de eventos permite auditar y verificar los intentos de accesos, los accesos y las operaciones perjudiciales, sean estas intencionales o no. El registro de eventos también es almacenado en un respaldo en nube.

19. CAMBIO DE CLAVE

El esquema de operación del PSC AUTHENTICSING y su plataforma tecnológica de certificación se encuentran completamente configurados para que el cliente produzca su par de claves (pública y privada). Siempre y en todo caso el compromiso de clave derivará del mismo cliente, AUTHENTICSING no producirá el par de claves (pública y privada).

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

20. PLAN DE RECUPERACIÓN EN CASO DE DESASTRES

20.1 El procedimiento y desarrollo de gestión de incidentes y vulnerabilidades.

AUTHENTICSING ha decretado un plan de continuidad de negocio y recuperación ante desastres (PRD), ante el acontecimiento de un eventual compromiso parcial o total de la Infraestructura de Clave Pública (ICP) de la Autoridad de Certificación (AC) AUTHENTICSING. El plan de recuperación y restablecimiento ante desastre o accidentes es revisado periódicamente a la luz de los cambios riesgos en el ambiente. El plan de recuperación ante desastre o accidentes está orientado a:

20.2 Alteración de los recursos, hardware, software y/o datos.

El PSC AUTHENTICSING ha decretado un plan de continuidad de negocio y recuperación ante desastres, ante el acontecimiento de un eventual compromiso parcial o total de la Infraestructura de Clave Pública (ICP). El plan para la recuperación ante desastre es revisado periódicamente a la luz de los cambios riesgos en el ambiente.

- Desastres naturales y terminación.
- Fallas/corrupción de recursos de computación;
- Compromiso de la Integridad de la Clave (Pública y Privada).

La alta dirección, representada por un director, el Gerente general, el consultor de tecnología y los equipos de operadores de informática, deben tomar en consideración los correctivos y emprender con cada una de las actividades requeridas y necesarias para restaurar y mejorar la plataforma tecnológica de certificación en el momento de presentarse un incidente o evento de desastre. En el plan de continuidad de negocio y recuperación ante desastre o accidentes, se especificará cada procedimiento y ejecución a realizar en cada uno de los escenarios considerados como desastre y a continuación se mencionan los principales compromisos de cada uno de los cargos a la hora de ejecutarse el plan de recuperación:

- Un director junto al gerente general declaran el escenario de desastre y aprueban la activación del plan de contingencia.
- El consultor de tecnología gestiona, supervisa y apoya la ejecución de todas las actividades de recuperación del desastre
- Los operadores ejecutan las actividades de restauración del servicio.

20.3 Procedimiento de actuación ante la vulnerabilidad de la clave privada de una autoridad.

AUTHENTICSING, tiene como previsto activar el HSM (para

la firma de los certificados) de forma local y solo en presencia del consultor de tecnología y el Gerente general, considerado como uno de sus escenarios de desastre, el compromiso de su clave privada, y las acciones que serán llevadas a cabo luego de detectar el mencionado compromiso que son las nombradas a continuación:

Suspensión inmediata del servicio de venta y generación de certificados electrónicos.

- Comunicar a la compañía aseguradora que mantiene la fianza de operación del PSC.
- Examinar el motivo del compromiso, y realizar un informe técnico detallando cada una de las razones por las que se vio comprometida la clave privada del PSC AUTHENTICSING.
- Determinar junto con SUSCERTE las acciones que se deben tomar para la reactivación del servicio de emisión de certificados.
- Declaración de PSC AUTHENTICSING del escenario de desastre.
- Comunicado a SUSCERTE del compromiso de la clave, para la inmediata revocación del certificado de AUTHENTICSING.
- Publicación del evento en la Página Web de AUTHENTICSING.
- Comunicar a los clientes del PSC AUTHENTICSING vía correo electrónico

20.4 Seguridad de las instalaciones tras un desastre natural o de otro tipo.

El centro de datos desde donde opera la Autoridad de Certificación (AC) mantiene las pólizas o instrumentos emitidos por empresas de seguros solventes y reconocidos, a los efectos de mantener un respaldo en caso de alguna ocurrencia de contingencia que afecte la integridad física de la referida sede administrativa y pueda ofrecer una seguridad y garantía de su continuidad operacional.

Sin embargo, lo anterior, en caso de algún desastre o evento que inhabilite la operación regular del centro de datos donde opera el PSC AUTHENTICSING. Igualmente AUTHENTICSING mantiene convenio de operación de centro alterno en caso de algún daño permanente que imposibilite y restrinja la operación regular del centro de datos de la empresa Daycohost.

21. CESE DE LAS ACTIVIDADES DEL PSC.

El PSC AUTHENTICSING tiene considerado en la premisa de que ocurra una suspensión de operaciones, las premisas siguientes:

- Finalidad por vencimiento de acreditación.
- Finalidad por cese de operaciones.
- Finalidad por revocación de acreditación. En este caso, y solo por razones comprobadas de incumplimiento, llevará a cabo la ejecución de la garantía y seguridad solicitada por SUSCERTE al momento de la acreditación
- Finalidad derivada de aspectos tecnológicos.

En el tal caso de alguna ocurrencia de cualquier de las premisas antes mencionados el PCS AUTHENTICSING, estará en toda la obligación de colocar a disposición de SUSCERTE el repositorio de todos los certificados emitidos durante su gestión, incluyendo la condición de cada uno de ellos.

22. CONTROLES DE SEGURIDAD TÉCNICA (DPC)

22.1 Entrega de la clave privada.

Generación del par de claves: El PSC AUTHENTICSING, genera su par de claves (pública y privada) utilizando un dispositivo de hardware criptográfico (HSM) que cumple con los estándares de la FIPS 140-1 Nivel tres (3). El esquema o diseño de operación del PSC AUTHENTICSING y su plataforma Tecnológica de Certificación, se encuentran configurados para que el cliente genere su par de claves (pública y privada). Siempre y en todo caso el compromiso de clave derivará del mismo cliente dado que AUTHENTICSING no genera el par de claves (pública y privada).

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

22.2 Entrega de la clave pública

El esquema de operación del PSC AUTHENTICSING y su plataforma tecnológica de certificación, se encuentran configurados para que el cliente genere su par de claves (pública y privada) siempre y en todo caso el compromiso de clave derivará del mismo cliente porque el PSC ATUHENOLOGY no genera el par de claves (pública y privada). En virtud de lo anterior, si el cliente extravía su clave

privada o la misma se ve comprometida, se deberá proceder a la emisión de un nuevo certificado y deberá cumplir el proceso de contratación del PSC a tales efectos.

22.3 Disponibilidad de la clave pública.

AUTHENTICSING se encuentra en la obligación de mantener en su repositorio y disponible su clave pública, la cual cualquier cliente o parte interesada puede acceder a través de la página Web de AUTHENTICSING (https://www.authenology.com.ve)

22.4 Tamaño de las claves.

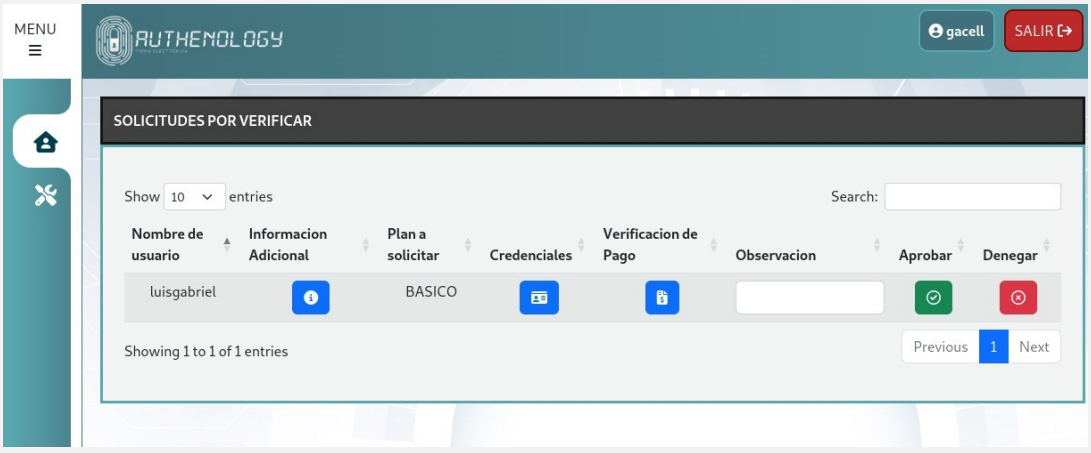
Los módulos de la raíz de certificación de la Autoridad de Certificación (AC) y las claves tienen una longitud de clave de 384bits y utiliza el algoritmo de curva elíptica.

22.5 Parámetros de generación de la clave pública y verificación de la calidad.

Los parámetros utilizados para la generación de las claves públicas cumplen con los requerimientos FIPS 140-2 Nivel tres (3). La generación del par de claves (pública y privada) que utiliza la plataforma de certificación de AUTHENTICSING es un proceso sencillo, pero tiene como requerimientos precauciones especiales. A continuación, se describen los pasos a seguir para la generación del par de claves, y cuáles son las precauciones que deben tomarse a fin de garantizar la protección de la clave privada:

- El usuario final debe ingresar a la página web del PSC AUTHENTICSING www.authenology.com.ve y presionar clic sobre el enlace sistema de certificación www.authenology.com.ve y de esta manera podrá ingresar al sistema de certificación.
- Allí debe de verificar que los datos contenidos están correctos, esta solicitud está compuesta en cuatro (04) partes:

Imagen # 3



Esquema de Operación

- ❖ Información del Usuario: Este punto contiene el nombre y apellido del usuario que fue proporcionado al PSC AUTHENTICSING.
- ❖ Subject: Información general del usuario que dependiendo del tipo de certificado algunos punto s serán obligatorios, a continuación, se nombrara en lista los punto s, y cuáles son los obligatorios por certificados:

Tipo de Certificado	Nombre	Organización	Organización	Titulo	Email	País	Estado	Dirección
Representante legal de la empresa privada	✓	✓	✓	✓	✓	✓	✓	✓
Representante legal de la empresa publica	✓	✓	✓	✓	✓	✓	✓	✓
Empleados de empresa	✓	✓	✓	✓	✓	✓	✓	✓
Profesional titulado	✓			✓	✓	✓	✓	✓
Persona natural	✓				✓	✓	✓	✓
Funcionario Publico	✓	✓	✓	✓	✓	✓	✓	✓
Factura Electrónica	✓							

X

Tipo de Certificado	Nombre	Organización	Organización	Titulo	Email	País	Estado	Dirección

- Información del nombre alternativo: En esta sección debe de contener el número de RIF o C.I. del signatario.
- Opciones de clave: En esta sección es requerido escoger el Proveedor de Servicios Criptográfico (CSP), es importante tomar en cuenta que, si el certificado se va a instalar en un Etoken criptográfico, los drivers del dispositivo deben de estar instalados previamente en el equipo que se va a utilizar para generar el par de claves (Pública y Privada) del usuario. Seguidamente, el usuario debe aceptar los términos y condiciones para habilitar el botón “Generar”. Luego de presionar el botón “Generar”, el usuario tendrá la opción de proteger su clave privada con un nivel de seguridad alto utilizando una contraseña segura. Seguido a la aprobación de la solicitud por la Autoridad de Certificación (AC) del PSC AUTHENTICSING enviará al correo del usuario un link donde logrará descargar el certificado. El procedimiento de generación de par de claves mencionado, asegura y garantiza la privacidad de la clave privada del usuario, ya que el usuario es quien la genera, el PSC AUTHENTICSING solo garantiza la vinculación del individuo con la clave pública, dicha clave pública está asociada a su vez a la clave privada.

22.6 Hardware/software de generación de claves.

El software utilizado por el PSC AUTHENTICSING para la generación del par de claves y certificados es una combinación de la Autoridad de Certificación (AC) de Microsoft y Software especializado en certificación electrónica. La Autoridad de Certificación (AC) utiliza un módulo criptográfico para almacenar de forma segura su clave privada. Dicho modulo criptográfico o HSM marca YUBICO y modelo YUBIHSM2, posee certificaciones FIPS 140-2, y todas las especificaciones técnicas de este dispositivo de seguridad se indican a continuación:

22.6.1 Algoritmos Criptográficos soportados.

- Cryptographic interfaces (APIs)

- Microsoft CNG (KSP)
- PKCS#11 (Windows, Linux, macOS)
- Native YubiHSM Core Libraries (C, python)

➢ Cryptographic capabilities

- Hashing (used with HMAC and asymmetric signatures)
- SHA-1, SHA-256, SHA-384, SHA-512

➢ RSA

- 2048, 3072, and 4096 bit keys
- Signing using PKCS#1v1.5 and PSS
- Decryption using PKCS#1v1.5 and OAEP

➢ Elliptic Curve Cryptography (ECC)

- Curves: secp224r1, secp256r1, secp256k1, secp384r1, secp521r, bp256r1, bp384r1, bp512r1, curve25519
- Signing: ECDSA (all except curve25519), EdDSA (curve25519 only)
- Decryption: ECDH (all except curve25519)

➢ Key wrap

- Import and export using NIST AES-CCM Wrap at 128, 196, and 256 bits

➢ Random numbers

- On-chip True Random Number Generator (TRNG) used to seed NIST SP 800-90 AES 256 CTR_DRBG

➢ Attestation

- Asymmetric key pairs generated on-device may be attested using a factory certified attestation key and certificate, or using your own key and certificate imported into the HSM

22.6.2 Referencias.

A los efectos de documentar y proveer información del hardware criptográfico utilizado por la Autoridad de Certificación (AC), se señala la dirección web que se indica a continuación: **(https://www.yubico.com/products/hardware-security-**

module/). Adicionalmente, el módulo criptográfico utilizado por la Autoridad de Certificación (AC) puede soportar la generación de claves de 386 bits y tiene la capacidad de firmar y cifrar.

22.7 Propósitos de utilización de claves:

La Clave de privada del PSC AUTHENTICSING puede ser utilizada para:

- Firma de Certificados a las autoridades de certificación de pólizas.
- Firma de certificados establecidos en la presente DPC.
- Firma de listas de revocación de certificado.
- Firma de certificados para la certificación cruzada, aprobada por SUSCERTE y la gerencia general y el consultor de tecnología de AUTHENTICSING.

23. PROTECCIÓN DE LA CLAVE PRIVADA.

23.1 Estándares para los módulos criptográficos.

El módulo criptográfico usado por la infraestructura de clave pública (ICP) del PSC AUTHENTICSING, está certificado para cumplir con los requerimientos de FIPS nivel 3. En el caso de la raíz de certificación de AUTHENTICSING, dicho modulo se mantiene fuera de línea.

23.2 Control “N” de “M” de la clave privada:

La Clave privada del PSC AUTHENTICSING, se encuentra bajo control multipersona. Es activa mediante la inicialización del Software de la Autoridad de Certificación (AC) por medio de una combinación de operadores de la AC, Administradores del HSM y usuarios del sistema operativo. Este es el único procedimiento de activación de la clave.

23.3 Custodia de la clave privada.

La clave privada de la Autoridad de Certificación (AC) está protegida por un HSM. La Autoridad de Certificación (AC) ha establecido los pasos a seguir para la instalación del HSM, los mismos se detallan en breve:

- Instalación de los drivers: Se necesitará instalar los drivers respectivos al HSM en el servidor de certificación (CA).
- Instalación física
- Creación del Mundo de Seguridad. Se creará el Mundo de Seguridad bajo los comandos establecidos y siguiendo los siguientes parámetros:
- Se crearán los perfiles y toles dentro del mundo de seguridad.

23.4 Copia de seguridad de la clave privada.

El respaldo de la clave privada se realiza en dos (2) unidades de CD/DVD (la principal y la de respaldo) selladas con un precinto y almacenadas en una caja de seguridad. La clave de cifrado de la raíz de certificación del PSC AUTHENTICSING solamente se respalda para los fines de recuperación ante Desastres.

23.5 Archivo de la clave privada.

La clave privada de la Autoridad de Certificación (AC se encuentra almacenada en un componente de hardware denominado HSM, el cual es el encargado de respaldarla y cifrarla. Tanto el respaldo como el cifrado son almacenados en una unidad de cinta, la cual el administrador de la Autoridad de Certificación (AC) se asegurará de mantener a resguardo en un lugar seguro y fuera del centro de datos.

23.6 Inserción de la clave privada en el módulo criptográfico.

La Autoridad de Certificación (AC) ha establecido los parámetros y lineamientos bajo los cuales se hará la generación de claves, las mismas se nombran en breve:

- Se generará el nuevo mundo de seguridad.
- Se instalará la autoridad de certificación bajo la modalidad de Subordinada y se generará la petición de certificado.
- SUSCERTE firmará la solicitud del certificado del PSC AUTHENTICSING.
- Se instalará y activará el certificado del PSC AUTHENTICSING.

23.7 Método de activación de la clave privada.

Para la activación de la clave privada es requerido y necesario utilizar tarjetas inteligentes, requiere dos de cuatro tarjetas de administrador y una de dos tarjetas de operador, además, es necesario el acceso al sistema operativo del servidor de certificación.

23.8 Método de destrucción de la clave privada.

La clave privada de origen de la Autoridad de Certificación (AC) puede ser destruida retornando al HSM a su estado original de fábrica y borrando todos los símbolos de respaldo.

23.9 Ranking del módulo criptográfico.

La Autoridad de Certificación (AC) usa un módulo criptográfico para almacenar de forma segura su clave privada. Dicho Modulo criptográfico o HSM marca YUBICO y modelo YUBIHSM2 y posee certificaciones FIPS 140-2.

Estos dispositivos se encuentran dentro de la categoría de hardware de alta seguridad, los cuales son utilizados por entidades bancarias y de seguridad de estado en todo el mundo, gozando de experiencia y seguridad comprobada.

24. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES.

24.1 Archivo de la clave pública.

La clave pública del PSC AUTHENTICSING es archivada según el formato PKCS#7, por un tiempo de diez (10) años.

24.2 Períodos operativos de los certificados y período de uso del par de claves.

El certificado del PSC AUTHENTICSING tendrá una validez de diez (10) años. Las firmas y los certificados electrónicos generados por el PSC AUTHENTICSING tienen un período de validez de un (1) año contados a partir de la fecha de activación de la firma o certificado electrónico por parte de la Autoridad de Certificación (AC) de AUTHENTICSING. El par de claves asociado a cada firma o certificado electrónico tiene igualmente el mismo lapso de vigencia que la firma o certificado del que se trate

25. DATOS DE ACTIVACIÓN.

25.1 Generación e instalación de datos de activación.

La generación del par de claves (pública y privada) que utiliza la plataforma de certificación de la Autoridad de Certificación (AC) AUTHENTICSING es un proceso sencillo, pero que requiere de precauciones especiales.

A continuación, se detallan cada uno de los pasos a seguir para la generación del par de claves y cuáles son las precauciones que deben tomarse a fin de asegurar y garantizar la protección de la clave privada:

- La validez de la identidad del individuo se ejecuta por parte de la Autoridad de Registro (AR) la cual le envía a la Autoridad de Certificación (AC) la información necesaria para que la creación del usuario dentro del sistema de y de esta forma garantizar la vinculación de identidad de la persona con su clave pública. El usuario final debe acceder a la página web de AUTHENTICSING (https://www.authenology.com.ve) y presionar click sobre el enlace Certificados

Electrónicos, posteriormente pulsar sobre el cuadro que señala el Sistema de certificación (https://), ingresar y registrarse en el sistema de certificación.

- Luego de registrarse, debe ingresar al aplicativo de solicitud de certificados colocando su información de acceso (login y password) y validar su dirección de correo electrónico.
- Después que este validada su dirección de correo electrónico, el usuario necesitará acceder al enlace certificados y realizar una petición de certificado, seleccionando el tipo de certificado (firma electrónica), ingresando la información personal solicitada, seleccionando el proveedor de servicios de cifrado (CSP) y presionando el botón Generar. *Nota: Hay que tener mucha precaución con el CSP y el equipo y/o dispositivo donde se está generando la petición de certificado, ya que es allí donde va a quedar instalado el certificado.*
- Al presionar el botón Generar se crean el par de claves (pública y privada), automáticamente es enviada la petición de certificado a la autoridad de registro para que sea validada presencialmente la identidad del usuario que está realizado la solicitud.
- El método de la generación de par de claves mencionado, asegura y garantiza la privacidad de la clave privada del usuario, ya que el usuario es quien la genera, AUTHENTICSING solo garantiza la vinculación del individuo con la clave pública, dicha clave pública está asociada a su vez a la clave privada.
- Una vez validada la identidad por la Autoridad de Registro (AR) y generado el certificado por la Autoridad de Certificación (AC), el cliente procede a descargar las firma o certificado electrónico en el repositorio de su computadora, aceptando la fuente de emisión del certificado.

25.2 Protección de datos de la activación.

La activación del certificado emitido, es realizado mediante el sistema de certificación del PSC AUTHENTICSING, limitándose en el equipo o el dispositivo donde se hayan generado el par de claves (Pública y Privada).

26. CONTROLES DE SEGURIDAD DEL COMPUTADOR.

26.1 Requisitos técnicos específicos.

El PSC AUTHENTICSING, ha determinado una serie de controles de seguridad aplicables a los equipos informáticos, tales como el buen uso de los equipos, controles de acceso físico y lógico, planes de auditorías, autenticación y las pruebas de seguridad, mecanismos de recuperación de claves y del sistema de AC de Authenticsing.

26.2 Calificaciones de seguridad computacional.

Como parte de las operaciones criptográficas que se llevan a cabo, se cuenta con equipos que operan bajo estándares de seguridad, de igual forma se aplican controles establecidos en el ISO 27002-2013 para el tratamiento de diversos procesos.

27. CONTROLES DE SEGURIDAD DE LA RED

- El control de acceso a la red está restringido a personal autorizado.
- Los componentes de red se encuentran localizados en instalaciones seguras con monitoreo permanente.
- La red es protegida por cortafuegos configurados con políticas de acceso y
- sistemas de alertas para evitar el acceso no autorizado.
- La comunicación de información sensible entre AC y las AR del PSC AUTHENTICSING, es realizada vía VPN incluyendo el uso de firmas electrónicas

28. PERFILES DE CERTIFICADOS LCR / OCSP

28.1 Perfil del certificado

- Los certificados del PSC AUTHENTICSING son emitidos conforme a las siguientes normas:
- RFC 6818: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, January 2013.
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile, March2004 (prevaleciendo en caso de conflicto la TS 101 862).
- ITU-T Recommendation X.509 (2016): Information Technology – Open System.
- Interconnection - The Directory: Authentication Framework.
- ETSI TS 101 862 V1.3.3 (2006-01): Qualified Certificate Profile, 2006.

28.2 Número de versión.

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

28.3 Extensiones del certificado.

Las extensiones de los certificados del PSC AUTHENTICSING autorizan

codificar información adicional en los certificados. Las extensiones estándar X.509 definen los siguientes puntos:

- SubjectKeyIdentifier.
- AuthorityKeyIdentifier.
- BasicConstraints.
- Certificate Policies.
- KeyUsage.
- LCRDistribucionPoint.
- SubjectAlternativeName.
- AuthorityInformationAccess.

28.4 Identificadores de objeto (OID) de los algoritmos.

La CA debe indicar una clave ECDSA utilizando el identificador de algoritmo id-ecPublicKey (OID: 1.2.840.10045.2.1).

El OID del algoritmo criptográfico usado por AUTHENTICSING es:

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

28.5 Formatos de nombres.

El formato y el significado asignado a los nombres para cada uno de las firmas y certificados electrónicos generados por AUTHENTICSING se encuentran detallados en el presente documento en el punto (12.1.3) de la Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC).

28.6 Identificador de objeto (OID) de la PC.

AUTHENTICSING, usará la definición de política de asignación de OID's según el árbol privado de numeración asignado por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).

28.7 Perfil de LCR / OCSP:

La lista de Certificados Revocados (LCR) es una lista de firmas y certificados electrónicos, en el que concretamente, se muestran cada uno de los números de serie de las firmas o certificados electrónicos revocados por una Autoridad de Certificación (CA), los números de serie que han sido revocados, ya no son válidos, y por ese motivo el usuario no debe confiar en ningún certificado incluido en la LCR del sistema. Una (LCR) es un archivo que contiene lo siguiente:

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

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

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

ESTRUCTURA DE DATOS DE LAS LISTA DE CERTIFICADOS REVOCADOS.	
Nombre del punto	**Valor**
Versión	V3 (Número de versión de la LCR)
Algoritmo	ECDSA-WHITH-SHA384 (Algoritmo de Firma)
DATOS DEL EMISOR	
CN	AUTHENTICSING
O	Sistema Nacional de Certificación Electrónica
C	VE (VENEZUELA)
PERIODO DE VALIDEZ	
Última Actualización	Contiene la fecha y hora en que fue emitida la LCR
Próxima Actualización	Fecha en que se emitirá la próxima LCR
Lista de certificados revocados	
Certificados Revocados	Contiene la lista de certificados revocados indicados por su número de serie y su fecha de revocación.

Extensiones	
Identificación de clave de la AC	Proporciona un medio para identificar la clave pública que corresponde a la clave privada utilizada para firmar una LCR (ID DE CLAVE)
Nombre alternativo del emisor	
DNS Name	www.authenology.com.ve
Otro nombre	
Punto de distribución del emisor	- https://www.authenology.com.ve/ac-raiz/authenologycrl.crl - https://www.authenology.com.ve/acraiz/

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

29. AUDITORIA DE CONFORMIDAD (DPC)

En el caso de la raíz de certificación de la Autoridad de Certificación (AC) es supervisada y auditada anualmente por la SUSCERTE, la cual en cualquier momento y con la frecuencia que considere apropiada puede realizar auditorías exhaustivas o parciales para determinar si el manejo de la clave criptográfica de la Autoridad de Certificación (AC) cumple con las directrices de Ley para operar como PSC.

Para el auditor externo se debe cumplir lo establecido en la Norma N°047 de SUSCERTE. En el caso de los auditores internos, estos no podrán tener relación Funcional con el área objeto de la auditoría.

29.1 Relación entre el auditor y la autoridad auditada:

Entre el PSC AUTHENTICSING y el auditor seleccionado, solamente existe una relación comercial que no causa dependencia. El PSC AUTHENTICSING contratará la auditoría de seguimiento ordenada por la SUSCERTE y el auditor prestará el servicio con la obligación de generar un informe de cumplimiento, el cual entregará al AUTHENTICSING y a SUSCERTE, y de mantener en todo momento la confidencialidad de la información a la cual tuvo acceso durante el proceso de auditoría.

29.2 Tópicos cubiertos por el control de conformidad.

Los tópicos cubiertos por la auditoria de cumplimiento incluyen:

- Seguridad física.
- Evaluación de tecnología.
- Administración de servicios CA.
- Investigación de personal.
- Documento de la Declaración de Prácticas de Certificación (DPC) y Políticas de Certificados (PC) y la política de certificados (PC) y otras políticas y documentos aplicables.
- Contractos.
- Protección de datos y consideraciones sobre privacidad.
- Planificación de recuperación ante desastres.

30. REQUISITOS COMERCIALES Y LEGALES (DPC y PC)

30.1 Aranceles

El decreto ley de mensajes de datos y firmas electrónicas establece la obligación del PSC AUTHENTICSING, de constituir garantías para su operación como organismo acreditado por ante la SUSCERTE. La normativa de SUSCERTE fija un pago de tasa de ley a los fines de optar a la acreditación como PSC, el monto de la referida tasa es de MIL UNIDADES TRIBUTARIAS (1000 U.T.). Igualmente se solicita una fianza a favor de SUSCERTE) cuyo monto es de CUARENTA Y UN MIL UNIDADES TRIBUTARIAS (41,000 U.T.). Esta fianza se constituye a los fines de garantizar la continuidad de operación del PSC AUTHENTICSING y en el supuesto de cese de operación; situación en la cual SUSCERTE asumirá el control y operación de la plataforma tecnológica del PSC AUTHENTICSING. Además, SUSCERTE decreta la obligación para el PSC AUTHENTICSING de mantener garantía constituida en forma de póliza de seguro y a favor de los clientes usuarios de firmas o certificados electrónicos generados por el PSC AUTHENTICSING Relación entre el auditor y la autoridad auditada:

Entre el PSC AUTHENTICSING y el auditor seleccionado, solamente existe una relación comercial que no causa dependencia. El PSC AUTHENTICSING contratará la auditoría de seguimiento ordenada por la SUSCERTE y el auditor prestará el servicio con la obligación de generar un informe de cumplimiento, el cual entregará al PSC AUTHENTICSING y a SUSCERTE, y de mantener en todo momento la confidencialidad de la información a la cual tuvo acceso durante el proceso de auditoría.

30.2 Responsabilidad financiera del PSC

Los límites de la responsabilidad del PSC AUTHENTICSING hacia sus clientes, está regulada mediante acuerdos contractuales con dichas clientes. La responsabilidad del PSC AUTHENTICSING para con los clientes, partes dependientes y cualquier otra entidad usuaria de firmas o certificados electrónicos generados por el PSC, está limitada contra reclamos de cualquier tipo, incluyendo los contractuales, ilegales, extra contractual y de naturaleza delictiva, en cada certificado en particular sin importar el número de transacciones, firmas electrónicas es o causas de acción que surjan o estén relacionadas con dicho certificado.

Cualquier servicio prestado con respecto a dicho certificado y en forma acumulativa. Todos y cada uno de los reclamos que surjan de la infraestructura de clave pública (ICP) con relación a un certificado (sin reparar en la entidad causante de los daños), estarán sujetos a los límites de responsabilidad aplicables a éstos de acuerdo con este documento de la declaración de prácticas de certificación (DPC) y política de certificados (PC). Sujeto a las limitaciones anteriores, el límite de responsabilidad agregada de la autoridad de certificación (AC) AUTHENTICSING hacia todos los clientes, partes dependientes y cualquier otra entidad, ni por todo el período de validez de un certificado emitido por la autoridad de certificación (AC (a menos que sea revocado o suspendido antes de su expiración), hacia todas las personas con relación a dicho certificado es de quince mil unidades tributarias (15.000 U.T.).

En ningún caso la responsabilidad de la autoridad de certificación (AC) excederá el límite antes mencionados.

30.3 Políticas de confidencialidad

30.3.1 Información Confidencial

Toda la recopilación y la utilidad de la información compilada por la Autoridad de Certificación (AC) del PSC AUTHENTICSING es realizada y cumpliendo con la legislación de Venezuela y basándose en las distinciones suministradas en este documento de la Política de Certificación (PC)y Declaración de Prácticas de Certificación (DPC) entre “Resumen de Información” e “Información de Identificación”. La información personal recopilada y usada por los proveedores de servicios de certificación operados por terceros necesitará cumplir con la legislación sobre protección de datos aplicable. En ausencia de alguna legislación

local, los PSC cumplirán con el estándar mínimo contemplado en este documento de la Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC). En los casos de suspensión de operaciones, se procederá a transferir a SUSCERTE los datos personales y demás datos correspondientes en su condición de ente rector electrónica.

De todas maneras, se debe buscar el almacenamiento y la disponibilidad de dichos datos para fines de mantener la condición de servicios de certificación a los clientes correspondientes. Los detalles sobre

Cómo PSC AUTHENTICSING recopila, procesa y almacena cada uno de los datos personales se encuentra en la política de modelo de operación de la Autoridad de Registro (AR) de la Autoridad de Certificación (AC) del PSC AUTHENTICSING. En adición a lo antes expuesto, se nombra que la información de identificación es la información obtenida para identificar positivamente una entidad y suministrar los servicios de certificación que ésta solicita. La información de identificación será tratada como información confidencial a menos que la entidad a la cual se refiere la información dé su consentimiento de manera explícita.

30.3.2 Información No Confidencial

Tipos de información no considerados confidenciales.

- Resumen de la información.
- Todos los certificados emitidos por la Infraestructura de Clave Pública (ICP) del PSC AUTHENTICSING, para el uso público pueden ser divulgados públicamente.
- Todos los Certificados emitidos por la Autoridad de Certificación (AC) AUTHENTICSING en su condición servicios de certificación a terceros también pueden ser divulgados públicamente

30.3.3 Publicación de Información sobre la Revocación o Suspensión de un Certificado

La Lista de Certificados Revocados (LCR), se constituye en un registro de todos aquellos certificados que, habiendo cumplido su proceso de generación y asignación de Ley, son revocados cuando se encuentra comprometida su clave, por solicitud del cliente, por uso indebido del certificado, por causa imputable al cliente o por suspensión de operación de la Autoridad de Certificación (AC). La LCR es publicada cada veinticuatro (24) horas en (www.authenticsing.com.ve).

Cada uno de los procesos de revocación de certificado es informado por el PSC AUTHENTICSING vía correo electrónico al Cliente propietario del certificado electrónico. Dicha notificación es elaborada con copia a SUSCERTE y se incluye en el depósito digitalizado mantenido por el PSC AUTHENTICSING.

30.3.4 Divulgación de Información a Autoridades Judiciales

La(s) razón(es) para la suspensión o revocación de un certificado pueden hacerse públicas de acuerdo con la ley aplicable o bajo la responsabilidad única y absoluta del PSC AUTHENTICSING.

La información sobre suspensión de certificados será revelada solo al cliente propietario del certificado o a SUSCERTE bajo el requerimiento derivado del proceso judicial y bajo el mandato de cumplimiento. Ningún documento o registro en poder de la Autoridad de Certificación (AC) o la Autoridad de Registro (AR) del PSC AUTHENTICSING será entregado a las agencias oficiales salvo que ocurran algunos de los hechos señalados a continuación:

- Se produzca debidamente una orden
- Solicitud judicial
- El representante oficial de la ley esté debidamente identificado
- Se cumpla con los demás procedimientos legales.

Como principio general, ningún documento confidencial o registro almacenado por la Autoridad de Certificación (AC) y Autoridad de Registro (AR) del PSC AUTHENTICSING es entregado a ninguna persona excepto donde:

- La persona que requiere la información es una persona autorizada para hacerlo y está debidamente identificada.
- Se produzca una solicitud de información debidamente documentada (Ej. que haya cumplido con todos los procedimientos legales).

Los servicios para la certificación prestados bajo la autoridad de terceros pueden ser objeto de este tipo de solicitudes de información, como evidencia civil o para propósitos de descubrimiento, relacionados con la Autoridad de Certificación (AC) del PSC AUTHENTICSING en cualquier jurisdicción donde los procedimientos legales apropiados se hayan cumplido.

31. PROTECCIÓN DE LA INFORMACIÓN PRIVADA/SECRETA

31.1 Información considerada privada

En AUTHENTICSING considerará información privada, a tenor de lo dispuesto en la Constitución de la República Bolivariana de Venezuela, la siguiente:

- Nombres y apellidos.
- Número de cédula de identidad y RIF.
- Direcciones y datos telefónicos del cliente.
- Datos suministrados en el proceso de contratación de firma o certificado electrónico.

31.2 Información considerada no privada

Tipos de información no considerados confidenciales:

- Resumen de información
- Todos los certificados emitidos por la infraestructura de clave pública (ICP) para uso público pueden ser divulgados públicamente
- Todos los certificados emitidos por la autoridad de certificación (AC) en su condición servicios de certificación a terceros también pueden ser divulgados públicamente.

31.3 Responsabilidad de proteger la información privada/secreta

El PSC AUTHENTICSING tiene la obligación de mantener a resguardo la información suministrada por los clientes contratantes de firmas o certificados electrónicos generados por el PSC AUTHENTICSING. A tales fines, se mantendrán los datos bajo archivo electrónico con certificados de seguridad asociados al acceso de la misma. El acceso a la información de los clientes solo estará limitado al representante de la Autoridad de Registro (AR) y al Gerente general del PSC AUTHENTICSING.

31.4 Consentimiento previo para el uso de información privada/secreta

La información dispuesta en archivos por el PSC AUTHENTICSING será manejada como información confidencial y la misma no será suministrada a terceros distintos al cliente propietario de la firma o certificado electrónico, salvo que medie aprobación expresa y autenticada en notaría pública por parte del cliente cuya información se trate, autorización realizada por escrito vía correo electrónico firmado o certificado por el cliente propietario de la firma o certificado electrónico o derivado de mandato judicial impuesto por Tribunal y derivado de causa en proceso.

31.5 9.4.5 Comunicación de la información a autoridades administrativas y/o judiciales

Respecto a la comunicación de la información, serán seguidos y aplicables los principios y requerimientos señalados en el presente Documento de la Declaración de Prácticas de Certificación (DPC) y la Política de Certificados (PC).

32. PROTECCIÓN DE LA INFORMACIÓN PRIVADA/SECRETA

32.1 Información considerada privada

En PSC AUTHENTICSING considerará información privada, a tenor de lo dispuesto en la Constitución de la República Bolivariana de Venezuela, la siguiente:

- Nombres y apellidos.
- Número de cédula de identidad y RIF.
- Direcciones y datos telefónicos del cliente.
- Datos suministrados en el proceso de contratación de firma o certificado electrónico.

32.2 Información considerada no privada

Tipos de información no considerados confidenciales:

- Resumen de información
- Todos los certificados emitidos por la infraestructura de clave pública (ICP) para uso público pueden ser divulgados públicamente
- Todos los certificados emitidos por la autoridad de certificación (AC) en su condición servicios de certificación a terceros también pueden ser divulgados públicamente

32.3 Responsabilidad de proteger la información privada/secreta

El PSC AUTHENTICSING tiene la obligación de mantener a resguardo la información suministrada por los clientes contratantes de firmas o certificados electrónicos generados por el PSC AUTHENTICSING. A tales fines, se mantendrán los datos bajo archivo electrónico con certificados de seguridad asociados al acceso de la misma. El acceso a la información de los clientes solo estará limitado al representante de la Autoridad de Registro (AR) y al Gerente general del PSC AUTHENTICSING.

32.4 Consentimiento previo para el uso de información privada/secreta

La información dispuesta en archivos por el PSC AUTHENTICSING será manejada como información confidencial y la misma no será suministrada a terceros distintos al cliente propietario de la firma o certificado electrónico, salvo que medie aprobación expresa y autenticada en notaría pública por parte del cliente cuya información se trate, autorización realizada por escrito vía correo electrónico firmado o certificado por el cliente propietario de la firma o certificado electrónico o derivado de mandato judicial impuesto por Tribunal y derivado de causa en proceso.

32.5 Comunicación de la información a autoridades administrativas y/o judiciales

Respecto a la comunicación de la información, serán seguidos y aplicables los principios y requerimientos señalados en el presente Documento de la Declaración de Prácticas de Certificación (DPC) y la Política de Certificados (PC).

33. DERECHO DE PROPIEDAD INTELECTUAL

33.1 Condición general.

los componentes que pueden ser propiedad intelectual de Terceros, todos los derechos de propiedad intelectual, incluyendo los derechos de autor en todos los directorios de certificados, Listas de Certificados Revocados (LCR) y certificados, a no ser que explícitamente se indique todo lo contrario, todas las prácticas, política, los documentos operacionales y de seguridad referentes a la Infraestructura de Clave Pública (ICP) del PSC AUTHENTICSING (electrónicos o no) así como los contratos, le pertenecen y seguirán siendo propiedad de PSC AUTHENTICSING. A través de los contratos correspondientes para la prestación de servicios de certificación, PSC AUTHENTICSING podrá otorgar una licencia a terceros para el uso de certificados, Listas de Certificados Revocados (LCR) y entre otras prácticas autorizadas y documentos de política en la medida que se requieran para la prestación de servicios de certificación de acuerdo con el presente documento de la Declaración de Prácticas de Certificación (DPC) y la Política de Certificados (PC).

33.2 Claves pública y privada.

Todos los derechos de propiedad intelectual de las claves pública y privada generadas estarán protegidos por la entidad por la que dichas claves fueron generadas o por la entidad designada por esta. Los servicios de certificación operados bajo la autoridad de clientes finales no obtendrán ningún derecho en lo absoluto en relación con los certificados, su contenido, formato o estructura.

33.3 Certificado.

En constante momento el PSC AUTHENTICSING se reserva el derecho de suspender o revocar cualquier tipo certificado de acuerdo con los procedimientos y las políticas establecidas en el actual documento de la Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC).

33.4 Nombres distinguidos.

Los derechos de propiedad intelectual, en nombres distinguidos y números de identificación de clientes, no son responsabilidad del PSC AUTHENTICSING, a menos que se especifique todo lo contrario a través de en un contrato o acuerdo.

33.5 Propiedad intelectual.

La propiedad intelectual del actual documento de la Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC), así como de toda la información, publicaciones y documentos generados por el PSC AUTHENTICSING y contenidos o no dentro de su página web www.authenology.com.ve son propiedad exclusiva del PSC AUTHENTICSING.

34. REPRESENTACIONES Y GARANTIAS

El PSC AUTHENTICSING mantiene un ejercicio autónomo como sociedad mercantil, respecto a sus marcas registradas y derechos de autor tutelados. Además el PSC AUTHENTICSING mantiene varios acuerdos de representación con distintas empresas de tecnología de la información, seguridad informática y certificación electrónica, así como proveedores de hardware criptográfico. Las garantías asociadas a los productos que mercadea y vende el PSC AUTHENTICSING distinto a firmas o certificados electrónicos, será tramitada por el PSC AUTHENTICSING y cumplida ante sus clientes.

35. LIMITACIONES DE RESPONSABILIDAD

35.1 Límites de responsabilidad y garantía limitada:

El enfoque de la Autoridad de Certificación (AC) en cuanto al uso de las Infraestructuras clave pública, certificados y firmas electrónicas, es permitir a organizaciones grandes y pequeñas, así como a las personas, que se beneficien de estas tecnologías de la manera menos agobiante y más eficiente.

Para conseguir esto, la Autoridad de Certificación (AC) suministra los servicios de

certificación descritos, en este documento de la Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC). El actual documento de la Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC), contempla cada una de las garantías suministradas por AUTHENTICSING, las cuales cubren la seguridad y regulaciones procedimentales que proveen varios niveles de seguridad y manejo del riesgo (bajo a alto).

La Autoridad de Certificación (AC) sigue los procedimientos establecidos en las referidas garantías y al hacerlo no pretende suministrar un cien por ciento de seguridad, lo que resulta imposible, con las condiciones de operación de los servicios de certificación. Al hacerlo, la Autoridad de Certificación (AC) simplemente busca incrementar el nivel general de cada seguridad. Por lo tanto, AUTHENTICSING asume la responsabilidad del cumplimiento de los procedimientos y las medidas de seguridad descritas en las garantías.

35.2 Deslinde de responsabilidades:

El PSC AUTHENTICSING decreta que no asumirá la responsabilidad de datos y procedimientos que, no se encuentren contemplados y señalados en la norma legal aplicable Decreto Ley Sobre Mensajes De Datos Y Firmas Electrónicas (LSMDFE), el Reglamento de la Ley Sobre Mensajes De Datos Y Firmas Electrónicas (RLSMDFE) y la normativa de SUSCERTE, dentro de esos procedimientos, garantías y procesos se describe lo siguiente:

- La de alcanzar resultados específicos.
- De comerciabilidad o idoneidad para un propósito específico,
- Con relación a la exactitud o confiabilidad de la información contenida en los Certificados que no sean suministrados y/o verificados por la Autoridad de Registro (AR).

- Que no están relacionadas con los temas cubiertos por este Documento de la Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC).
- Sobre la responsabilidad o estabilidad comercial o financiera de terceros que suministren los servicios de certificación bajo su propia autoridad o usando o dependiendo de los servicios de certificación, en los casos de doble certificación;
- Sobre la validez jurídica, la capacidad de satisfacer requerimientos formales o el estatus de prueba de las firmas electrónicas, certificados o claves criptográficas y
- Con relación a los asuntos fuera del control razonable de la Autoridad de Certificación (AC).
- Si la Autoridad de Certificación (AC) es responsable de su incumplimiento con las garantías o por cualquier otra razón, se procederá a la indemnización

contemplada en la fianza establecida por SUSCERTE, no obstante se observará, en todo momento que, el pago de daños excesivos que se pretendan fijar no aplicarán para aquellas actividades que no están directamente relacionadas con las condiciones de los servicios de certificación (de la misma manera que una autoridad pública no puede ser responsable por lo que una persona haga con una "Firma Electrónica"). La Autoridad de Certificación (AC) por lo tanto requiere que, los miembros de la comunidad de la infraestructura de clave pública de AUTHENTICSING, consientan con el hecho que AUTHENTICSING no asume responsabilidad por ningún tipo de daños que surjan de las circunstancias descritas más abajo (incluyendo daños especiales, consecuentes, incidentales, indirectos o punitivos), sin importar que haya sido notificada de ellos (o de su potencialidad) o no, o si éstos son razonablemente previsibles o no.

- Transacciones subyacentes entre los clientes y terceros, incluyendo las partes dependientes.
- Los servicios y/o productos de Terceros (incluyendo el hardware y software) que interactúan o usan los servicios de certificación, certificados, firmas electrónicas, etc.
- Si existe un retraso, mutilación, o pérdida u otros errores en relación con los datos o documentos mientras son creados, almacenados o comunicados.
- Dependencia inaceptable de un Certificado, una firma electrónica, una clave criptográfica o par clave, o los servicios de certificación a los cuales se refiere esta política de certificación y Declaración de Prácticas de Certificación (DPC).
- Incumplimiento de terceros (incluyendo miembros de la comunidad de Infraestructura de Clave Pública (ICP) de AUTHENTICSING) con protección de datos local o legislación sobre privacidad, legislación sobre protección al consumidor o cualquier otro cumplimiento legislativo o regulatorio requerido por la jurisdicción local.
- Cualquier daño indirecto o consecuente de pérdida: de utilidades, plusvalía, de ahorros estimados, de ganancias, negocios, información o interrupción de negocios.
- Para mayor protección de los riesgos relacionados con la condición de servicios de certificación y para garantizar la estabilidad a largo plazo de la Infraestructura de Clave Pública (ICP), el monto de cualquier daño reconocido también está limitado bajo las condiciones fijadas en la póliza de seguro requerida por la SUSCERTE para la operación del PSC AUTHENTICSING.

35.3 Limitaciones de pérdidas.

Los límites de la responsabilidad del PSC AUTHENTICSING hacia los clientes, está regulada mediante acuerdos contractuales con dichas clientes. Como referencia a estos contratos se incorporan esté documento de la Declaración de

Prácticas de Certificación (DPC) y Política de Certificados (PC) y las demás políticas de acreditación elaboradas por el PSC AUTHENTICSING y referidas en la Política de Seguridad de la Información de ésta. A menos que se haya acordado explícitamente o se haya incorporado explícitamente en una firma electrónica o certificado, la responsabilidad de AUTHENTICSING para con los clientes, proveedores o parte interesada, está limitada contra reclamos de cualquier tipo, incluyendo los contractuales, ilegales, extra contractual y de naturaleza delictiva, en cada certificado en particular sin importar el número de transacciones, firmas electrónicas o causas de acción que surjan o estén relacionadas con dicho certificado o cualquier servicio prestado con respecto a dicho certificado y en forma acumulativa.

Todos y cada uno de los reclamos que surjan de la Infraestructura de Clave Pública (ICP) con relación a una firma electrónica o certificado (sin reparar en la entidad causante de los daños o en la entidad que emitió el certificado o suministró los servicios de certificación), estarán sujetos a los límites de responsabilidad aplicables a éstos de acuerdo con este documento de la Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC). La responsabilidad máxima por certificado de la Infraestructura de Clave Pública (ICP) del PSC AUTHENTICSING, se establecerá en el certificado correspondiente.

El límite de responsabilidad por certificado, aplicará sin reparar en el número de transacciones, firmas electrónicas o causas de acción que surjan o estén relacionadas a dicho certificado o cualquier servicio suministrado con respecto a dicho certificado y sobre una base acumulativa. Sujeto a las limitaciones anteriores, el límite de responsabilidad agregada de la Autoridad de Certificación (AC) del PSC AUTHENTICSING hacia todos los clientes, partes dependientes y cualquier otra entidad que no sean entidades Infraestructura de Clave Pública (ICP) subordinadas, ni por todo el período de validez de un certificado emitido por la Autoridad de Certificación (AC) del PSC AUTHENTICSING (a menos que sea revocado o suspendido antes de su expiración), hacia todas las personas con relación a dicho Certificado es de quince mil unidades tributarias (15.000 U.T.). En ningún caso la responsabilidad del PSC AUTHENTICSING excederá el límite antes mencionados.

36. PLAZO Y FINALIZACIÓN

36.1 Plazo

Todo cliente que guarde o mantenga reclamo en contra del PSC AUTHENTICSING, deberá notificarlo en el más corto plazo y dentro de las dos (2) semanas siguientes a la ocurrencia del hecho considerado como fundamento o

base de reclamo. Todo reclamo será tramitado y guardará relación directa con el período de vigencia de la firma o certificado electrónico generado por el PSC AUTHENTICSING. No serán tramitados reclamos luego de vencido el período de vigencia de una firma o certificado electrónico.

36.2 Terminación

Todo reclamo generado por cliente propietario de firma o certificado electrónico deberá ser tramitado y sustanciado por el PSC AUTHENTICSING, manteniendo evidencia escrita de cada proceso.

El acuerdo o finalización de cada reclamo producirá un documento de acuerdo entre el PSC AUTHENTICSING y el cliente que corresponda, dejando sentado la solución al reclamo, la fecha y la conformidad y finiquito de Ley otorgado por el cliente del cual se trate.

37. MODIFICACIONES

37.1 Procedimientos de Publicación y Notificación

Los procedimientos de publicación y notificación son un componente importante de la gestión de certificados electrónicos y se utilizan para garantizar que los usuarios y las partes interesadas tengan acceso a información precisa y actualizada sobre los certificados electrónicos emitidos, así como de las políticas y normas que rigen al PSC AUTHENTICSING.

El proceso de publicación y notificación de los cambios efectuados la documentación de las políticas y normas que rigen al PSC AUTHENTICSING que requiera una publicación en su sitio web www.authenology.com.ve de conformidad con los lineamientos impuestos por SUSCERTE deberá cumplir previamente los pasos contemplados en el presente documento, contar con la aprobación de SUSCERTE para proceder a su publicación y notificación a los clientes de la actualización vía correo electrónico; Internamente el PSC AUTHENTICSING dejará constancia acerca de cada modificación realizada a su documentación a través del uso del formato para ajuste de documentos.

37.2 Procedimientos de Cambio de Especificaciones

Los procedimientos de cambio son procesos formalizados y documentados que se utilizan y estipulan para gestionar, controlar y efectuar los cambios y modificaciones en la DCP - PC, y en sus políticas, normas y procesos técnicos y cualquier otro aspecto relevante que afecten a la DPC - PC. . El objetivo de estos

procedimientos de cambio y/o modificación es garantizar que estos cambios se gestionen de manera efectiva y que se minimicen los riesgos y las interrupciones para el PSC AUTHENTICSING, sus clientes y aliados comerciales

Los procedimientos de cambio de especificaciones en las normas que afecten a la DPC – PC, cuando se presente algunos de los siguientes casos:

- Cambios estructurales de la organización.
- Cambios en los procesos
- Actualización en la Normativa, por parte de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).
  - Inclusión de un tipo de CE de los ya existentes.
  - Inclusión de una nueva entidad en la jerarquía de confianza del PSC AUTHENTICSING.
  - Documentación con más de un (1) año, sin modificación o actualización, deberá imprimirse como una nueva versión.
  - Cambios en la plataforma tecnológica del PSC AUTHENTICSIN, que impliquen una transformación de los modelos operativos.

- Toda modificación deberá ser notificada y aprobada previamente por la SUSCERTE.

37.3 Procedimientos de Aprobación

Los procesos asociados a la aprobación y modificación o ajuste de la documentación del PSC AUTHENTICSING serán reglamentados por una política de documentación y gestión documental que implementara el PSC AUTENTICSING.

38. RESOLUCIÓN DE CONFLICTOS.

38.1 Resolución extrajudicial de conflictos.

El PSC AUTHENTICSING y el cliente reconocen que la solución pronta y equitativa de las controversias que puedan producirse en relación con la operación, generación o venta de la firma electrónica y certificados electrónicos, causando tanto en sus propios intereses como en la ejecución del servicio contratado. A este fin, manifiestan su decisión de realizar todos los esfuerzos posibles para resolver cada una de las controversias que puedan plantearse mediante negociación a los niveles convenientes. Si la controversia no se ha resuelto a través de la negociación antes referida, dentro de los quince (15) días

hábiles después de iniciada la misma, entonces, a solicitud del usuario contratante se someterá la controversia a SUSCERTE, en virtud de lo establecido en el numeral 13 del artículo 22 el Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas. La solución solo alcanzada con la mediación de SUSCERTE y acepada por las partes, será vinculante y de obligatorio cumplimiento.

38.2 Jurisdicción competente.

En el presunto caso de no haber sido resueltos los posibles conflictos existentes de conformidad con lo establecido en el punto anterior “Resolución extrajudicial de conflicto”, el cliente solicitante estará en libertad de acudir a la vía ordinaria de juicio, siendo la Jurisdicción competente la de los tribunales de la Circunscripción Judicial del Área Metropolitana de Caracas.

39. LEGISLACIÓN APLICABLE.

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

- Constitución Bolivariana de Venezuela.
- Decreto 1.204 con Fuerza de Ley Sobre Mensajes de Datos y Firmas electrónicas (LSMDFE).
- Reglamento Parcial de la Ley Sobre Mensajes de Datos y Firmas Electrónicas LSMDFE).
- Ley Orgánica de Procedimientos Administrativos (LOPA).
- Ley Orgánica de Administración Pública (LOAP).
- Y cualquier otras normas complementarias dictada por la Superintendencia de Servicios de Certificación Electrónica.

40. OBLIGACIONES Y RESPONSABILIDAD CIVIL (DPC y PC)

40.1 Obligaciones y responsabilidad civil.

40.1.1 Obligaciones de la Autoridad de Registro (AR):

- La Autoridad de Registro (AR) del PSC AUTHENTICSING asume bajo el presente documento, el cumplimiento de una serie de requerimientos técnicos, legales y procedimentales, los cuales son nombrados a continuación:
- Acatar y cumplir cada uno de los mandatos de la Constitución de la República Bolivariana de Venezuela, del Decreto Ley Sobre Mensajes De Datos y Firmas Electrónicas (LSMDFE), su reglamento (RLSMDFE) y de los demás cuerpos normativos, leyes, decretos, reglamentos o resoluciones gubernamentales que sean sancionados y publicados en gaceta oficial y que regulen la materia de certificación electrónica o de autoridad de certificación electrónica y que sean de obligatorio cumplimiento.
- Acatar las directrices y normativas técnicas emanadas de SUSCERTE.
- Cumplir y mantener vigente los recaudos y requisitos requeridos para la acreditación como proveedor de servicios de certificación electrónica bajo los mandatos del decreto ley sobre mensajes de datos y firmas electrónicas (LSMDFE), su reglamento (RLSMDFE) o los cuerpos normativos que los sustituyan y regulen la actividad de las autoridades de certificación.
- Presentar, mantener y cumplir con la vigencia de la póliza de seguro requerida por SUSCERTE para operar una autoridad de certificación electrónica.
- Cumplir los contratos de prestación de servicios de certificación mantenidos con los clientes de la autoridad de certificación.
- Mantener y actualizar la documentación del PSC AUTHENTICSING.
- Publicar en la página web (www.authenticsing.com.ve) el documento de la Declaración de Prácticas de Certificación (DPC) y la Política de Certificados (PC), la información sobre Lista de Certificados Revocados (LCR) y la política de vida de certificados del PSC AUTHENTICSING, así como toda la documentación que sea de obligatorio cumplimiento a tenor de lo dispuesto en el decreto ley sobre mensajes de datos y firmas electrónicas o la normativa emanada de SUSCERTE.
- Mantener y asegurar la confidencialidad de la información suministrada por los clientes usuarios del servicio de certificación electrónica. La única excepción de confidencialidad será derivada de requerimiento judicial o legal de información de los clientes por parte de una autoridad judicial legitima y competente para realizar el requerimiento de información y

siempre derivado del procedimiento legal que garantice la debida notificación del cliente propietario de la información, con el fin de mantener la protección a la intimidad prevista en la Constitución de la República Bolivariana de Venezuela.

- Mantener un registro y archivo de las contrataciones de servicios del PSC AUTHENTICSING por un lapso de diez (10) años contados a partir de la fecha de suscripción de cada uno de los contratos para la adquisición de certificados de certificación electrónica.
- Mantener y actualizar la documentación que sea de obligatorio cumplimiento a tenor de lo dispuesto en el Decreto Ley Sobre Mensajes De Datos y Firmas Electrónicas o la normativa SUSCERTE.
- Verificar que los signatarios clientes de AUTHENTICSING envíen toda la documentación necesaria según el tipo de certificado electrónico que deseen adquirir.
- Validar que la información entregada por el signatario sea correcta.
- Acreditar a todos aquellos signatarios que cumplan con los requisitos establecidos por el PSC AUTHENTICSING.
- Identificar y proponer mejoras en el proceso de acreditación, con el fin de facilitar el proceso de acreditación de los signatarios.
- Cumplir las políticas de empresa en materia de informática, administración y recursos humanos.
- Cumplir la normativa laboral y demás leyes de corte social que regulen la relación entre el PSC AUTHENTICSING y sus trabajadores.
- Cumplir las normas legales aplicables a la materia de certificación electrónica y el marco legal aplicable a la gestión regular del PSC AUTHENTICSING.

40.1.2 Obligaciones de la Autoridad de Certificación (AC).

- El PSC AUTHENTICSING asume bajo el presente documento el cumplimiento de una serie de requerimientos técnicos, legales y procedimentales, los cuales se señalan a continuación:
- Acatar y cumplir los mandatos de la Constitución de la República Bolivariana de Venezuela, del decreto ley sobre mensajes de datos y firmas electrónicas (LSMDFE), su reglamento (RLSMDFE) y de los demás cuerpos normativos, leyes, decretos, reglamentos o resoluciones gubernamentales que sean sancionados y publicados en gaceta oficial y que regulen la materia de certificación electrónica o de autoridad de certificación electrónica y que sean de obligatorio cumplimiento. Acatar las directrices y normativas técnicas emanadas de SUSCERTE.
- Cumplir y mantener vigente los recaudos y requisitos requeridos para la

acreditación como proveedor de servicios de certificación electrónica bajo los mandatos del decreto ley sobre mensajes de datos y firmas electrónicas (LSMDFE), su reglamento (RLSMDFE) o los cuerpos normativos que los sustituyan y regulen la actividad de las autoridades de certificación.

- Presentar, mantener y cumplir con la vigencia de la póliza de seguro requerida por SUSCERTE para operar una Autoridad de Certificación electrónica.
- Cumplir cada uno de los contratos de prestación de servicios de certificación mantenidos con los clientes de la Autoridad de Certificación.
- Mantener y actualizar la documentación del PSC AUTHENTICSING, en especial el documento de la Declaración de Prácticas de Certificación (DPC) y la Política de Certificados (PC), la Lista de Certificados Revocados (LCR).
- Publicar en la página web (www.authenticsing.net.ve) el documento de la Declaración de Prácticas de Certificación (DPC) y la Política de Certificados (PC), la información acerca de la lista de certificados revocados (LCR), así como toda la documentación que sea de obligatorio cumplimiento a tenor de lo dispuesto en el decreto ley sobre mensajes de datos y firmas electrónicas o la normativa emanada de SUSCERTE.
- Cumplir y asegurar la ejecución de auditorías de cumplimiento anuales por parte de auditores acreditados ante SUSCERTE.
- Custodiar y asegurar la confidencialidad de la información suministrada por los clientes usuarios del servicio de certificación electrónica. La única excepción de confidencialidad será derivada de requerimiento judicial o legal de información de los clientes por parte de una autoridad judicial legitima y competente para realizar el requerimiento de información y siempre derivado de procedimiento legal que garantice la debida notificación del cliente propietario de la información, con el fin de mantener la protección a la intimidad prevista en la Constitución de la República Bolivariana de Venezuela.
- Mantener un registro y archivo de las contrataciones de servicios de certificación electrónica por un lapso de diez (10) años contados a partir de la fecha de suscripción de cada uno de los contratos para la adquisición de certificados de certificación electrónica.
- Custodiar y renovar el contrato de prestación de servicios con el centro de datos desde donde opera la plataforma de certificación de la Autoridad de Certificación (AC) AUTHENTICSING.
- Mantener y actualizar la documentación que sea de obligatorio cumplimiento a tenor de lo dispuesto en el decreto ley sobre mensajes de datos y firmas electrónicas o la normativa emanada de SUSCERTE.

40.2 Obligaciones de los terceros de buena fe:

Los clientes usuarios finales de certificados electrónicos emitidos por la autoridad de certificación (AC) así como los terceros de buena fe, deben cumplir las condiciones siguientes:

- Acceder a la página web del PSC AUTHENTICSING (www.authenology.com.ve) y activar los botones de compra de certificados electrónicos.
- Seleccionar el tipo de certificado que desea el cliente.
- Leer y aceptar el contenido del contrato de prestación de servicios de certificación.
- Leer y aceptar las prácticas de certificación del PSC AUTHENTICSING.
- Cumplir y completar bajo fe de juramento el ingreso de datos y contactos de personas jurídicas o naturales, según sea el caso.
- Cancelar electrónicamente el importe de costo del certificado electrónico.
- Generar sus claves criptográficas.
- Cumplir con la remisión de información soporte de sus datos y contactos, en original o copia certificada al casillero postal señalado en la página web del PSC AUTHENTICSING (www.authenology.com.ve).
- Asistir a la entrevista fijada por la autoridad de registro (AR) de para la validación de datos y contactos del cliente.
- Cumplir con el uso contratado y aceptado del certificado electrónico adquirido por el cliente.
- Asistir a las oficinas administrativas del PSC AUTHENTICSING dentro de las cuarenta y ocho (48) horas siguientes a la revocación y publicación del certificado del cliente en la Lista de Certificados Revocados (LCR) de la Autoridad de Certificación (AC) AUTHENTICSING.
- Verificar los costos asociados al registro, renovación de los certificados en la Página Web (www.authenology.com.ve).
- En todos los casos, al aceptar o recibir el certificado emitido a éste, el cliente garantiza lo siguiente:
  - Que los datos contenidos en el certificado son exactos.
  - Confiar en el contenido y uso del certificado electrónico.
  - Que la clave criptográfica privada asociada con la clave pública contenida en el certificado no ha sido comprometida.
  - Que sólo usará el par de clave criptográfica y los certificados electrónicos de acuerdo con los usos autorizados para el tipo y/o clase correspondiente

- ❖ Que ejercerá el cuidado razonable para evitar el uso sin autorización de la clave criptográfica privada asociada a la clave pública contenida en el certificado;
- ❖ Que el cliente cumplirá con las obligaciones tributarias asociadas a la venta del certificado electrónico, fijada por la legislación que regula la materia de impuestos, tasas o contribuciones dentro de la República Bolivariana de Venezuela.

- ➢ Notificará a otros clientes usuarios del certificado, a la Autoridad de Certificación (AC) y a otros Proveedores de Servicios de Certificación que procesaron su emisión (Ej. Autoridad de Registro autorizada), previo a la expiración del Certificado, lo siguiente:
  - ❖ Que la clave privada ha sido extraviada, robada, o está potencialmente comprometida;
  - ❖ Que ha perdido el control de su clave privada debido a que su contraseña ha sido comprometida o por otra razón;
  - ❖ Inexactitud o cambios al contenido del certificado; y/o
  - ❖ Que el cliente final desea suspender o revocar un certificado por cualquier razón que considere apropiada.

Todas los clientes que deseen confiar en la Infraestructura de Clave Pública (ICP) del PSC AUTHENTICSING, las Listas de Certificados Revocados (LCR), las cadenas de certificados, el presente documento de la Declaración de Prácticas de Certificación (DPC) y la Política de Certificados (PC), pólizas de certificado u otros servicios de certificación o cualquier otra información publicada por el PS C AUTHENTICSING, se les exige estar de acuerdo con los contratos de adquisición de firmas electrónicas y certificados electrónicos, que a tales efectos hayan suscrito en la página web (www.authenology.com.ve) y en adición asumir las obligaciones siguientes:

- ➢ Comprobar la validez, suspensión o revocación del certificado, utilizando información actualizada sobre el estado del certificado en la Lista de Certificados Revocados (LCR).
- ➢ Tomar en cuenta cualquier limitación sobre el uso y límites de responsabilidad del certificado;
- ➢ Confiar en las Firmas Electrónicas y Certificados solamente cuando dicha confianza sea razonable. Al considerar la viabilidad de la dependencia, los aspectos a tomar en cuenta incluirán si:
  - ❖ La Firma Electrónica fue creada durante el período de validez del certificado
  - ❖ La Firma Electrónica puede verificarse exitosamente

- ❖ Todas las huellas digitales de la clave pública de los certificados dentro de las cadenas de certificados correspondientes son verificadas exitosamente
- ❖ Los certificados en la cadena de certificados son validados exitosamente
- ❖ No existen circunstancias adicionales que puedan afectar la confiabilidad de la firma electrónica, certificado, cadena de certificado o Lista de Certificados Revocados (LCR).

41. CONFORMIDAD CON LEY APLICABLE.

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

42. 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.

42.1 Mecanismo de desarrollo del documento:

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

42.2 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 documento de la Declaración de Prácticas de Certificación (DPC) y la Política de Certificados (PC), 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.

42.3 Mecanismo para aprobación de los ajustes al documento:

Cada ajuste o modificación del documento de la Declaración de Prácticas de Certificación (DPC) y la Política de Certificados (PC), tendrá que contar con la aprobación de la alta dirección del 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.

43. 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.

44. ESQUEMA DE UN CONJUNTO DE DISPOSICIONES (RFC 3647, Sección 6).

ESTRUCTURA DE DOCUMENTO

RFC 3647-Sección 6	Estructura Authenticsing
1.INTRODUCCIÓN	CUMPLE/NO CUMPLE
1.1 Descripción general	CUMPLE
1.2 Nombre del documento e identificación	CUMPLE
1.3 participantes de PKI	CUMPLE
1.3.1 Autoridades de certificación	CUMPLE
1.3.2 Autoridades de registro	CUMPLE
1.3.3 Suscriptores	CUMPLE
1.3.4 Parte que confían	CUMPLE
1.3.5 Otros participantes	CUMPLE
1.4 Uso del certificado	CUMPLE
1.4.1 Usos apropiados del certificado	CUMPLE
1.4.2 Usos prohibidos del certificado	CUMPLE
1.5.1 Organización que administra el documento	CUMPLE
1.5.2 Persona de contacto	CUMPLE
1.5.3 Persona que determina la idoneidad del CPS para la poliza	CUMPLE
1.5.4 Procedimientos de aprobación de la CPS	CUMPLE
1.6 Definiciones y siglas	CUMPLE
2. RESPONSABILIDADES DE PUBLICACIÓN Y DEPÓSITO	CUMPLE/NO CUMPLE
2.1 Repositorios	CUMPLE
2.2 Publicación de información de certificación	CUMPLE
2.3 Hora o frecuencia de publicación	CUMPLE
2.4 Controles de acceso a los repositorios	CUMPLE
3. IDENTIFICACIÓN Y AUTENTICACIÓN (11)	CUMPLE/NO CUMPLE

3.1 Denominación	CUMPLE
3.1.1 Tipos de nombres	CUMPLE
3.1.2 Necesidad de que los nombres sean significativos	CUMPLE
3.1.3 Anonimato o seudónimo de los suscriptores	CUMPLE
3.1.4 Reglas para interpretar varias formas de nombres	CUMPLE
3.1.5 Unicidad de los nombres	CUMPLE
3.1.6 Reconocimiento, autenticación y función de las marcas	CUMPLE
3.2 Validación de identidad inicial	CUMPLE
3.2.1 Método para acreditar la posesión de clave privada	CUMPLE
3.2.2 Autenticación de la identidad de la organización	CUMPLE
3.2.3 Autenticación de identidad individual	CUMPLE
3.2.4 Información del abonado no verificada	CUMPLE
3.2.5 Validación de autoridad	CUMPLE
3.2.6 Criterios de interoperación	NO CUMPLE
3.3 Identificación y autenticación para solicitudes de nueva clave	CUMPLE
3.3.1 Identificación y autenticación para la renovación de claves de rutina	CUMPLE
3.3.2 Identificación y autenticación para nueva clave después de la revocación	CUMPLE
3.4 Identificación y autenticación para solicitud de revocación	CUMPLE
4. REQUISITOS OPERATIVOS DEL CICLO DE VIDA DEL CERTIFICADO (11)	CUMPLE/NO CUMPLE

4.1 Solicitud de Certificado	CUMPLE
4.1.1 ¿Quién puede presentar una solicitud de certificado?	CUMPLE
4.1.2 Proceso de inscripción y responsabilidades	CUMPLE
4.2 Tramitación de la solicitud de certificado	CUMPLE
4.2.1 Realizar funciones de identificación y autenticación	CUMPLE
4.2.2 Aprobación o rechazo de solicitudes de certificado	CUMPLE
4.2.3 Tiempo para procesar las solicitudes de certificado	CUMPLE
4.3 Emisión de certificados	CUMPLE
4.3.1 Acciones de CA durante la emisión de certificados	CUMPLE
4.3.2 Notificación al suscriptor por parte de la CA de la emisión de certificado	CUMPLE
4.4 Aceptación del certificado	CUMPLE
4.4.1 Conducta que constituye la aceptación del certificado	CUMPLE
4.4.2 Publicación del certificado por parte de la CA	CUMPLE
4.4.3 Notificación de emisión de certificado por parte de la CA a otras entidades	CUMPLE
4.5 Uso de par de claves y certificados	CUMPLE
4.5.1 Uso de certificado y clave privada del suscriptor	CUMPLE
4.5.2 Uso de certificado y clave pública del usuario de confianza	CUMPLE
4.6 Renovación de certificado	CUMPLE

4.6.1 Circunstancia para la renovación del certificado	CUMPLE
4.6.2 Quién puede solicitar la renovación	CUMPLE
4.6.3 Tramitación de solicitudes de renovación de certificados	CUMPLE
4.6.4 Notificación de nueva emisión de certificado al suscriptor	CUMPLE
4.6.5 Conducta que constituye la aceptación de un certificado de renovación	CUMPLE
4.6.6 Publicación del certificado de renovación por parte de la AC	CUMPLE
4.6.7 Notificación de la emisión del certificado por parte de la CA a otros	CUMPLE
4.7 Nueva clave del certificado	CUMPLE
4.7.1 Circunstancias para la nueva clave del certificado	CUMPLE
4.7.2 Quién puede solicitar la certificación de una nueva clave pública	CUMPLE
4.7.3 Procesamiento de solicitudes de nueva clave de certificado	CUMPLE
4.7.4 Notificación de nueva emisión de certificado al suscriptor	CUMPLE
4.7.5 Conducta que constituye la aceptación de un certificado con nueva clave	CUMPLE
4.7.6 Publicación del certificado con nueva clave por parte de la CA	CUMPLE
4.7.7 Notificación de la emisión del certificado por parte de la CA a otros	CUMPLE
4.8 Modificación del certificado	CUMPLE
4.8.1 Circunstancia de modificación del certificado	CUMPLE
4.8.2 Quién puede solicitar la	CUMPLE

modificación del certificado	
4.8.3 Tramitación de solicitudes de modificación de certificado	CUMPLE
4.8.4 Notificación de nueva emisión de certificado al suscriptor	CUMPLE
4.8.5 Conducta que constituye la aceptación del certificado modificado	CUMPLE
4.8.6 Publicación del certificado modificado por la CA	CUMPLE
4.8.7 Notificación de la emisión del certificado por parte de la CA a otros entidades	CUMPLE
4.9 Revocación y suspensión del certificado	CUMPLE
4.9.1 Circunstancias de revocación	CUMPLE
4.9.2 ¿Quién puede solicitar la revocación?	CUMPLE
4.9.3 Procedimiento de solicitud de revocación	CUMPLE
4.9.4 Período de gracia de solicitud de revocación	CUMPLE
4.9.5 Plazo dentro del cual la CA debe procesar la solicitud de revocación	CUMPLE
4.9.6 Requisito de verificación de revocación para partes que confían	CUMPLE
4.9.7 Frecuencia de emisión de CRL (si corresponde)	CUMPLE
4.9.8 Latencia máxima para CRL (si corresponde)	CUMPLE
4.9.9 Disponibilidad de verificación de estado/revocación en línea	CUMPLE
4.9.10 Requisitos de verificación de revocación en línea	CUMPLE
4.9.11 Otras formas de anuncios de revocación disponibles	CUMPLE

4.9.12 Requisitos especiales relacionados con compromisos clave	CUMPLE
4.9.13 Circunstancias de suspensión	CUMPLE
4.9.14 ¿Quién puede solicitar la suspensión?	CUMPLE
4.9.15 Procedimiento para solicitud de suspensión	CUMPLE
4.9.16 Límites del período de suspensión	CUMPLE
4.10 Servicios de estado de certificado	CUMPLE
4.10.1 Características operativas	CUMPLE
4.10.2 Disponibilidad del servicio	CUMPLE
4.10.3 Funciones opcionales	CUMPLE
4.11 Fin de suscripción	CUMPLE
4.12 Custodia y recuperación de claves	CUMPLE
4.12.1 Políticas y prácticas clave de custodia y recuperación	CUMPLE
5. INSTALACIONES, GESTIÓN Y CONTROLES OPERACIONALES (11)	CUMPLE/NO CUMPLE
5.1 Controles físicos	CUMPLE
5.1.1 Ubicación del sitio y construcción	CUMPLE
5.1.2 Acceso físico	CUMPLE
5.1.3 Energía y aire acondicionado	CUMPLE
5.1.4 Exposiciones al agua	CUMPLE
5.1.5 Prevención y protección contra incendios	CUMPLE
5.1.6 Almacenamiento de medios	CUMPLE
5.1.7 Eliminación de residuos	CUMPLE
5.1.8 Copia de seguridad externa	CUMPLE
5.2 Controles procesales	CUMPLE
5.2.1 Roles confiables	CUMPLE

5.2.2 Número de personas necesarias por tarea	CUMPLE
5.2.3 Identificación y autenticación para cada rol	CUMPLE
5.2.4 Funciones que requieren separación de funciones	CUMPLE
5.3 Controles de personal	CUMPLE
5.3.1 Requisitos de calificaciones, experiencia y autorización	CUMPLE
5.3.2 Procedimientos de verificación de antecedentes	CUMPLE
5.3.3 Requisitos de formación	CUMPLE
5.3.4 Frecuencia y requisitos de reentrenamiento	CUMPLE
5.3.5 Frecuencia y secuencia de rotación de puestos	CUMPLE
5.3.6 Sanciones por acciones no autorizadas	CUMPLE
5.3.7 Requisitos del contratista independiente	CUMPLE
5.3.8 Documentación suministrada al personal	CUMPLE
5.4 Procedimientos de registro de auditoría	CUMPLE
5.4.1 Tipos de eventos registrados	CUMPLE
5.4.2 Frecuencia del registro de procesamiento	CUMPLE
5.4.3 Período de retención del registro de auditoría	CUMPLE
5.4.4 Protección del registro de auditoría	CUMPLE
5.4.5 Procedimientos de copia de seguridad del registro de auditoría	CUMPLE
5.4.6 Sistema de recopilación de	CUMPLE

auditorías (interno versus externo)	
5.4.7 Notificación al sujeto causante del evento	CUMPLE
5.4.8 Evaluaciones de vulnerabilidad	CUMPLE
5.5 Archivo de registros	CUMPLE
5.5.1 Tipos de registros archivados	CUMPLE
5.5.2 Período de conservación del archivo	CUMPLE
5.5.3 Protección del archivo	CUMPLE
5.5.4 Procedimientos de copia de seguridad de archivos	CUMPLE
5.5.5 Requisitos para el sellado de tiempo de los registros	NO CUMPLE
5.5.6 Sistema de recopilación de archivos (interno o externo)	CUMPLE
5.5.7 Procedimientos para obtener y verificar información de archivo	CUMPLE
5.6 Cambio de clave	CUMPLE
5.7 Compromiso y recuperación ante desastres	CUMPLE
5.7.1 Procedimientos de manejo de incidentes y compromisos	CUMPLE
5.7.2 Los recursos informáticos, el software y/o los datos están dañados	CUMPLE
5.7.3 Procedimientos de compromiso de clave privada de la entidad	CUMPLE
5.7.4 Capacidades de continuidad del negocio después de un desastre	CUMPLE
5.8 Terminación de CA o RA	CUMPLE
6. CONTROLES TÉCNICOS DE SEGURIDAD (11)	CUMPLE/NO CUMPLE
6.1 Generación e instalación de pares de claves	CUMPLE

6.1.1 Generación de pares de claves	CUMPLE
6.1.2 Entrega de clave privada al suscriptor	CUMPLE
6.1.3 Entrega de clave pública al emisor del certificado	CUMPLE
6.1.4 Entrega de clave pública de CA a partes que confían	CUMPLE
6.1.5 Tamaños de clave	CUMPLE
6.1.6 Generación de parámetros de clave pública y control de calidad	CUMPLE
6.1.7 Propósitos de uso de claves (según el campo de uso de claves X.509 v3)	CUMPLE
6.2 Protección de clave privada e ingeniería de módulos criptográficos	CUMPLE
6.2.1 Estándares y controles del módulo criptográfico	CUMPLE
6.2.2 Control de varias personas con clave privada (n de m)	CUMPLE
6.2.3 Custodia de clave privada	CUMPLE
6.2.4 Copia de seguridad de clave privada	CUMPLE
6.2.5 Archivo de clave privada	CUMPLE
6.2.6 Transferencia de clave privada hacia o desde un módulo criptográfico	CUMPLE
6.2.7 Almacenamiento de clave privada en módulo criptográfico	CUMPLE
6.2.8 Método de activación de la clave privada	CUMPLE
6.2.9 Método de desactivación de la clave privada	CUMPLE
6.2.10 Método de destrucción de la clave privada	CUMPLE
6.2.11 Clasificación del módulo	CUMPLE

criptográfico	
6.3 Otros aspectos de la gestión de pares de claves	CUMPLE
6.3.1 Archivo de clave pública	CUMPLE
6.3.2 Períodos operativos del certificado y períodos de uso del par de claves	CUMPLE
6.4 Datos de activación	CUMPLE
6.4.1 Generación e instalación de datos de activación	CUMPLE
6.4.2 Protección de datos de activación	CUMPLE
6.4.3 Otros aspectos de los datos de activación	NO CUMPLE
6.5 Controles de seguridad informática	CUMPLE
6.5.1 Requisitos técnicos específicos de seguridad informática	CUMPLE
6.5.2 Calificación de seguridad informática	CUMPLE
6.6 Controles técnicos del ciclo de vida	CUMPLE
6.6.1 Controles de desarrollo del sistema	CUMPLE
6.6.2 Controles de gestión de seguridad	CUMPLE
6.6.3 Controles de seguridad del ciclo de vida	CUMPLE
6.7 Controles de seguridad de la red	CUMPLE
6.8 Sellado de tiempo	NO CUMPLE
7. PERFILES DE CERTIFICADO, CRL Y OCSP	CUMPLE/NO CUMPLE
7.1 Perfil de certificado	CUMPLE
7.1.1 Número(s) de versión	CUMPLE
7.1.2 Extensiones de certificado	CUMPLE
7.1.3 Identificadores de objetos de algoritmo	CUMPLE

7.1.4 Formas de nombre	CUMPLE
7.1.5 Restricciones de nombre	CUMPLE
7.1.6 Identificador de objeto de política de certificado	CUMPLE
7.1.8 Sintaxis y semántica de calificadores de políticas	CUMPLE
7.1.9 Semántica de procesamiento para las Políticas de Certificación críticas	CUMPLE
7.2 Perfil CRL	CUMPLE
7.2.1 Número(s) de versión	CUMPLE
7.2.2 CRL y extensiones de entrada CRL	CUMPLE
7.3 Perfil OCSP	CUMPLE
7.3.1 Número(s) de versión	CUMPLE
7.3.2 Extensiones OCSP	CUMPLE
8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES	CUMPLE/NO CUMPLE
8.1 Frecuencia o circunstancias de la evaluación	CUMPLE
8.2 Identidad/calificaciones del evaluador	CUMPLE
8.3 Relación del tasador con la entidad evaluada	NO CUMPLE
8.4 Temas cubiertos por la evaluación	CUMPLE
8.5 Acciones tomadas como resultado de la deficiencia	NO CUMPLE
8.6 Comunicación de resultados	CUMPLE
9. OTROS ASUNTOS LEGALES Y COMERCIALES	CUMPLE/NO CUMPLE
9.1 Tarifas	NO CUMPLE
9.1.1 Tarifas de emisión o renovación de certificados	NO CUMPLE
9.1.2 Tarifas de acceso al certificado	NO CUMPLE

9.1.3 Tarifas de acceso a la información de revocación o estado	NO CUMPLE
9.1.4 Tarifas por otros servicios	NO CUMPLE
9.1.5 Política de reembolso	NO CUMPLE
9.2 Responsabilidad financiera	NO CUMPLE
9.2.1 Cobertura de seguro	NO CUMPLE
9.2.2 Otros activos	NO CUMPLE
9.2.3 Cobertura de seguro o garantía para entidades finales	NO CUMPLE
9.3 Confidencialidad de la información comercial	CUMPLE
9.3.1 Alcance de la información confidencial	CUMPLE
9.3.2 Información que no está dentro del alcance de la información confidencial	CUMPLE
9.3.3 Responsabilidad de proteger la información confidencial	CUMPLE
9.4 Privacidad de la información personal	CUMPLE
9.4.1 Plan de privacidad	CUMPLE
9.4.2 Información tratada como privada	CUMPLE
9.4.3 Información no considerada privada	CUMPLE
9.4.4 Responsabilidad de proteger la información privada	CUMPLE
9.4.5 Aviso y consentimiento para utilizar información privada	CUMPLE
9.4.6 Divulgación conforme a proceso judicial o administrativo	CUMPLE
9.4.7 Otras circunstancias de divulgación de información	CUMPLE
9.5 Derechos de propiedad intelectual	CUMPLE

9.6 Declaraciones y garantías	CUMPLE
9.6.1 Declaraciones y garantías de CA	CUMPLE
9.6.2 Declaraciones y garantías de RA	CUMPLE
9.6.3 Declaraciones y garantías del suscriptor	CUMPLE
9.6.4 Declaraciones y garantías de la parte que confía	CUMPLE
9.6.5 Declaraciones y garantías de otros participantes	CUMPLE
9.7 Renuncias de garantías	NO CUMPLE
9.8 Limitaciones de responsabilidad	CUMPLE
9.9 Indemnizaciones	NO CUMPLE
9.10 Plazo y terminación	NO CUMPLE
9.10.1 Término	CUMPLE
9.10.2 Terminación	CUMPLE
9.10.3 Efecto de la terminación y supervivencia	CUMPLE
9.11 Avisos individuales y comunicaciones con los participantes	CUMPLE
9.12 Enmiendas	NO CUMPLE
9.12.1 Procedimiento de modificación	NO CUMPLE
9.12.2 Mecanismo y plazo de notificación	NO CUMPLE
9.12.3 Circunstancias bajo las cuales se debe cambiar el OID	NO CUMPLE
9.13 Disposiciones para la resolución de disputas	NO CUMPLE
9.14 Ley aplicable	CUMPLE
9.15 Cumplimiento de la legislación aplicable	CUMPLE
9.16 Disposiciones varias	CUMPLE
9.16.1 Acuerdo completo	CUMPLE

9.16.2 Asignación	CUMPLE
9.16.3 Divisibilidad	CUMPLE
9.16.4 Ejecución (honorarios de abogados y renuncia de derechos)	CUMPLE
9.16.5 Fuerza mayor	CUMPLE
9.17 Otras disposiciones	- CUMPLE

--- Fin de Documento ---