Declaración de Prácticas de Certificación de Advantage Security

Versión 2.1.1
Advantage Security
OID : 2.16.484.101.10.316.2.1.1.1.1.1.2

Nota: Los OID`s: 2.16.484.101.10.316.1.1.1.1.2.2 y 2.16.484.101.10.316.2.1.1.1.1.2.1, fueron publicados erróneamente.

Av. Prolongación Reforma 625,
Desp. 402 Torre Lexus Paseo de las Lomas,
Santa Fe México, DF C.P. 01330
+52 55 50814362
www.advantage-security.com

Declaración de Prácticas de Certificación de Advantage Security

Impreso en los Estados Unidos Mexicanos.
Fecha de revisión: Noviembre 2009

Advantage Security
Av. Prolongación Reforma 625,
Desp. 402 Torre Lexus Paseo de las Lomas, Santa Fe
México, DF C.P. 01330

Attn: Desarrollos de Prácticas. Tel: +52 55 50 81 43 60 Fax: +52 Fax +52 55 50814376

Agradecimiento
Advantage Security reconoce la ayuda de muchas personas especializadas en diversas áreas de negocios, derecho, política y tecnología, que revisaron el documento.

Contenido

Versión 2.1.1 1

Advantage Security 1

OID : 2.16.484.101.10.316.2.1.1.1.1.1.2 1

Declaración de Prácticas de Certificación de Advantage Security 2

1. Introducción 5

1.1 Control de Versiones CPS 6

1.2 Compendio 6

a) Papel de la CPS de Advantage Security y otros Documentos de Prácticas. 7

b) Antecedentes relativos a Certificados Digitales y la Jerarquía de la Secretaría de Economía 9

c) Cumplimiento con las Normas Aplicables 9

1.2.1 Compendio de Política 10

1.2.2 Servicios de la jerarquía de la Secretaría de Economía que ofrece Advantage Security y CA 12

1.4.4.1 Aplicaciones Adecuadas 16

1.4.4.2 Solicitudes Restringidas 16

1.4.4.3 Aplicaciones Prohibidas 17

1.5 Detalles del Contacto 17

2. Disposiciones Generales 18

2.1 Obligaciones 18

2.2 Responsabilidad 20

2.3 Responsabilidad Financiera 23

2.4 Interpretación y Exigibilidad 27

2.5 Comisiones 28

2.6 Publicación y Repositorio 29

2.7 Auditoria de Cumplimiento 31

2.8 Confidencialidad y Privacidad 32

2.9 Derechos de Propiedad Intelectual 33

3. Identificación y Autenticación 34

3.1 Registro Inicial 34

3.2 Nueva Clave y Renovación de Rutina 40

3.3 Reposición de la Clave y Renovación de Rutina para los Certificados del Suscriptor Usuario Final 42

3.4 Petición de Revocación 43

3.5 Requisitos de Documentos Presentados 44
4. Requisitos de Operación 44
4.1 Solicitud del Certificado 44
4.2 Emisión de Certificado 45
4.3 Aceptación de Certificado 46
4.4 Suspensión y Revocación del Certificado 46
4.5 Procedimientos de Auditoria de Seguridad 50
4.6 Archivo de Registros 52
4.7 Cambio de Situación de la Clave 53
4.8 Recuperación de Desastres y Compromiso de la Clave 54
4.9 Cese de la AC 56
5. Controles de Seguridad del Personal, de Procedimientos y Físicos 57
5.1 Controles Físicos 57
5.2 Controles de procedimiento 59
5.3 Controles de Personal 60
6. Controles de Seguridad Técnicos 63
6.1 Generación e Instalación del Par de Claves 63
6.2 Protección de la Clave Privada 65
6.3 Otros Aspectos de la Administración del Par de Claves 69
6.4 Datos de Activación 70
6.5 Controles de Seguridad de la Computadora 71
6.6 Controles Técnicos del Ciclo de Vida 72
6.7 Controles de Seguridad de la Red 73
6.8 Controles de Ingeniería del Módulo Criptográfico 73
7. Certificado y Perfil de la CRL 73
7.1 Perfil del Certificado 73
7.2 Perfil de la CRL 76
8. Administración de Especificaciones 77
8.1 Procedimientos de Cambio de Especificación 77
8.2 Políticas de Publicación y Notificación 78
8.3 Procedimientos de Aprobación de la CPS 79

1. Introducción

Este documento son las Prácticas de Certificación de Advantage Security CPS (Certificación Practice Statement), y esta basado en los Códigos de Prácticas de Certificación de CA. Declara las prácticas que las autoridades de certificación de Advantage Security las "CA´s" (Certificación Authority) emplean al prestar servicios de certificación que comprenden de manera enunciativa y no limitativa, Administración de Certificados, de acuerdo con los requisitos específicos de las Políticas de Certificados (Certificate Policies). Los CPS describen a la jerarquía de la Secretaría de Economía, la cual Advantage Security junto con CA es uno de los proveedores de certificación.

El CPS es la declaración de política principal que rige a Advantage Security como proveedor de servicios de certificación en la jerarquía de la Secretaría de Economía. Establece los requisitos de negocios, legales y técnicos para aprobar, emitir, administrar, usar, revocar y renovar Certificados digitales dentro de dicha jerarquía y prestar servicios fiables asociados. Estos requisitos, llamados las "Normas del a Secretaría de Economía," protegen la seguridad e integridad de la jerarquía de la Secretaría de Economía, se aplican a todos los participantes de la jerarquía y, por ese conducto, proporcionan la garantía de confianza uniforme a través de la jerarquía. Puede encontrar más información sobre la jerarquía de la Secretaría de Economía y las Normas de los mismos en Políticas de Certificados.[1]

La Secretaría de Economía y cada Prestador de Servicios de Certificación (PSC) tienen poder sobre una parte de la jerarquía de la Secretaría de Economía. La parte le la jerarquía de la Secretaría de Economía controlada por Advantage Security y CA se llama su "Subdominio" de la jerarquía. El Subdominio de una PSC consiste en la parte de la jerarquía que está bajo su control. Un Subdomino de Advantage Security comprende entidades subordinadas a éste como sus Clientes, Entidades de Registro y Partes que Confían.

Advantage Security y CA tienen una CPS que rige su Subdominio dentro de la jerarquía de la Secretaría de Economía. Mientras que las CP establecen los requisitos que deben cubrir los participantes en la jerarquía de la Secretaría de Economía, esta CPS describe la forma en que Advantage Security cubre estos requisitos dentro del Subdominio de Advantage Security para la jerarquía de la Secretaría de Economía, que está ubicado primordialmente en la Ciudad de México, México. Específicamente, esta CPS describe las prácticas que utiliza Advantage Security para:

2. Administrar con seguridad la infraestructura central que soporta a la jerarquía de la Secretaría de Economía, y

[1] Las CPS se publican en forma electrónica dentro del Repositorio de Advantage Security en https://ca.advantage-security.com/psceconomia/CPSv2.1.1.pdf Advantage Security también ofrece las CPS en formato de Adobe Acrobat pdf o Word, a solicitud enviada a contacto2@advantage-security.com. También se pueden obtener copias en papel mandando una solicitud por escrito a Av. Prolongación Reforma 625 Desp. 402 – Paseo de las Lomas Santa Fé – México, DF 01330 Attn: Prácticas de Certificación.

3. Emitir, administrar, revocar y renovar los certificados de la jerarquía de la Secretaría de Economía.

Dentro del Subdominio de Advantage Security de la jerarquía de la Secretaría de Economía, de acuerdo con los requisitos de las CP y sus Normas.[2]

1.1 Control de Versiones CPS

El CPS 2.2 es la versión más reciente. Los cambios que se han hecho de la versión anterior, la 2.1, son las siguientes:

1. OID del certificado de la Autoridad Certificadora
2. OID del certificado de Usuario
3. Dirección de la CRL
4. Publicación del método de consulta OCSP
5. Cambio de algoritmo MD2 y MD5 a SHA1withRSA
6. OID de la Política de Certificación

1.2 Compendio

Esta CPS se aplica específicamente a:

1. La Autoridad Certificadora y Registradora de Advantage Security
2. Certificados digitales de usuarios finales.

En general, la CPS también rige el uso de los servicios de la jerarquía de la Secretaría de Economía entregados por Advantage Security como PSC de la jerarquía de la Secretaría de Economía y todas las personas físicas y morales que estarían usando dichos servicios (en forma colectiva, los "Participantes del Subdomino de Advantage Security como PSC de la Secretaría de Economía"). Las AC privadas y las jerarquías que manejan Advantage Security están fuera del alcance de esta CPS.

Hay una clase de certificados en la jerarquía de la Secretaría de Economía, la Clase 2 , y las CP describen la forma en que esta Clase corresponde a la clase de solicitudes con requisitos de seguridad común. Las CP son un solo documento que define las políticas de los certificados y establece las Normas de la jerarquía de la Secretaría de Economía para los certificados digitales Clase 2.

Advantage Security le ofrece certificados digitales Clase 2 de la Secretaría de Economía. Esta CPS describe la forma en que Advantage Security cubre los requisitos de las CP de certificados digitales Clase 2 en su Subdominio. Por consiguiente, la CPS, como un solo documento, cubre las prácticas y procedimientos relativos a la emisión y administración de certificados digitales Clase 2

[2] Aunque la Secretaría de Economía certifica a las Prestadoras de Servicios de, las prácticas relativas de una PSC se cubren en la CPS de la PSC, no la CPS de la Secretaría de Economía

a) Papel de la CPS de Advantage Security y otros Documentos de Prácticas.

La CP describe a un nivel general la infraestructura global de negocios, legal y técnica de la jerarquía de la Secretaría de Economía. Esta CPS aplica entonces las Normas de la jerarquía de la Secretaría de Economía de las CP a los Participantes del Subdominio de Advantage Security y explica prácticas específicas de Advantage Security en respuesta a las CP. Específicamente, la CPS describe, entre otros:

1. Las obligaciones de las Autoridades de Certificación, las Autoridades de Registro, los Suscriptores y las Partes Que Confían dentro del Subdominio de Advantage Security de la jerarquía de la Secretaría de Economía.

2. Los asuntos legales que se cubren en los Contratos de los Suscriptores y los Contratos de las Partes que Confían dentro del Subdominio de Advantage Security.

3. Auditorias y revisiones relacionadas de seguridad y prácticas que emprendan Advantage Security y los Participantes del Subdominio de Advantage Security.

4. Métodos usados dentro del Subdominio de Advantage Security para confirmar la identidad de los Solicitantes del Certificado para certificados digitales Clase 2.

5. Procedimientos operativos para los servicios de ciclo de vida del Certificado que se emprenden en el Subdominio de Advantage Security : Solicitudes, emisión, aceptación, revocación y renovación de Certificados.

6. Procedimientos de seguridad operativa para registro de auditorías, retención de registros y recuperación de desastres que se usan dentro del Subdominio de Advantage Security.

7. Prácticas de seguridad física, de personal, de administración de la clave y lógica de los Participantes del Subdominio de Advantage Security.

En muchos casos, la CPS se refiere a estos documentos auxiliares cuando se trata de prácticas detalladas, específicas, que implementan las Normas de la jerarquía de la Secretaría de Economía, en las que la inclusión de los puntos específicos de la CPS podría comprometer la seguridad del Subdominio de Advantage Security de la jerarquía de la Secretaría de Economía.

El cuadro 1 es una matriz que muestra varios documentos de prácticas de la jerarquía de la Secretaría de Economía y de Advantage Security, si están disponibles para el público, y sus ubicaciones. La lista del cuadro 1 no tiene el propósito de ser completa. Observe que los documentos que no se pongan expresamente a disposición del público son confidenciales, con el fin de preservar la seguridad de la jerarquía de la Secretaría de Economía

Documentos	*Condición*	*Cuando está disponible para el público*
Documentos Auxiliares y Operativos		
Políticas de Seguridad de Advantage Security	Confidencial	N/A
Guía de Requisitos de Seguridad y Auditoria	Confidencial	N/A
Guía de Referencia de Ceremonias de la Clave	Confidencial	N/A
Plan de Administración de Claves	Confidencial	N/A
Plan de Continuidad de Negocios y Recuperación de Desastres	Confidencial	N/A
Política de Seguridad Física	Confidencial	N/A
Proceso de Administración de Infraestructura de Informática	Confidencial	N/A
Procedimientos que Informen de las Características de los Procesos de Creación y Verificación de Firma Electrónica Avanzada	Confidencial	N/A
Políticas de la Seguridad de la Información	Confidencial	N/A
Documento de Procedimiento de Selección, Reclutamiento y Evaluación de Personal	Confidencial	N/A
Modelo Operacional de la Autoridad Certificadora	Confidencial	N/A
Modelo Operacional de la Autoridad Registradora	Confidencial	N/A
Definición de Controles de Acceso al Área de Generación de Certificados	Confidencial	N/A
Manual del Solicitud de Certificado	Público	https://ca.advantage-security.com/psceconomia/manual.pdf
Guía del Administrador del Servicio de Administración de la Clave de Managed PKI	Confidencial	N/A

Otros documentos específicos de Advantage Security		
Declaración de Prácticas de Certificación de Advantage Security	Pública	Repositorio de Advantage Security de conformidad con el artículo 2.6.1 de la CPS. Ver https://ca.advantage-security.com/psceconomia/CPSv2.1.1.pdf
Contratos auxiliares de Advantage Security (Contratos del Suscriptor)	Público	Repositorio de Advantage Security de conformidad con el artículo 2.6.1 de la CPS. Ver https://ca.advantage-security.com/psceconomia/ConvenioSuscriptor.pdf

Cuadro 1 – Disponibilidad de los Documentos de Prácticas

b) Antecedentes relativos a Certificados Digitales y la Jerarquía de la Secretaría de Economía

Esta CPS asume que el lector generalmente conoce las Firmas Digitales, las infraestructuras de las claves públicas (las PKI) y la jerarquía de la Secretaría de Economía. De lo contrario, Advantage Security aconseja que el lector obtenga cierta capacitación en el uso de la criptografía de claves públicas y la infraestructura de claves públicas como se implementan en jerarquía de la Secretaría de Economía. La información general sobre educación y capacitación se puede obtener en Advantage Security en http://www.pscadvantage.com

Asimismo, viene un breve resumen de los papeles de los diferentes Participantes de jerarquía de la Secretaría de Economía en el artículo 1.1(b) de las CP.

c) Cumplimiento con las Normas Aplicables

Las prácticas que se indican en esta CPS tienen el propósito de cubrir o superar los requisitos de las normas industriales generalmente aceptadas y en desarrollo, incluyendo el Programa WebTrust AICPA/CICA WebTrust para las Autoridades de Certificación, ANS X9.79:2001 PKI Practices and Policy Framework (Marco General de Prácticas y Políticas de la Infraestructura de Claves Públicas 2001) y otras normas de la industria relacionadas con la operación de las CA.

La estructura de esta CPS corresponde generalmente a Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (Marco General de Políticas del Certificado y Prácticas de Certificación de la Infraestructura de Claves Públicas X.509 de Internet), conocido como RFC 2527 del Grupo Operativo de Ingeniería de Internet y el organismo de normas de Internet. El marco general RFC 2527 se ha convertido en una norma en la industria de la infraestructura de claves públicas (PKI). Esta CPS se conforma al marco general RFC 2527, con el fin de hacer que se le facilite el mapeo y las comparaciones de políticas, las evaluaciones y la interoperación a las personas que utilizan o piensan utilizar los servicios de Advantage Security y CA.

Advantage Security ha hecho que la CPS se conforme a la estructura de RFC 2527 cuando sea posible, aunque es necesario que haya pequeñas variaciones en el título y el detalle debido a la complejidad de los modelos de negocios de Advantage Security. Mientras que Advantage Security se propone continuar la política de adherirse al RFC 2527 en el futuro, Advantage Security se reserva el derecho de desviarse de la estructura de la RFC 2527 como sea necesario; por ejemplo, mejorar la calidad de la CPS o su conveniencia para los Participantes del Subdomino de Advantage Security. Asimismo, puede que la estructura de la CPS no corresponda a versiones futuras del RFC 2527.

1.2.1 Compendio de Política

Advantage Security una clase de servicios de certificación, la Clase 2, que corresponden a la Clase de Certificado cuyas políticas se describen en las CP. El certificado digital Clase 2 ofrece una funcionalidad y función de seguridad específica y corresponde a un nivel específico de confianza. Los Participantes del Dominio de Advantage Security solamente puede seleccionar el certificado digital Clase 2.

Una de las funciones de las CP es describir el certificado digital Clase 2 en detalle.[3]No obstante, esta sección resume el Certificado Clase 2 que ofrece Advantage Security dentro de su Subdominio.

Los Certificados de la Clase 2 ofrecen el nivel más alto de garantías dentro del Subdominio de Advantage Security. Los Certificados de la Clase 2 se emiten a personas físicas y morales con respecto a las AC y AR. Los Certificados individuales Clase 2 se pueden usar para firmas digitales, encripción y control de acceso, incluyendo como prueba de identidad, en las transacciones de alto valor. Los Certificados individuales de la Clase 2 dan garantías de la identidad del Suscriptor, con base en la presencia personal (física) del Suscriptor ante la persona que confirma la identidad del Suscriptor usando, por lo menos, una forma bien reconocida de identificación expedida por el gobierno de México y otra credencial de identificación. Los Certificados de persona moral de la Clase 2 ofrecen garantías de la identidad de los Suscriptores con base en la confirmación de que la organización del Suscriptor existe en realidad, que la organización ha autorizado la Solicitud del Certificado y que la persona que presenta la Solicitud de Certificado en nombre del Suscriptor estaba autorizada para hacerlo. Los Certificados de persona moral de la Clase 2 para los servidores también ofrecen garantías de que el Suscriptor tiene derecho de usar el nombre de dominio que está anotado en la Solicitud de Certificado.

Los Certificados Advantage Security de persona moral Clase 2 “(ver el artículo 1.1.2.2.1 de las CP) se expiden para una empresa con el fin de que la use un representante debidamente autorizado, que utiliza el Certificado en nombre de la empresa. Los Certificados Advantage Security para personas morales de la Clase 2 ofrecen la garantía de que la persona que controla la clave privada de la empresa está autorizada para fungir en nombre de la empresa en transacciones que se lleven a cabo usando la clave privada correspondiente a la clave pública del Certificado.

[3] Vea el artículo 1.1.1 de las CP.

El cuadro 2 siguiente resume la Clase 2 de Certificado que ofrece Advantage Security en cumplimiento con las CP. Expone las propiedades de cada clase de Certificado, con base en si se expiden para personas físicas o morales, Oficina se Servicios de Autenticación (en donde trabajan los Agentes Certificadores), o se expiden a los Administradores de Advantage Security.

Las especificaciones para la Clase de Certificados en las CP, como se resumen en esta CPS, establecen el nivel mínimo de garantías que se estipulan en dicha Clase. Por ejemplo, cualquier Certificado de la Clase 2 puede usarse para firmas digitales, encripción y control de acceso cuando es necesario comprobar la identidad; es decir, para solicitudes que requieren un alto nivel de garantías. No obstante, por contrato o dentro de ambientes específicos (como el ambiente entre compañías), los Participantes del Subdominio de Advantage Security están autorizados para usar los procedimientos de validación más fuertes de los que se usan dentro de las CP, o usar Certificados para aplicaciones de mayor seguridad que las que se describen en el artículo 1.1.1, 1.3.4.1 de la CPS. Sin embargo, dicho uso estar á limitado a las entidades y estará sujeto al artículo 2.2.1.2, 2.2.2.2 de la CPS, y estas entidades será las únicas responsables por el daño o responsabilidad que cause dicho uso.

Clase	*Expedido a*	*Servicios bajo los cuales están disponibles los Certificados 4*	*Confirmación de la Identidad de los Solicitantes de Certificado (Artículo 3.1.8.1, 3.1.9 de la CPS)*	*Solicitudes que implementan o contemplan los usuarios (Artículo 1.3.4.1 de la CPS)*
Clase 2	Personas	Usuarios Finales (Personas Físicas)	Presencia personal, verificación de identificación oficial .	Mejorar la seguridad del correo electrónico a través de la encripción de confidencialidad, firmas digitales para autenticación y control de acceso basado en la Web. Entrega un nivel más alto de seguridad en comparación con otros tipos de certificados, como la banca en línea, el acceso a la base de datos de la organización e intercambio de información confidencial, incluyendo como prueba de identidad para transacciones de valor alto.
		Usuarios finales como representantes legales (Personas Morales)	Presencia personal, verificación de identificación oficial y llamada de verificación. Verificación de estatus como representante legal.	Mejorar la seguridad del correo electrónico a través de la encripción de confidencialidad, firmas digitales para autenticación y control de acceso basado en la Web. Entrega un nivel más alto de seguridad en comparación con otros tipos de certificados, como la banca en línea, el acceso a la base de datos de la organización e intercambio de información confidencial, incluyendo como prueba de identidad para transacciones de valor alto.

	Organizaciones	Sitios Web	Verificación de la base de datos de terceros o de otros documentos que muestren la existencia de la organización. Verificación de la validación por teléfono (o un procedimiento comparable) a la organización para confirmar el empleo y la facultad del representante de la organización y al representante para confirmar su Solicitud de Certificado. La carta que confirma la Solicitud de Certificado se envía al representante	Mejorar la seguridad del correo electrónico que se envía a nombre de una organización a través del encripción de confidencialidad, firmas digitales para autenticación y control de acceso basado en la Web. Las solicitudes que necesitan de un alto nivel de garantías en comparación con las otras Clases, como obtener acceso a una red externa interempresarial o llevar a cabo transacciones de alto valor en un intercambio interempresarial.

Cuadro 2 – Propiedades de Certificación que afectan la Confianza

1.2.2 Servicios de la jerarquía de la Secretaría de Economía que ofrece Advantage Security y CA

La jerarquía de la Secretaría de Economía ofrece una serie de servicios para ayudar en el despliegue, administración y uso de Certificados, como se describe por completo en el artículo 1.1.2 de las CP. Esta sección trata sobre los servicios de la jerarquía de la Secretaría de Economía que ofrece Advantage Security de conformidad con el artículo 1.1.2 de las CP. Para mayor información sobre alguno de estos programas, consulte el sitio Web de Advantage Security en http://www.pscadvantage.com/spa/Paginas/Default.aspx. Todos estos servicios están sujetos a contratos específicos con Advantage Security. El cuadro 3 resume la oferta de servicios de la jerarquía de la Secretaría de Economía de Advantage Security.

Servicios de la Jerarquía de la Secretaría de Economía	*Explicación en las CP*	*Oferta de Advantage Security*
Servicios de Distribución de Certificados		
Certificados de Personas Físicas y Morales	Artículo 1.1.2.1.1 de las CP	Certificados Digitales Advantage Security
Otros documentos específicos de Advantage Security		
Servicios de Autenticación	Artículo 1.1.2.2.1 de las CP	Servicios de autenticación de proveedores externos (outsourced)
		Oficina de Servicio de Autenticación
Servicios de Estampilla de Tiempo	Artículo 1.1.2.2.2 de las CP	Servicios de Estampilla de Tiempo de Advantage Security

Cuadro 3 – Oferta de Servicios de VTN de Advantage Security

1.2.2.1 Servicios de Distribución del Certificado

1.2.2.1.1 Programa Afiliado de CA

Advantage Security es un Centro de Servicio como se describe en el artículo 1.1.2.1.2 de CP, lo cual significa que Advantage Security puede aprobar o rechazar Solicitudes de Certificados Digitales. Estos Centros de Servicio ("Centros de Servicio") llevan a cabo funciones de validación para aprobar o rechazar solicitudes de Certificados Digitales para Identificaciones de personas físicas o morales o de Certificados de Servidor. Advantage Security y CA son un "Centro de Procesamiento," como se describe en el artículo 1.1.2.1.2 de las CP, lo cual significa que Advantage Security y CA han establecido un alojamiento seguro para las instalaciones, entre otros, sistemas de AC/AR, incluyendo los módulos criptográficos que tienen las claves privadas que se usan para la emisión de Certificados. Advantage Security y CA fungen como una AC/AR en la jerarquía de la Secretaría de Economía y lleva a cabo todos los servicios de ciclo de vida del Certificado de emitir, administrar, revocar y renovar.

1.2.2.2 Servicios de Certificación de Valor Agregado

1.2.2.2.1 Servicios de Autenticación

Advantage Security le ofrece a las organizaciones servicios de autenticación de proveedores externos (outsourced) y servicios de la Oficina de Servicio de Autenticación, como se describen con más detalle en el artículo 1.1.2.2.1 de las CP. Con los servicios de autenticación de proveedores externos, Advantage Security confirma la identidad de los Solicitantes de Certificado en nombre de los Clientes. Puede que estos Clientes deseen obtener con proveedores externos la autenticación de toda o parte de su base de usuarios de Suscriptores. La prestación de servicios de autenticación por proveedores externos está sujeta a un contrato con Advantage Security.

En la medida en que Advantage Security conduzca ciertas actividades de autenticación para los Clientes, entonces Advantage Security estaría obligado a cumplir con las obligaciones de esta CPS del Cliente en su nombre. Sin embargo, el cumplimiento de dichas obligaciones no libera al Cliente de las obligaciones en la CPS, en la medida en que el retiene las responsabilidades de autenticación de partes de su base de usuario o de otras funciones, como iniciar solicitudes de revocación.

El programa de la Oficina de Servicio de Autenticación de Advantage Security permite que Advantage Security confirme la identidad de los Suscriptores usuarios finales en nombre de una organización ó persona física. Advantage Security le proporciona este servicio a organizaciones como los operadores de una red externa o mercado interempresarial (B2B) o B2C que celebra el contrato adecuado con Advantage Security para estos servicios ("Clientes de ADVANTAGE SECURITY "). Conforme al programa de Oficina de Servicio de Autenticación, Advantage Security ofrece Certificados individuales y de los representantes legales de organizaciones que interactúan con el Cliente de Advantage Security ("Certificados de Advantage Security Organizacionales Clase 2 ").

Ocasionalmente, Advantage Security puede tener subcontratos con otras entidades para proporcionar los servicios de autenticación de fuentes externas (outsourced) y de los servicios

de la Oficina de Servicio de Autenticación. Cuando Advantage Security celebra subcontratos para estos servicios, sus contratos con estos subcontratistas exigen que los subcontratistas cubran todos los requisitos de seguridad y otros que debería cubrir Advantage Security para proporcionar dichos servicios al tenor de esta CPS.

1.2.2.2.2 Servicio de Estampilla de Tiempo que ofrece Advantage Security

Advantage Security ofrece el "Servicio de Estampilla de Tiempo Advantage Security ," como se establece en el artículo 1.1.2.2.2 de las CP. La prestación de estos servicios de parte de Advantage Security está sujeta a los términos de los "Códigos de Prácticas de Autoridades de Estampilla de Tiempo".

1.3 Identificación

Este documento es la Declaración de Prácticas de Certificación de Advantage Security . Los Certificados de la jerarquía de la Secretaría de Economía contienen valores del identificador de objeto que corresponden a certificados Clase 2.

1.4 Comunidad y Aplicabilidad

La comunidad que rige esta CPS es el Subdominio de Advantage Security dentro de la jerarquía de la Secretaría de Economía. La jerarquía de la Secretaría de Economía es una infraestructura de claves públicas (PKI) que aloja una gran comunidad pública con diversas necesidades de comunicaciones e información segura. El Subdominio de Advantage Security es la parte de la jerarquía de la Secretaría de Economía que está regida por esta Declaración de Prácticas de Certificación, y esta última es el documento que rige el Subdominio de la jerarquía de la Secretaría de Economía de Advantage Security. La mayoría de los Participantes del Subdominio de Advantage Security de la jerarquía de la Secretaría de Economía se encuentran en México.

1.4.1 Prestadores de Servicios de Certificación

El término Prestadores de Servicios de Certificación (PSC) es un término general que se refiere a todas las entidades que emiten Certificados dentro de la jerarquía de la Secretaría de Economía.

Cada Prestador de Servicios de Certificación es una entidad que tiene derecho para emitir certificados dentro de la jerarquía de la Secretaría de Economía. En la actualidad hay un tipo de certificado que se puede emitir, certificados Clase 2 . Las PSC que emiten Certificados a Suscriptores están Subordinadas a las CP. Los recipientes de certificados dentro de la jerarquía de la Secretaría de Economía cae en tres categorías: (1) Advantage Security mismo, (2) los Agentes Certificadores de Advantage Security y (3) los Clientes de Advantage Security.

La Autoridad Certificadora (AC) y Autoridad Registradora (AR) de Advantage Security y CA lleva a cabo todas las funciones de la AC y AR. Los Clientes de designados como Agentes Certificadores (AgC) se convierten en un representante de Advantage Security que puede cumplir con parte del proceso de validación y aprobación de Advantage Security. Los Clientes AgC de Advantage Security hacen un contrato con Advantage Security y CA para llegar a ser AgC. No obstante, los Clientes AgC de Advantage Security obtienen de Advantage Security

todas las funciones frontales y de fondo, salvo la obligación de iniciar la revocación de Certificados emitidos por la AC del Cliente de Advantage Security, de acuerdo con el artículo 4.4.1.1 de la CPS.

1.4.2 Autoridades Registradoras

Dentro del Subdominio de Advantage Security de la jerarquía de la Secretaría de Economía, las AR cae en una categoría: (1) Advantage Security, en su papel de Proveedor de ADVANTAGE SECURITY y (2) los Agentes Certificadores de Advantage Security . Se permiten otros tipos de AR con el consentimiento por escrito por anticipado de Advantage Security, y si estas AR cumplen con las obligaciones que tienen los Clientes, sujetos a las modificaciones necesarias en virtud de las diferencias que existan entre la tecnología de Advantage Security y CA y la tecnología que usan estas AR y los términos de un contrato adecuado. Las AR ayudan a la AC al realizar funciones frontales de confirmación de la identidad, aprobación o rechazo de Solicitudes de Certificado, solicitudes de revocación de Certificados y aprobación o rechazo de solicitudes de renovación.

1.4.3 Entidades Finales

El cuadro 4 muestra los tipos de Suscriptores de cada Clase y tipo de Certificado que se ofrece Advantage Security como Prestador de Servicios de Certificación de la Secretaría de Economía

Clase	*Emitido a*	*Servicios bajo los cuales están disponibles los Certificados*	*Tipos de Suscriptores*
Clase 2	Personas Físicas	Usuarios	Cualquier persona, incluyendo a los miembros del público en general.
	Personas Morales	Representantes Legales	Organizaciones cuyas claves privadas están controladas por representantes autorizados de las organizaciones, en donde los procedimientos de autenticación han confirmado que dichos representantes tienen la facultad de fungir en nombre de sus organizaciones respectivas.
		Oficina de Servicio de Autenticación (Agentes Certificadores)	Representantes que funjen como Agentes Certificadores de Advantage Security.

Cuadro 4 – Tipos de Suscriptor es dentro del Subdominio de Advantage Security

1.4.4 Aplicabilidad

Esta CPS se aplica a todos los Participantes del Subdominio de Advantage Security , incluyendo Advantage Security , Clientes, Revendedores, Suscriptores y Partes que Confían. Esta CPS se aplica al Subdominio de Advantage Security de la jerarquía de la Secretaría de Economía y a la infraestructura central de Advantage Security que soporta a dicha jerarquía. Esta CPS describe las prácticas que rigen el uso de los Certificados dentro del Subdominio de Advantage Security

con certificados Clase 2 , como se describe en las CP. El certificado digital Clase 2 generalmente es el apropiado para usar con las aplicaciones que se indican en el artículo 1.3.4.1 de las CP y el artículo 1.1.1 de la CPS (cuadro 2). Sin embargo, por contrato o dentro de ambientes específicos (como un ambiente entre compañías), se les permite a los Participantes de la jerarquía de la Secretaría de Economía que usen Certificados para aplicaciones de mayor seguridad que las que se describen en el artículo 1.1.1, 1.3.4.1 de la CPS. Sin embargo, dicho uso estará limitado a esas entidades y sujeto al artículo 2.2.1.2, 2.2.2 de la CPS, y estas entidades serán responsables exclusivamente por el daño o responsabilidad que cause el mencionado uso.

1.4.4.1 Aplicaciones Adecuadas

Ver en el artículo 1.3.4.1 de las CP y el artículo 1.1.1 de la CPS (cuadro 2) las aplicaciones adecuadas. Sin embargo, estos listados no tienen el propósito de ser completos. Los Certificados Individuales y algunos Certificados organizacionales permiten que las Partes que Confían verifiquen las firmas digitales. Los Participantes del Subdominio de Advantage Security reconocen y convienen en que, en la medida en que lo permitan las leyes, cuando se necesite que una transacción sea por escrito, un mensaje u otro registro que lleve una firma digital verificable con referencia a un Certificado de la jerarquía de la Secretaría de Economía es válido, efectivo y exigible en un grado no inferior al grado que tendría si dicho mensaje o registro hubiera sido escrito y firmado en papel. Sujeta a las leyes aplicables, una firma digital o transacción que se lleve a cabo con referencia a un Certificado de la jerarquía de la Secretaría de Economía, será efectiva no importa la ubicación geográfica en la que se emita el Certificado de de la jerarquía de la Secretaría de Economía o se cree o use a firma digital, y no importa la ubicación geográfica del domicilio social de la AC o el Suscriptor.

1.4.4.2 Solicitudes Restringidas

En general, los Certificados de la jerarquía de la Secretaría de Economía son Certificados para fines múltiples. Los Certificados de la jerarquía de la Secretaría de Economía pueden usarse Globalmente y para interoperar con diversas Partes que Confían en todo el mundo. Este uso es permitido y los Clientes que utilizan Certificados dentro de su propio ambiente pueden ponerle más restricciones al uso del Certificado dentro de estos ambientes. Sin embargo, Advantage Security y otros Participantes del Subdominio de Advantage Security no son responsables de supervisar ni de hacer cumplir esas restricciones en estos ambientes.

No obstante, ciertos Certificados de la jerarquía de la Secretaría de Economía tienen una función limitada. Por ejemplo, no se pueden usar Certificados de AgC para ninguna función que no sean las funciones de AgC. Además, los Certificados del cliente son para solicitudes del cliente y no se usarán como Certificados de servidor ni organizacionales. Asimismo, los Certificados organizacionales Clase 2 que se emiten a los dispositivos tienen una función limitada para los servidores de la Web en los dispositivos de tráfico de la Web (si se trata de Identificaciones de Servidor Seguro e Identificaciones de Servidor Global) y la firma de objetos (si se trata de Certificados de firma de objetos). Por otra parte, los Certificados del Administrador sólo se usarán para llevar a cabo las funciones del Administrador.

Además, con respecto a los Certificados de la jerarquía de la Secretaría de Economía X.509 Versión 3, la extensión de uso de la clave tiene el fin de limitar los propósitos técnicos con respecto a los cuales una clave privada que corresponda a la clave pública de un Certificado,

puede usarse dentro de la jerarquía de la Secretaría de Economía. Ver el artículo 6.1.9 de las CP.

Asimismo, los Certificados del Suscriptor usuario final no se usarán como Certificados de AC. Esta restricción la confirma la ausencia de una extensión de Limitaciones Básicas. Ver el artículo 7.1.2.4 de las CP. Sin embargo, la eficacia de las limitaciones basadas en la extensión, está sujeta a la operación de software fabricado o controlado por entidades que no sean Advantage Security.

Más generalmente, los Certificados se usarán sólo en la medida en que el uso sea congruente con las leyes aplicables, y sobre todo, se usarán sólo en la medida en que lo permitan las leyes de exportación o importación aplicables.

1.4.4.3 Aplicaciones Prohibidas

Los Certificados de la jerarquía de la Secretaría de Economía no están diseñados, destinados ni autorizados para usarlos ni para revenderlos como equipo de control en circunstancias peligrosas, ni para usos que requieran desempeño a prueba de fallas, como la operación de instalaciones nucleares, sistemas de navegación o comunicación de aviones, sistemas de control de tráfico aéreo, o sistemas de control de armas, en donde una falla podría dar como resultado directamente la muerte, una lesión personal o un grave daño al ambiente.

1.5 Detalles del Contacto

1.5.1 Organización de la Administración de Especificaciones

La organización que administra esta CPS es el grupo de Desarrollo de Prácticas de Advantage Security . Las preguntas al grupo de Desarrollo de Prácticas de Advantage Security deben dirigirse como sigue:

Advantage Security, S. de R.L. de C.V.
Av. Prolongación Reforma 625, Desp. 402
Torre Lexus Paseo de las Lomas, Santa Fe
México, DF C.P. 01330

At'n: Desarrollo de Prácticas – CPS
Advantage Security
Teléfono: +52 55 50 814360
Fax: +52 55 50 81 43 67
contacto2@advantage-security.com

1.5.2 Contacto

Dirija las preguntas sobre la CPS a contacto2@advantage-security.com, o a la siguiente dirección:

Advantage Security, S. de R.L. de C.V.
Av. Prolongación Reforma 625, Desp. 402
Torre Lexus Paseo de las Lomas, Santa Fe
México, DF C.P. 01330
Attn: Practices Development – CPS
Teléfono: +52 55 50814360
Fax: +52 55 50814367
contacto2@advantage-security.com

2. Disposiciones Generales

2.1 Obligaciones

2.1.1 Obligaciones de la Autoridad Certificadora (AC)

Las AC llevan a cabo obligaciones específicas que aparecen a través de esta CPS. Estas disposiciones de la CPS especifican obligaciones de cada categoría de AC: Advantage Security (en su papel de Centro de Servicio) y Clientes de Advantage Security.

Asimismo, Advantage Security hace todo lo comercialmente razonable para garantizar que los Contratos del Suscriptor y los Contratos de la Parte que Confía obliguen a los Suscriptores ya las Partes que Confían dentro del Subdominio de Advantage Security. Ejemplos de este empeño son, de manera enunciativa y no limitativa, la exigencia de la aceptación de un Contrato del Suscriptor como condición de la inscripción o la exigencia de la aceptación de un Contrato de la Parte que Confía, como condición para recibir la información del estado del Certificado. De igual modo, los Revendedores (cuando así lo exija el contrato), deben utilizar los Contratos del Suscriptor y los Contratos de la Parte que Confía, de acuerdo con los requisitos que le imponga Advantage Security . Los Contratos del Suscriptor y los Contratos de la Parte que Confía son utilizados por Advantage Security , y los Revendedores deben incluir las disposiciones que exigen el artículo 2.22.4 de la CPS.

2.1.2 Obligaciones de la Autoridad Registradora (AR)

Las AR ayudan a un Centro de Procesamiento o AC del Centro de Servicio realizando funciones de validación, aprobando o rechazando Solicitudes de Certificado, solicitando la revocación de Certificados y aprobando solicitudes de renovación. Las disposiciones de la CPS especifican las obligaciones de cada categoría de AR: Clientes de certifiados de Agentes Certifiadores (AgC) y Advantage Security en su papel de Proveedor de servicios de AR.

Asimismo, Advantage Security , como Proveedor de Servicios AR, garantiza que los Contratos del Suscriptor y los Contratos de la Parte que Confía obliguen a los Suscriptores y a las Partes que Confían dentro de los Subdominio, de acuerdo con el artículo 2.1.1 de la CPS

.

2.1.3 Obligaciones del Suscriptor

Las obligaciones del Suscriptor en las CP se aplican a los Suscriptores dentro del Subdominio de Advantage Security, a través de esta CPS, mediante los Contratos del Suscriptor aprobados por Advantage Security y la Secretaría de Economía. Ciertos Contratos del Suscriptor en vigor dentro del Subdominio de Advantage Security aparecen en: https://ca.advantage-security.com/psceconomia/FRequestCertificate.aspx

Dentro del Subdominio de Advantage Security , los Contratos del Suscriptor requieren que los Solicitantes del Certificado ofrezcan información completa y precisa sobre sus Solicitudes de Certificado y manifiesten su consentimiento al Contrato del Suscriptor aplicable como condición para obtener un Certificado.

Los Contratos del Suscriptor aplican las obligaciones específicas que aparecen en las CP y en la CPS a los Suscriptores en el Subdominio de Advantage Security . Los Contratos del Suscriptor exigen que los Suscriptores usen sus Certificados de acuerdo con el artículo 1.3 de la CPS.

También exigen que los Suscriptores protejan sus claves privadas de acuerdo con el artículo 6.16.2, 6.4 de la CPS. Conforme a estos Contratos del Suscriptor, si un Suscriptor descubre o

tiene motivos para creer que ha habido un Compromiso de la Clave Privada del Suscriptor o de los datos de activación que protegen dicha Clave Privada, o la información del Certificado es incorrecta o ha cambiado, el Suscriptor de inmediato debe:

1) Notificar a la entidad que aprobó la Solicitud del Certificado del Suscriptor, ya sea la AC la AR, de acuerdo con el artículo 4.4.1.1 de la CPS y solicitar la revocación de la petición del Certificado de acuerdo con el artículo 3.4, 4.4.3.1 de la CPS.

2) Notificar a cualquier persona en la que el Suscriptor razonablemente espere confiar o a la que espere proporcionarle los servicios como apoyo del Certificado del Suscriptor o una firma digital verificable con referencia al Certificado del Suscriptor.

Los Contratos del Suscriptor exigen que los Suscriptores dejen de usar sus claves privadas al final de sus periodos de uso de la clave conforme al artículo 6.3.2 de la CPS.

2.1.4 Obligaciones de la Parte que Confía

Las obligaciones de la Parte que Confía en las CP se aplican a las Partes que Confían dentro del Subdominio de Advantage Security, a través de esta CPS, mediante los Contratos de la Parte que Confía de Advantage Security . Los Contratos de la Parte que Confía que están en vigor dentro del Subdominio de Advantage Security aparece en: https://ca.advantage-security.com/psceconomia/AcuerdoVerificador.pdf

Los acuerdos de suscriptor son las siguientes:

- Acuerdo de Suscriptor de Cliente
- Acuerdo Maestro de Servicios
- Acuerdo de Uso de Software

Los Contratos de la Parte que Confía dentro del Subdominio de Advantage Security declaran que antes de cualquier acto de confianza, las Partes que Confían deben evaluar independientemente la conveniencia de uso de un Certificado para cualquier fin determinado y decidir que el Certificado, de hecho, se usará para un fin adecuado. Declaran que las AC y AR de Advantage Security, no son responsables de evaluar la conveniencia de uso de un Certificado.

Los Contratos de la Parte que Confía declaran específicamente que las Partes que Confían no deben usar Certificados más allá de las limitaciones del artículo 1.3.4.2 de la CPS ni par a los fines prohibidos en el artículo 1.3.4.3 de la CPS.

Los Contratos de la Parte que Confía declaran, además, que las Partes que Confían deben utilizar el software y/o el hardware apropiado para realizar la verificación de la firma digital u otras operaciones criptográficas que desean realizar, como condición para confiar en los Certificados con respecto a cada una de estas operaciones. Dichas operaciones comprenden la identificación de una Cadena de Certificados y la verificación de las firmas digitales de todos los Certificados de la Cadena de Certificados. Conforme a estos Contratos, las Partes que Confían no deben confiar en un Certificado, a menos que estos procedimientos de verificación tengan éxito.

Los Contratos de la Parte que Confía también exigen que las Partes que Confían comprueben el estado de un Certificado en el que desean confiar, al igual que todos los Certificados de su Cadena de Certificados, de acuerdo con el artículo 4.4.10, 4.4.12 de la CPS. Si alguno de los Certificados de la Cadena de Certificados fue anulado, de acuerdo con los Contratos de la Parte que Confía, la Parte que Confía no debe confiar en el Certificado del Suscriptor del usuario final o en otro Certificado anulado de la Cadena de Certificados.

Finalmente, los Contratos de la Parte que Confía declaran que el consentimiento de sus términos es condición para usar o de otro modo confiar en los Certificados. Las Partes que Confían que también son Suscriptores convienen en estar obligadas por los términos de la Parte que Confía de este artículo, cláusulas de exclusión de garantías y limitaciones de responsabilidad cuando convienen en un Contrato del Suscriptor.

Los Contratos de la Parte que Confía declaran que si todas las verificaciones arriba descritas tienen éxito, la Parte que Confía tiene derecho de confiar en el Certificado, siempre y cuando la confianza en el Certificado sea razonable en las circunstancias. Si las circunstancias indican la necesidad de garantías adicionales, la Parte que Confía debe obtener dichas garantías para que la citada confianza se considere razonable.

Los Contratos de la Parte que Confía declaran que las Partes que Confían no deben supervisar, invertir, ni interferir con la ingeniería de la implementación técnica de la jerarquía de la Secretaría de Economía, salvo mediante previa aprobación por escrito de Advantage Security y la Secretaría de Economía, y de otro modo no comprometerá intencionalmente la seguridad de la jerarquía de la Secretaría de Economía

2.1.5 Obligaciones de Repositorio

Advantage Security es el responsable de las funciones de repositorio para sus propias AC y los Clientes de Advantage Security. Advantage Security publica los Certificados que emite en el repositorio que se establece en el cuadro 5, de acuerdo con el artículo 2.6 de la CPS.

AC	*Entidad que emite el Certificado en nombre de la AC*	*Repositorio aplicable*
Todas las AC de Advantage Security	Advantage Security	Repositorio de Advantage Security
El Cliente de Advantage Security	Advantage Security	Repositorio de Advantage Security

Cuadro 5 – Repositorios aplicables por tipo de CA

A la revocación del Certificado del Suscriptor de un usuario final, Advantage Security publica el aviso de dicha anulación en el repositorio que requiere el cuadro 5. Advantage Security emite CRLs para los Clientes de Advantage Security dentro de su Subdominio, de conformidad con el artículo 2.6, 4.4.9, 4.4.11 de la CPS. Asimismo, los Clientes pueden usar el protocolo del Estado del Certificado en Línea (“OCSP”, por sus siglas en inglés), Advantage Security presta servicios OCSP de conformidad con el artículo 2.6, 4.4.9, 4.4.11 de la CPS.

2.2 Responsabilidad

2.2.1 Responsabilidad de la Autoridad de Certificación

Las garantías, cláusulas de exclusión de garantía y limitaciones de garantía entre Advantage Security, los Revendedores y sus Clientes respectivos dentro del Subdominio de Advantage Security, se establecen en los contratos celebrados entre ellos y los rigen. Este artículo 2.2.1 de la CPS se relaciona sólo con las garantías que ciertas AC (Advantage Security) deben hacerle a los Suscriptores usuarios finales que reciben Certificados de ellos y a las Partes que Confían, las cláusulas de exclusión de garantías que deben hacerle a dichos Suscriptores y las Partes que Confían, y las limitaciones de responsabilidad que deben colocar en dichos Suscriptores y Partes que Confían. En virtud de que los Clientes de Advantage Security le encargan (outsource) todas las funciones frontales y de fondo a Advantage Security, los requisitos de garantía de esta sección no se aplican a los Clientes de Advantage Security.

Advantage Security utiliza y (cuando se requiere) los Revendedores deben usar los Contratos del Suscriptor y los Contratos de la Parte que Confía, de acuerdo con el artículo 2.1.1 de la CPS. No obstante Clientes de los Revendedores deben ser aprobados por un Agente certificador de Advantage Security y deben aceptar los términos y condiciones establecidos en el Contrato de Suscriptor de Cliente de Advantage Security. Los requisitos de que los contratos del Suscriptor contengan las siguientes garantías, cláusulas de exclusión de garantías y limitaciones de responsabilidad, se aplican a los Clientes y a los Revendedores que usan los Contratos del Suscriptor. Advantage Security se apega a dichos requisitos en sus Contratos del Suscriptor.

Las prácticas de Advantage Security relativas a las garantías, cláusulas de exclusión de garantía y limitaciones en los Contratos de la Parte que Confía, se aplican a Advantage Security . Observe que los términos aplicables a las Partes que Confían también se incluirán en los Contratos del Suscriptor, además de los Contratos de la Parte que Confía, pues los Suscriptores a menudo fungen también como Partes que Confían.

2.2.1.1 Garantías de la Autoridad Certificadora para los Suscriptores y las Partes que confían

Los Contratos del Suscriptor de Advantage Security comprenden, y otros Contratos del Suscriptor comprenderán, una garantía para los Suscriptores de que:

- No hay falsas declaraciones sustanciales de hecho en el Certificado que conozcan o se deriven de las entidades que aprueban la Solicitud del Certificado o emitan el Certificado;
- No hay errores en la información del Certificado que introdujeron las entidades que aprueban la Solicitud de Certificado o que emiten el Certificado, debido a que no se puso el debido cuidado en el manejo de la Solicitud del Certificado o la creación del Certificado;
- Sus Certificados cubren todos los requisitos sustanciales de esta CPS,
- Los servicios de revocación y el uso de un repositorio se conforman con esta CPS en todos los aspectos sustanciales.

Los Contratos de la Parte que Confía de Advantage Security contienen una garantía para las Partes que Confían razonablemente en un Certificado, de que:

- Toda la información que contiene dicho Certificado o que se incorpora en él mediante referencia, salvo por la Información del Suscriptor No Verificada, es exacta;

- Con respecto a los Certificados que aparecen en el repositorio de Advantage Security, que el Certificado fue emitido a la persona u organización que se nombre en el Certificado como Suscriptor, y que el Suscriptor ha aceptado el Certificado, de acuerdo con el artículo 4.3 de la CPS, y

- Que las entidades que aprueban la Solicitud de Certificado y emiten el Certificado han cumplido sustancialmente con esta CPS cuando emiten el Certificado.

2.2.1.2 Cláusulas de Exclusión de Garantías de la Autoridad de Certificación

En la medida en que lo permitan las leyes aplicables, los Contratos del Suscriptor de Advantage Security y los Contratos de la Parte que Confía desconocen, y otros Contratos del Suscriptor desconocerán, las posibles garantías de Advantage Security , incluyendo cualquier garantía de comerciabilidad o conveniencia para un fin en particular.

2.2.1.3 Limitaciones de Responsabilidad de la Autoridad de Certificación

En la medida en que lo permitan las leyes aplicables, los Contratos del Suscriptor de Advantage Security y los Contratos de la Parte que Confía limitan, y otros Contratos del Suscriptor limitarán, la responsabilidad de Advantage Security. Las limitaciones de responsabilidad incluyen la exclusión de daños indirectos, especiales, incidentales y consecuenciales. También comprenden las siguientes capacidades de responsabilidad que limitan los daños de Advantage Security relativos a un Certificado específico:

Clase	*Capacidades de responsabilidad*
Clase 2	Cien mil dólares de los Estados Unidos ($ 100,000.00 US)

Cuadro 6 – Capacidades de Responsabilidad

2.2.1.4 Fuerza Mayor

En la medida en que lo permitan las leyes, los Contratos del Suscriptor de Advantage Security y los Contratos de las Partes que Confían comprenden, y otros Contratos del Suscriptor comprenderán, una cláusula de fuerza mayor que va a proteger a Advantage Security.

2.2.2 Responsabilidad de la Autoridad de Registro

Las garantías, cláusulas de exclusión de garantía y las limitaciones de responsabilidad entre una AR y la AC a la que está ayudando a emitir Certificados, o el Revendedor aplicable, se exponen en los contratos que celebren entre ellas y están regidas por ellos. Advantage Security, en su papel de AR Proveedor de Advantage Security, utiliza los Contratos del Suscriptor y los Contratos de la Parte que Confía de acuerdo con el artículo 2.1.12.1.2 de la CPS, los cuales tienen sus propias garantías, cláusulas de exclusión y limitaciones.

2.2.3 Responsabilidad del Suscriptor

2.2.3.1 Garantías del Suscriptor

Los Contratos del Suscriptor de Advantage Security exigen que los Suscriptores garanticen que:

- Cada firma digital creada que usa la clave privada que corresponde a la clave pública que se anota en el Certificado es la firma digital del Suscriptor y el Certificado ha sido aceptado y está funcionando (no se venció ni revocó) en el momento en que se creó la firma digital.
- Ninguna persona no autorizada ha tenido alguna vez acceso a la clave privada del Suscriptor.
- Todas las declaraciones que haga el Suscriptor en la Solicitud de Certificado que presentó el Suscriptor, son verdaderas.
- Toda la información proporcionada por el Suscriptor y que se contiene en el Certificado, es verdadera.
- El Certificado se utiliza exclusivamente para los fines autorizados y legales, congruentes con esta CPS.
- El Suscriptor es el Suscriptor usuario final y no una CA, y no está usando la clave privada correspondiente a ninguna clave pública anotada en el Certificado, para fines de firmar digitalmente algún Certificado (o cualquier otro formato de clave pública certificada) o CRL, en calidad de AC o de otro modo.

Otros Contratos del Suscriptor también contendrán estos requisitos:

El usuario debe de generar su llave privada confidencialmente y en su propio dispositivo de hardware o software. No se permiten herramientas centralizadas de generación de llaves privadas ni el respaldo centralizado de los mismos.

2.2.3.2 Compromiso de la Clave Privada

Las CP establecen Normas de la jerarquía de la Secretaría de Economía para la protección de las claves privadas de los Suscriptores, las cuales se incluyen en virtud del artículo 6.2.7.1 de la CPS en los Contratos del Suscriptor. Estos contratos declaran que los Suscriptores que no cumplan con estas Normas de la jerarquía de la Secretaría de Economía son los únicos responsables por las pérdidas o daños que se originen de esa falta de cumplimiento.

2.2.4 Confiabilidad de la Parte que Confía

Los Contratos del Suscriptor y los Contratos de la Parte que Confía exigen que las Partes que Confían reconozcan que cuentan con información suficiente para tomar una decisión informada con respecto a la medida en que optan por confiar en la información de un Certificado, que son responsables únicamente por decidir si confían o no en esa información, y que se harán cargo de las consecuencias legales de su incumplimiento con las obligaciones de la Parte que Confía establecidas en el artículo 2.1.4 de la CPS.

2.3 Responsabilidad Financiera

2.3.1 Indemnización de parte de los Suscriptores y las Partes que Confían

2.3.1.1 Indemnización de parte de los Suscriptores

En la medida en que lo permitan las leyes aplicables, el Contrato del Suscriptor de Advantage Security exige, y otros Contratos del Suscriptor exigirán, que los Suscriptores indemnicen a Advantage Security y a cualquier AC o AR que no sea de Advantage Security por:

- Falsedad o declaración de hecho falsa por el Suscriptor sobre la Solicitud de Certificado del Suscriptor;
- Que el Suscriptor no divulgue un hecho substancial sobre la Solicitud de Certificado, si la declaración falsa u omisión se hizo en forma negligente o con el propósito de engañar a alguna parte;
- Que el Suscriptor no haya protegido su clave privada, usado un Sistema Confiable, o de otro modo, tomado las debidas precauciones para evitar el compromiso, pérdida, divulgación, modificación o uso autorizado de la clave privada del Suscriptor;
- Que el Suscriptor haya usado un nombre (incluyendo de manera enunciativa y no limitativa dentro de un nombre común, nombre de dominio o dirección de correo electrónico) que infrinja los Derechos de Propiedad Intelectual de un tercero.

2.3.1.2 Indemnización de parte de los que Confían

En la medida en que lo permitan las leyes aplicables, los Contratos del Suscriptor y los Contratos de la Parte que Confía de Advantage Security exigen, y otros Contratos del Suscriptor exigirán, que las Partes que Confían indemnicen a Advantage Security y a cualquier AC o AR que no sea de Advantage Security por:

- El incumplimiento de la Parte que Confía con las obligaciones de una Parte que Confía;
- La confianza de una Parte que Confía en un Certificado que razonablemente no sea acorde a las circunstancias, o
- El incumplimiento de la Parte que Confía con la verificación de la condición de dicho Certificado para determinar si el Certificado está vencido o anulado.

2.3.2 Relaciones Fiduciarias

En la medida en que lo permitan las leyes aplicables, los Contratos del Suscriptor y los Contratos de la Parte que Confía de Advantage Security desconocen, y otros Contratos del Suscriptor desconocerán, las relaciones fiduciarias que existan entre Advantage Security o una AC o AR que no sea de Advantage Security, por una parte, y un Suscriptor o Parte que Confía, por la otra.

2.3.3 Procesos Administrativos

Advantage Security contará con los recursos financieros suficientes para mantener sus operaciones y llevar a cabo sus deberes, y deben ser razonablemente capaces de soportar el riesgo de la responsabilidad para con los Suscriptores y las Partes que Confían. Los Clientes de de Advantage Security también mantendrá un nivel comercialmente razonable de cobertura de seguro por los errores y omisiones, ya sea a través de un programa de seguro de errores y

omisiones con una aseguradora o una retención para auto asegurados. Esta exigencia de seguro no se aplica a las entidades gubernamentales.

2.3.4 Algunas Responsabilidades Adicionales a las Partes

La presente cláusula establecerá de manera enunciativa más no limitativa algunas obligaciones adicionales relativas a las partes, e incluso de terceros que pudieran verse involucrados con el certificado que por medio del presente convenio se solicita de "ADVANTAGE SECURITY" S. DE R.L. DE C.V.

A) Obligaciones de la Autoridad Registradora (AR)

Las Autoridades Registradoras prestarán su colaboración con el Centro de Procesamiento realizando funciones de validación, aprobando o rechazando Solicitudes de Certificado, solicitando la revocación de Certificados y aprobando solicitudes de renovación.

B) Obligaciones del Suscriptor

Las obligaciones del Suscriptor serán aplicables a todos aquellos Suscriptores dentro del Subdominio de Advantage Security, mediante los Contratos del Suscriptor aprobados por Advantage Security y la Secretaría de Economía.

Dentro del Subdominio de Advantage Security, los Contratos del Suscriptor requieren que los Solicitantes del Certificado ofrezcan información completa y precisa sobre sus Solicitudes de Certificado y manifiesten su consentimiento al Contrato del Suscriptor aplicable como condición para obtener un Certificado.

A Los Contratos del Suscriptor y a los Suscriptores que soliciten un certificado al amparo del Subdominio de Advantage Security les son aplicables las obligaciones específicas que aparecen en la declaración de prácticas de certificación de "ADVANTAGE SECURITY, S. DE R.L. DE C.V."
Los Contratos del Suscriptor exigen que los Suscriptores usen sus Certificados de acuerdo con lo establecido en la mencionada declaración de prácticas de certificación, en donde entre otras obligaciones, se exigen que los Suscriptores protejan, resguarden y no publiquen o revelen a terceros sus claves privadas. Conforme a estos Contratos del Suscriptor, si un Suscriptor descubre o tiene motivos para creer que su Clave Privada del Suscriptor o de los datos de activación que protegen dicha Clave Privada, ha sido comprometida, o si la información del Certificado es incorrecta o ha cambiado, el Suscriptor de inmediato deberá:

Notificar a "ADVANTAGE SECURITY, S. DE R.L. DE C.V.", y solicitar la revocación de la petición del Certificado, asimismo deberá notificar a cualquier persona en la que el Suscriptor razonablemente espere confiar o a la que espere proporcionarle los servicios como apoyo del Certificado del Suscriptor o una firma digital verificable con referencia al Certificado del Suscriptor.

Los Contratos del Suscriptor exigen que los Suscriptores dejen de usar sus claves privadas al finalizar sus periodos de vigencia.

Los Contratos del Suscriptor declaran que los Suscriptores no supervisarán, interferirán con ni invertirán la ingeniería de la implementación técnica de la jerarquía de la Secretaría de Economía, salvo mediante aprobación previa por escrito de Advantage Security y la Secretaría de Economía, y de otro modo no comprometerá intencionalmente la seguridad de la jerarquía de la Secretaría de Economía.

C) Obligaciones de la Parte que Confía

Todas aquellos terceros que se involucren con los suscriptores que obtengan un certificado y que en virtud de dicho certificado consoliden una relación basada en la confiabilidad que representa dicho certificado serán denominados para efectos del presente convenio como “La Parte que confía”.

La Parte que Confía dentro del Subdominio de Advantage Security, antes de cualquier acto de confianza, deberán evaluar independientemente la conveniencia de uso de un Certificado para cualquier fin determinado y decidir que el Certificado, de hecho, se usará para un fin adecuado. Dichos terceros deberán estar conscientes de que las Autoridades Certificadoras y Advantage Security, no son responsables de evaluar la conveniencia de uso de un Certificado.

A fin de allegarse de información correcta, veraz atribuible y susceptible de verificarse las Partes que Confían deben de utilizar el software y/o el hardware apropiado para realizar la verificación de la firma digital u otras operaciones criptográficas que desean realizar, como condición para confiar en los Certificados con respecto a cada una de estas operaciones. Dichas operaciones comprenden la identificación de una Cadena de Certificados y la verificación de las firmas digitales de todos los Certificados de la Cadena de Certificados. Conforme a estos Contratos, las Partes que Confían no deben confiar en un Certificado, a menos que estos procedimientos de verificación tengan éxito.

Las Partes que Confían deberán comprobar el estado de un Certificado en el que desean confiar, al igual que todos los Certificados de su Cadena de Certificados. Si alguno de los Certificados de la Cadena de Certificados fue anulado, no deberán confiar en el Certificado del Suscriptor del usuario final o en otro Certificado anulado de la Cadena de Certificados.

Las Partes que Confían tienen derecho de confiar en el Certificado, siempre y cuando la confianza en el Certificado sea razonable en las circunstancias. Si las circunstancias indican la necesidad de garantías adicionales, la Parte que Confía debe obtener dichas garantías para que la citada confianza se considere razonable.

D) Garantías de la Autoridad Certificadora para los Suscriptores y las Partes que Confían

Los Contratos del Suscriptor de Advantage Security comprenden, y otros Contratos del Suscriptor comprenderán, una garantía para los Suscriptores de que:

- No hay falsas declaraciones sustanciales de hecho en el Certificado que conozcan o se deriven de las entidades que aprueban la Solicitud del Certificado o emitan el Certificado;

- No hay errores en la información del Certificado que introdujeron las entidades que aprueban la Solicitud de Certificado o que emiten el Certificado.

- Toda la información que contiene dicho Certificado o que se incorpora en él mediante referencia, salvo por la Información del Suscriptor No Verificada, es exacta;

- Con respecto a los Certificados que aparecen en el repositorio de Advantage Security , que el Certificado fue emitido a la persona u organización que se nombre en el Certificado como Suscriptor, y que el Suscriptor ha aceptado el Certificado.

11. LÍMITES DE RESPONSABILIDAD.

Esta cláusula se aplica a la responsabilidad al tenor del convenio (incluyendo la trasgresión de la garantía), agravio (incluyendo negligencia y/o estricta responsabilidad) y cualquier otra forma de reclamación legal o equitativa. Si se entabla alguna demanda, acción, litigio, arbitraje u otro tipo de proceso relativo a los servicios materia del presente Convenio del Suscriptor, la responsabilidad total de las Partes, estará limitada, en conjunto, a la siguiente suma:
CLASE Montos de Responsabilidad CDJSE $ 5,000.00 US. (moneda de curso legal en los estados unidos de América)

Los límites de responsabilidad que se establecen en esta cláusula serán los mismos, no importa el número de firmas digitales, transacciones o reclamaciones relacionadas con dicho certificado. Las Partes no estarán obligadas a pagar más de la limitación de responsabilidad total a la que se hace referencia en la presente cláusula.

2.4 Interpretación y Exigibilidad

2.4.1 Leyes que rigen

Sujetas a las limitaciones que se presenten en las leyes aplicables, las leyes de los Estados Unidos Mexicanos regirán la exigibilidad, interpretación y validez de esta CPS, a pesar de las disposiciones contractuales o de otra opción de leyes y sin la obligación de establecer un nexo comercial con los Estados Unidos Mexicanos. Se hace esta opción de leyes para garantizar procedimientos uniformes y la interpretación para todos los Participantes del Subdominio de Advantage Security, no importa en dónde estén ubicados.

Esta disposición de las leyes que rigen se aplica sólo a esta CPS. Los contratos que incorporan la CPS mediante referencia pueden tener sus propias disposiciones sobre las leyes que rigen, siempre y cuando este artículo 2.4.1 de la CPS rija la exigibilidad, interpretación y validez de los términos de la CPS por separado y aparte de las disposiciones restantes de dichos contratos, sujeta a las limitaciones que se presenten en las leyes aplicables.

Esta CPS está sujeta a las leyes, reglas, reglamentos, estatutos, decretos y órdenes, incluyendo de manera enunciativa y no limitativa, las restricciones sobre software de exportación o importación, hardware o información técnica.

2.4.2 Divisibilidad, Supervivencia, Fusión, Aviso

En la medida en que lo permitan las leyes aplicables, los Contratos del Suscriptor y los Contratos de la Parte que Confía de Advantage Security contienen, y otros Contratos del

Suscriptor contendrán, cláusulas de divisibilidad, supervivencia, fusión y aviso. Una cláusula de divisibilidad de un contrato evita que la determinación de invalidez o inexigibilidad de una cláusula del contrato deteriore el resto del contrato. Una cláusula de supervivencia especifica que las disposiciones de un contrato pueden continuar en vigor, a pesar de la rescisión o vencimiento del contrato. Una cláusula de fusión manifiesta que todos los entendimientos relativos al objeto de un contrato están incorporados en el contrato. Una cláusula de aviso de un contrato estipula la forma en que las partes se van a dar avisos entre sí. cláusula del contrato deteriore el resto del contrato. Una cláusula de supervivencia especifica que las disposiciones de un contrato pueden continuar en vigor, a pesar de la rescisión o vencimiento del contrato. Una cláusula de fusión manifiesta que todos los entendimientos relativos al objeto de un contrato están incorporados en el contrato. Una cláusula de aviso de un contrato estipula la forma en que las partes se van a dar avisos entre sí.

2.4.3 Procedimientos de Resolución de Conflictos

2.4.3.1 Conflictos que surjan entre Advantage Security y los Clientes

Los conflictos que surjan entre Advantage Security y uno de sus Clientes se resolverán de acuerdo con las disposiciones del contrato aplicable entre las partes

2.4.3.2 Conflictos con los Suscriptores Usuarios Finales y las Partes que Confían

En la medida en que lo permitan las leyes aplicables, los Contratos del Suscriptor y los Contratos de la Parte que Confía de Advantage Security contienen, y otros Contratos del Suscriptor contendrán, una cláusula de resolución de conflictos. La cláusula manifiesta que los procedimientos de resolución de conflictos exigen de un periodo de negociación mínimo de sesenta (60) días, seguido de la litigación en el Distrito Federal, cuando se trate de reclamantes que sean residentes mexicanos o, cuando se trate de los demás reclamantes, arbitraje administrado por la Cámara de Comercio Internacional (“CCI”), de acuerdo con las Reglas de CCI de Conciliación y Arbitraje.

2.5 Comisiones

2.5.1 Emisión de Certificado o Comisión de Renovación

Advantage Security tiene derecho de cobrarles a los Suscriptores usuarios finales por la emisión, administración y renovación de los Certificados.

2.5.2 Comisiones de Acceso del Certificado

Ni Advantage Security ni los Clientes cobran comisión como condición para hacer que un Certificado esté disponible en el repositorio o de otro modo hacer que los Certificados estén disponibles para las Partes que Confían.

2.5.3 Comisiones de Acceso de Información de Revocación o de Condición

Advantage Security no cobra comisión como condición para hacer que las CRL que exige el artículo 4.4.9 de la CPS estén disponibles en un repositorio o, de otro modo, estén disponibles para las Partes que Confían. Sin embargo, Advantage Security cobra una comisión por ofrecer CRL personalizado, servicios OCSP u otros servicios de revocación e información del estado, de valor agregado. Advantage Security no permite el acceso a la información de revocación, información del estado del Certificado, o la impresión de la hora en su repositorio, a terceros que proporcionen productos o servicios que utilicen dicho estado del Certificado, sin el previo consentimiento por escrito de Advantage Security.

2.5.4 Comisiones para otros Servicios, como la Información de Política

Advantage Security no cobra comisiones por el acceso a las CP ni a esta CPS. El uso que se haga para fines que no sean simplemente ver el documento, como su reproducción, redistribución, modificación o creación de trabajos derivados, está sujeto a un contrato de licencia con la entidad que posea los derechos de autor del documento.

2.5.5 Política de Reembolso

Advantage Security se apega y está detrás de prácticas y políticas rigurosas para emprender operaciones de certificación y emitir certificados. No obstante, si por alguna razón un suscriptor no está completamente satisfecho con el certificado que le emitieron, el suscriptor puede solicitar que Advantage Security anule el certificado dentro de los treinta (30) días siguientes a la emisión y le haga un reembolso al suscriptor. Después del periodo de treinta (30) días, un suscriptor puede solicitar que Advantage Security anule el certificado y haga un reembolso si Advantage Security ha violado una garantía u otra obligación substancial de conformidad con esta CPS en relación con el suscriptor o el certificado del suscriptor. Después de que Advantage Security anule el certificado del suscriptor, Advantage Security acreditará de inmediato la cuenta de la tarjeta de crédito del suscriptor (si se pagó el certificado con tarjeta de crédito), o de otro modo rembolsará al suscriptor con un cheque, por la suma total de las comisiones aplicables pagadas por el certificado. Para solicitar un reembolso, llame a servicio al cliente al 52 55 50 81 43 60. Esta política de reembolso no es un recurso exclusivo y no limita los otros recursos que puedan estar disponibles para los suscriptores.

2.6 Publicación y Repositorio

2.6.1 Publicación de Información de la CA

CA es el responsable de la función de repositorio con respecto a:

- Las Autoridades de Certificación Primaria Públicas de CA (PCA) y de las Autoridades de Certificación de Infraestructura/ Administrativas de CA (CA) que soportan a la jerarquía de la Secretaría de Economía, y
- Advantage Security es responsable de la función de repositorio de las AC de Infraestructura, Administrativos de Advantage Security , y
- Las AC de Advantage Security , las AC de los Clientes de managed PKI y las AC de los Clientes de Advantage Security que emiten Certificados dentro del Subdominio de la jerarquía de la Secretaría de Economía de Advantage Security .

Advantage Security publica cierta información de la AC en la sección de repositorio del sitio Web de Advantage Security en https://ca.advantage-security.com/pscEconomia/legal.html como se describe a continuación.

Advantage Security publica las CP la jerarquía de la Secretaría de Economía, esta CPS, los Contratos del Suscriptor y los Contratos de la Parte que Confía en la sección de repositorio del sitio Web de Advantage Security.

Advantage Security publica Certificados de acuerdo con el cuadro 7 siguiente.

Tipo de Certificado	*Requisitos de Publicación*
Los Certificados AC de la Secretaría de Economía	Están disponibles para las Partes que Confían a través de la inclusión en el software de explorador actual y como parte de la Cadena de Certificados que se pueden obtener con el Certificado del Suscriptor usuario final a través de las funciones de consulta que se describen a continuación.
Certificados de la AC emisora de Advantage Security	Están disponibles para las Partes que Confían como parte de la Cadena de Certificados que pueden obtenerse con el Certificado del Suscriptor usuario final a través de las funciones de consulta que se describen a continuación.
Certificados del Respondedor de OCSP	Están disponibles a través de la consulta del servidor https://ca.advantage-security.com/psceconomia/ocspresponder.cer
Certificados del Suscriptor Usuario Final	Están disponibles para las partes que confían a través de funciones de consulta en el repositorio de Advantage Security en: https://ca.advantage-security.com/psceconomia/FDownloadCertificate.aspx

Cuadro 7 – Requisitos de Publicación del Certificado

Advantage Security publica información del estado del Certificado de acuerdo con el artículo 4.4.11 de la CPS.

2.6.2 Frecuencia de la Publicación

Las actualizaciones de esta CPS se publican de acuerdo con el artículo 8 de las CPS. Las actualizaciones de los Contratos del Suscriptor y los Contratos de la Parte que Confía, se publican cuando es necesario. Los Certificados se publican cuando se expiden. La información del estado del Certificado se publica de acuerdo con el artículo 4.4.9 y 4.4.11 de la CPS.

2.6.3 Controles de Acceso

La información que se publica en la parte del repositorio del sitio Web de Advantage Security es información públicamente accesible. El acceso de sólo lectura a dicha información no tiene restricción. Advantage Security exige que las personas convengan en un Contrato de la Parte que Confía o Contrato de Uso de CRL como condición para acceder a los Certificados, la información del estado del Certificado o las CRL. Advantage Security ha implementado medidas de seguridad lógicas y físicas para evitar que las personas no autorizadas agreguen, supriman o modifiquen datos del repositorio.

2.6.4 Repositorios

Ver el artículo 2.1.5 de la CPS.

2.7 Auditoria de Cumplimiento

Se lleva a cabo una auditoria anual SAS 70 Tipo II, o una comparable de las operaciones del centro de datos de Advantage Security y CA y las operaciones de administración clave que soportan a los servicios de la AC y AR. Las AC de otras Prestadoras de Servicios de Certificación no se auditan específicamente como parte de la auditoria de las operaciones de Advantage Security.

Además de las auditorias de cumplimiento, Advantage Security tendrá derecho de realizar otras revisiones e investigaciones para garantizar la confiabilidad del Subdominio de de la jerarquía de la Secretaría de Economía de Advantage Security, el cual comprende de manera enunciativa y no limitativa:

- Advantage Security o su representante autorizado tendrán derecho, a su única y exclusiva discreción, a llevar a cabo en cualquier momento una "Auditoria/ Investigación Exigente" de sí mismo o de un Cliente, en caso de que Advantage Security o su representante autorizado tengan motivos para creer que la entidad auditada no ha logrado cumplir con las Normas de la jerarquía de la Secretaría de Economía, ha sufrido un incidente o Compromiso, o ha actuado o dejado de actuar, de modo que el incumplimiento de la entidad, el incidente o Compromiso, o la acción o falta de acción plantee una amenaza real o potencial a la seguridad o integridad de la jerarquía de la Secretaría de Economía.
- Advantage Security o su representante autorizado tendrá derecho de efectuar "Revisiones Suplementarias de la Administración de Riesgos" de sí mismo o de un Cliente después de descubrimientos incompletos o excepcionales de una Auditoria de Cumplimiento o como parte del proceso global de administración de riesgos en el curso ordinario de los negocios.

Advantage Security o su representante autorizado tendrán derecho de delegar la realización de estas auditorías, revisiones e investigaciones a un despacho de auditoría de terceros. Las entidades que están sujetas a una auditoria, revisión o investigación, colaborarán en forma razonable con Advantage Security y el personal que lleva a cabo la auditoria, revisión o investigación.

2.7.1 Frecuencia de la Auditoria de Cumplimiento de la Entidad

Las auditorias de cumplimiento se llevan a cabo anualmente para garantizar una operación continua y confiable.

2.7.2 Requisitos de la Identidad del Auditor

Las auditorias de cumplimiento de la AC de Advantage Security las lleva a cabo un despacho de contadores públicos que:

- Demuestra la pericia en tecnología de infraestructura de clave pública, herramientas y técnicas de seguridad de la información, auditoria de seguridad y la función de atestación de terceros, y
- Está acreditado por el Instituto Norteamericano de Contadores Públicos Certificados (AICPA, o sus siglas en inglés) o una entidad similar, el cual exige la posesión de una cierta serie de aptitudes, medidas de garantía de la calidad como

la revisión de iguales, las pruebas de competencia, las normas con respecto a la debida asignación del personal a los compromisos y los requisitos para la educación profesional continua.

2.7.3 Relación del Auditor con la Parte Auditada

Las auditorias de cumplimiento de las operaciones de Advantage Security las lleva a cabo un despacho de contadores públicos que es independiente de Advantage Security.

2.7.4 Temas que cubre la Auditoria

El alcance de la auditoria anual SAS 70 Tipo II de Advantage Security y CA o una auditoria comparable, comprende controles ambientales de la CA, operaciones de administración clave controles de la AC de Infraestructura/ Administrativa.

2.7.5 Medidas que se toman en virtud de Deficiencias

Con respecto a las auditorias de cumplimiento de las operaciones de Advantage Security y CA, las excepciones o deficiencias importantes que se identificaron durante la Auditoria de Cumplimiento darán como resultado la determinación de las acciones que deben realizarse. Esta determinación la toma la dirección de Advantage Security con el insumo que recibe del auditor La dirección de Advantage Security es la responsable de desarrollar e implementar un plan de acción correctivo. Si Advantage Security determina que dichas excepciones o deficiencias plantean una amenaza inmediata a la seguridad o integridad de la jerarquía de la Secretaría de Economía, se desarrollará un plan de acción correctivo en 30 días y se implementará dentro de un periodo comercialmente razonable. Con respecto a excepciones o deficiencias menos graves, la Dirección de Advantage Security y CA evaluará la importancia de dichos asuntos y determinará el curso de acción adecuado.

2.7.6 Comunicaciones de los Resultados

Los resultados de la auditoria de cumplimiento de las operaciones de Advantage Security pueden darse a conocer a discreción de la dirección de Advantage Security.

2.8 Confidencialidad y Privacidad

Advantage Security ha implantado una política de privacidad, que se encuentra en: (https://ca.advantage-security.com/psceconomia/GrupoAdvantageInformedePrivacidad.pdf), en cumplimiento con el artículo 2.8 de las CP.

2.8.1 Tipos de Información que debe mantenerse Confidencial y Privada

Los siguientes registros de Suscriptores, sujetos al artículo 2.8.2 de la CPS, se mantienen confidenciales y privados (“Información Confidencial/Privada”):

- Registros de solicitudes de CA, ya sean aprobadas o no;
- Registros de Solicitudes de Certificado (sujetas al artículo 2.8.2 de la CPS),
- Registros de Transacciones (tanto registros completos como el rastreo de auditorías de transacciones);

- Registros de rastreo de auditorías de la jerarquía de la Secretaría de Economía que crea o retiene Advantage Security , CA o un Cliente
- Los informes de auditoría de Advantage Security y CA creados por Advantage Security y CA o sus auditores respectivos (ya sean internos o públicos).
- Planeación de contingencia y planes de recuperación de desastres, y
- Medidas de seguridad que controlan las operaciones del hardware y software de Advantage Security y CA y la administración de servicios de Certificados y los servicios de inscripción designados.

2.8.2 Tipos de Información que no se considera Confidencial ni Privada

Los Participantes del Subdominio de Advantage Security reconocen que los Certificados, la revocación de Certificados y otra información del estado, el repositorio de Advantage Security la información contenida en ellos no se considera Información Confidencial/ Privada. La información que no se considere expresamente Confidencial/Privada de conformidad con el artículo 2.8.1 de la CPS, no se considerará ni confidencial ni privada. Esta sección está sujeta a las leyes de privacidad aplicable.

2.8.3 Divulgación de Información de Revocación/ Suspensión de Certificados

Ver el artículo 2.8.2 de la CPS.

2.8.4 Publicación a los Funcionarios Judiciales

Los Participantes del Subdominio de Advantage Security reconocen que Advantage Security tendrán derecho de divulgar la Información Confidencial/ Privada si, de buena fe, Advantage Security cree que es necesaria la divulgación en respuesta a las citaciones y órdenes de registro. Esta sección está sujeta a las leyes de privacidad aplicables.

2.8.5 Publicación en virtud de una Exhibición Civil

Los Participantes del Subdominio de Advantage Security reconocen que Advantage Security tendrá derecho de divulgar Información Confidencial/ Privada, de buena fe, si Advantage Security cree que la divulgación es necesaria en respuesta a un proceso judicial, administrativo legal de otra naturaleza durante el proceso de exhibición de un juicio civil o administrativo, como citaciones, interrogatorios, solicitudes de admisión y solicitudes de desahogo de pruebas. Esta sección está sujeta a leyes de privacidad aplicables.

2.8.6 Divulgación a Petición del Propietario

La política de privacidad de Advantage Security contiene disposiciones de política de privacidad que se relacionan con la divulgación de Información Confidencial/ Privada a la persona que se lo divulga a Advantage Security. Esta sección está sujeta a las leyes de privacidad aplicables.

2.9 Derechos de Propiedad Intelectual

La asignación de Derechos de Propiedad Intelectual entre los Participantes del Subdomino de Advantage Security que no sean los Suscriptores y las Partes que Confían, está regida por los contratos aplicables entre dichos Participantes del Subdomino de Advantage Security. Los

siguientes incisos del artículo 2.9 de la CPS se aplican a los Derechos de Propiedad Intelectual con respecto a los Suscriptores y a las Partes que Confían.

2.9.1 Derechos de Propiedad en los Certificados e Información de Revocación

Advantage Security tiene todos los Derechos de Propiedad Intelectual en los Certificados y la información de revocación que emiten. Advantage Security y los Clientes otorgan el permiso para reproducir y distribuir los Certificados en forma no exclusiva y libre de regalías, siempre y cuando se reproduzcan por completo y que el uso de Certificados se sujete al Contrato de la parte que Confía que viene como referencia en el Certificado. Advantage Security y los Clientes otorgarán el permiso de usar información de revocación para llevar a cabo funciones de la Parte que Confía sujetos al Contrato de Uso de CRL aplicable, el Contrato de la Parte que Confía o cualesquiera otros contratos aplicables.

2.9.2 Derechos de Propiedad en las CP

Los Participantes del Subdominio de Advantage Security reconocen que Advantage Security retiene los Derechos de Propiedad Intelectual en esta CPS.

2.9.3 Derechos de Propiedad en los Nombres

Un Solicitante de Certificado conserva todos los derechos que tiene (en su caso) si alguna marca registrada, marca de servicio o nombre comercial contenido en alguna Solicitud de Certificado y nombre distinguido dentro de cualquier Certificado emitido a dicho Solicitante de Certificado.

2.9.4 Derechos de Propiedad en las Claves y el Material Clave

Los pares de claves que corresponden a los Certificados de Advantage Security y a los Suscriptores usuarios finales, son propiedad de Advantage Security y los Suscriptores usuarios finales que son los Sujetos respectivos de estos Certificados, no importa el medio físico dentro del cual están almacenados y protegidos, y dichas personas retienen todos los Derechos de Propiedad Intelectual en estos pares de claves. A pesar de lo anterior, las claves públicas Raíz de CA y los Certificados Raíz que las contienen, incluyendo todas las claves públicas de la AC y los Certificados autofirmados, son propiedad de Advantage Security, el cual otorga la licencia a los fabricantes de software y hardware para reproducir dichos Certificados de raíz para poner copias en dispositivos de hardware o en software confiables. Finalmente, sin limitar la generalidad de lo anterior, las Acciones Secretas de una clave privada de la AC son propiedad de la AC, y ésta retiene el Derecho de Propiedad Intelectual de dichas Acciones Secretas.

3. Identificación y Autenticación

3.1 Registro Inicial

3.1.1 Tipos de Nombres

Los Certificados de la AC de Advantage Security contienen Nombres Distinguidos X.501 en los campos del Emisor y el Sujeto. Los Nombres Distinguidos de la AC de Advantage Security consisten en los elementos que se especifican en el Cuadro 8 siguiente:

Atributo	*Valor*

País (P) =	"Estados Unidos de México", o no se usa.
Organización (O) =	"Advantage Security S de RL de CV".
Unidad Organizacional (OU) =	Los Certificados de la AC de Advantage Security puede contener múltiples atributos de la OU. Estos atributos pueden contener uno o más de los siguientes: · Nombre de la AC · Jerarquía de la Secretaria de Economía · Una declaración que haga referencia al Contrato de la Parte que Confía que rija los términos de uso del Certificado, y · Un aviso de derechos de autor.
Estado o provincia (E) =	Distrito Federal
Localidad (L) =	México
Nombre Común (CN) =	Advantage Security

Cuadro 8 – Atributos del Nombre Distinguido en los Certificados de la AC

Los Certificados del Suscriptor usuario final contienen un nombre distinguido X.501 en el campo del nombre del Sujeto y consiste en los elementos que se especifican en el cuadro 9 siguiente.

Atributo	*Valor*
País (P) =	"MX"
Organización (O) =	El atributo de la organización se usa como sigue: · "Advantage Security S de RL de CV." para el Respondedor OCSP de Advantage Security y los Certificados individuales. · El nombre organizacional del Suscriptor para los Certificados del servidor de la Web. · No se usa para los Certificados de firma del código/ objeto.
Unidad Organizacional (OU) =	Los Certificados del Suscriptor usuario final de Advantage Security puede contener múltiples atributos de la OU. Estos atributos pueden contener uno o más de lo siguiente: · Unidad organizacional del Suscriptor (para los Certificados organizacionales) · Jerarquía de la Secretaria de Economía · Una declaración que haga referencia al Contrato de la Parte que Confía que rija los términos de uso del Certificado · Un aviso de derechos de autor · "Autenticado por Advantage Security " y "Miembro, Jerarquía de la Secretaria de Economía" en los Certificados cuyas solicitudes fueron autenticadas por Advantage Security · Texto para describir el tipo de Certificado.
Estado o Provincia (E) =	Indica el Estado o Provincia
Localidad (L) =	Indica la Localidad del Suscriptor

Nombre Común (NC) =	Este atributo comprende: · El nombre del Respondedor OCSP (para los Certificados del Respondedor OCSP) · Nombre del dominio (para Certificados del servidor de la Web) · Nombre de la organización (para los Certificados de firma del código/ objeto) · Nombre (para los Certificados individuales).
Dirección de correo electrónico (E) =	Dirección de correo electrónico para los Certificados individuales Clase 2.

Cuadro 9 – Atributos del Nombre Distinguido en los Certificados del Suscriptor Usuario Final

El elemento de Nombre Común (CN=) del nombre distinguido del Sujeto de los Certificados del Suscriptor usuario final se autentica cuando se trata de los Certificados Clase 2 .

- El valor del nombre común autenticado que se incluye en los nombres distinguidos del Sujeto del Certificado organizacional es un nombre de dominio (cuando se trata de Identificaciones del Servidor Seguro e Identificaciones del Servidor Global) o el nombre legal de la organización o unidad dentro de la organización.
- Sin embargo, el valor del nombre común autenticado incluido en el nombre distinguido del Sujeto del Certificado ADVANTAGE SECURITY Organizacional Clase 2 , es el nombre personal aceptado del representante organizacional autorizado para usar la clave privada de la organización y el elemento de la organización (O=) es el nombre legal de la organización
- El valor del nombre común que se incluye en el nombre distinguido del Sujeto de los Certificados individuales representa el nombre personal aceptado generalmente de la persona.

3.1.2 Necesidad de que los Nombres sean Significativos

Los Certificados del Suscriptor usuario final Clase 2 contienen nombres con semántica que se entiende comúnmente y que permite la determinación de la identidad de la persona o la organización que es el Sujeto del Certificado. No se permiten los seudónimos de los suscriptores usuarios finales (nombres que no sean el nombre verdadero personal o de la organización) en esos Certificados.

Se permite el uso de pseudónimos sólo para los Certificados del Suscriptor usuarios finales clase 2.

Los certificados de la AC de Advantage Security contienen nombres con semántica que se entiende comúnmente y permite la determinación de la identidad de la AC que es el Asunto del Certificado.

3.1.3 Singularidad de los Nombres

Advantage Security garantiza que los Nombres Distinguidos del Asunto son únicos dentro del dominio de una AC específica a través de elementos automatizados del proceso de inscripción del Suscriptor.

3.1.4 Procedimiento de Resolución de Conflictos por Reclamaciones de Nombres.

Se prohíbe que los Solicitantes de Certificado usen nombres en sus Solicitudes de Certificado que infrinjan los Derechos de Propiedad Intelectual de otros. Sin embargo, Advantage Security no verifica si un Solicitante de Certificado tiene Derechos de Propiedad Intelectual con el nombre que aparece en la Solicitud de Certificado, ni arbitra, media o de otro modo resuelve algún conflicto relativo a la propiedad de algún nombre de dominio, nombre comercial, marca registrada o marca de servicio. Advantage Security tiene derecho, sin responsabilidad ante ningún Solicitante de Certificado, de rechazar o suspender cualquier Solicitud de Certificado en virtud de tal conflicto.

3.1.5 Registro, Autenticación y Marcas Registradas

Ver el artículo 3.1.4 de la CPS.

3.1.6 Método para comprobar la posesión llave privada

Advantage Security verifica la posesión de parte del Solicitante del Certificado de una clave privada, a través del uso de una petición de certificado firmada digitalmente, de conformidad con el estándar PKCS #10, otra demostración equivalente criptográficamente, u otro método aprobado por Advantage Security.

Cuando Advantage Security genera un par de claves en nombre de un Suscriptor (por ejemplo, cuando se colocan claves pregeneradas en tarjetas inteligentes), este requisito no es aplicable.

3.1.7 Autenticación de la Identidad de la Organización

Advantage Security confirma la identidad de los Suscriptores usuarios finales organizacionales Clase 2 y otro tipo de información de inscripción que se le proporcione a los Solicitantes de Certificado (salvo por la Información del Suscriptor no verificada), de acuerdo con los procedimientos que se establecen en los incisos que siguen. Además de los siguientes procedimientos, el Solicitante del Certificado debe demostrar que tiene legalmente la clave privada que le corresponde al a clave pública que se va a anotar en el Certificado, de acuerdo con el artículo 3.1.6 de la CPS.

3.1.7.1 Autenticación de la Identidad de los Suscriptores Usuarios finales Organizacionales

3.1.7.1.1 Autenticación de los certificados digitales al Menudeo

Advantage Security confirma la identidad de un Solicitante de Certificado de un Certificado de persona moral, mediante:

- La verificación de que existe la organización, a través del uso de por lo menos un servicio de comprobación de la identidad de un tercero o base de datos o, alternativamente, de documentación organizacional emitida por, o presentada ante, el gobierno de los Estados Unidos de México que confirme la existencia de la organización, y
- Presencia física del solicitante ante un Agente Certificador de Advantage Security , y
- La confirmación con el contacto organizacional adecuado por teléfono, correo o un procedimiento comparable de cierta información sobre la organización, de que la

organización ha autorizado la Solicitud de Certificado y que la persona que presenta la Solicitud de Certificado en nombre de la Organización está autorizada para hacerlo.

Se realizan procedimientos adicionales con respecto a tipos específicos de Certificados, como se describe en el siguiente cuadro 10.

Tipo de Certificado	*Procedimientos Adicionales*
Certificados de todos los Servidores	Advantage Security verifica que el Solicitante del Certificado sea el propietario registrado del nombre de dominio del servidor que es el Sujeto del Certificado, o que de otro modo esté autorizado para usar el dominio.
Certificados Advantage Security de Persona Moral Clase 2	Advantage Security confirma con el contacto organizacional adecuado por teléfono, correo o un procedimiento comparable: · el empleo del representante que presenta la Solicitud de Certificado en nombre del Solicitante de Certificado, y · Presencia física del solicitante ante un Agente Certificador de Advantage Security , y · la facultad del representante para actuar en nombre del Solicitante del Certificado. Advantage Security confirma con el representante del Solicitante del Certificado por teléfono, correo y/o un procedimiento comparable, que la persona nombrada como representante ha presentado la Solicitud de Certificado.

Cuadro 10 – Procedimientos de Autenticación Específicos

3.1.7.1.2 Autenticación de los Certificados Advantage Security de Persona Moral Clase 2

Los servicios de Advantage Security como Proveedor de Certificados Digitales de la Jerarquía de la Secretaría de Economía comprenden los siguientes pasos para confirmar la identidad de un Solicitante de Certificado para el Certificado Advantage Security Organizacional Clase 2:

La determinación de que la organización existe usando por lo menos un servicio de comprobación de la identidad de terceros o base de datos, o alternativamente, documentación organizacional emitida por el gobierno aplicable o presentada ante éste, que confirme la existencia de la organización;

- La confirmación por teléfono, correo confirmatorio y/o procedimiento comparable para el Solicitante del Certificado para confirmar cierta información sobre la organización, confirmar que la organización ha autorizado la Solicitud de Certificado, confirmar el empleo de un representante que presenta la Solicitud de Certificado en nombre del Solicitante de Certificado, y confirmar la autoridad del representante para fungir en nombre del Solicitante del Certificado, y
- Una confirmación por teléfono, correo confirmatorio y/o procedimiento comparable para el representante del Solicitante del Certificado para confirmar que la persona nombrada como representante ha presentado la Solicitud de Certificado.

Advantage Security puede subcontratar dichos servicios, siempre y cuando el subcontratista cubra estos requisitos, y todos los demás requisitos que imponga Advantage Security cuando lleve a cabo estos servicios de conformidad con la CPS.

3.1.7.2 Autenticación de la identidad de los Agentes Certificadores

Con respecto a las Solicitudes de Certificado de Agentes certificadores (AgC) de Advantage Security, el personal autorizado de éste crea, procesa y aprueba peticiones de certificado usando un proceso controlado que requiere de la participación de múltiples empleados de confianza de Advantage Security.

Los Agentes Certificadores y Advantage Security celebran contratos antes de llegar a ser AgC. Advantage Security autentica la identidad de AgCs antes de la aprobación final de su estado como AgC, llevando a cabo las revisiones necesarias para la confirmación de la identidad de los Suscriptores usuarios finales organizacionales que se indican en el artículo 3.1.8.1 de la CPS, salvo que en lugar de una Solicitud de Certificado, se hace la validación de una solicitud para que llegue a ser AgC de Advantage Security. Asimismo, cuando se trata de AgCs, Advantage Security confirma que la persona identificada como Agente Autorizado está autorizada para fungir en esa capacidad. Opcionalmente, Advantage Security puede exigir la comparecencia personal de un representante autorizado de la organización ante el personal autorizado de Advantage Security.

En algunos casos, Advantage Security puede delegar la responsabilidad por la autenticación de un Cliente potencial de Advantage Security, a un tercero confiable, tal como un Corredor Público o Notario. El procedimiento de los Corredores Públicos o Notarios para la autenticación de dicha identidad organizacional debe presentarse a la aprobación de Advantage Security y la Secretaría de Economía, y dicha aprobación es condición para que un Corredor Público o Notario inicie sus operaciones como proveedor de los servicios de la Oficina de Servicios de Autenticación, como fuere el caso. Dichos procedimientos deben cubrir los requisitos que se especifican en el párrafo anterior.

3.1.8 Autenticación de la identidad individual

Con respecto a los Certificados individuales Clase 2, Advantage Security (en nombre de su propia AC) y el Agente Certificador confirma que:

El Solicitante del Certificado es la persona identificada en la Solicitud del Certificado.

El Solicitante del Certificado posee legalmente la clave privada que le corresponde a la clave pública que se va a anotar en el Certificado, de acuerdo con el artículo 3.1.6 de la CPS, y

La información que se va a incluir en el Certificado es precisa.

Asimismo, Advantage Security lleva a cabo los procedimientos más detallados que se describen a continuación para Certificados Clase 2.

3.1.8.1 Certificados Individuales Clase 2

3.1.8.1.1 Certificados Individuales Clase 2

La autenticación de las Solicitudes de Certificados Individuales Clase 2, se basa en la presencia personal (física) del Solicitante de Certificado ante un representante autorizado (Agente

Certificador) de Advantage Security , notario o corredor público u otro funcionario con autoridad comparable dentro de la jurisdicción del Solicitante de Certificado. El agente, notario, corredor público u otro funcionario, aprobado por Advantage Security, verifica la identidad del Solicitante de Certificado contra una forma bien reconocida de identificación emitida por el gobierno de los Estados Unidos de México, como un pasaporte, CURP, credencial IFE o Pasaporte y otra credencial de identificación.

3.1.8.1.2 Certificados del Agente Certificador Clase 2

Se usan varios Certificados del Administrador para controlar el acceso a los sistemas de AC y AR de Advantage Security y para autorizar ciertas acciones dentro de la jerarquía de la Secretaría de Economía. Los tipos específicos de Certificados del Administrador Clase 2 se anotan en el artículo 1.3.1 de la CPS.

Advantage Security autentica las Solicitudes de Certificado del Administrador Clase 2 para los Agentes Certificadores (AgCs):

- Advantage Security autentica la existencia e identidad de la entidad que emplea o tiene al Agente Certificador, de conformidad con el artículo 3.1.8.1.2 de la CPS.
- Advantage Security confirma el empleo y la autorización de la persona llamada Agente Certificador en la Solicitud del Certificado para fungir como Administrador

Advantage Security también aprueba las Solicitudes de Certificado para sus propios Agentes

Certificadores y Administradores. Éstos son “Personas de Confianza” dentro de su organización respectiva (ver el artículo 5.2.1 de la CPS). En este caso, la autenticación de sus Solicitudes de Certificado se basa en la confirmación de su identidad, con respecto a su empleo o retención como contratista independiente (ver el artículo 5.2.3 de la CPS), procedimientos de verificación de los antecedentes (ver el artículo 5.3.2 de la CPS), y autorización para fungir como Administrador.

3.2 Nueva Clave y Renovación de Rutina

Antes de que se venza un Certificado del Suscriptor existente, es necesario que el Suscriptor obtenga un nuevo certificado para mantener la continuidad del uso del Certificado. Advantage Security exige, por lo general, que el Suscriptor genere un nuevo par de claves para sustituir al par de claves que se vence (lo que se define técnicamente como “reposición de clave”). No obstante, en algunos casos (es decir, cuando se trata de certificados de servidor Web), Advantage Security permite que los Suscriptores soliciten un certificado nuevo para un par de claves existente (que se define técnicamente como “renovación”). El cuadro 11 siguiente describe los requisitos de Advantage Security para la renovación de la clave de rutina (la emisión de un certificado nuevo para un nuevo par de claves que sustituye a un par de claves existente) y la renovación (emisión de un nuevo certificado para un par de claves existentes).

Hablando en general, tanto “Reposición de Clave” como “Renovación” se describen comúnmente como “Renovación del Certificado”, concentrándose en el hecho de que el Certificado antiguo se está sustituyendo por un nuevo Certificado y no dando énfasis en si se genera o no un nuevo par de claves. Esta distinción no es importante con respecto a todas las Clases y Tipos de Certificados de Advantage Security, salvo por los Certificados de Servidor

Clase 2 , pues siempre se genera un nuevo par de claves como parte del proceso de sustitución del Certificado del Suscriptor usuario final de Advantage Security .

Sin embargo, con respecto a los Certificados de Servidor Clase 2, debido a que le par de claves se genera en el servidor de la Web y la mayoría de las herramientas de generación de claves del servidor Web permiten la creación de una nueva Petición de Certificado con respecto a un par de claves existente, hay una distinción entre “reposición de clave” y “renovación”.

Clase y Tipo de Certificado	*Requisitos de Reposición de Clave y Renovación de Rutina*
Certificados Clase 2 y del Agente Certificador Clase 2	Para este tipo de Certificados, los pares de claves del Suscriptor las genera el navegador como parte del proceso de inscripción en línea. El Suscriptor no tiene la opción de presentar un par de claves existente para “renovación”. De conformidad, para estos tipos de Certificados, la renovación de la clave está soportada y la renovación del Certificado.
Certificados de Servidor Clase 3	Con respecto a las Identificaciones del Servidor, los pares de claves del Suscriptor se generan fuera del proceso de inscripción en línea (es decir, se generan en un servidor de Web). La mayoría de las herramientas de generación de claves del servidor, permite que el Suscriptor cree una nueva Petición de Firma de Certificado (CSR) con relación a un par de claves usado con anterioridad. De conformidad, con respecto a las Identificaciones del Servidor Seguro y las Identificaciones del Servidor Global, tanto la reposición de la clave como la renovación del Certificado están soportadas.

Cuadro 11 – Requisitos de Reposición de la Clave y de Renovación de Rutina

3.2.1 Reposición de la Clave y Renovación de Rutina para los Certificados del Suscriptor Usuario Final.

Los Certificados del Suscriptor que no se hayan revocado, se pueden sustituir (es decir, reponer la clave o renovar), de acuerdo con el cuadro 12 siguiente:

Programación	*Requisito*

Dentro de los 30 días anteriores y los 30 días posteriores al vencimiento del Certificado	Con respecto a los Certificados de Advantage Security , Advantage Security autentica a los Suscriptores, buscando la sustitución del Certificado mediante el uso de la Frase de Desafío. Como parte del proceso de registro inicial, los Suscriptores eligen y presentan una Frase de Desafío con su información de inscripción. Al reponer una clave o renovar un Certificado dentro de un periodo específico, si un Suscriptor presenta correctamente la Frase de Desafío del Suscriptor con la información de reinscripción del Suscriptor, y la información de inscripción (que no sea la información del contacto) no ha cambiado, se emite automáticamente un nuevo Certificado. Después de hacer una reposición de clave o renovación de este modo, y en casos por lo menos alternativos de reposición de clave o renovación posterior, la AC o la AR reconfirmará la identidad del Suscriptor, de acuerdo con los requisitos que se indican en el artículo 3.1.8.1 de la CPS o la autenticación de una Solicitud de Certificado original. La autenticación de una petición para sustituir un Certificado Advantage Security de persona moral Clase 2 , exige el uso de una Frase de Desafío, al igual que de procedimientos de autenticación con respecto a una Solicitud de Certificado original, de conformidad con el artículo 3.1.8.1.2 de la CPS.
Después de 30 días del vencimiento del Certificado	En este caso, los requisitos que se indican en el artículo 3.1.8.1 de la CPS para la autenticación de una Solicitud de Certificado original, se usan para sustituir el Certificado del Suscriptor usuario final. Para la autenticación de una petición para sustituir un Certificado Advantage Security de persona moral Clase 2 , es necesario usar una Frase de Desafío, al igual que procedimientos de autenticación con respecto a una Solicitud de Certificado original, conforme al artículo 3.1.8.1.2 de la CPS.

Cuadro 12 – Requisitos de Reposición de Clave y Renovación de Rutina para los Certificados del Suscriptor Usuario Final

3.3 Reposición de la Clave y Renovación de Rutina para los Certificados del Suscriptor Usuario Final.

No se permite la reposición de claves después de la revocación, si:

- La revocación se debió a que el Certificado, se emitió a una persona que no es la que se nombra como Asunto del Certificado;
- El Certificado, se emitió sin la autorización de la persona nombrada Asunto de dicho Certificado, o
- La entidad que aprueba la Solicitud del Certificado del Suscriptor, descubre o tiene motivos para creer que un hecho substancial de la Solicitud del Certificado es falso.

Sujeto al inciso anterior, los Certificados del Suscriptor, que han sido revocados, se pueden sustituir (es decir, reponer la clave de acuerdo con el cuadro 13 siguiente).

Programación	*Requisito*

Antes de que venza el Certificado	Para la sustitución de un Certificado de persona moral o física después de la revocación del Certificado, Advantage Security verifica que la persona que busca la sustitución del certificado sea, de hecho, el Suscriptor (si son personas físicas) o un representante legal autorizado (si son de persona moral), mediante el uso de una Frase de Desafió, como se describe en el artículo 3.2.1 de la CPS. Además de este procedimiento, se utilizan los requisitos para la validación de una Solicitud de Certificado original en el artículo 3.1.8.1de la CPS, para sustituir un Certificado después de la revocación. Dichos Certificados contienen el mismo nombre distinguido del Asunto que el nombre distinguido del Certificado que se está sustituyendo. La autenticación de una petición para sustituir un Certificado Advantage Security de persona moral Clase 2 , exige el uso de una Frase de Desafío, al igual que los procedimientos de autenticación de una Solicitud de Certificado original, de conformidad con el artículo 3.1.8.1.2 de la CPS.
Después del vencimiento del Certificado	En este caso, los requisitos que se indican en el artículo 3.1.8.1 de la CPS para la autenticación de una Solicitud de Certificado original, se usará para sustituir un Certificado del Suscriptor usuario final. La autenticación de un petición para sustituir un Certificado Advantage Security de persona moral Clase 2 , exige el uso de una Frase de Desafío, al igual que de procedimientos de autenticación para una Solicitud de Certificado original, conforme al artículo 3.1.8.1.2 de la CPS.

Cuadro 13 – Requisitos de Sustitución del Certificado después de la Revocación

3.4 Petición de Revocación

Antes de la revocación de un Certificado, Advantage Security verifica que la revocación haya sido pedida por el Suscriptor del Certificado, la entidad que aprobó la Solicitud de Certificado. Entre los procedimientos aceptables para autenticar las peticiones de revocación del suscriptor, se encuentran

- Hacer que el Suscriptor presente la Frase de Desafío del Suscriptor y revoque el Certificado automáticamente si corresponde a la Frase de Desafío que está en el registro
- Comunicación con el Suscriptor en donde se proporcionen garantías razonables a la luz de la Clase de Certificado que la persona u organización que pide la revocación es, en realidad, el Suscriptor. Dependiendo de las circunstancias, dicha comunicación puede comprender uno o más de los medios siguientes: teléfono, fax, correo electrónico, correo postal o servicio de mensajería.

Los Administradores de Advantage Security tienen derecho de pedir la revocación de los Certificados del Suscriptor usuario final dentro del Subdominio de Advantage Security. La identidad de los Administradores se autentican a Advantage Security mediante el control de acceso, usando SSL y autenticación del cliente antes de permitir que lleven a cabo funciones de revocación.

3.5 Requisitos de Documentos Presentados

Para la identificación física de los aspirantes a los certificados digitales, en presencia física de las Entidades de Registro deberán presentar documentos vigentes en copia y original de:

- Credencial para Votar (IFE)
- Pasaporte
- Cedula Profesional
- Cartilla Militar.

4. Requisitos de Operación

4.1 Solicitud del Certificado

4.1.1 Solicitudes de Certificado para los Certificados de los Suscriptores Usuarios Finales

Con respecto a los Certificados de Advantage Security, todos los Solicitantes de Certificado que sean usuarios finales pasarán por un proceso de inscripción, que consiste en:

- Llenar una Solicitud de Certificado y dar la información requerida;
- Generar o encargarse de que se haya generado un par de claves de acuerdo con el artículo 6.1 de la CPS;
- El Solicitante de Certificado entrega su clave pública, directamente o a través de un Agente Certificador autorizado, a Advantage Security, de acuerdo con el artículo 6.1.3 de la CPS;
- Demostrar a Advantage Security de acuerdo con el artículo 3.1.6 de la CPS que el Solicitante del Certificado posee la clave privada que le corresponde a la clave pública entregada a Advantage Security , y
- Manifestar su consentimiento al Contrato del Suscriptor pertinente.

La entidad que procesa la Solicitud de Certificado y la entidad que emite el Certificado, de acuerdo con el artículo 4.2 de la CPS, pueden ser dos entidades distintas, como se muestra en el cuadro siguiente.

Clase/Categoría de Certificado	*Entidad que procesa las Solicitudes de Certificado*	*Entidad que emite el Certificado*
Certificado de persona Física Clase 2	Advantage Security	Advantage Security
Certificado de Persona Moral Clase 2	Advantage Security	Advantage Security
Certificados de Agente Certificador Clase 2	Advantage Security}	Advantage Security
Certificado de Servidor Clase 2	Advantage Security, como Proveedor de ADVANTAGE SECURITY	Advantage Security
Certificados del Empleado de la AC de Advantage Security Clase 2	Advantage Security	Advantage Security

Cuadro 14 – Entidades que reciben las Solicitudes de Certificado

4.1.2 Solicitudes de Certificados de la AC, AR, Infraestructura y Empleado

4.1.2.1 Certificados de la Autoridad Registradora

Advantage Security opera una AC administrativa, que puede emitir certificados a las AR y los sistemas de las AR, incluyendo:

- El personal de Advantage Security (los Administradores de la AR de Advantage Security) que procesa Solicitudes de Certificado en nombre de la AC de Advantage Security.
- Los servidores de la Administración Automatizada, que procesan las Solicitudes de Certificado para los Agentes Certificadores, tal como los corredores públicos o notarios

Con respecto a estas AR, como suscriptores de la AC Administrativa pertinente, se aplican los requisitos para los Certificados del Administrador Clase 2 indicados en el artículo 4.1.1 de la CPS.

4.1.2.2 Certificados de Infraestructura

Advantage Security también opera varias AC de Infraestructura, que emiten Certificados a los componentes de la infraestructura de Advantage Security (por ejemplo, los Respondedores OCSP que proporcionan información del estado del Certificado).

4.1.2.3 Certificados del Empleado de Advantage Security.

Advantage Security emite certificados Clase 2 a sus empleados después de la presentación exitosa y procesamiento de una Solicitud de Certificado.

4.2 Emisión de Certificado

4.2.1 Emisión de Certificados del Suscriptor Usuario Final

Después de que un Solicitante de Certificado presenta una Solicitud de Certificado, Advantage Security intenta confirmar la información de la Solicitud de Certificado (que no sea la Información del Suscriptor no Verificada), de conformidad con el artículo 3.1.8.1 de la CPS. Cuando se han llevado a cabo exitosamente todos los procedimientos de autenticación necesarios de acuerdo con el artículo 3.1 de la CPS, Advantage Security aprueba la Solicitud de Certificado. Si la autenticación no tiene éxito, Advantage Security rechaza la Solicitud del Certificado y la notificación de rechazo se manda por correo electrónico a la dirección que especificó el usuario durante su solicitud original

Se crea y se emite un Certificado después de la aprobación de una Solicitud de Certificado o después de la recepción de una petición de la AR para emitir el Certificado. Advantage Security crea y le emite a un Solicitante de Certificado, uno que se base en la información de una Aprobación de Certificado después de la aprobación de la mencionada Solicitud de Certificado. Cuando un Agente Certificador de un tercero autorizado verifica una Solicitud de Certificado y le comunica la verificación a Advantage Security, este último aprueba la Solicitud de Certificado y genera un Certificado y se lo emite al Solicitante de Certificado. Los

procedimientos de esta sección también se usan para la emisión de Certificados, con relación a la presentación de una petición para sustituir (es decir, renovar o reemplazar la clave) un Certificado. Los correos de notificación de confirmación, aprobación o rechazo de mandan al correo que ingresa el cliente en el formulario de solicitud de certificado digital.

4.2.2 Emisión de Certificados de AR e Infraestructura

Advantage Security autentica la identidad de las entidades que deseen ser Clientes, de acuerdo con el artículo 3.1.8.2 de la CPS y en cuanto se aprueba, emite los Certificados necesarios para llevar a cabo sus funciones de AR. Antes de que Advantage Security celebre un contrato con el Cliente solicitante conforme al artículo 4.1.2 de la CPS, la identidad del Cliente potencial se confirma con base en las credenciales presentadas y la presencia física. La celebración de dicho contrato indica la aprobación final y total de la solicitud de parte de Advantage Security . La decisión de aprobar o rechazar la solicitud del Cliente es exclusivamente a discreción de Advantage Security . Después de dicha aprobación, Advantage Security emite el Certificado al cliente AR, de acuerdo con el artículo 6.1 de la CPS.

Con respecto a los componentes de la infraestructura de Advantage Security (por ejemplo, los Respondedores OCSP), personal autorizado de Advantage Security crea y aprueba las peticiones de Certificado a través de un proceso controlado que exige la participación de múltiples Personas de Confianza.

4.3 Aceptación de Certificado

Al generar un Certificado, Advantage Security le avisa a los Suscriptores que sus Certificados están disponibles y les informa sobre el medio de obtener dichos Certificados.

Cuando se emiten, los Certificados se ponen a la disposición de los Suscriptores usuarios finales, ya sea permitiéndoles descargarlos del sitio Web o mediante un mensaje que se le envía al Suscriptor y que contiene el Certificado. Por ejemplo, Advantage Security le puede enviar al Suscriptor un NIP que el Suscriptor ingresa en una página de inscripción Web para obtener el Certificado. También se le puede enviar el Certificado al Suscriptor en un mensaje de correo electrónico. El hecho de descargar el Certificado o de instalarlo desde un mensaje en el que viene adjunto, constituye la aceptación del Certificado de parte del Suscriptor.

4.4 Suspensión y Revocación del Certificado

4.4.1 Circunstancias de Revocación

4.4.1.1 Circunstancias para revocar los certificados del Suscriptor Usuario Final

Se revoca un Certificado del Suscriptor usuario final, si:

- Advantage Security, un Cliente o un Suscriptor tiene motivos para creer que ha habido un Compromiso de la clave privada de un Suscriptor, o lo sospecha firmemente;
- Advantage Security o un Cliente tiene motivos para creer que el Suscriptor ha violado sustancialmente una obligación, declaración o garantía substancial al tenor del Contrato del Suscriptor aplicable
- El Contrato del Suscriptor que se celebra con el Suscriptor se ha rescindido;

- La afiliación entre una organización que es Suscriptor de un Certificado de Advantage Security de persona moral Clase 2 y el representante legal que controla la clave privada del Suscriptor, se ha rescindido o concluye de otro modo
- Advantage Security o un Cliente tiene motivos para creer que el Certificado fue emitido de manera no substancial de acuerdo con los procedimientos que exige esta CPS el Certificado fue emitido a una persona que no es la nombrada como Asunto del Certificado, o el Certificado fue emitido sin la autorización de la persona nombrada como Asunto de dicho Certificado;
- Advantage Security o un Cliente tiene motivos para creer que un hecho substancial de una Solicitud de Certificado es falsa
- Advantage Security o un Cliente determina que no se cumplió o no se renunció a un prerrequisito substancial para la Emisión del Certificado;
- Cuando se trate de Certificados organizacionales Clase 2, cambia el nombre de la organización del Suscriptor;
- La información que tiene el Certificado, que no sea la Información del Suscriptor No Verificada, es incorrecta o ha cambiado, o
- El Suscriptor solicita la revocación del Certificado, de acuerdo con el artículo 3.4 de la CPS.

Advantage Security también puede revocar un Certificado del Administrador si la facultad del Administrador para fungir como Agente Certificador o Administrador se dio por terminada o de otro modo concluyó.

Los Contratos del Suscriptor de Advantage Security exigen que los Suscriptores usuarios finales notifiquen de inmediato a Advantage Security que se sabe o se sospecha de un compromiso de su clave privada, de acuerdo con los procedimientos del artículo 4.4.3.1 de la CPS.

Al revocar un certificado se cambia el estatus del mismo en la lista CRL y con el servicio OCSP. También se manda un correo electrónico al cliente con la confirmación del rechazo y la razón por la cual se rechazó el certificado digital.

4.4.1.2 Circunstancias para Revocar Certificados de AR o de Infraestructura

Advantage Security revocará los Certificados de la AR o de infraestructura, si:

- Advantage Security descubre o tiene motivos para creer que se ha comprometido la clave privada de AR o de infraestructura;
- El contrato que celebran la AR con Advantage Security se dio por terminado;
- Advantage Security descubre o tiene motivos para cree que el Certificado se emitió de manera que no se conforma substancialmente a los procedimientos que exige esta CPS, el Certificado se emitió en una entidad que no es la que se nombra como Asunto del Certificado, o el Certificado se emitió sin la autorización de la entidad nombrada como el Asunto del Certificado.
- Advantage Security determina que no se cumplió o no se renunció a un prerrequisito substancial para la emisión de un Certificado, o
- La AR solicita la revocación del Certificado.

Advantage Security exige que los Clientes de Advantage Security le avisen a Advantage Security cuando se necesita la revocación, de acuerdo con los procedimientos del artículo 4.4.3.1 de la CPS.

4.4.2 ¿Quién puede pedir la revocación?

4.4.2.1 ¿Quién puede pedir la Revocación de un Certificado del Suscriptor Usuario Final?

Las siguientes entidades pueden pedir la revocación de un Certificado del Suscriptor usuario final.

- Advantage Security o el Agente Certificador que aprobó la Solicitud de Certificado del Suscriptor puede pedir la revocación de Certificados del Suscriptor o del Administrador, de acuerdo con el artículo 4.4.1.1 de la CPS.
- Los Suscriptores individuales pueden pedir la revocación de sus propios Certificados individuales.
- Cuando se trate de Certificados de persona moral, sólo un representante debidamente autorizado de la organización tiene derecho de pedir la revocación de Certificados emitidos a la organización.
- Un representante debidamente autorizado de Advantage Security cuyo Administrador recibió un Certificado del Administrador o de Agente Certificador, tiene derecho a pedir la revocación de un Certificado del Administrador o de Agente Certificador.

4.4.2.2 ¿Quién Quién puede pedir la Revocación de un Certificado de la AR o de Infraestructura?

Las siguientes entidades pueden pedir la revocación de un Certificado de AR o de infraestructura:

- Sólo Advantage Security tiene derecho de pedir o iniciar la revocación de los Certificados emitidos a sus propios componentes de las AR o de infraestructura.
- Advantage Security puede iniciar la revocación de cualquier Certificado de AR o infraestructura Cliente de Advantage Security, de acuerdo con el artículo 4.4.1.2 de la CPS.
- Los Clientes de Advantage Security tienen derecho, a través de sus representantes debidamente autorizados, de pedir la revocación de sus propios Certificados de AR o infraestructura.

4.4.3 Procedimiento para Pedir la Revocación

4.4.3.1 Procedimiento para pedir la Revocación de un Certificado del Suscriptor Usuario Final

Un Suscriptor usuario final que pide la revocación, debe de comunicar esta petición a Advantage Security, quien a su vez iniciará la revocación del certificado de inmediato.

4.4.3.2 Procedimiento para la Petición de Revocación de un Certificado de la AC o RA

Una AR que pida la revocación de su Certificado de AR, tiene que comunicar la petición a Advantage Security. Entonces, Advantage Security revocará el Certificado. Advantage Security también puede iniciar la revocación de un Certificado de AR.

4.4.4 Periodo de Gracia de la Petición de Revocación

Las peticiones de revocación deben presentarse tan pronto como sea posible.

4.4.5 Circunstancias para la Suspensión

Advantage Security por lo general no ofrece servicios de suspensión con respecto a Certificados de Suscriptor usuario final.

4.4.6 Frecuencia de Emisión de las CRL

Advantage Security publica CRLs que muestran la revocación de Certificados de Advantage Security y ofrece servicios de verificación del estado. Las CRL de las AC son mantenidos por la Secretaría de Economía y por ende los certificados AC de Advantage Security tiene el punto de distribución (CDP) de la Secretaría de Economía, para que se puede validar el estatus de los mismos. Los Certificados vencidos se eliminan de la CRL a partir de los treinta (30) días siguiente al vencimiento del Certificado.

4.4.7 Requisitos de Verificación de la Lista de Revocación de Certificados

Las Partes que Confían deben verificar el estado de los Certificados en los que desean confiar. Un método con el que las Partes que Confían pueden verificar el estado del Certificado es consultando la CRL publicada por Advantage Security.

- Con respecto a la AC de Advantage Security, las CRL se divulgan en el Repositorio de la Secretaría de Economía en http://ac.economia.gob.mx/crl/se.crl.
- Con respecto a los certificados de usuario final (persona física persona moral) las CRL se divulgan en https://ca.advantage-security.com/psceconomia/crl/pscadv.crl

4.4.8 Disponibilidad de Verificación de la Revocación / Estado en Línea.

Además de la publicación de las CRL, Advantage Security proporciona información del estado del Certificado a través de funciones de consulta en el repositorio de Advantage Security.

La información del estado del Certificado se puede obtener a través de funciones de consulta basadas en la Web, a través del Repositorio de Advantage Security en:

https://ca.advantage-security.com/psceconomia/FDownloadCertificate.aspx (para los Certificados Individuales) y

Advantage Security también proporciona información sobre el estado del Certificado de OCSP.

Los Clientes que cuentan con el servicio de OCSP pueden revisar el estado del Certificado a través del uso del OCSP. El URL para el Respondedor OCSP es http://201.159.133.146:1520/OCSP

4.4.9 Requisitos de Verificación de la Revocación en Línea

Si una Parte que Confía no revisa el estado del Certificado en el que la Parte que Confía desea confiar consultando la CRL pertinente más reciente, la Parte que Confía debe revisar el estado del Certificado, usando uno de los métodos aplicables que se describen en el artículo 4.4.10 de la CPS.

4.4.10 Requisitos Especiales relativos al Compromiso de la Clave

Además de los procedimientos que se describen en el artículo 4.4.8 – 4.4.9 de la CPS, Advantage Security emplea métodos comercialmente razonables para avisar a las Partes que Confían potenciales, si Advantage Security descubre o tiene motivos para creer que se ha comprometido la clave privada de una AC de Advantage Security.

4.4.11 Certificados de Prueba

Se podrán emitir certificados de prueba para que los usuarios puedan comprobar el uso del mismo, para ello, el certificado de prueba deberá contener datos ficticios y deberá contener en algún lado, la mención de que es un certificado de prueba.

4.5 Procedimientos de Auditoria de Seguridad

4.5.1 Tipos de Eventos Registrados

Advantage Security registra en forma manual o automática los siguientes eventos importantes:

- Eventos de administración del ciclo de vida de la clave de la AC, incluyendo:
  - Generación, respaldo, almacenamiento, recuperación, archivo y destrucción de Claves.
- Eventos de administración del ciclo de vida del certificado del Suscriptor, incluyendo:
  - Solicitudes, Renovación, reposición de clave y revocación de Certificados
  - Éxito fracaso en el procesamiento de peticiones
  - Generación y emisión de Certificados y CRLs.
- Eventos relativos a la seguridad, incluyendo
  - Éxito o fracaso en el intento de acceso al sistema PKI
  - Acciones PKI y del sistema de seguridad que lleva a cabo el personal de Advantage Security
  - Archivos o registros sensibles a la seguridad leídos, escritos o suprimidos
  - Cambios en el perfil de seguridad
  - Caídas del sistema, fallas en el hardware y otras anomalías
  - Actividad el firewall y del ruteador
  - Entrada/salida de visitantes a las instalaciones de la AC.

Entre los datos del registro, se encuentran los siguientes detalles

- Fecha y hora del registro
- Número de serie o secuencia del registro, cuando se trata de registros diarios automáticos
- Identidad de la entidad que genera el registro

- Tipo de registro.

La información de registro de la Solicitud del Certificado de la AR de Advantage Security y de los Agentes Certificadores, incluyendo:

- Tipo de documento(s) de identificación presentado(s) por el Solicitante del Certificado
- Registro de los datos y números de identificación o la combinación de éstos (por ejemplo, el número del Pasaporte del Solicitante del Certificado) de los documentos de identificación, si se aplica
- Lugar donde se almacenan las copia de las solicitudes y los documentos de identificación
- Identidad de la entidad que acepta la solicitud
- Método usado para validar los documentos de identificación, en su caso
- Nombre de la AR que presenta, si se aplica.

.

4.5.2 Frecuencia del Registro de Procesamiento

Los registros de auditoria se examinan por lo menos cada semana en busca de eventos de seguridad y de operación. Asimismo, Advantage Security revisa si en sus registros de auditoria actividad sospechosa o inusual en respuesta a las alertas que se generan con base en irregularidades e incidentes dentro de los sistemas de AC y AR de Advantage Security.

El procesamiento del registro de auditoria consiste en una revisión de los registros y documentos de auditoria en busca de todos los eventos importantes en un resumen del registro de auditoria. Entre las revisiones del registro de auditoria se encuentran la verificación de que el registro no haya sido alterado, una breve inspección de todos los asientos del registro y una investigación más completa de las alertas o irregularidades de los registros. Las acciones que se lleven a cabo con base en las revisiones del registro de auditoría, también se pueden documentar.

4.5.3 Periodo de Retención para el Registro de Auditoria

Los registros de auditoría se retienen en el sitio por lo menos dos (2) meses después del procesamiento y, en lo sucesivo, se archivan de acuerdo con el artículo 4.6.2 de la CPS.

4.5.4 Protección del Registro de Auditoria

Los archivos de registro de auditoría electrónicos y manuales están protegidos de ser vistos, modificados y suprimidos sin autorización, o de otro modo alterados mediante el uso de controles de acceso físico y lógico.

4.5.5 Procedimientos de Respaldo del Registro de Auditoria

Se crean respaldos incrementales de los registros de auditoría todos los días y se hacen respaldos completos cada semana.

4.5.6 Sistema de Cobranza de Auditoria

Se generan y registran datos de auditoría automatizados a nivel de solicitud, red y sistema operativo. Los datos de auditoría que se generan en forma manual, son registrados por el personal de Advantage Security.

4.5.7 Notificación al sujeto que causa el evento

Cuando el sistema de cobranzas de auditoría registra un evento, no se necesita dar ningún aviso a la persona, organización, dispositivo o solicitud que provocó el evento.

4.5.8 Análisis de Vulnerabilidades

Los eventos del proceso de auditoria se registran, en parte, para vigilar las vulnerabilidades del sistema. Los análisis de vulnerabilidades ("AV") se llevan a cabo, revisan y enmiendan después de un examen de estos eventos supervisados. Los AV se basan en datos de registro automatizados de tiempo real y se llevan a cabo a diario, cada mes y cada año, de acuerdo con los requisitos de la Guía de Requisitos de Seguridad y Auditoria. Un AV mensual sirve como insumo de la Auditoria de Cumplimiento anual.

4.6 Archivo de Registros

4.6.1 Tipos de Eventos Registrados

Además de los registros de auditoría que se especifican en el artículo 4.5 de la CPS, Advantage Security lleva registros que comprenden documentos de:

- El cumplimiento de Advantage Security con la CPS y otras obligaciones conforme a estos contratos con sus Suscriptores, y
- Acciones e información que son substanciales para cada Solicitud de Certificado y para la creación, emisión, uso, revocación, vencimiento y reposición de la clave o renovación de todos los Certificados que emite desde el Centro de Procesamiento/ Servicio de Advantage Security.

Los registros de los eventos del ciclo de vida del Certificado de Advantage Security comprenden:

- La identidad del Suscriptor nombrado en cada Certificado;
- La identidad de las personas que solicitan la revocación del Certificado;
- Otros hechos que se declaran en el Certificado, y
- Ciertos hechos materiales previsibles relacionados con la emisión de Certificados,
- Incluyendo de manera enunciativa y no limitativa, información pertinente para concluir
- En forma exitosa una Auditoria de Cumplimiento conforme al artículo 2.7 de la CPS

Se pueden guardar los registros en forma electrónica o en impresión, siempre y cuando dichos registros tienen un índice, se almacenen, conserven y reproduzcan en forma precisa y completa.

4.6.2 Periodo de Retención del Archivo

Los registros asociados con un Certificado se guardan por lo menos durante los periodos que se indican a continuación, después de la fecha en que se venza o revoque el Certificado:

- Treinta (30) años para los Certificados Clase 2.

Si es necesario, Advantage Security puede implementar periodos de retención más largos, con el fin de cumplir con las leyes aplicables.

4.6.3 Protección del Archivo

Advantage Security protege sus registros archivados compilados bajo el artículo 4.6.1 de la CPS, de modo que sólo Personas de Confianza autorizadas tengan permiso de acceder a los datos archivados. Los datos archivados electrónicamente están protegidos contra la vista, modificación, supresión u otras alteraciones no autorizadas, a través de la implementación de controles de accesos físicos y lógicos apropiados. Los medios que guardan los datos de los archivos y las aplicaciones necesarias para procesar los datos del archivo, se guardan para garantizar que se puede acceder a los datos archivados durante el periodo que se indica en el artículo 4.6.2 de la CPS.

4.6.4 Procedimientos de Respaldo del Archivo

Advantage Security respalda en forma incremental archivos electrónicos de la información que emite del Certificado a diario, y lleva a cabo respaldos completos cada semana. Se guardan copias de registros en papel, que se compilan conforme al artículo 4.6.1 de la CPS en instalaciones de recuperación de desastres fuera de las oficinas, de conformidad con el artículo 4.8 de la CPS.

4.6.5 Requisitos para estampar la hora en los Registros

Los registros de Certificados, las CRL y otros de bases de datos de revocación, contienen información sobre la hora y la fecha. Debe hacerse notar que, en contraste con el Servicio de Estampilla de Tiempo de Advantage Security, dicha información del tiempo no está basada en la criptografía (ver el artículo 1.1.2.2.2 de la CPS).

4.6.6 Procedimientos para obtener y verificar la Información del Archivo

Ver el artículo 4.6.3 de la CPS.

4.7 Cambio de Situación de la Clave

Los pares de claves de Advantage Security se retiran del servicio a fines de sus duraciones máximas respectivas, como se define en el artículo 6.3.2 de la CPS. Los Certificados de la AC de Advantage Security se pueden renovar mientras la vida acumulada del certificado del par de claves de la AC no supere la máxima vida del par de claves de la AC. Se generarán nuevos pares de claves conforme se necesite, por ejemplo, para sustituir los pares de clave de la AC que se están retirando, para adicionar pares de claves activos, existentes, y soportar nuevos servicios de acuerdo con el artículo 6.1 de la CPS.

Antes del vencimiento del Certificado de la AC para una AC raíz, se establecen los procedimientos de cambio de la clave para facilitar una transición continua a las entidades que están dentro de la jerarquía de la AC. El proceso de cambio de clave de la AC de Advantage Security exige que:

- Una AC raíz deje de emitir nuevos Certificados de la AC Subordinada, a más tardar 60 días antes del momento ("Fecha en que se detiene la Emisión") en que la duración restante del par de claves de la AC Superior es igual al Periodo de Validez del Certificado aprobado para el (los) tipo(s) de Certificados específicos que emiten las AC Subordinadas en la jerarquía de la AC Superior.
- Al hacer la validación exitosa del Suscriptor usuario final, las peticiones de Certificado que se reciban después de la "Fecha en que detiene la Emisión", los Certificados serán firmados con un nuevo par de claves de la AC.
- La AC Superior continúa emitiendo CRLs firmadas con la clave privada de la AC raíz, hasta que llegue la fecha de vencimiento del último Certificado emitido usando el par de claves original.

4.8 Recuperación de Desastres y Compromiso de la Clave

Advantage Security ha implantado una combinación robusta de controles físicos, lógicos y de procedimiento para minimizar el riesgo y el impacto potencial del Compromiso de la clave o de un desastre. Asimismo, Advantage Security ha implementado los procedimientos de recuperación de desastres que se describen en el artículo 4.8.2 de la CPS y los procedimientos de respuesta del Compromiso Clave que se describen en el artículo 4.8.3 de la CPS. Los procedimientos de Compromiso y recuperación de desastres de Advantage Security han sido desarrollados para minimizar el impacto potencial de dicho suceso y restaurar las operaciones de Advantage Security dentro de un tiempo razonable.

4.8.1 Corrupción de los Recursos de Computación, Software, y/o Datos

En caso de corrupción de los recursos de computación, software y/o datos, se da a conocer a Seguridad de Advantage Security y se estatuyen los procedimientos de manejo de incidentes. Estos procedimientos exigen el adecuado escalamiento, investigación de incidentes y espuesta de incidentes. Si es necesario, se estatuirán los procedimientos de compromiso de la clave o recuperación de desastres de Advantage Security.

4.8.2 Recuperación de Desastres

Advantage Security y CA ha implementado un sitio de recuperación de desastres que se encuentra a más de 1,600 km (1000 millas) de las instalaciones de seguridad principales de Advantage Security y CA. Éste último ha desarrollado, implementado y probado un plan de recuperación de desastres para mitigar los efectos de cualquier tipo de desastre natural o causado por el hombre. Este plan por lo general se prueba, verifica y actualiza para que opere en caso de desastre.

Los planes de recuperación de desastres detallados están funcionando para abordar la restauración de los servicios de los sistemas de información y las funciones clave de los negocios. El sitio de recuperación de desastres de Advantage Security y CA ha implementado las protecciones de seguridad física y controles de operación que exige la Guía de Seguridad y Requisitos de Auditoria para darle una estructura segura y sólida de las operaciones de respaldo.

En caso de un desastre natural o provocado por el hombre que exija del cese de operaciones temporal o permanente de las instalaciones primarias de Advantage Security y CA , el Equipo

de Respuesta de Urgencia (VERT, por sus siglas en inglés) de CA y Advantage Security , inicia el proceso de recuperación de desastres de éste.

Advantage Security y CA tiene la capacidad de restaurar o recuperar operaciones dentro de las veinticuatro (24) horas siguientes al desastre, por lo menos con soporte para las siguientes funciones:

- Emisión del Certificado;
- Revocación del Certificado;
- Publicación de la información de revocación, y
- Entrega de información de recuperación de la clave a los Agentes Certificadores

La base de datos de recuperación de desastres de Advantage Security y CA está sincronizada regularmente con la base de datos de producción dentro de los límites de tiempo que se indican en la Guía de Requisitos de Seguridad y Auditoria. El equipo de recuperación de desastres de Advantage Security y CA está protegido con protecciones de seguridad física comparables a los segmentos de seguridad física que se indican en el artículo 5.1.1 de la CPS.

El plan de recuperación de desastres de Advantage Security y CA ha sido diseñado para ofrecer una recuperación plena en una semana después del desastre que ocurrió en el sitio primario de Advantage Security y CA . Advantage Security y CA prueba su equipo en su sitio primario para soportar funciones de la AC o la AR después de todos los desastres, salvo uno de dimensiones considerables que podría hacer que las instalaciones dejaran de funcionar. Se revisan los resultados de esas pruebas y se guardan para fines de auditoria y planeación. Cuando se puede, se reanudan las operaciones en el sitio primario de Advantage Security y CA en cuanto es posible después de un desastre mayor.

Advantage Security y CA conserva un hardware y respaldos redundantes de su AC y el software de su sistema de infraestructura en las instalaciones de recuperación de desastres. Asimismo, las claves privadas de la AC se respaldan y conservan para fines de recuperación de desastres, de acuerdo con el artículo 6.2.4 de la CPS.

Advantage Security y CA conserva respaldos fuera de sus oficinas de información importante de la AC con respecto a las AC de Advantage Security y CA , al igual que los Centros de los Clientes de Advantage Security Sytems. Dicha información comprende de manera enunciativa y no limitativa: registros de aplicaciones, datos de Solicitudes de Certificado, datos de auditoria (conforme al artículo 4.5 de la CPS), y registros Raíz de datos de todos los Certificados emitidos.

4.8.3 Compromiso de Clave

Cuando se sospeche o se sepa de un Compromiso de la clave privada de una AC de Advantage Security o infraestructura de Advantage Security, los procedimientos de Respuesta del Compromiso Clave de Advantage Security establecen que el Equipo de Respuesta de incidentes de Compromiso (CIRT, por sus siglas en inglés). Este equipo, que incluye al personal de Seguridad, Operaciones de Negocios Criptográficos, Servicios de Producción y otros representantes de administración de Advantage Security, evalúa la situación, desarrolla un

plan de acción e implementa el plan de acción con la aprobación de la administración ejecutiva de Advantage Security.

Si se necesita la revocación del Certificado de la AC, se llevan a cabo los siguientes procedimientos

- Se revoca el certificado digital de la AC directamente en las páginas de control de ciclo de vida de la Secretaría de Economía, para que la Secretaría de Economía pueda actualizar sus CRLs;
- El estado de revocado del Certificado se le notifica a las Partes que Confían a través del repositorio de Advantage Security, de acuerdo con el artículo 4.4.9 de la CPS;
- Se llevarán a cabo tareas comercialmente razonables para dar un aviso adicional de la revocación a todos los Participantes de la jerarquía de la Secretaría de Economía afectados, y
- La AC generará un nuevo par de claves, de acuerdo con el artículo 4.7 de la CPS, salvo cuando se dé por terminada la AC, de acuerdo con el artículo 4.9 de la CPS.

4.9 Cese de la AC

En caso de que sea necesario que una AC de Advantage Security deje de operar, Advantage Security hace una tarea comercialmente razonable para avisarle a los Suscriptores, Partes que Confían y otras entidades afectadas, sobre dicho cese, antes del cese de la AC. Cuando es necesaria el cese de la CA, Advantage Security y el Cliente aplicable, desarrollará un plan para minimizar la perturbación de los Clientes, Suscriptores y Partes que Confían. Estos planes de cese pueden abordar lo siguiente, como se aplique:

- Entrega del aviso a las partes a las que afecta el cese, como los Suscriptores, Partes que Confían y Clientes, informándoles del estado de la AC;
- Manejo del costo de dicho aviso;
- Revocación del Certificado que emite Advantage Security a la AC,
- Preservación de los archivos y registros de la AC durante el tiempo que exige el artículo 4.6 de la CPS;
- Continuación de los servicios de soporte del Suscriptor y el cliente;
- Continuación de los servicios de revocación, como la emisión de CRL o el mantenimiento de servicios de verificación del estado;
- Revocación de Certificados no revocados y no vencidos de los Suscriptores usuarios finales y las AC subordinadas, si es necesario;
- Pago de la compensación (si es necesario) a los Suscriptores a quienes se les revocan sus Certificados no vencidos y no revocados conforme al plan o disposición de cese, o en forma alternativa, la emisión de Certificados de sustitución de parte de la AC del sucesor;
- Disposición de la clave privada de la AC y las contraseñas de hardware que contienen dicha clave privada, y
- Disposiciones que se necesitan para la transición de los servicios de la AC a un sucesor de la AC.

5. Controles de Seguridad del Personal, de Procedimientos y Físicos

Advantage Security ha implementado la Política de Seguridad de Advantage Security, el cual soporta los requisitos de seguridad de esta CPS.

5.1 Controles Físicos

5.1.1 Localización y construcción del sitio

Las operaciones de la AC y de la AR de Advantage Security se llevan a cabo dentro de las instalaciones de Advantage Security en la Ciudad de México, México, y Mountain View California, USA, y cubren los Requisitos de Seguridad y Auditoria. Todas las operaciones de las AC y AR de Advantage Security se llevan a cabo dentro de un ambiente protegido físicamente, destinado para frenar, prevenir y detectar la penetración cubierta o abierta.

Las instalaciones primarias de Advantage Security tienen hasta siete niveles de seguridad, como se describe en el artículo de la CPS, y:

- Las operaciones de validación de la AR se llevan a cabo dentro del Nivel 3
- Las funciones de la AC se llevan a cabo dentro del Nivel 4
- Módulos criptográficos de la AC en línea, almacenados en el Nivel 5
- Módulos criptográficos de la AC fuera de línea, almacenados en el Nivel 7.

5.1.2 Acceso Físico

Los sistemas de la AC de Advantage Security están protegidos por cuatro niveles de seguridad física, con acceso al nivel inferior necesario antes de tener acceso al nivel superior. Asimismo, el sistema de seguridad comprende tres niveles adicionales para la seguridad de la administración de la clave. Las características y requisitos de cada nivel se describen en el cuadro 15 siguiente:

Nivel	*Descripción*	*Mecanismos de Control de Acceso*
Nivel 1 de Seguridad Física	El nivel uno de la seguridad física se refiere a la barrera de seguridad física más externa de sus instalaciones.	El acceso a este nivel requiere del uso de un distintivo de la tarjeta de proximidad del empleado. El acceso físico al nivel uno se registra automáticamente y se graba en video.
Nivel 2 de Seguridad Física	El nivel dos comprende áreas comunes, como baños y pasillos comunes.	El nivel dos hace valer el control de acceso individual de todas las personas que entran a las áreas comunes de las instalaciones de la AC, a través del uso de un distintivo de la tarjeta de proximidad del empleado. El acceso físico al nivel dos se registra automáticamente.
Nivel 3 de Seguridad Física	El nivel tres es el primer nivel al que se lleva a cabo la actividad de operación sensible de la AC. La actividad de operación sensible de la AC es cualquier actividad relacionada con el ciclo de vida del proceso de certificación, como la autenticación, verificación y emisión.	El nivel tres hace valer el control de acceso individual a través del uso de dos autenticaciones de factor, como la biométrica. El personal que no es escoltado, incluyendo los empleados que no son de confianza o los visitantes, no pueden entrar a un área de seguridad nivel tres. El acceso físico al nivel tres se registra automáticamente.

Nivel 4 de Seguridad Física	Descripción Mecanismos de Control de Acceso Nivel 4 de Seguridad Física El nivel cuatro es el nivel en el que ocurren las operaciones especialmente sensibles de la AC. Hay dos áreas distintitas del nivel cuatro: el centro de datos del nivel 4 en línea y el salón de ceremonias de la clave del nivel 4 fuera de línea.	El centro de datos del nivel cuatro hace valer el control de acceso individual y el salón de ceremonias de la clave hace valer el control doble, cada uno mediante el uso de dos autenticaciones de factor, como la biométrica. Las personas aprobadas para tener acceso sin escolta al nivel cuatro, deben cumplir con la Política del Empleado de Confianza. El acceso físico al nivel cuatro se registra automáticamente.
Niveles 5 a 7 de Administración de la Clave	Los niveles cinco a siete de la Administración de la Clave sirven para proteger el almacenamiento tanto en línea como fuera de línea de las tarjetas HSM y el material para poner claves.	Las HSM en línea están protegidas a través del uso de gabinetes cerrados. Las HSM están protegidas a través del uso de cajas fuertes, gabinetes y contenedores cerrados. el acceso a las HSM está restringido, de acuerdo con la segregación de los requisitos de deberes de Advantage Security y CA . La apertura y cierre de gabinetes o contenedores en estos niveles se registra para fines de auditoria. El acceso físico restrictivo progresivamente privilegio el control de acceso a cada nivel.

Cuadro 15 – Niveles de Seguridad Física

5.1.3 Acondicionamiento de Energía y Aire

Las instalaciones seguras de Advantage Security y CA están equipadas con:

- sistemas de alimentación para garantizar el acceso continuo ininterrumpido a la energía eléctrica y
- sistemas de calefacción/ventilación/acondicionamiento de aire, para controlar la temperatura y la humedad relativa, primarios y de respaldo.

5.1.4 Exposición de Agua

Advantage Security y CA ha tomado medidas de precaución razonables para minimizar el impacto de la exposición al agua a los sistemas de Advantage Security.

5.1.5 Prevención de Incendios y Protección contra éstos

Advantage Security ha tomado las medidas de precaución necesarias para evitar y apagar incendios u otro tipo de exposición dañina a las flamas o al humo. Las medidas de prevención de incendios y protección contra éstos de Advantage Security se han diseñado para cumplir con reglamentos de seguridad contra incendios locales.

5.1.6 Almacenamiento de Medios

Todos los medios que contienen software y datos de producción, información de auditoria, archivos o de respaldo, se almacenan dentro de las instalaciones de Advantage Security o en otro almacén fuera de éstas, con los controles de acceso físicos y lógicos apropiados, diseñados para limitar el acceso al personal autorizado y proteger a estos medios de daños accidentales (por ejemplo, de agua, fuego y electromagnéticos).

5.1.7 Destrucción de Desechos

Los documentos y materiales sensibles se rompen antes de eliminarlos. Antes de desechar los medios que se usan para recopilar o transmitir información sensible, se hacen ilegibles. Los dispositivos criptográficos se destruyen físicamente o se desmagnetizan o borran, de acuerdo con la guía de los fabricantes, antes de desecharlos. Otros desechos se destruyen de acuerdo con los requisitos normales de destrucción de desechos de Advantage Security.

5.1.8 Respaldo fuera de las Instalaciones

Advantage Security y CA lleva a cabo respaldos de rutina de los datos de sistema críticos, los datos de registro de auditoria y otro tipo de información sensible.

5.1.9 Política y procedimiento para el uso y reciclaje de medios de almacenamiento de información sensible

Advantage Security y CA cuenta con un sistema automatizado de respaldo de toda la información sensible. Estos respaldos se llevan a cabo en cintas magnéticas en formato digital. El sistema de respaldo está configurado para llevar a cabo respaldos incrementales diariamente, completos semanalmente y se transfiere la información respaldada en las cintas cada treinta días naturales a medios permanentes. Estos medios permanentes se almacenan en una caja de seguridad bancaria fuera de las oficinas principales de Advantage Security y CA

5.1.10 Política y procedimientos para autorizar la extracción de las instalaciones de equipo, información y software

Todo equipo, información y software que ingrese y egresa instalaciones de Advantage Security y CA debe de ser registrado por un control de acceso lógico y/o físico.

5.2 Controles de procedimiento

5.2.1 Funciones de Confianza

Las Personas de Confianza por lo general comprenden a todos los empleados, contratistas y consultores que tienen acceso o controlan las operaciones de autenticación o criptográficas que pueden afectar en forma substancial:

- la validación de la información en las Solicitudes de Certificado;
- la aceptación, rechazo u otro tipo de procesamiento de las Solicitudes de Certificado, peticiones de revocación o de renovación, o información de inscripción;
- la emisión o revocación de Certificados, incluyendo al personal que tiene acceso a partes restringidas de su repositorio;
- el manejo de información o peticiones del Suscriptor.

Entre las Personas de Confianza se encuentran, de manera enunciativa a y no limitativa

- personal de atención al cliente,
- personal de operaciones de negocios criptográficos,
- personal de seguridad,
- personal de administración de sistemas,
- personal de ingeniería designado, y

- ejecutivos que están destinados a manejar la confiabilidad de la infraestructura

Advantage Security toma en consideración las categorías de personal identificado en esta sección como Personas de Confianza que tienen un Puesto de Confianza. Las personas que quieren ser de Confianza mediante la obtención de una Posición de Confianza, deben llenar los requisitos de selección del artículo 5.3 de la CPS.

5.2.2 Número de Personas que se necesitan por Tarea

Advantage Security mantiene procedimientos de política y riguroso control para garantizar la segregación de los deberes, con base en las responsabilidades en el empleo. Las tareas más sensibles, como el acceso al hardware criptográfico de la AC (unidad de firma criptográfica o HSM) y al material asociado de la clave, y su administración, requieren de varias Personas de Confianza.

Estos procedimientos de control interno, están diseñados para garantizar que, como máximo, se requieran de dos personas de confianza para tener el acceso físico o lógico al dispositivo. El acceso al hardware criptográfico de la AC lo hacen valer estrictamente varias Personas de Confianza a través de su ciclo de vida, desde la recepción de entrada e inspección hasta la destrucción final lógica y/o física. Una vez que se activa un módulo con claves de operación, se invocan otros accesos de control para conservar el control de separación sobre el acceso tanto físico como lógico al dispositivo. Las personas que tienen acceso físico a los módulos, no tienen "Acciones Secretas" y viceversa. Los requisitos para los datos de activación de la clave privada y las Acciones Secretas se indican en el artículo 6.2.7 de la CPS.

Otras operaciones, como la validación y emisión de Certificados Clase 2, requieren de la participación de por lo menos 2 Personas de Confianza.

5.2.3 Identificación y Autenticación de cada Función

La verificación de la identidad de todo el personal que quiere ser Persona de Confianza, se lleva a cabo a través de la presencia personal (física) de dicho personal ante las Personas de Confianza que se encargan de los Recursos Humanos de Advantage Security o de las funciones de seguridad y verifican las formas bien reconocidas de identificación (por ejemplo, los pasaportes y las licencias de manejo). Además, la identidad se confirma a través de los procedimientos de verificación de antecedentes del artículo 5.3.1 de la CPS.

Advantage Security garantiza que el personal haya alcanzado el Estado de Confianza y se le haya dado la aprobación del departamento antes de que a dicho personal:

- se le hayan emitido dispositivos de acceso y se le haya dado acceso a las instalaciones necesarias;
- se le haya emitido credenciales electrónicas para acceder a funciones específicas y realizarlas en los sistemas de la AC, la AR u otros de tecnología de la información de Advantage Security.

5.3 Controles de Personal

5.3.1 Requisitos de Antecedentes y Visto Bueno

El personal que quiere ser Persona de Confianza, debe presentar un comprobante de los antecedentes, calificaciones y experiencia que se le piden para llevar a cabo las responsabilidades del empleo potencial en forma competente y satisfactoria, al igual que comprobante de cualesquiera vistos buenos del gobierno, en su caso, que sean necesarios para llevar a cabo servicios de certificación conforme a contratos gubernamentales. El personal que ocupa Puestos de confianza, repite las verificaciones de los antecedentes por lo menos cada 5 años.

Adicionalmente el personal de Advantage Security debe firmar un acuerdo de confidencialidad durante el proceso de contratación y durante su empleo. Cuando un empleado termina su relación laboral con Advantage Security se siguen todos los pasos necesarios para revocar sus accesos lógicos y físicos incluyendo el recibo de gafetes, llaves criptográficas, bloqueo de cuentas, etc. y la notificación a todos los empleados y guardias de Advantage Security del estatus de esa persona.

5.3.2 Procedimientos de Verificación de los Antecedentes

Antes de iniciar el empleo en un Papel de Confianza, Advantage Security lleva a cabo verificaciones de los antecedentes, que comprenden lo siguiente:

- confirmación de empleo anterior,
- verificación de referencia profesional,
- confirmación del grado educativo más alto o más importante obtenido,
- búsqueda de antecedentes (locales, estatales o provinciales y nacionales),
- verificación de registros de crédito/ financieros, búsqueda de registros de la licencia de manejo, y
- búsqueda de registros de la Administración del Seguro Social.

En la medida en que algunos de los requisitos que impone esta sección no se pueden satisfacer, en virtud de la prohibición o limitación de las leyes locales o de otras circunstancias, Advantage Security utilizará una técnica de investigación sustituta que permitan las leyes y que proporcione considerable información similar, incluyendo de manera enunciativa y no limitativa, la obtención de la verificación de los antecedentes, realizada por la dependencia gubernamental aplicable.

Entre los factores revelados en una verificación de antecedentes que puedan considerarse fundamentos para rechazar a candidatos a que ocupen Puestos de Confianza o que tomen medidas en contra de una Persona de Confianza existente, generalmente se encuentran los siguientes:

- Declaraciones falsas hechas por el candidato o la Persona de Confianza,
- Referencias personales altamente desfavorables o no confiables,
- Ciertas condenas penales, e
- Indicaciones de falta de responsabilidad financiera.

El personal de recursos humanos y de seguridad evalúa los informes que contienen estos datos, y éste determina el curso de acción apropiado a la luz del tipo, magnitud y frecuencia de la conducta revelada en la verificación de los antecedentes. Estas acciones pueden

comprender medidas que incluyan la cancelación de ofertas de empleo que se les hayan hecho a los candidatos para ocupar Puestos de Confianza o el cese de las Personas de Confianza existentes.

El uso de información revelada en la verificación de los antecedentes para llevar a cabo estas acciones, está sujeto a las leyes federales, estatales y locales aplicables.

5.3.3 Requisitos de Capacitación

Advantage Security le proporciona a su personal capacitación al contratarlo, así como la capacitación en el empleo necesaria para que el personal lleve a cabo las responsabilidades de su empleo en forma competente y satisfactoria. Advantage Security revisa periódicamente sus programas de capacitación, como sea necesario.

Los programas de capacitación de Advantage Security se ajustan a las responsabilidades de la persona y los puntos importantes que comprenden, son:

Conceptos básicos de la PKI,

- Responsabilidades del puesto,
- Políticas y procesamientos de seguridad y operación de Advantage Security ,
- Uso y operación del hardware y software desplegado,
- Elaboración de informes y manejo de Incidentes y Compromisos, y
- Procedimientos de recuperación de desastres y continuidad de los negocios.

5.3.4 Frecuencia y Requisitos de Nuevos Cursos de Capacitación

Advantage Security proporciona cursos de capacitación de recordatorio y actualización a su personal, en la medida y frecuencia necesarias para garantizar que dicho personal mantenga el nivel necesario de pericia para llevar a cabo las responsabilidades de su puesto en forma competente y satisfactoria. Se da capacitación en seguridad periódica en forma continua.

5.3.5 Sanciones para Acciones no Autorizadas

Se toman las medidas disciplinarias adecuadas cuando se llevan a cabo acciones no autorizadas ose violan las políticas y procedimientos de Advantage Security. Las medidas disciplinarias pueden comprender hasta el cese y se aplican de acuerdo con la frecuencia y severidad de las acciones no autorizadas.

5.3.6 Requisitos del Personal que se Contrata

En circunstancias limitadas, se pueden utilizar contratistas o consultores independientes para ocupar Puestos de Confianza. A dicho contratista o consultor se le aplican los mismos criterios funcionales y de seguridad que se le aplican a los empleados de Advantage Security en un puesto comparable.

Los contratistas y consultores independientes que no han cumplido con los procedimientos de verificación de los antecedentes que se indican en el artículo 5.3.2 de la CPS, pueden acceder a las instalaciones seguras de Advantage Security , sólo en la medida en que sean escoltados y supervisados directamente por Personas de Confianza.

Todo el personal autorizado que esté laborando en Advantage Security debe de tener un gafete visible con una foto. El contratista o consultor que esté dentro de las instalaciones debe de tener un gafete de visitante. Los controles de acceso de todos los empleados, contratistas, consultores y visitantes se determinarán según las políticas de empleados confiables, detallado en el documento “ASS Política de Empleados de Confianza”. Los gafetes de visitante se emiten solamente con el recibo de una identificación oficial vigente y los gafetes permanentes de los empleados serán emitidos por el Gerente de Seguridad solamente después de que el empleado haya cumplido con todos los requisitos de Empleado de Confianza.

5.3.7 Documentación que se proporciona al Personal

El personal de Advantage Security que participa en la operación de los servicios de PKI de Advantage Security debe leer esta CPS, las CP de la jerarquía de la Secretaría de Economía y la Política de Seguridad de Advantage Security. Esta última les proporciona a sus empleados la capacitación necesaria y los documentos requeridos para llevar a cabo las responsabilidades de su puesto en forma competente y satisfactoria.

6. Controles de Seguridad Técnicos

6.1 Generación e Instalación del Par de Claves

6.1.1 Generación del Par de Claves

Varias personas preseleccionadas, capacitadas y de confianza generan el par de claves de la AC usando los Sistemas de Confianza y los procesos que proporcionan la seguridad y la fuerza criptográfica necesaria a las claves generadas. Con respecto a las AC Raíz Emisoras, los módulos criptográficos que se usan para la generación de claves, satisfacen los requisitos del nivel 3 de FIPS 1401.

Todos los pares de claves de la AC se generan en Ceremonias de Generación de Claves pre planeadas, de acuerdo con los requisitos de la Guía de Referencia de la Ceremonia de la Clave, la Guía del Usuario de la Herramienta de Administración de la Clave de la AC y la Guía de Requisitos de Seguridad y Auditoria. Todas las personas involucradas registran, fechan y firman las actividades que se llevan a cabo en cada ceremonia de generación de claves. Estos registros se guardan para fines de auditoria y rastreo, durante el tiempo que la Administración de Advantage Security considere apropiado.

Advantage Security recomienda que la generación del par de claves para los Agentes Certificadores se lleve a cabo usando el módulo criptográfico certificado nivel 2 FIPS 1401.

Por lo general, el Suscriptor se encarga de la generación de los pares de claves del Suscriptor usuario final. Cuando se trata de Certificados Clase 2 , Certificados de firma del código/ objeto Clase 2 , el Suscriptor usa tradicionalmente un módulo criptográfico certificado nivel 1 FIPS 1401, que viene con su software de explorador, par la generación de claves.

Cuando se trata de Certificados del servidor, el Suscriptor tradicionalmente usa la utilidad de generación de claves que viene con el software del servidor de la Web.

6.1.2 Entrega de la Clave Privada a la Entidad

Los pares de clave del Suscriptor usuario final son generados tradicionalmente por el Suscriptor usuario final; por consiguiente, en esos casos, no se aplica la entrega de la clave privada a los Suscriptores.

Advantage Security no pregenera los pares de claves de la AR o del Suscriptor usuario final para clientes de la jerarquía de la Secretaría de Economía.

6.1.3 Entrega de la Clave Pública al Emisor del Certificado

Los Suscriptores usuarios finales y las AR presentan su clave pública a Advantage Security para la certificación electrónicamente a través del uso de una Solicitud de Firma de Certificado (CSR PKCS#10) u otro paquete firmado digitalmente en una sesión asegurada por Secure Sockets Layer (SSL). Cuando los pares de claves de la AR o del Suscriptor usuario final son generadas por Advantage Security , este requisito no es aplicable.

6.1.4 Entrega de la Clave Pública de la AC a los Usuarios

Advantage Security hace que los Certificados de la AC para sus AC Raíz estén disponibles para los Suscriptores y Partes que Confían a través de su inclusión en el software del explorador de la Web de Microsoft y Netscape. Conforme se generan nuevos certificados de la AC Raíz, Advantage Security les proporciona esos nuevos Certificados a los fabricantes del explorador, para incluirlos en nuevas versiones y actualizaciones del explorador.

Advantage Security generalmente proporciona la cadena de certificada completa (incluyendo la AC emisora y las ACs de la cadena) al Suscriptor usuario final al emitir el Certificado. La AC de Advantage Security también se puede descargar del Directorio LDAP en directorio.advantagesecurity.com.

6.1.5 Tamaños de la clave

Los pares de claves de la AC de Advantage Security son de por lo menos RSA de 1024 bits. La llave pública que se encuentra dentro del certificado digital AC de Advantage Security tiene un tamaño de 2084 bits. Advantage Security recomienda que las Autoridades de Registradoras y los Suscriptores usuarios finales generan pares de clave RSA de 1024 bits, pero en la actualidad permite el uso de pares de claves RSA de 512 bits para soportar ciertas aplicaciones de legado y servidores de Web.

6.1.6 Generación de la Clave del Hardware/Software

Advantage Security genera sus claves de partes de la AC en los módulos criptográficos de hardware apropiados, de acuerdo con el artículo 6.2.1 de la CPS. Los pares de claves de la RA y el Suscriptor usuario final pueden generarse en hardware o software.

6.1.7 Fines de Uso de la Clave

Con respecto a los Certificados X.509 Versión 3, Advantage Security por lo general llena la extensión KeyUsage (Uso de la Clave) de los Certificados, de acuerdo con la RFC 2459: “Certificado de Infraestructura de la Clave Pública Internet X.509 y Perfil de la CRL, de enero de 1999”. La extensión KeyUsage de los Certificados X.509 Versión 3 de Advantage Security está poblada de acuerdo con el cuadro 16 de continuación, con las siguientes excepciones:

- La extensión KeyUsage no se usa con los certificados digitales de servidor SSL y los Certificados Individuales Clase 2 .
- La criticidad de la extensión KeyUsage se puede fijar en “TRUE” segura y sólida con respecto a otros Certificados en el futuro.

		Acs	*Suscriptores Usuarios Finales de Servidor y que firman el Código/ Objeto Clase 2 ; contraseñas de Administración Automatizada*	*Firma del Par de Claves Dobles (Gerente de Clave de Managed PKI)*	*Cifrado del Par de Claves Dobles (Managed PKI Key Manager)*
Criticidad		FALSO	FALSO	FALSO	FALSO
0	digitalSignature	Clear	Set	Set	Clear
1	nonRepudiation	Clear	Clear	Clear	Clear
2	keyEnciphermen t	Clear	Set	Clear	Set
3	dataEnciphermen t	Clear	Clear	Clear	Clear
4	keyAgreement	Clear	Clear	Clear	Clear
5	keyCertSign	Set	Clear	Clear	Clear
6	CRLSign	Set	Clear	Clear	Clear
7	encipherOnly	Clear	Clear	Clear	Clear
8	decipherOnly	Clear	Clear	Clear	Clear

Cuadro16 – Ajustes de la Extensión KeyUsage

6.2 Protección de la Clave Privada

Advantage Security ha implementado una combinación de controles físicos, lógicos y procesales para garantizar la seguridad de las claves privadas de la AC de Advantage Security y el Cliente de Advantage Security . Los controles lógicos y procesales se describen en el artículo 6.2 de la CPS. Los controles de acceso físico se describen en el artículo 5.1.2 de la CPS. Por contrato, se exige que los suscriptores tomen las medidas de precaución necesarias para evitar la pérdida, divulgación, modificación o uso no autorizado de las claves privadas.

6.2.1 Normas para los Módulos Criptográficos

Para la generación de pares de claves de la AC Raíz Emisora y el almacenamiento de claves privadas de la AC, Advantage Security y CA usan módulos criptográficos de hardware que están certificados en el Nivel 3 de FIPS 1401 ó substancialmente cubren los requisitos de éste.

6.2.2 Clave Privada (n de m) Control de Múltiples Personas

Advantage Security ha implementado mecanismos técnicos y procesales que requieren de la participación de varias personas de confianza para que lleven a cabo operaciones criptográficas sensibles de la AC. Advantage Security utiliza la "Participación Secreta" para dividir los datos de activación necesarios para hacer uso de la clave privada en partes por separado llamadas"Acciones Secretas", que tiene personas capacitadas y de confianza llamadas "Accionistas." Se requiere un número de umbral de las Acciones Secretas (n) del número total de Acciones Secretas creadas y distribuidas para un módulo criptográfico de hardware particular (m), para activar una clave privada de la AC almacenada en el módulo.

El cuadro 17 siguiente muestra el número de umbral de la participación requerida y el número total de acciones distribuidas para los tipos diferentes de ACs de Advantage Security. Cabe hacer notar que el número de acciones distribuidas para contraseñas de recuperación de desastres es inferior al número distribuido para contraseñas operativas, en tanto que el número de umbral de acciones requeridas sigue siendo el mismo. Las Acciones Secretas se protegen de acuerdo con el artículo 6.4.2 de la CPS.

Entidad	*Acciones Secretas que se requieren para habilitar a la Clave Privada de la AC a firmar Certificados del Suscriptor Usuario Final*	*Acciones Secretas Requeridas para firmar el Certificado de la AC*	*Total de Acciones Secretas Distribuidas*	*Acciones de Recuperación de Desastres*	
				Acciones necesarias	*Total de Acciones*
AC Raíz Clase 2	no aplica	3	12	3	5

Cuadro 17 – Distribución y Umbrales de la Acción Secreta

6.2.3 Política de la Clave Privada

Advantage Security no entrega en depósito claves privadas de la AC, AR y del Suscriptor usuario final a ningún tercero con el fin de que acceda el cuerpo de seguridad. Advantage Security tampoco mantiene un depósito de las llaves privadas generadas por los Suscriptores de usuario final. Es responsabilidad del usuario final generar su propia llave privada, los términos y condiciones se detallan en el Acuerdo de Suscriptor aplicable.

6.2.4 Respaldo de la Clave Privada

Advantage Security crea copias de respaldo de las claves privadas de la AC para fines de recuperación de rutina y recuperación de desastres. Estas claves se almacenan en forma encriptada dentro de los módulos criptográficos del software y los dispositivos de almacenamiento de las claves asociadas. Los módulos criptográficos que se usan para el almacenamiento de las claves privadas de la AC, cubren los requisitos del artículo 6.2.1 de la

CPS. Las claves privadas de la AC se copian en módulos criptográficos de hardware de respaldo, de acuerdo con el artículo 6.2.6 de la CPS.

Los módulos que contienen copias de respaldo en el sitio de claves privadas de la AC, están sujetos a los requisitos del artículo 5.1, 6.2.1 de la CPS. Los módulos que contienen copias de recuperación de desastres de las claves privadas de la AC, están sujetos a los requisitos del artículo 4.8.2 de la CPS.

Advantage Security no almacena copias de las claves privadas de la AR. Vea en el artículo 6.2.3 de la CPS, el respaldo de las claves privadas del Suscriptor usuario final.

6.2.5 Archivo de la Clave Privada

Cuando las pares de claves de la AC de Advantage Security llega al final de periodo de validez, estos pares de claves de la AC se archivarán durante un periodo de por lo menos 10 años. Los pares de las claves de la AC llegan al fin de su periodo de validez, dichos pares de claves de la AC se archivarán durante un periodo de por lo menos 5 años. Los pares de claves de la AC archivados, se almacenarán en forma segura usando módulos criptográficos de software que cubran los requisitos del artículo 6.2.1 de la CPS. Los controles de los procedimientos evitan que los pares de claves de la AC archivados se devuelvan al uso de producción. Al final del periodo de archivo, las claves privadas de la AC archivadas se destruirán en forma segura, de acuerdo con el artículo 6.2.9 de la CPS.

Advantage Security no archiva copias de las claves privadas de la AR ni del Suscriptor.

6.2.6 Entrada de la Clave Privada al Módulo Criptográfico

Advantage Security genera pares de claves de la AC en los módulos criptográficos de hardware en los que las claves se van a usar. Asimismo, Advantage Security saca copias de dichos pares de claves de la AC para fines de recuperación de rutina y de recuperación de desastres. Cuando los pares de claves de la AC se respaldan en otro módulo criptográfico de hardware, esos pares de claves se transportan entre los módulos en forma encriptada.

6.2.7 Método de Activación de la Clave Privada

Todos los Participantes del subdominio de Advantage Security deben proteger los datos de activación de sus claves privadas, de manera que no se pierdan, sean robados, modificados, se divulguen o se usen en forma no autorizada.

6.2.7.1 Claves Privadas del Suscriptor Usuario Final

Esta sección se aplica a las Normas de la jerarquía de la Secretaría de Economía para proteger los datos de activación de las claves privadas de los Suscriptores usuarios finales para el Subdomino de Advantage Security. Asimismo, los Suscriptores tienen la opción de usar mecanismos de protección de la clave privada disponibles en la actualidad, incluyendo el uso de tarjetas inteligentes, dispositivos de acceso biométricos y otros códigos de hardware para almacenar claves privadas. Se alienta el uso de dos mecanismos de autenticación de factor (por ejemplo, contraseña y frase de pase, biométrica y contraseña o biométrica y frase de pase).

6.2.7.1.1 Certificados de Personas Morales, Físicas y de Servidor Clase 2

La Norma de la Jerarquía de la Secretaría de Economía para la protección de la clave privada Clase 2 es para que los Suscriptores:

- Usen una tarjeta inteligente, otro dispositivo de hardware criptográfico, un dispositivo de acceso biométrico, una contraseña, o una protección de una fuerza equivalente para autenticar al Suscriptor antes de la activación de la clave privada, y
- Tomen las medidas razonables comercialmente para la protección física de la estación de trabajo del Suscriptor, para evitar el uso de la estación de trabajo o el servidor y su clave privada asociada sin la autorización del Suscriptor.

Se recomienda el uso de una contraseña junto con una tarjeta inteligente, otro dispositivo de hardware criptográfico o un dispositivo de acceso biométrico, de acuerdo con el artículo 6.4.1 de la CPS. Cuando se desactivan, las claves privadas se guardarán sólo en forma encriptada.

6.2.7.2 Claves Privadas de los Administradores

6.2.7.2.1 Administradores y Agentes Certificadores

La Norma de la jerarquía de la Secretaría de Economía para la protección de la clave privada de los Administradores y Agentes Certificadores, les exige que:

Usen una tarjeta inteligente, dispositivo de acceso biométrico o contraseña, de acuerdo con el artículo 6.4.1 de la CPS, o una forma de seguridad de fuerza equivalente para autenticar al Administrador, antes de la activación de la clave privada, lo que incluye, por ejemplo, una contraseña para operar la clave privada, un procedimiento de entrada de Windows o una contraseña del ahorrador de pantalla, o una contraseña para entrar en la red; y · Tomar las medidas comercialmente razonables para la protección física de la estación de trabajo del Administrador, para evitar el uso de la estación de trabajo y su clave privada asociada, sin la autorización del Administrador o Agente Certificador.

Se recomienda el uso de una contraseña junto con una tarjeta inteligente, un dispositivo de acceso biométrico, de acuerdo con el artículo 6.4.1 de la CPS, para autenticar al Administrador o Agente Certificador antes de activar la clave privada.

Cuando de desactivan, las llaves privadas se almacenarán encriptados.

6.2.7.3 Claves Privadas en manos de Advantage Security

Las claves privadas de la AC de Advantage Security se activan con un número de umbral de Accionistas que proporcionan sus datos de activación (contraseñas o frases de pase), de acuerdo con el artículo 6.2.2 de la CPS. Con respecto a las AC fuera de línea de Advantage Security , la clave privada de la AC se activa para una sesión (por ejemplo, para la certificación de una AC Subordinada o un caso en el que la AC firme una CRL) después de la cual se desactiva y el módulo se regresa al almacenamiento seguro. Para las AC en línea de Advantage Security, la clave privada de la AC se activa durante un periodo indefinido y el módulo sigue

estando en línea en el centro de datos de producción hasta que se saca de la línea a la AC (por ejemplo, para el mantenimiento del sistema). Los Accionistas de Advantage Security tienen que salvaguardar sus Acciones Secretas y firmar un contrato en el que reconocen sus responsabilidades como Accionistas.

6.2.8 Método de Desactivación de la Clave Privada

Las claves privadas de la AC de Advantage Security se desactivan al quitarse del lector de contraseña. Las claves privadas de la AR de Advantage Security (que se usa para la autenticación de la solicitud de la AR), se desactivan cuando desconectan el sistema. Es necesario que las AR de Advantage Security desconecten sus estaciones de trabajo cuando salen de su área de trabajo.

Las claves privadas de los Administradores de los Clientes, las AR y los Suscriptores usuarios finales se pueden desactivar después de cada operación, desconectando su sistema, o quitando una tarjeta inteligente del lector de la tarjeta inteligente, dependiendo del mecanismo de autenticación que emplea el usuario. Las claves privadas de los Administradores del Cliente, la AR y los Suscriptores usuarios finales se pueden desactivar después de cada operación, al desconectar su sistema, o al quitar la tarjeta inteligente del lector de tarjetas inteligentes, dependiendo del mecanismo de autenticación que utilice el usuario. En todos los casos, los Suscriptores usuarios finales tienen la obligación de proteger adecuadamente su(s) clave(s) privada(s) de acuerdo con el artículo 2.1.3, 6.4.1 de la CPS.

6.2.9 Método de Destrucción de la Clave Privada

A la conclusión de la vida de operación de la AC de Advantage Security , se archivan una o más copias de la clave privada de la AC, de acuerdo con el artículo 6.2.5 de la CPS. Las copias restantes de la clave privada de la AC se destruyen en forma segura. Asimismo, las claves privadas de la AC archivadas se destruyen en forma segura cuando concluyen sus periodos de archivo. Las actividades de destrucción de la clave de la AC requieren de la participación de varias personas de confianza.

Cuando se requiere, Advantage Security destruye las claves privadas de la AC, de manera que garantice en forma razonable que no quedan restos de a clave que pudieran dar como resultado la reconstrucción de la clave. Advantage Security utiliza la función de desmagnetización y borrado de sus módulos criptográficos de hardware y otros medios apropiados para garantizar la destrucción completa de las claves privadas de la AC. Cuando se llevan a cabo, se registran las actividades de destrucción de la clave de la AC.

6.3 Otros Aspectos de la Administración del Par de Claves

6.3.1 Archivo de la Clave Pública

Los Certificados de la AC, AR y Suscriptor usuario final de Advantage Security, están respaldados y archivados como parte de los procedimientos de respaldo de rutina de Advantage Security

6.3.2 Periodos de Uso para las Claves Públicas y Privadas

El Periodo de Operaciones de un Certificado termina a su vencimiento o revocación. El Periodo de Operación de los pares de claves es igual al Periodo de Operación de los Certificados asociados, salvo que las claves privadas pueden continuar usándose en el desencriptado y las claves públicas pueden continuar usándose en la verificación de firmas. Los Periodos de Operación máximos para los Certificados de Advantage Security emitidos en la fecha efectiva de esta CPS o después, se establecen en el siguiente cuadro 18.

Asimismo, las AC de Advantage Security dejan de emitir Certificados nuevos en la fecha apropiada antes del vencimiento del Certificado de la AC, de modo que ningún Certificado emitido por una AC Subordinada se venza después del vencimiento de algún Certificado de la AC Superior.

Certificado emitido por:	*Clase 2*
AC Raíz, emisoras, autofirmadas	Hasta 30 años
AC al Suscriptor usuario final	Hasta 10 años

Cuadro 18 – Periodos de Operación del Certificado

Salvo como se apuntó en esta sección, los Participantes en el Subdomino de Advantage Security dejarán de usar por completo los pares de claves después del vencimiento de sus periodos de uso.

Los Certificados emitidos por las AC a los Suscriptores usuarios finales no pueden tener Periodos de Operación superiores a dos años.

Advantage Security también opera varias AC de ase emisoras autofirmadas de legado, que son parte de la jerarquía de la Secretaría de Economía. Los Certificados del Suscriptor usuario final que emiten estas AC, cubren los requisitos de la AC para los Certificados del Suscriptor usuario final que se indican en el cuadro 18 anterior. Los requisitos de estas AC se describen en el cuadro 19 siguiente.

Certificado de la AC emitido por:	*Periodo de Operación del Certificado de la AC*	*Clase de Certificados del Suscriptor Usuario Final emitidos*
AC Editores del Software Comercial (autofirmados)	Hasta 10 años	Equivalente a Clase 2
CA Raíz de Estampilla de Tiempo (autofirmada)	Hasta 10 años	Equivalente a Clase 2

Cuadro 19 – Requisitos par a las AC Raíz, Emisoras, de Legado

6.4 Datos de Activación

6.4.1 Generación e Instalación de los Datos de Activación

Los datos de activación (Acciones Secretas) que se usan para proteger contraseñas que contienen las claves privadas de Advantage Security, se generan de acuerdo con los requisitos del artículo 6.2.2 de la CPS y la Guía de Referencia de la Ceremonia de la Clave. Se registra la creación y distribución de las Acciones Secretas.

Las AR de Advantage Security tienen que seleccionar contraseñas fuertes para proteger sus claves privadas. Las directrices para la selección de las contraseñas de Advantage Security exigen que las contraseñas:

- sean generadas por el usuario;
- tengan por lo menos ocho caracteres;
- tengan por lo menos un carácter alfabético y un carácter numérico;
- tengan por lo menos una letra minúscula;
- no contengan muchas repeticiones del mismo carácter;
- no sean iguales al nombre del perfil del operador, y
- no contengan una subcadena larga del nombre de perfil del usuario.

Advantage Security recomienda firmemente que las AR y los Suscriptores usuarios finales escojan contraseñas que cubran los mismos requisitos. Advantage Security también recomienda el uso de dos mecanismos de autenticación de factores (por ejemplo, contraseña y frase de pase, biométrica y contraseña o biométrica y frase de pase) para la activación de la clave privada.

6.4.2 Protección de datos de Activación

Los Accionistas de Advantage Security deben salvaguardar sus Acciones Secretas y firman un contrato reconociendo sus responsabilidades de Accionistas.

Las AR de Advantage Security deben almacenar sus claves privadas del Administrador o la AR en forma encriptada, usando la protección de contraseña y su opción de “alta seguridad” del explorador.

Advantage Security recomienda firmemente que los Administradores del Cliente, las AR y los Suscriptores usuarios finales, almacenen sus claves privadas en forma encriptada y protejan sus claves privadas a través del uso de una contraseña de hardware y/o una frase de pase fuerte. Se promueve el uso de dos mecanismos de autenticación de factor (por ejemplo, contraseña y frase de pase, biométrica y contraseña, o biométrica y frase de pase).

6.4.3 Otros Aspectos de los Datos de Activación

Ver el artículo 6.4.1 y 6.4.2 de la CPS.

6.5 Controles de Seguridad de la Computadora

Advantage Security lleva a cabo todas las funciones de AC y AR usando Sistemas Confiables que cubran los requisitos de la Guía de Requisitos de Seguridad y Auditoria de Advantage Security . Los Agentes Certificadores que estén fuera de las instalaciones de Advantage Security deben de cumplir con los mismos requisitos de seguridad para garantizar la confidencialidad de sus llaves privadas.

6.5.1 Requisitos Técnicos de Seguridad de la Computadora Específicos

Advantage Security garantiza que los sistemas que tienen software y archivos de datos de la AC sean Sistemas Confiables protegidos contra acceso no autorizado. Además, Advantage Security limita el acceso a los servidores de producción a las personas que tienen un motivo de

negocios válido para dicho acceso. Los usuarios de aplicación general no tienen cuentas en los servidores de producción.

La red de producción de Advantage Security está separada lógicamente de otros componentes.

Esta separación evita el acceso a la red, salvo a través de procesos de aplicación definidos Advantage Security usa firewalls para proteger la red de producción de la intrusión interna y externa y limitar la naturaleza y la fuente de actividades de la red a la que puedan acceder los sistemas de producción.

Advantage Security exige el uso de contraseñas que tienen una longitud de caracteres mínima y una combinación de caracteres alfanuméricos y especiales. Advantage Security exige que se cambien las contraseñas en forma periódica.

El acceso directo a las bases de datos de Advantage Security que soportan el repositorio de Advantage Security, está limitado a las Personas de Confianza del grupo de operaciones de Advantage Security que tienen un motivo válido para dicho acceso.

6.5.2 Clasificación de Seguridad de la Computadora

Una versión del software del Centro de Procesamiento nuclear de Advantage Security y CA ha cumplido con los requisitos de garantía EAL 4 de ISO/IEC 154083: 1999, Tecnología de la información – Técnicas de seguridad – Criterios de evaluación para la seguridad de la TI Parte 3: Requisitos de garantía de la seguridad, con base en una evaluación de un laboratorio independiente de los Criterios Comunes del software frente al Objetivo de Seguridad del entro de Procesamiento de Advantage Security y CA . Este último puede, ocasionalmente, evaluar nuevas versiones del software del Centro de Procesamiento bajo Criterios Comunes. Favor de ponerse en contacto con Advantage Security para obtener más información sobre la versión del Centro de Servicio que se está usando en este momento, y si cumple con el requisito de garantía de EAL 4.

6.6 Controles Técnicos del Ciclo de Vida

6.6.1 Controles de Desarrollo del Sistema

Advantage Security desarrolla e implementa las solicitudes de acuerdo con las normas de administración del desarrollo y cambio de sistemas. Advantage Security también proporcionan software a sus Agentes Certificadores para que lleven a cabo las funciones de AR y algunas de AC. Este software se desarrolla de acuerdo con las normas de desarrollo de sistemas de Advantage Security

El software desarrollado de Advantage Security Systems y CA, cuando se cargó por primera vez, ofrece un método para verificar que el software del sistema proveniente de Advantage Security y CA o de Advantage Security, no ha sido modificado antes de la instalación, y es la versión planeada para usarse.

6.6.2 Controles de Administración de la Seguridad

Advantage Security tiene mecanismos y/o políticas en funcionamiento para controlar y supervisar la configuración de sus sistemas de AC. Advantage Security crea una comprobación aleatoria de todos los paquetes de software y de las actualizaciones del software de Advantage Security. Esta comprobación aleatoria se usa para verificar la integridad de dicho software en

forma manual. A la instalación y en forma periódica en lo sucesivo, Advantage Security valida la integridad de sus sistemas de AC.

6.7 Controles de Seguridad de la Red

Advantage Security lleva a cabo todas sus funciones de AC y AR usando redes protegidas de acuerdo con la Guía de Requisitos de Seguridad y Auditoria, para evitar el acceso no autorizado y otro tipo de actividad maliciosa. Advantage Security protege sus comunicaciones de información sensible a través del uso de la encriptación y la firmas digitales.

6.8 Controles de Ingeniería del Módulo Criptográfico

Los módulos criptográficos que usa Advantage Security y CA , cubren los requisitos del artículo 6.2.1 de la CPS.

7. Certificado y Perfil de la CRL

7.1 Perfil del Certificado

El artículo 7.1 de la CPS define el Perfil del Certificado de Advantage Security y los requisitos de contenido de los Certificados de la jerarquía de la Secretaría de Economía emitidos conforme a esta CPS.

Los Certificados de Advantage Security se conforman con (a) ITUT Recomendación X.509 (1997): Tecnología de la Información – Interconexión de los Sistemas Abiertos – El Directorio Marco de Autenticación, junio de 1997, y (b) RFC 2459: Internet X.509 Certificado de Infraestructura de la Clave Privada y Perfil de la CRL, enero de 1999 (“RFC 2459”).

7.1.1 Número(s) de Versión

Los Certificados de la AC de Advantage Security y del Suscriptor usuario final son Certificados X.509 Versión 3.

7.1.2 Extensiones del Certificado

Cuando se usan Certificados X.509 Versión 3, Advantage Security llena los Certificados con las extensiones que exige el artículo 7.1.2.17.1.2.8 de la CPS. Las extensiones privadas son permisibles mientras su uso sea congruente con las CP de la jerarquía de la Secretaría de Economía y esta CPS.

7.1.2.1 Uso de Claves

Cuando se usan Certificados X.509 Versión 3, Advantage Security llena la extensión KeyUsage, de acuerdo con el artículo 6.1.9 de la CPS. El campo de criticidad de esta extensión se pone en FALSE.

7.1.2.2 Extensión de las Políticas de los Certificados

Los Certificados del Suscriptor usuario final X.509 Versión 3 de Advantage Security usa la extensión de CertificatePolicies (Políticas de los Certificados). La extensión de CertificatePolicies se puebla con el identificador de objeto aplicable para las CP de la jerarquía de la Secretaría de Economía, de acuerdo con el artículo 7.1.6 de la CPS y con los calificadores

de política que se establecen en el artículo 7.1.8 de la CPS. El campo de criticidad de esta extensión se pone en FALSE.

7.1.2.3 Restricciones Básicas

Advantage Security llena los Certificados de la AC X.509 Versión 3 con extensión de BasicConstraints (Restricciones Básicas) y el Tipo de Asunto se pone en AC. Los Certificados del Suscriptor usuario final también están poblados con una extensión de BasicConstraints y el Tipo de Sujeto es igual a la Entidad Final. La criticidad de la extensión de BasicConstraints generalmente se pone en FALSE, salvo por la AR de la oficina de Servicios de Autenticación Clase 2 de Advantage Security. La criticidad de esta extensión se puede poner en TURE con respecto a otros Certificados en el futuro.

Los Certificados de la AC X.509 Versión 3 de Advantage Security emitidos para que tengan un campo de "pathLenConstraint" de la extensión de BasicConstraints puesto en el número máximo de certificados de la AC que pueden seguir a este Certificado en una trayectoria de certificación.

Los Certificados del Suscriptor usuario final tienen un campo "pathLenConstraint" puesto en un valor de "0", el cual indica que sólo el Certificado del Suscriptor usuario final puede seguir la trayectoria de certificación.

7.1.2.4 Uso de la Clave Extendida

Advantage Security hace uso de la extensión ExtendedKeyUsage (Uso de la Clave Extendida) en los tipos específicos de Certificados X.509 Versión 3 de Advantage Security que se describen en el cuadro 21 siguiente. Con respecto a otros tipos de Certificados, Advantage Security no usa la extensión de ExtendedKeyUsage.

Tipo de Certificado	*Tipo de Certificado*
Autoridad de Certificadora (AC)	AC del Servidor Internacional Clase 3
Respondedor OCSP	Respondedores OCSP Primarios Públicos Clase 2 Respondedor OCSP del Servidor Seguro
Certificados del Servidor de Web Clase 2	Identificadores del Servidor Seguro Identificadores del Servidor Global

Cuadro 21 – Certificados que usan la Extensión ExtendedKeyUsage

Con respecto a los Certificados, Advantage Security puebla la extensión de ExtendedKeyUsage (Uso de la Clave Ampliado), de acuerdo con el cuadro 22 siguiente.

		CA del Servidor Internacional Clase 2	*Respondedores OCSP*	*Identificaciones del Servidor Seguro*	*Identificaciones del Servidor Global*
Criticidad		FALSO	FALSO	FALSO	FALSO
0	ServerAuth	Clear	Clear	Set	Clear
1	ClientAuth	Clear	Set	Set	Clear
2	CodeSigning	Clear	Clear	Clear	Clear
3	EmailProtection	Clear	Set	Clear	Clear
4	ipsecEndSystem	Clear	Clear	Clear	Clear

5	ipsecTunnel	Clear	Clear	Clear	Clear
6	ipsecUser	Clear	Clear	Clear	Clear
7	TimeStamping	Clear	Clear	Clear	Clear
8	OCSP Signing	Clear	Set	Clear	Clear
-	Microsoft Server Gated Crypto (SGC) OID: 1.3.6.1.4.1.311.10.3.3	Clear	Clear	Clear	Set
-	Netscape SGC OID: 2.16.840.1.113730.4.1	Set	Clear	Clear	Set
-	TBD – OID: 2.16.840.1.113733.1.8.1	Set	Clear	Clear	Clear

Cuadro 22 – Ajustes de la Extensión ExtendedKeyUsage

7.1.2.5 Puntos de Distribución de la CRL

Los Certificados del Servidor Seguro X.509 Versión 3 y del Suscriptor usuario final Individual Clase 2 de Advantage Security utilizan la extensión CRLDistributionPoints (Puntos de Distribución de la CRL) que contiene la URL del lugar en el que una Parte que Confía puede obtener una CRL para verificar el estado del Certificado de la CA. El campo de criticidad de esta extensión se ajusta en FALSE. El uso de los Puntos de Distribución CRL se soportarán para otras AC de Advantage Security AC en el futuro.

7.1.2.6 Identificador de la Clave de Autoridad

Advantage Security llena la extensión Authority Key Identifier (Identificador de la Clave de la Autoridad) de los Certificados del Suscriptor usuario final X.509 Versión 3 que emite la AC de Advantage Security. El Identificador de la Clave de Autoridad está compuesto de la comprobación aleatoria SHA1 de 60 bits de la clave pública de la AC que emite el Certificado.

El campo de criticidad de esta extensión se pone en FALSE. El uso de la extensión del Identificador de la Clave de Autoridad se puede soportar para otras AC de Advantage Security en el futuro.

7.1.2.7 Identificador de la Clave del Sujeto

Cuando Advantage Security llena los Certificados de la jerarquía de la Secretaría de Economía X.509 Versión 3 con una extensión subjectKeyIdentifier, se genera el Identificador de Clave basado en la clave pública del Certificado del Sujeto. Cuando se usa esta extensión, el campo de criticidad de esta extensión se pone en FALSE.

7.1.2.8 Algoritmo de Firma del Certificado

El algoritmo de firma del certificado es SHA1 con RSA

7.1.3 Identificadores de Objetos (OID) de la Política de Certificados y Declaración de Prácticas de Certificación.

El identificador de objeto de la Política de Certificados de la Autoridad Certificadora del PSC Advantage Security es: 2.16.484.101.10.316.2.1.1.1.1.1.2

El identificador de objeto de la Declaración de Prácticas de Certificación de la Autoridad Certificadora del PSC Advantage Security es: 2.16.484.101.10.316.2.1.1.1.1.1.2

Nota: Los OID`s: 2.16.484.101.10.316.1.1.1.1.2.2 y 2.16.484.101.10.316.2.1.1.1.1.2.1, fueron publicados erróneamente.

Formas del Nombre

Advantage Security llena los Certificados de la jerarquía de la Secretaría de Economía con un Nombre Distinguido del Emisor y del Sujeto, de acuerdo con el artículo 3.1.1 del CPS.

Asimismo, Advantage Security comprende dentro de los Certificados del Suscriptor usuario final un campo de Unidad Organizacional que contiene un aviso que manifiesta que se establecen los términos de uso del Certificado en una URL que es indicador del Contrato de la Parte que Confía. Sólo se permiten excepciones al requisito anterior cuando limitaciones de espacio, formateo o interoperabilidad dentro de los Certificados hacen que dicha Unidad Organizacional no pueda usarse junto con la aplicación para la que están destinados los Certificados.

7.1.4 Identificador del Objeto de la Política del Certificado

Cuando se usa la extensión de Políticas del Certificado, los Certificados contienen el identificador del objeto de la Política del Certificado que le corresponde a la Clase de Certificado apropiada, como se manifiesta en el artículo 1.2 de la CPS. Con respecto a los Certificados de Legado que se emiten antes de la publicación de la CP de la jerarquía de la Secretaría de Economía, que incluyen la extensión de Políticas del Certificado, los Certificados se refieren a la CPS de Advantage Security.

7.1.5 Sintaxis y Semántica de los Calificadores de Política

Advantage Security llena los Certificados de la jerarquía de la Secretaría de Economía X.509 Versión 3 con un calificador de política dentro de la extensión de CertificatePolicies (Políticas de Certificado). Por lo general, estos Certificados contienen un calificador indicador de la CPS que apunta al Contrato de la Parte que Confía o la CPS de la jerarquía de la Secretaría de Economía.

Asimismo, algunos Certificados contienen un Calificador del Aviso del Usuario que apunta al Contrato de la Parte que Confía aplicable.

7.2 Perfil de la CRL

Advantage Security emite CRL que se conforman con RFC 2459. Como mínimo, las CRL de Advantage Security contienen los campos básicos y contenidos que se indican en el siguiente Cuadro 23:

Campo	*Valor o restricción del Valor*
Versión	Ver el artículo 7.2.1 de la CPS.
Algoritmo de la Firma	Algoritmo usado para firmar la CRL. Las CRL se firman usando md5RSA (OID: 1.2.840.113549.1.1.4) de acuerdo con RFC 2459.

Emisor	La entidad que firmó y emitió la CRL. El Nombre del Emisor de la CRL es conforme a los requisitos del Nombre Distinguido del Emisor que se indican en el artículo 7.1.4 de la CPS.
Fecha Efectiva	Fecha de emisión de la CRL. Las CRL de Advantage Security son efectivas al emitirlas.
Siguiente Actualización	Fecha en que se emitirá la siguiente CRL. La siguiente fecha de Actualización de las CRL de Advantage Security se establece de la siguiente manera: 3 meses a partir de la Fecha Efectiva para las AC de Advantage Security y 10 días a partir de la Fecha Efectiva para otras AC de Advantage Security. La frecuencia de la emisión de la CRL va de acuerdo con los requisitos del artículo 4.4.9 de la CPS.
Certificados Revocados	La lista de los certificados revocados, incluyendo el Número de Serie del Certificado revocado y la Fecha de Revocación.

Cuadro 23 – Campos Básicos del Perfil de la CRL

7.2.1 Número(s) de Versión

Advantage Security emite actualmente CRL X.509 Versión 1.

8. Administración de Especificaciones

8.1 Procedimientos de Cambio de Especificación

El grupo de Desarrollo de Prácticas de Advantage Security le hará modificaciones a esta CPS. Las modificaciones serán en forma de documento que contenga una forma modificada de la CPS o una actualización. Las versiones modificadas o las actualizaciones se vincularán con la sección de Actualizaciones de Prácticas y Avisos del Repositorio de Advantage Security que se encuentra en: https://ca.advantage-security.com/psceconomia/legal.html Las actualizaciones sobreseen cualesquiera disposiciones designadas o conflictivas de la versión de referencia de la CPS.

8.1.1 Conceptos que tienen que cambiar sin Aviso

Advantage Security se reserva el derecho de modificar la CPS sin dar aviso de las modificaciones que no son sustanciales, incluyendo de manera enunciativa y no limitativa de errores tipográficos, cambios a las URL, y cambios para contactar información. La decisión de Advantage Security de designar las modificaciones como sustanciales y no sustanciales, será a discreción exclusiva de Advantage Security.

8.1.2 Conceptos que tienen que cambiar con Aviso

Advantage Security y CA periódicamente harán modificaciones sustanciales a la CPS. Los cambios planeados serán publicados en https://ca.advantage-security.com/psceconomia/legal.html Las modificaciones de la versión anterior a la versión vigente del CPS se registrarán en la sección 1.1 del CPS.

Adicionalmente el documento Aviso de adendums sugeridos a Procesos de Certificación (CPS) versión 2.1 de Advantage Security especifica los conceptos que pueden cambiar con aviso.

8.1.2.1 Lista de Conceptos

Modificaciones substanciales son los cambios que Advantage Security considera que son sustanciales al tenor del artículo 8.1.1 de la CPS.

8.1.2.2 Mecanismo de Notificación

El grupo de Desarrollo de Prácticas de Advantage Security publicará los cambios propuestos a la CPS en la sección de Actualizaciones y Avisos de Prácticas del Repositorio de Advantage Security, el cual se ubica en: https://ca.advantage-security.com/psceconomia/legal.html Advantage Security solicita las modificaciones propuestas a la CPS de otros Participantes del Subdomino de Advantage Security. Si este último considera que esta modificación es conveniente y propone aplicar la modificación, Advantage Security dará aviso de esa modificación, de acuerdo con esta sección.

A pesar de lo que se diga en esta CPS en contrario, si Advantage Security cree que es necesario hacerle modificaciones sustanciales inmediatas a la CPS para detener o prevenir una violación la seguridad de la jerarquía de la Secretaría de Economía, Advantage Security tendrá derecho de hacer estas modificaciones mediante la publicación en el Repositorio de Advantage Security Repositorio. Estas modificaciones entrarán en vigor de inmediato a su publicación.

8.1.2.3 Periodo de Comentarios

Salvo como se indica en el artículo 8.1.2.2 de la CPS, el periodo de comentario para cualesquiera modificaciones substanciales a la CPS será de quince (15) días, a partir de la fecha en la que se publiquen las modificaciones en el Repositorio de Advantage Security Repositorio. Cualquier Participante del Subdominio de Advantage Security tendrá derecho de presentar sus comentarios al grupo de Desarrollo de las Prácticas de Advantage Security hasta el final del periodo de comentarios.

8.1.2.4 Mecanismo para manejar comentarios

El grupo de Desarrollo de Prácticas de Advantage Security considerará los comentarios sobre las modificaciones propuestas. Advantage Security : (a) permitirá que las modificaciones propuestas entren en vigor sin modificación; (b) cambiará las modificaciones propuestas y las repoblará como una nueva modificación de conformidad con el artículo 8.1.2.2 de la CPS, o (c)retirará las modificaciones propuestas. Advantage Security tiene derecho de retirar las modificaciones propuestas poniendo un aviso en la sección de Actualizaciones y Avisos de Prácticas del Repositorio de Advantage Security Repositorio. A menos que las modificaciones propuestas se cambien o retiren, entrarán en vigor al vencimiento del periodo de comentarios conforme al artículo 8.1.2.3 de la CPS.

8.1.3 Cambios que exigen Cambios en la Política de Certificados OID o el Indicador de la CPS

Ver el artículo 8.1.3 de la CPS.

8.2 Políticas de Publicación y Notificación

8.2.1 Artículos que no se publicaron en la CPS

Los documentos de seguridad que Advantage Security Systems considera confidencial, no se divulgan al público. Entre los documentos de seguridad confidenciales incluyen los documentos que se identifican en el artículo 1.1(a) de la CPS, Cuadro 1, como los documentos que no están disponibles para el público.

8.2.2 Distribución de la CPS

Esta CPS se publica en forma electrónico dentro del Repositorio de Advantage Security en https://ca.advantage-security.com/psceconomia/CPSv2.1.1.pdf La CPS está disponible en formato de Adobe Acrobat pdf. Advantage Security también pone la CPS disponible en Adobe formato de Word mediante solicitud enviada a contacto2@advantage-security.com. La CPS se pueden adquirir en papel con el grupo de Desarrollo de Prácticas de Advantage Security, enviando una solicitud a:

Advantage Security, At'n: CPS
Av. Prolongación Reforma 625, Desp. 402
Torre Lexus
Paseo de las Lomas, Santa Fe
México, DF C.P. 01330

8.3 Procedimientos de Aprobación de la CPS

Aprobación de este CPS y addenda subsecuentes será hecho por la Autoridad de administración de Políticas de Advantage Security. La aprobación de este CPS y addenda subsecuentes serán registrados por medio de un documento de notificación de actualización o por medio de un formulario adendado al CPS. Las versiones actualizadas y los addenda serán publicados en: https://ca.advantage-security.com/psceconomia/legal.html Las versiones actualizadas del CPS serán considerados como las versiones vigentes del mismo. La Autoridad de Administración Políticas determinará si se debe cambiar los identificadores de objetos de la política de certificados que corresponden a cada clase de certificado.

Acrónimos y Definiciones

Cuadro de Acrónimos

Acrónimo	*Término*
ANSI	The American National Standards Institute (Instituto Norteamericano de Normas Nacionales).
B2B	Interempresarial.
BXA	The United States Bureau of Export Administration of the United States Department of Commerce (Oficina de Administración de Exportaciones de los Estados Unidos del Departamento de Comercio de los Estados Unidos).
AC	Autoridad de Certificadora.
CP	Política de Certificados.
CPS	Declaración de Prácticas de Certificación.
CRL	Lista de Revocación de Certificados.
NGS	Nivel de garantía de la seguridad (de acuerdo con Criterios Comunes).
EDI	Intercambio Electrónico de Datos.
EDIFACT	Transferencia electrónica de datos para administración, comercio y transporte (normas establecidas por la Comisión Económica para Europa de las Naciones Unidas).
FIPS	Normas Federales de Procesamiento de Información de los Estados Unidos.
CCI	Cámara de Comercio Internacional.
BRC	Bloque de Recuperación de Claves.
EVSL	Evaluación de la vulnerabilidad de la seguridad lógica.
OCSP	Protocolo del Estado del Certificado en Línea.

OF X	Intercambio Financiero Abierto.
PCA	Autoridad de Certificación Primaria.
NIP	Número de Identificación Personal.
PKCS	Norma de Criptografía de la Clave Pública.
PKI	Infraestructura de Clave Pública.
AAP	Autoridad de Administración de la Política.
RA	Autoridad de Registro.
RFC	Solicitud de Comentarios.
SAS	Declaración sobre Normas de Auditoria (promulgada por el Instituto Norteamericano de Contadores Públicos Certificados).
S/MIME	Extensiones seguras de correo de Internet para fines múltiples.
SSL	Capa segura de socket (Secure Socket Layer).
VTN	CA Trust Network.
WAP	Protocolo de aplicación inalámbrica.
WTLS	Capa inalámbrica de seguridad de transporte.

Definiciones

Término	*Definición*
Autoridad de Certificación Administrativa (CA Administrativa)	Un tipo de AC de Advantage Security que emite certificados para las AR de Advantage Security , Agentes Certificadores, Administradores Afiliados y servidores de Administración Automatizados.
Administrador	Una Persona de Confianza dentro de la organización de un Centro de Procesamiento, Centro de Servicio que lleva a cabo la validación y otras funciones de la AC o AR.
Certificado del Administrador	Un Certificado emitido a un Administrador que sólo se puede usar para llevar a cabo funciones de AC o de AR.
Filial	Un tercero de confianza importante, por ejemplo en la industria de tecnología, telecomunicaciones, o servicios financieros, que haya celebrado un contrato con CA para ser un canal de distribución y servicios con un territorio específico.
Guía del Programa de Auditoria de Filiales	Un documento de CA que contenga los requisitos para las Auditorias de Cumplimiento de las Filiales, incluyendo Objetivos de Control de Administración de Certificados contra los que se va a auditar a las Filiales.
Persona Afiliada	Persona física relacionada con una entidad determinada (i) como funcionario, director, empleado, socio, contratista, interno u otra persona dentro de la entidad; (ii) como miembro de una comunidad de intereses registrada de Advantage Security , o (iii) como una persona que mantiene una relación con la entidad, cuando la entidad tiene un negocio u otros registros que dan las garantías apropiadas de identidad a esa persona.
Cliente de ADVANTAGE SECURITY	Entidad que contrata con Advantage Security para obtener servicios de la Oficina de Servicios de Autenticación. Un Cliente de Advantage Security es una AC, y está nombrado como tal dentro de los Certificados emitidos por su AC, pero obtiene todas las funciones de AC de un Proveedor de Advantage Security

Proveedor de ADVANTAGE SECURITY	Una entidad Advantage Security que ofrece servicios de la Oficina de Servicios de Autenticación a los Clientes de Advantage Security . Un Proveedor de Advantage Security funge como proveedor externo de funciones de fondo para un Cliente de Advantage Security y como AR para un Cliente de Advantage Security
Oficina de Servicios de Autenticación	Un servicio dentro de la jerarquía de la Secretaría de Economía mediante el cual Advantage Security lleva a cabo la mayoría de las funciones de AR frontales o de AC de fondo en nombre de una organización.
Administración Automatizada	Un procedimiento mediante el cual se aprueba automáticamente Solicitudes de Certificado si la información de inscripción corresponde a la información contenida en la base de datos.
Módulo de Software de Administración Automatizado	Software proporcionado por Advantage Security que lleva a cabo Administración Automatizada.
Certificado	Un mensaje que, por lo menos, indica el nombre o identifica a la AC, identifica al Suscriptor, contiene la clave pública del Suscriptor, identifica el Periodo de Operación del Certificado, contiene el número de serie del Certificado y está firmado digitalmente por la AC.
Solicitante del Certificado	Una persona u organización que pide la emisión de un Certificado por una AC.
Solicitud de Certificado	Una petición de un Solicitante de Certificado (o agente autorizado del Solicitante de Certificado) a una AC para la emisión de un Certificado.
Cadena de Certificado	Una lista ordenada de los Certificados, que contiene un Certificado del Suscriptor usuario final y Certificados de la AC, que termina en un Certificado Raíz.
Objetivos de Control de Administración del Certificado	Criterios que debe cubrir una entidad, con el fin de satisfacer la Auditoria de Cumplimiento.
Políticas de los Certificados (CP)	El documento titulado "Políticas de los Certificados de Advantage Security " y es la declaración de política principal que rige a a certificados de la jerarquía de la Secretaría de Economía.
Lista de Revocación de Certificados (CRL)	Una lista emitida periódicamente (o exigentemente), firmada en forma digital por una AC, de Certificados identificados que han sido revocados antes de sus fechas de vencimiento. La lista generalmente indica el nombre de usuario de la CRL, la fecha de emisión, la fecha de la siguiente emisión programada de la CRL, los números de serie de los Certificados revocados y la hora y motivos específicos de la revocación.
Solicitud de Firma de Certificado	Mensaje que transmite una solicitud de emisión de Certificado.
Autoridad de Certificación (CA)	Entidad autorizada para emitir, administrar, revocar y renovar Certificados.
Declaración de Prácticas de Certificación (CPS)	Declaración de las prácticas que Advantage Security utiliza para aprobar o rechazar Solicitudes de Certificado y emitir, administrar y revocar Certificados, y exige que las empleen sus Clientes. En el contexto de esta CPS, "CPS" se refiere a este documento.

Frase de Desafío	Una frase secreta que escoge un Solicitante de Certificado durante la inscripción de un Certificado. Cuando se emite un Certificado, el Solicitante del Certificado se convierte en Suscriptor y una AC o AR puede usar la Frase de Desafío para autenticar al Suscriptor cuando éste trata de revocar o renovar el Certificado del Suscriptor.
Clase	Un nivel específico de garantías, como se define dentro de la CPS. Ver el artículo 1.1.1 de la CPS. Las distinciones se resumen en el artículo 1.1.1 de la CPS.
Certificado de Advantage Security Clase 2	Certificado Clase 2 , emitido por Advantage Security o un Agente Certificador de Advantage Security.
Centro de Servicio al Cliente	Centro de Servicio que es Filiar que proporciona Certificados del cliente en la línea de negocios ya sea del Consumidor o de Empresa.
Auditoria de Cumplimiento	Una auditoria periódica que se le practica a un Centro de Procesamiento o Centro de Servicio para determinar su conformidad con las Normas de la jerarquía de la Secretaría de Economía que se le aplican.
Compromiso	Una violación (o sospecha de violación) de una política de seguridad, en la que pudo haber habido una divulgación no autorizada, o pérdida de control sobre información sensible. Con respecto a las claves privadas, un Compromiso es una pérdida, robo, divulgación, modificación, uso no autorizado, u otro compromiso de la seguridad de dicha clave privada.
Información Confidencial/ Privada	La información que debe mantenerse en forma confidencial y privada, de conformidad con el artículo 2.8.1 de la CPS.
Consumidor, como en Centro de Servicio del Consumidor	Línea de negocios que una Filial emprende para proporcionar Certificados al Menudeo a Solicitantes de Certificado.
Contrato de Uso de la CRL	Contrato que establece los términos y condiciones bajo los que se puede usar una CRL o la información.
Cliente	Organización que es Cliente Advantage Security.
Recibo Digital	Objeto de datos creado con respecto al Servicio de Estampilla de Tiempo que ofrece Advantage Security y firma digitalmente la Autoridad que estampa la Hora y comprende la comprobación aleatoria de un documento o serie de datos y un sello de la hora que muestra que el documento o datos existieron en un momento determinado.
Intercambio de Datos Electrónicos (EDI)	El intercambio de una computadora a otra de transacciones de negocios, como órdenes de compra, facturas y avisos de pago, de acuerdo con las normas aplicables.
Certificado de Intercambio de Datos Electrónicos (Certificado EDI)	Un Certificado organizacional Clase 2 que permite que haya firmas digitales en los mensajes de Intercambio Electrónico de Datos y la encripción de mensajes de EDI.
Empresa, como en el Centro de Servicio de Empresa	Una línea de negocios en la que entra una Filial para proporcionar servicios de certificación digital.
Guía de Seguridad de Empresa	Documento que establece los requisitos y prácticas de seguridad para los Clientes.

Auditoria Exigente/ Investigación	Auditoria o investigación de Advantage Security en la que éste tiene motivos para creer que hubo un incumplimiento de la entidad con las Normas de la jerarquía de la Secretaría de Economía, un incidente o Compromiso relativo a la entidad, o una amenaza real o potencial a la seguridad de la jerarquía de la Secretaría de Economía planteada por la entidad.
Identificación del Servidor Global	Certificado organizacional Clase 2 usado para soportar sesiones SSL entre los exploradores de la Web y los servidores de la Web que se encriptan usando una fuerte protección criptográfica congruente con las leyes de exportación aplicables.
Servidor Global en el Sitio	Igual que arriba pero incorpora tecnología (SGC) Server Gateway Crypto.
Go Secure!	Una serie (suite) de servicios de plugandplay que se construyen sobre los servicios de cliente y están diseñados para acelerar las solicitudes de comercio electrónico.
Autoridad Certificadora de Infraestructura (AC de Infraestructura)	Tipo de AC de Advantage Security que emite Certificados para componentes de la infraestructura de Advantage Security que soporta ciertos servicios de Advantage Security . Las AC de Infraestructura no emiten Certificados de la AC, AR o del Suscriptor usuario final
Derechos de Propiedad Intelectual	Derechos bajo uno o más de los siguientes: patente, secreto industrial, marca registrada y cualquier otro derecho de propiedad intelectual.
Autoridad Certificadora Intermedia (CA Intermedia)	Autoridad de Certificación cuyo Certificado se encuentra dentro de una Cadena de Certificados entre el Certificado de la AC Raíz y el Certificado de la Autoridad de Certificación que emitió el Certificado del Suscriptor usuario final.
Guía de Referencia de la Ceremonia de la Clave	Documento que describe los requisitos y prácticas de la Ceremonia de Generación de la Clave.
Ceremonia de Generación de la Clave	Procedimiento mediante el cual se genera un par de claves de AC o AR, transferencia de la llave privada a un módulo de hardware seguro y el respaldo/almacén del mismo.
Autenticación Manual	Procedimiento mediante el cual un Administrador que usa una interfase basada en la Web, revisa y aprueba en forma manual, una por una, las Solicitudes de Certificado.
Información del Suscriptor No Verificada	La información presentada por un Solicitante de Certificado a una AC o AR, y que se incluye dentro de un Certificado, que no ha sido confirmada por la AC o la AR y con respecto a la cual la AC o AR aplicable no da garantías que no sea que la información fue presentada por el Solicitante del Certificado.
Sin repudio	Atributo de una comunicación que ofrece protección contra una parte de una comunicación que niega falsamente su origen, negando que se presentó o negando su entrega. La negación de origen comprende la negación de que una comunicación se originó de la misma fuente que una secuencia de uno o más mensajes previos, aun si la identidad asociada con el remitente se desconoce. Nota: sólo la adjudicación de un tribunal, panel de árbitros, u otro tribunal puede finalmente evitar el repudio. Por ejemplo, una firma digital que se verifique con referencia a un Certificado de la jerarquía de la Secretaría de Economía puede ofrecer una prueba que apoye la determinación de No repudio de un tribunal, pero en sí misma no constituye un No repudio.

Protocolo del Estado del Certificado en Línea (OCSP)	Protocolo para darle a las Partes que Confían información del estado del Certificado de tiempo real.
Periodo de Operación	El periodo que empieza en la fecha y hora en que se emite un Certificado (o en una fecha y hora posterior, si se indica en el Certificado) y que termina en la fecha y hora en la que se vence el Certificado o se revoca antes.
PKCS #10	Norma #10 de Criptografía de la Clave Pública, desarrollada por RSA Security Inc., la cual define una estructura para una Solicitud de Firma de certificado.
PKCS #12	Norma #12 de Criptografía de la Clave Pública, desarrollada por RSA Security Inc., la cual define un medio seguro para la transferencia de claves privadas.
Autoridad de Administración de Política (AAP)	Organización dentro de Advantage Security , responsable de promulgar esta política a través de jerarquía de la Secretaría de Economía.
Autoridad de Certificación Primaria (PCA)	CA que funge como base de la AC con respecto a una Clase de Certificados específica y emite Certificados a las AC subordinadas a ella.
Centro de Procesamiento	Organización de Advantage Security que crea un alojamiento seguro, entre otros, los módulos criptográficos que se usan para la emisión de Certificados, entre otros, los módulos criptográficos usados para la emisión de Certificados. En las líneas de negocios del Consumidor y del Sitio Web, los Centros de Procesamiento fungen como AC dentro de jerarquía de la Secretaría de Economía y llevan a cabo todos los servicios del ciclo de vida del Certificado de emitir, administrar, revocar y renovar Certificados. En la línea de negocio de Empresa, los Centros de Procesamiento proporcionan servicios del ciclo de vida en nombre de sus Clientes.
Infraestructura de la Clave Pública (PKI)	La arquitectura, organización, técnicas, prácticas y procedimientos que soportan colectivamente la implementación y operación de un sistema criptográfico de clave pública, basado en el Certificado. La PKI de jerarquía de la Secretaría de Economía consiste en sistemas que colaboran para proporcionar e implementar la jerarquía de la Secretaría de Economía.
Autoridad de Registro (AR)	Entidad aprobada por una AC para ayudar a los Solicitantes de Certificado a solicitar Certificados, y a aprobar o rechazar Solicitudes de Certificado, revocar Certificados o renovar Certificados.
Parte que Confía	Persona u organización que funge basándose en un certificado y/o firma digital.
Contrato de la Parte que Confía	Contrato que usa una AC que establece los términos y condiciones bajo los cuales una persona u organización funge como Parte que Confía.
Certificado al Menudeo	Certificado que emite Advantage Security , en calidad de AC, a personas u organizaciones, que presentan su solicitud una por una a Advantage Security en su sitio Web.
RSA	Sistema criptográfico de clave pública inventado por Rivest, Shamir, y Adelman.
Acción Secreta	Porción de una clave privada de la AC o porción de los datos de activación necesaria para operar la clave privada de una AC conforme a un contrato de Participación Secreta.

Participación Secreta	La práctica de dividir la clave privada de una AC o los datos de activación para operar la clave privada de una AC, con el fin de hacer valer el control de varias personas sobre las operaciones de clave privada de la CA, de conformidad con el artículo 6.2.2 de la CPS.
Identificación del Servidor Seguro	Certificado organizacional Clase 2 , usado para soportar sesiones entre los exploradores de la Web y los servidores de la Web.
Secure Sockets Layer (SSL)	El método estándar de la industria para proteger comunicaciones de la Web desarrollada por Netscape Communications Corporation. El protocolo de seguridad de SSL proporciona encripción de datos, autenticación del servidor, integridad de mensajes y autenticación del cliente opcional para una conexión de, Protocolo de Control de la Transmisión/ Protocolo de Internet.
Guía de Requisitos de Seguridad y Auditoria	Documento de Advantage Security que establece los requisitos de seguridad y prácticas para los Centros de Procesamiento y los Centros de Servicio.
Revisión de la Seguridad y las Prácticas	Revisión de Advantage Security antes de que se le permita a una Filial ser operativa.
Criptografía con Acceso del Servidor	Tecnología que permite que los servidores de la Web a los que se emitió una Identificación del Servidor Global, creen una sesión SSL con un explorador que esté encriptado usando una protección criptográfica fuerte.
Centro de Servicio del Servidor	Centro de Servicio que es Filial que proporciona Identificaciones del Servidor Seguro e Identificaciones del Servidor Global, ya sea en el Sitio Web o en la línea de negocios de Empresa.
Centro de Servicio	Filial que no aloja unidades de firma de Certificado para la emisión de Certificados, con el fin de emitir Certificados para una Clase o tipo específico, sino que depende de un Centro de Procesamiento para llevar a cabo la emisión, administración, revocación y renovación de los citados Certificados.
Subdominio	Porción de jerarquía de la Secretaría de Economía que controla una entidad y todas las entidades subordinadas a ésta dentro de la jerarquía de la Secretaría de Economía.
Sujeto o Asunto	El tenedor de una clave privada que le corresponde a una clave pública. El término "Sujeto" o "Asunto" puede, cuando se trata de un Certificado organizacional, referirse al equipo o dispositivo que tiene una clave privada. A un Sujeto se le asigna un nombre no ambiguo, que se destina a la clave pública contenida en el Certificado del Sujeto.
Suscriptor	Cuando se trata de un Certificado individual, una persona que es Sujeto de un Certificado a se le ha emitido uno. Cuando se trata de un Certificado organizacional, una organización que es propietaria del equipo o dispositivo que es el Sujeto de un Certificado y al que se le ha emitido éste. Un Suscriptor puede usar un Certificado, y está autorizado a usarlo. Un Suscriptor puede usar la clave privada que le corresponde a la clave pública anotada en el Certificado, y la puede usar.
Contrato del Suscriptor	Contrato usado por una AC o AR que establece los términos y condiciones bajo las cuales un persona u organización funge como Suscriptor
Entidad Superior	Entidad sobre una cierta entidad dentro de la jerarquía de la Secretaría de Economía (jerarquía Clase 2).

Revisión de la Administración del Riesgo Suplementaria	Revisión de una entidad de parte de Advantage Security después de encontrar casos incompletos o excepcionales en una Auditoria de Cumplimiento de la entidad o como parte de un proceso de administración de riesgos global en el curso ordinario de los negocios.
Revendedor	Entidad que comercializa servicios en nombre de Advantage Security o una Filial a mercados específicos.
Autoridad de Estampilla de Tiempo	La entidad de Advantage Security que firma Recibos Digitales como parte del Servicio de Estampilla de Tiempo.
Persona de Confianza	Empleado, contratista o consultor de una entidad dentro de jerarquía de la Secretaría de Economía, responsable de manejar la confiabilidad infraestructural de la entidad, sus productos, sus servicios, sus instalaciones y/o sus prácticas, como se define más adelante en el artículo 5.2.1 de la CPS.
Posición de Confianza	Las posiciones dentro de una entidad de jerarquía de la Secretaría de Economía que debe ocupar una Persona de Confianza.
Sistema Confiable	Hardware, software, y procedimientos de computación que son razonablemente seguros de intrusión y mal uso; proporcionan un nivel razonable de disponibilidad, confiabilidad y operación correcta; están adaptados razonablemente para cumplir con las funciones para la que fueron hechos, y hacen valer la política de seguridad aplicable. Un sistema confiable no es necesariamente un "sistema de confianza" como se reconoce en la nomenclatura gubernamental clasificada.
Repositorio de Advantage Security	La base de datos de Certificados de Advantage Security y otra información pertinente de Advantage Security como miembro de la jerarquía de la Secretaría de Economía que está accesible en línea.
Política de Seguridad de Advantage Security	El documento de más alto nivel que describe las políticas de seguridad de Advantage Security.
Participantes en el Subdominio de Advantage Security	Persona u organización que es uno o más de los siguientes dentro del Subdominio de Advantage Security de jerarquía de la Secretaría de Economía: Advantage Security , un Cliente, un Revendedor, un Suscriptor o una Parte que Confía.
Participante en jerarquía de la Secretaría de Economía	Persona u organización que es uno o más de los siguientes dentro de jerarquía de la Secretaría de Economía, un Prestador de Servicios de Certificación, un Cliente, un Revendedor, un Suscriptor o una Parte que Confía.
Normas de la jerarquía de la Secretaría de Economía	Los requisitos comerciales, legales y técnicos para emitir, administrar, revocar, renovar y usar Certificados dentro de jerarquía de la Secretaría de Economía.
Anfitrión de Web	Entidad que aloja el sitio Web de otra, como un proveedor de servicio de Internet, un integrador de sistemas, un Revendedor, un asesor técnico y un proveedor de servicios de aplicación, o una entidad similar.
Programa del Anfitrión de Web	Programa que permite que los Anfitriones de la Web se inscriban para obtener Identificaciones de Servidor Seguro e Identificaciones de Servidor Global en nombre de los Suscriptores usuarios finales que son clientes de Anfitriones de la Web.
Sitio Web, como en el Centro de Servicio de Sitios Web	Línea de negocios en la que entra una Filial para proporcionar Certificados al Menudeo de Identificaciones del Servidor Seguro e Identificaciones del Servidor Global, uno por uno, a los Solicitantes de Certificado.