PSC Advantage

Advantage Security, S. de R.L. de C.V.
Políticas de Certificación

Versión 2.0

Fecha de Efectividad: 1 de Septiembre 2005

OID 2.16.484.101.10.316.2.1.1.1.1.1.2

Políticas de Certificación de Advantage Security, S. de R.L. de C.V.

©2005 Advantage Security, S. de R.L. de C.V. Todos los derechos reservados.
Impreso en los Estados Unidos de América

Fecha de publicación 1 de septiembre de 2005.

Avisos de marcas

Sin limitación a los derechos reservados anteriormente y excepto como lo establece la licencia a continuación, ninguna parte de esta publicación puede ser reproducida, almacenada o introducida en un sistema de recuperación o transmitida, de cualquier forma o por cualquier medio, (electrónico, mecánico, fotocopia, registro, o en contrario) sin el previo permiso de Advantage Security, S. de R.L. de C.V.

Independientemente de lo anterior, el permiso se otorga para reproducir y distribuir estas Políticas de Certificación de Advantage Security de manera no exclusiva libres de regalías, en la inteligencia de que (i) el aviso de derechos de autor anterior y los párrafos iniciales sean prominentemente exhibidos al principio de cada copia y (ii) este documento sea reproducido exactamente en su totalidad, completo con los créditos del documento a Advantage Security, S. de R.L. de C.V..

Las solicitudes de cualquier otro permiso para reproducir estas Políticas de Certificación de Advantage Security, (así como las solicitudes de las copias de Advantage Security), deben ser dirigidas a Advantage Security, S. de R.L. de C.V., Av. Prolongación Reforma 625 Desp. 402 – Paseo de las Lomas Santa Fé – México DF 01330 - Atención Desarrollo de Prácticas Te: +52 55 5081 4366 Fax: +52 55 5081 4376 o practicas@advantage-security.com.

INTRODUCCIÓN

La Jerarquía de la Secretaría de Economía (JSE) es una PKI de México que comprende una gran comunidad pública y ampliamente distribuida de usuarios con diversas necesidades de comunicación y seguridad de información. Advantage Security ofrece servicios de JSE junto con una red de Prestadores de Servicios de Certificación (PSC) en México.

Este documento, las políticas de "La Jerarquía de la Secretaría de Economía" (CP) es el establecimiento principal de políticas que gobiernan la JSE. La CP establece los requerimientos de negocios, legales y técnicos para aprobar, emitir, administrar, utilizar, cancelar y renovar los Certificados digitales dentro de la JSE y proporcionar servicios de confiabilidad asociados para todos los participantes dentro de la JSE. Estos requerimientos protegen la seguridad e integridad de la JSE y comprenden reglas que aplican consistentemente en toda la JSE, proporcionado con ellos el aseguramiento de una confiabilidad uniforme en toda la JSE. La CP no es un contrato legal entre Advantage Security y los participantes de la JSE; más bien establece las obligaciones contractuales entre Advantage Security y los participantes de la JSE por medio de los contratos con dichos participantes.

Este documento está dirigido a:

- Proveedores de Servicios de Certificación de JSE de PKI, que tienen que operar en términos de sus propias Declaraciones de Prácticas de Certificación (CPS *por su siglas en inglés*) mismas que cumplen con los requerimientos establecidos por la CP.
- Los Suscriptores de certificados de la JSE que necesitan comprender cómo son autentificados y cuáles son sus obligaciones como Suscriptores de la JSE y cómo se protegen conforme a la JSE.
- Partes Confiables que necesitan comprender qué tanta confianza tener en un Certificado de JSE, o en una firma digital utilizando ese Certificado.

La CP, sin embargo, no controla ningún servicio de proporcionado por Advantage Security, por ejemplo, aprueban solicitudes de certificación y subcontratan con Advantage Security las funciones de soporte final de expedición de certificados, administración, cancelación y renovación. Ya que la CP aplica únicamente a la JSE, no aplica a estas jerarquías privadas.

1.1 Panorama

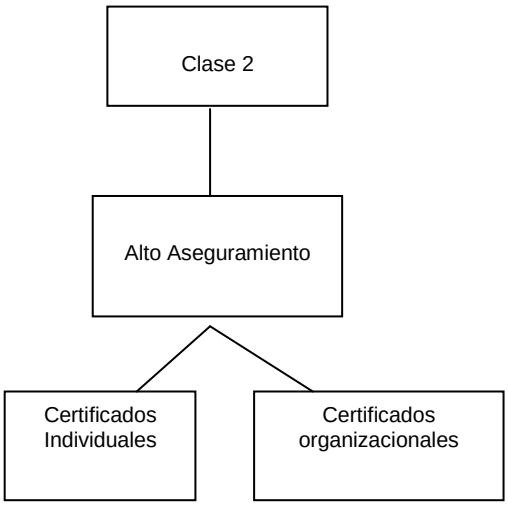
Un panorama de la estructura de la JSE se muestra en el Diagrama 1 a continuación. En la parte superior de la jerarquía está la CP que establece las políticas bajos las cuales los participantes de la JSE deben operar.

Las Autoridades Registradoras (ARs) son entidades que autentifican solicitudes de certificados conforme a la JSE. Advantage Security actúa como AR para los certificados que expide. En algunos casos, Advantage Security puede subcontratar a Agentes Certificadores salvo a previa autorización de la Secretaría de Economía y por ende puede celebrar relaciones contractuales con dichos Agentes Certificadores. Estos Agentes Certificadores se integran a la AR de Advantage Security, autentificando solicitudes de

Certificado para personas físicas y morales. Advantage Security entonces expedirá estas solicitudes autentificadas de certificación.

Los Certificados Digitales podrán ser utilizados por los Suscriptores para asegurar los sitios Web, el código de firma digitalmente u otro contenido, documentos firmados digitalmente y/o correos electrónicos. A la persona que finalmente recibe un documento firmado o comunicación o accesa un sitio Red seguro es referida como la parte confiable, por ejemplo, esa persona está confiando en el Certificado y tiene que tomar la decisión de si puede confiar en el o no. Una Parte Confiable debe confiar en un Certificado en términos de si el contrato de la Parte Confiable está incluido en el Certificado.

El diagrama 1 a continuación proporciona un resumen de las clases de certificados conforme a la JSE, a quién pueden ser expedidos y sus respectivos niveles de aseguramiento basados en los procedimientos de identificación y autenticación requeridas por cada uno. Esta CP describe a detalle la identificación y autenticación llevada a cabo para cada Clase de Certificado.



Diagramas 1. Clases de Certificados de la JSE

1.2 Nombres del Documento e Identificación

Este documento es la política de certificación de Advantage Security dentro de la JSE (CP). Advantage Security, actuando como la empresa que define la política, ha asignado a extensión de valor de identificador objeto para cada Clase de Certificado expedido conforme a Advantage Security dentro de la JSE. Los valores de identificador utilizados para las Clases de Certificados de Suscriptor usuario final:

- Política de Certificado: 2.16.484.101.10.316.2.1.1.1.1.1.2
- Participantes de la PKI

1.2.1 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 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 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.

1.2.2 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 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.

1.2.3 Suscriptores

Los Suscriptores bajo la JSE incluye a todos los usuarios finales (incluyendo la entidad) de Certificados expedidos por una PSC de la JSE. Un Suscriptor es una entidad nombrada como Suscriptor usuario final de un certificado. Los Suscriptores usuario final podrán ser personas físicas, organizaciones o componentes de infraestructura tales como sistemas de seguridad, ruteadores, servidores confiables u otros dispositivos utilizados para asegurar las comunicaciones dentro de una organización.

Cuando se utiliza “Asunto” es para indicar una distinción del Suscriptor. Cuando se utiliza “Suscriptor” podrá significar solamente el Suscriptor como una entidad distinta pero podrá también utilizar el término para comprender los dos. El contexto de su uso en esta CP referirá el entendimiento correcto.

Las ACs son técnicamente Suscriptores de Certificados dentro de la JSE, ya sea como una PSC que expide un Certificado autofirmado y co-firmado por la Secretaría de Economía para sí misma. Las referencias a las “entidades finales“ y los “Suscriptores” en esta CP sin embargo, aplican solamente para los Suscriptores usuarios finales.

1.2.4 Partes Confiables

Una Parte Confiable es una persona o entidad que actúa con la confianza de un Certificado y/o una firma digital expedida conforme a la JSE. Una Parte Confiable podrá o no podrá también ser un Suscriptor dentro de la JSE.

1.3 Uso de Certificado.

1.3.1 Usos Apropiados de Certificado

1.3.1.1 Certificados Expedidos a Personas

Los Certificados individuales se utilizan normalmente por las personas para firmar y encriptar los correos electrónicos y para autenticar las solicitudes (autenticación de clientes). Mientras que los usos más comunes de Certificados individuales se incluyen en la Tabla a continuación, un certificado individual podrá ser utilizado para otros propósitos, en la inteligencia de que una Parte Confiable pueda razonablemente confiar en ese Certificado y que el uso no esté prohibido en contrario por la Ley, por esta CPA, por cualquier CPS conforme a la cual el certificado haya sido expedido y de conformidad con cualquier acuerdo con los Suscriptores.

Clase de Certificado	**Nivel de Aseguramiento**	**Uso**		
Certificados Clase 2	**Nivel alto de aseguramiento**	**Firma**	**Encriptación**	**Autenticación de Cliente**

Tabla 1. Uso de Certificado Individual

1.3.1.2 Los Certificados Expedidos a Organizaciones

Los Certificados Organizacionales, también conocidos como certificados de persona moral, son expedidos después de que se autentifica que la Organización legalmente y las características de esta otra organización incluidas en el Certificado (excluyendo información del Suscriptor no verificado) existen, por ejemplo, la titularidad de un dominio de Internet o correo electrónico. No es la intención de esta CP limitar los tipos de usos de Certificados Organizacionales. Mientras que los usos más comunes se incluyen en la tabla a continuación, un Certificado organizacional podrá ser utilizado para otros

propósitos, en la inteligencia de que una Parte Confiable pueda razonablemente confiar en que este Certificado y el uso no está en contrario prohibido por la Ley, por esta CP, por cualquier CPS bajo la cual el Certificado haya sido expedido y conforme a cualquier contrato con Suscriptores.

Clase de Certificado	**Nivel De Aseguramiento**	**Uso**			
Certificados Clase 2	**Nivel alto de aseguramiento**	**Firma código contenido**	**Sesiones SSL-internet seguro**	**Autentificación**	**Firma y encriptación**
	✓	✓	✓	✓	✓

Tabla 2. Uso de Certificado Organizacional[1]

1.3.1.3 Nivel de Aseguramiento

Certificados de aseguramiento alto, son Certificados individuales y de organización Clase 2 que proporcionan un alto nivel de aseguramiento de la identidad del Suscriptor.

1.3.2 Usos Prohibidos de Certificado

Los Certificados se utilizarán únicamente en la medida en que el uso sea consistente con las leyes aplicables.

Los Certificados de la JSE no están diseñados, no tienen el propósito o no están autorizados para uso o reventa como equipo de control en circunstancias peligrosas para usos que requieran desempeño de error-seguridad, tal como la operación de instalaciones nucleares, navegación aérea o sistemas de comunicación, sistemas de control de tráfico aéreo o sistemas de control de armas, donde una falla podría llevar directamente a la muerte, lesiones corporales o a daño ambiental grave. Los Certificados de Clientes (certificados de persona física) son para las aplicaciones de los clientes y no se utilizarán como Certificados de servidor o u organizacionales (certificados de persona moral).

Los Certificados AC no podrán ser utilizados para ninguna función excepto funciones de AC. Además los Certificados de Suscriptor de Usuario Final no serán utilizados como Certificados AC.

1.4 Administración de Política

1.4.1 Organización que Administra el Documento

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

1.4.2 Persona de Contacto

At'n: Desarrollo de Prácticas – CPS
Advantage Security, S. de R.L. de C.V.
Teléfono: +52 55 5292 6000
Fax: +52 55 5292 6000 x250
practicas@advantage-security.com

1.4.3 Persona que Determina la Adecuación de la CP a la Política

El Gerente de Administración de la Política de Advantage Security determina la adecuación y la aplicabilidad de esta CP.

1.4.4 Procedimiento de Aprobación de CP

La aprobación de este CP y las modificaciones posteriores se harán mediante la PMA. Las modificaciones serán ya sea en el formato de un documento que contenga un formato modificado de la CP o un aviso de actualización. Las versiones modificadas o las actualizaciones serán asociadas a la sección de Actualizaciones de Prácticas y Avisos del Depósito de Advantage Security ubicado en: https://www.advantage-security.com/repositorio. Las actualizaciones reemplazan cualquier disposición designada o en conflicto de la versión referenciada de la CP. La PMA determinará si los cambios a la CP requieren un cambio en los identificadores objeto de las políticas de Certificado que corresponden a cada Clase de Certificado.

1.5 Definiciones de Acrónimos

Véase el apéndice A de la tabla de acrónimos y definiciones

2 Publicación y Responsabilidades del Depósito

2.1 Depósitos

Advantage Security es responsable de mantener un depósito en línea públicamente accesible, así como información de cancelación con relación a dichos Certificados.

2.2 Publicación de Información de Certificado

Advantage Security mantiene un depósito con base en la Red que permite a las Partes Confiables hacer solicitudes en línea con relación a cancelaciones y a otra información del estatus del Certificado. Advantage Security proporciona a las Partes Confiables la información de cómo encontrar el depósito adecuado para validar el estatus del Certificado, y, si el OCSP (Protocolo en Línea del Estatus del Certificado) está disponible, cómo encontrar el contestador OCSP correcto.

Advantage Security publicará en todo momento una versión actual de:

- Esta CP
- El CPS,
- Contratos del Suscriptor
- Contratos de Parte Confiable

2.3 Tiempo o Frecuencia de Publicación

La información de la AC se publica inmediatamente después de que se pone a disposición de la AC. Advantage Security ofrece CRLs que muestran la cancelación de los Certificados de Advantage Security y ofrecen los servicios de revisión de estatus a través de los Depósitos de Advantage Security. Si un Certificado listado en una CRL vence, podrá ser retirado de las CRLs expedidas subsecuentemente después del vencimiento del Certificado.

2.4 Controles de Acceso en Depósitos

Advantage Security no utilizará intencionalmente medios técnicos de acceso limitado a esta CP, sus CPS, Certificados, información de estatus de Certificado o las CRLs. Advantage Security sin embargo, requerirán que las personas celebren un Contrato de Persona Confiable o un Contrato de Uso de CRL como una condición para acceder a los Certificados, a la información de estatus del Certificado o a las CRLs. Advantage Security establecerá controles para prevenir que personas no autorizadas incluyan, eliminen o modifiquen registros de depósito.

3 Identificación y Autenticación

3.1 Nombres

A menos que se indique en contrario en esta CP, las CPs relacionadas o el contenido del Certificado digital, los nombres que aparecen en los Certificados expedidos de conformidad con la JSE son autentificados.

3.1.1 Tipo de Nombres

Los Certificados de Suscriptor de usuario final contienen un nombre distinguido en el campo del nombre del Asunto.

El nombre distinguido del sujeto de los Certificados del Suscriptor de usuario final incluyen un el nombre común (CN=). El valor de nombre común autentificado incluido en los nombres distinguidos de sujeto de Certificados organizacionales será un nombre de dominio, una dirección de correo electrónico organizacional, el nombre legal de la organización dentro de la organización o el nombre del representante de la organización autorizado para utilizar la clave privada de la organización. El componente (o =) será el nombre legal de la Organización, el valor de nombre común incluido en el nombre distinguido del sujeto de los Certificados individuales representará el nombre personal generalmente aceptado de la persona. Los nombres comunes se han autentificado. Los Certificados de Advantage Security también podrán contener una referencia al Contrato de Parte Confiable en sus nombres distinguidos.

3.1.2 Necesidad de Nombres con Significado

Los Certificados de Suscriptor Clase 2 de usuario final incluirán nombres con significado en el siguiente sentido: Los Certificados del Suscriptor de usuario final Clase 2 contendrán nombres con semánticas comúnmente entendidas que permitan la determinación de la identidad de la persona o de la organización que sea el sujeto del Certificado.

3.1.3 Exclusividad de Nombres

Los nombres de los Suscriptores dentro de la JSE, serán únicos. Un Suscriptor podrá tener uno o más Certificados con el mismo Nombre Distinguido del asunto.

3.1.4 Reconocimiento, Autenticación y Papel de las Marcas

Los Solicitantes de Certificados no usarán nombres en sus solicitudes de Certificado que infrinjan los derechos de propiedad intelectual de otros. Ni se les requerirá a Advantage Security que determinen si un Solicitante de Certificado tiene derechos de propiedad intelectual en el nombre que aparece en una solicitud de Certificado o para entablar arbitraje, transigir o en contrario resolver cualquier disputa que se relacione con la titularidad de cualquier nombre de dominio, nombre comercial, marca o marca de servicio y Advantage Security, sin la responsabilidad ante ningún Solicitante de Certificado de rechazar o suspender cualquier solicitud de Certificado debido a dicha disputa.

3.2 Validación de Identidad Inicial

3.2.1 Método para probar la posesión de la Clave Privada

El solicitante de Certificado debe demostrar que tiene los derechos legales sobre la clave privada que corresponde a la clave pública que se listará en el Certificado. El método para probar la posesión de una clave privada será PKCS #10, otra

demostración equivalente criptográficamente u otro método aprobado por Advantage Security.

3.2.2 Autentificación de la Identidad de la Organización

Cada vez que un Certificado contenga un nombre de organización la identidad de la organización y otra información relacionada proporcionada por los solicitantes del Certificado, (excepto para información del Suscriptor no verificado) es confirmada de conformidad con los procedimientos establecidos en los procesos de validación documentados de Advantage Security.

Como mínimo Advantage Security:

- Determinará que la organización existe utilizando por lo menos la identidad de un tercero que pruebe el servicio o la base de datos, o alternativamente, documentación organizacional expedida o presentada ante una Agencia gubernamental aplicable o autoridad reconocida que confirme la existencia de la organización.
- Confirmarán por teléfono, mediante correo postal, o procedimiento comparable con el Solicitante de Certificado cierta información de la organización, de que la organización ha autorizado la solicitud de Certificado y que la persona que presenta la solicitud de Certificado en representación del solicitante de certificación está autorizada para hacerlo. Cuando un Certificado incluya el nombre de una persona como un representante autorizado de la organización, también se confirmará que esa persona trabaja en esa organización y su autoridad para actuar en representación de la misma.

En el caso de que un nombre de dominio o una dirección de correo electrónico se incluyan en el Certificado Advantage Security autentifique el derecho de la organización para utilizar ese nombre de dominio ya sea como un nombre de dominio totalmente calificado o un dominio de correo electrónico.

3.2.3 Autentificación de Identidad Individual

Los procedimientos de autentificación para la identidad individual varían conforme a la clase de Certificado. El estándar mínimo de autentificación para el Certificado de la JSE se explica en la Tabla 3 a continuación.

Clase de Certificado	Autentificación de Identidad
Clase 2	La autentificación de Certificados Individuales Clase 2 está basada en la presencia personal (física) del solicitante del Certificado ante una agente de la AC o AR o ante un notario público u otro funcionario con capacidad comparable dentro de la jurisdicción del solicitante del Certificado. El representante, notario u otro funcionario revisará la identidad del solicitante de Certificado contra una identificación con fotografía expedida por el gobierno bien reconocida, tal como el

	pasaporte, cedula profesional y otra credencial de identificación. El Certificado de administrador Clase 2 también incluirá autentificación de la organización y una confirmación de la organización de que la persona trabaja en esa organización y de la autorización para actuar como administrador de la misma. Advantage Security, podrá también tener la oportunidad de aprobar solicitudes de Certificado para sus propios administradores. Los administradores son "Personas de Confianza" conocidos como Agentes Certificadores dentro de una organización. En este caso, la autentificación de sus solicitudes de Certificado se basará en la confirmación de su identidad con relación a su trabajo o retención como un contratista independiente y los procedimientos de revisión de antecedentes.

Tabla 3. Autentificación de identidad de una Persona

3.2.4 Validación de Autoridad

En el caso de que el nombre de una persona esté asociado con el nombre de una Organización en un certificado de tal manera que indique la afiliación de la persona o la autorización para actuar en representación de la Organización, la AC o la AR:

- Determina que la organización existe utilizando por lo menos el servicio de un tercero identificador o una base de datos o alternativamente, documentación de la empresa expedida o presentada ante agencias gubernamentales aplicables o autoridad reconocida que confirme la existencia de la organización, y
- Utiliza información contenida en los registros de negocios o bases de datos de información de negocios (directorios de empleados o clientes) de una AR que apruebe certificados para sus propias personas afiliadas o confirma por teléfono, por correo postal o con un procedimiento comparable con la organización, que la persona que presenta la Solicitud de Certificado trabaja en la organización y, cuando sea el caso, su autoridad para actuar en representación de la organización.

3.3 Identificación y Autentificación de solicitudes de Reclave

Antes del vencimiento de un Certificado de Suscriptor, es necesario que el Suscriptor obtenga un nuevo Certificado para mantener la continuidad del uso de Certificado. Las ACs y las ARs generalmente requieren que el Suscriptor genere una nueva clave par para reemplazar la clave par que se vence ("técnicamente definido como reclave"). Sin

embargo, en ciertos casos (por ejemplo para Certificados de servidor Red) los Suscriptores podrán solicitar un nuevo Certificado para una clave par existente, técnicamente definida “renovación”.

En términos generales, tanto la “Reclave” y “Renovación” son descritas comúnmente como una renovación de Certificados” enfocándose en el hecho de que el Certificado anterior está siendo reemplazado con un nuevo Certificado y no enfatizándose en si una nueva clave para se genera o no para todas las clases y tipos de Certificados Advantage Security, excepto para los Certificados de servidor de clase 2, esta distinción no es importante ya que una nueva clave par siempre se genera como parte del proceso de reemplazo de Certificado de Suscriptor de usuario final de Advantage Security. Sin embargo, existe una diferencia “re-claves” y “renovación” porque la clave par del Suscriptor se genera en el servidor Red y la mayoría de las herramientas de generación de clave en el servidor Red permiten la creación de una nueva solicitud de Certificado para una clave par ya existente.

3.3.1 Identificación y Autentificación para Rutina de Reclave

La entidad que aprueba una solicitud de Certificado para el Suscriptor de un usuario final será responsable de autentificar una solicitud de re-clave o renovación. Los procedimientos de re-clave aseguran que la persona u organización que busca renovar/obtener una re-clave para un Certificado de Suscriptor de usuario final es de hecho el Suscriptor del Certificado.

Un procedimiento aceptable es a través del uso de una Challenge Phrase (o el equivalente de la misma), o la prueba de la titularidad de la clave privada. Los Suscriptores escogen y presentan con su información de registro una Challenge Phrase. En el momento de la renovación de un Certificado, si un Suscriptor presenta correctamente la Challenge Phrase del Suscriptor (o el equivalente de la misma) con la información de nuevo registro de Suscriptor y la información de registro (incluyendo la información de contacto[2]) no ha cambiado, automáticamente se expide un Certificado de renovación.

Después de hacer la re-clave o la renovación de esta manera, y por lo menos las instancias y alternativas de re-claves o renovaciones posteriores la AC o la AR reconfirman la identidad del Suscriptor de acuerdo con los requerimientos de identificación y autentificación de solicitud de una solicitud original de Certificado.[3]

3.3.2 Identificación y Autentificación para Re-clave después de cancelación

La re-clave/renovación después de la cancelación no ocurre debido a:

- El Certificado fue expedida a una persona que era la persona nombrada como el asunto de Certificado o
- El Certificado fue expedido sin la autorización de la persona o identidad nombrada como el asunto de dicho Certificado o,

[2] Si la información de contacto ha cambiado mediante un procedimiento de cambio de contacto formal aprobado el Certificado todavía calificará para renovación automatizada.
[3] La autentificación de una solicitud para re-clave/renovación de un Certificado ASB Organizacional Clase 2, sin embargo, requiere el uso de una “Challenge Phrase”, así como la misma identificación y autentificación como para la Solicitud de Certificado original

- La identidad que aprueba la solicitud de Certificado de Suscriptor descubre o tiene razones para creer que un hecho importante en la solicitud del Certificado es falso.
- El Certificado se considera que puede dañar la JSE.

La renovación de un Certificado individual después de una cancelación debe asegurar que la persona que busque la renovación es, de hecho el Suscriptor. Un procedimiento aceptable es el uso de una “Challenge Phrase” (o el equivalente de la misma). Además de este procedimiento u otro procedimiento aprobado de Advantage Security los requerimientos para la identificación y autentificación de una solicitud de Certificado original serán utilizados para la renovación de un Certificado después de la cancelación.

3.4 Identificación y Autentificación de Solicitud de Cancelación

Los procedimientos de cancelación aseguran antes de cualquier cancelación de un certificación que la cancelación ha de hecho sido solicitada por el Suscriptor del Certificado, la entidad que aprueba la solicitud de Certificado o el centro de procesamiento aplicable.

Los procedimientos aceptables de autentificación para las solicitudes de cancelación de un Suscriptor incluyen.

- Que el Suscriptor presente para el Certificado la Challenge Phrase de Suscriptor (o el equivalente de la misma) y cancele el Certificado automáticamente si coincide la Challenge Phrase (o el equivalente de la misma) que se tiene en registros
- Recibir un mensaje del Suscriptor que solicite la cancelación y contenga una firma digital verificable con referencia al Certificado que se cancelará.
- Comunicación con el Suscriptor que proporcione aseguramiento razonable en base a la clase de Certificado de que la persona u organización solicitando la cancelación es, de hecho el Suscriptor. Dicha comunicación dependiendo de las circunstancias podrá incluir uno o más de lo siguiente: teléfono, fax, correo electrónico, dirección de correos o servicios de mensajería.

Los Agentes Certificadores tienen la capacidad de solicitar la cancelación de Certificados de Suscriptor usuario final dentro del Subdominio de la AC y AR. Advantage Security autentificará la identidad de los Agentes Certificadores mediante los controles de acceso utilizando el SSL y la autentificación del cliente antes de permitirles que lleven a cabo funciones de cancelación y otro procedimiento aprobado de la JSE.

Las solicitudes para cancelar un Certificado AC serán autentificadas por la entidad superior de la entidad solicitante para asegurar que la cancelación ha sido de hecho solicitada por la CA.

4 Certificados de Requerimientos Operacionales de Ciclo de Vida

4.1 Solicitud de Certificado

4.1.1 ¿Quién puede presentar una solicitud de Certificado?

A continuación se encuentra una lista de las personas que podrán presentar solicitudes de Certificado:

- Cualquier persona que sea el sujeto de Certificado
- Cualquier representante autorizado de una organización o entidad
- Cualquier representante autorizado de una AC
- Cualquier representante autorizado de una AR

4.1.2 Proceso de Registro y Responsabilidades

4.1.2.1 Suscriptores de Certificado de usuario final

Todos los Suscriptores de Certificados de usuario final manifestarán su consentimiento ante el contrato de Suscriptor relacionado que contiene las manifestaciones y garantías descritas en la sección 9.6.3 y pasarán un proceso de registro consistente en:

- Completar una solicitud de Certificado y proporcionar información veraz y correcta.
- General o hacer que se genere una clave par.
- Entregar su clave pública, directamente o a través de un AR al centro de procesamiento
- Demostrar la posesión de la clave privada correspondiente a la clave pública entregada al centro de procesamiento.

4.2 Proceso de solicitud de Certificado

4.2.1 Llevando a cabo la identificación y las funciones de autentificación

Una AR llevará a cabo la identificación y autentificación de toda la información requerida del Suscriptor de conformidad con la sección 3.2

4.2.2 Aprobación o Rechazo de solicitudes de Certificado

Una AR aprobará una solicitud de un Certificado si se cumple con los siguientes criterios:

- Identificación y Autentificación exitosa de toda la información requerida del Suscriptor de conformidad con la sección 3.2
- El pago (se aplica) ha sido recibido

Un AR rechazará una solicitud de Certificado si:

- La identificación y autentificación de toda la información requerida del Suscriptor de conformidad con la sección 3.2 no puede ser completadas o
- El Suscriptor incumple en proporción la documentación de respaldo cuando se le solicite
- El Suscriptor incumple a las notificaciones dentro de un tiempo específico o
- El pago (se aplica) no ha sido recibido o
- La AR cree que el expedir un Certificado al Suscriptor podría presentar a la JSE una disrepute

4.2.3 Tiempo para Procesar las Solicitudes de Certificado

Advantage Security comienza procesando las solicitudes de Certificado dentro de un tiempo razonable a partir de la recepción. No hay una estipulación de tiempo para completar el procesamiento de una solicitud a menos que se indique en contrario en el que contrato del Suscriptor relacionado, la acepte ese u otro contrato entre los participante de la JSE.

Una solicitud de Certificado permanece activa hasta que se rechaza.

4.3 Expedición de Certificado

4.3.1 Acciones de la AC durante la expedición del Certificado

Un Certificado se crea y se expide después de que la AC aprueba la solicitud de Certificado o después de recibir una solicitud de AR para expedir el Certificado. La AC crea y expide un Certificado al solicitante de Certificado con base a la información establecida en una solicitud de Certificado después de la aprobación de dicha solicitud.

4.3.2 Notificaciones del Suscriptor por parte de la AC de la expedición

La AC que expide los Certificados a los Suscriptores de usuario final ya sea directamente o a través de una AR, notificarán los Suscriptores que han creado dichos Certificados y proporcionado los Suscriptores de los excesos a los Certificados notificándoles que sus Certificados están disponibles y los medios para obtenerlos. Los Certificados estarán a disposición de los Suscriptores usuarios finales, ya sea permitiéndoles bajándolos de un sitio Red o vía un mensaje enviado al Suscriptor que contiene el Certificado.

4.4 Aceptación del Certificado

4.4.1 Acciones que Constituyen la Aceptación de un Certificado

La siguiente acción constituye la aceptación de un Certificado:

- Bajar un Certificado o instalar un Certificado desde un mensaje que lo adjunta constituye la aceptación del Suscriptor del Certificado.
- La ambición del Suscriptor en objetar el Certificado o su contenido constituye la aceptación de un Certificado.

4.4.2 Publicación de un Certificado por parte de la AC

Los Centros de Procesamiento publican los Certificados que expidan en un depósito públicamente accesible.

4.4.3 Notificación de Expedición de Certificado por parte de la AC a otras entidades

Las ARs podrán recibir notificación de la expedición de Certificados que ellos aprueben.

4.5 Clave Par y Uso de Certificado

4.5.1 Clave Privada del Suscriptor y Uso de Certificado

El uso de la clave privada corresponde ante la clave pública en el Certificado solamente será permitida una vez que el Suscriptor haya celebrado el contrato de Suscriptor y aceptado el Certificado. El Certificado será utilizado legalmente de conformidad con el contrato de Suscriptor de Advantage Security en los términos de esta CP y la CPS relacionada. El uso Certificado debe ser consistente con las extensiones de campo de uso de clave incluidas en el Certificado (por ejemplo si la Firma Digital no está activada entonces el Certificado no debe utilizarse para firma).

Los Suscriptores protegerán sus claves privadas del uso no autorizada y descontinuarán el uso de la clave privada después del vencimiento o cancelación del Certificado.

4.5.2 Clave Pública de la Parte Confiable y Uso del Certificado

Las partes confiables aceptarán los términos del contrato de Parte Confiable aplicable como una condición para confiar en el Certificado.

La confianza en un Certificado debe ser razonable bajo las circunstancias. Si las circunstancias indican una necesidad de aseguramientos adicionales, la Parte Confiable debe obtener dichos aseguramientos para que dicha confianza se considere razonable.

Antes de cualquier acto de confianza las Partes Confiables independientemente evaluarán

- La adecuación del uso de un Certificado para cualquier propósito dado y determinar que el Certificado de hecho, será utilizado para un propósito adecuado que no esté prohibido o encontrado restringido por esta CP. Advantage Security no es responsable de la evaluación de la adecuación del uso de un Certificado.
- Que el Certificado se esté utilizando de conformidad con las extensiones de campo del Uso de Clave incluido en el Certificado (por ejemplo si la firma digital no está activada entonces no puede confiarse en el Certificado para validar una firma del Suscriptor)
- El Estado del Certificado y todas las ACs en la cadena que expidieron el Certificado. Si cualquiera de los Certificados en la Cadena de Certificados han sido canceladas, la Parte Confiable no confiará en el Certificado del Suscriptor de usuario final u otro Certificado Cancelado en la cadena de Certificados.

Asumiendo que el uso del Certificado es adecuado, las Partes Confiables utilizarán el programa de cómputo y/o adecuado para llevar a cabo la verificación de la firma digital u otras operaciones criptográficas que deseen llevar a cabo como una condición de confianza en los Certificados con relación a cada una de dichas operaciones. Dichas operaciones incluyen identificar una Cadena de Certificado y verificar las firmas digitales en todos los Certificados y la Cadena de Certificación.

4.6 Renovación del Certificado

La renovación del Certificado es la expedición del nuevo Certificado para el Suscriptor sin cambiar la clave pública o cualquier otra información al Certificado. La renovación del Certificado está respaldada por Certificados clase 2 en donde la clave par se

genera en un servidor Red ya que la mayoría de las herramientas de generación de clave de servidor Red permiten la creación de una nueva Solicitud de Certificado para una clave para existente.

4.6.1 Circunstancias de renovación de Certificado

Antes del vencimiento de un Certificado de Suscriptor existente, es necesario que el Suscriptor renueve un nuevo Certificado para mantener la continuidad del uso de Certificado. Un Certificado también podrá ser renovado después del vencimiento.

4.6.2 ¿Quién puede solicitar renovación?

Solamente el Suscriptor de un Certificado individual o un representante autorizado para un Certificado organizacional podrá solicitar la renovación de Certificado.

4.6.3 Solicitudes de Proceso de Renovación de Certificado

Los procesos de renovación aseguran que la persona u organización que busca renovar un Certificado de Suscriptor de usuario final es de hecho Suscriptor (o autorizado por el Suscriptor) del Certificado.

Un proceso aceptable es a través del uso de frases de reto (o el equivalente de las mismas), o la prueba de la titularidad de la clave privada. Los Suscriptores seleccionan y presentar con su base de registro una Challenge Phrase (o el equivalente de las mismas). Al momento de la renovación de un Certificado, si un Suscriptor presenta correctamente la Challenge Phrase del Suscriptor (o el equivalente de las mismas) con la información de nuevo registro del Suscriptor y la información de registro incluyendo la información de contacto [4] nada ha cambiado, un Certificado de renovación es automáticamente expedido. Después de la renovación de esta manera en por lo menos en una de las instancias alternativas de renovación subsecuente, la AC o la AR reconfirma la identidad del Suscriptor de acuerdo con los requerimientos especificados en esta CP para la autentificación de una solicitud de Certificado original.

Otro proceso distinto a este u otro proceso aprobado de Advantage Security, los requerimientos para la autentificación de una solicitud de Certificado original se utilizarán para renovar un Certificado del Suscriptor de usuario final.

4.6.4 Notificación de una nueva expedición de Certificado para Suscriptor

La notificación de expedición de una renovación de Certificado al Suscriptor es de conformidad con la sección 4.3.2

[4] Si la información de contacto ha cambiado vía un procedimiento de cambio de contacto formal aprobado, el Certificado todavía calificará para renovación automatizada.

4.6.5 Conducta que constituye la Aceptación de un Certificado de renovación

La conducta que constituye la aceptación de un Certificado renovado es de conformidad con la sección 4.4.1

4.6.6 Publicación del Certificado de renovación por parte de la CA

El Certificado renovado se publica en el depósito públicamente accesible del centro de procesamiento que lo expida.

4.6.7 Notificación de Expedición de Certificado por parte de la AC a otras Entidades

Las ARs podrán recibir notificación de la expedición de Certificado que ellos aprueben.

4.7 Certificado de Re-clave

El Certificado de re-clave en la solicitud de expedición de un nuevo Certificado que certifique la nueva clave pública. El Certificado de re-clave es responsable por todas las clases de Certificados.

4.7.1 Circunstancias para Certificado de re-clave

Antes del vencimiento de un Certificado de Suscriptor existente, es necesario para el Suscriptor hacer una re-clave de Certificado para mantener la continuidad del uso de Certificado. Un Certificado también será re-clave después del vencimiento.

4.7.2 ¿Quién puede solicitar certificación de una nueva clave pública?

Solamente el Suscriptor de un Certificado individual a un representante autorizado de un Certificado organizacional puede solicitar la renovación de un Certificado.

4.7.3 Solicitudes de Procesamiento de Certificado de re-clave

Los procedimiento de re-clave aseguran que la persona o la organización que busca renovar un Certificado del Suscriptor de usuario final es de hecho el Suscriptor (o el autorizado por el Suscriptor) del Certificado.

Un procedimiento aceptable es través del uso de una Challenge Phrase (o el equivalente de la misma), o la prueba de la titularidad de la clave privada. Los Suscriptores eligen y presentan con su información de registro una Challenge Phrase (o el equivalente de la misma). En el momento de la renovación de un Certificado, si un Suscriptor presenta correctamente la Challenge Phrase del Suscriptor (o el equivalente de la misma) con la información de nuevamente registro de Suscriptor y la información de registro incluyendo la información de contacto[5], automáticamente se expide la renovación de un Certificado.

[5] Si la información de contacto ha cambiado vía o un procedimiento de cambio de contacto formal aprobado, el Certificado todavía calificará para renovación automatizada.

Después de la re-clave de esta manera, y por lo menos en una de las instancias alternativas de re-clave posterior la AC o la AR reconfirmarán la identidad del Suscriptor de conformidad con los requerimientos especificados en esta CP para la autentificación de una solicitud de Certificado original.

Otro proceso distinto a este u otro proceso aprobado de Advantage Security, los requerimientos para la autentificación de una solicitud de Certificado original se utilizarán para la re-clave de un Certificado del Suscriptor de usuario final.

4.7.4 Notificación de expedición de nuevos Certificados del Suscriptor

La notificación de expedición de un Certificado de re-clave al Suscriptor está de conformidad con la sección 4.3.2

4.7.5 Conductas que Constituye Aceptación de un Certificado de Re-clave

La conducta que constituye la aceptación de un Certificado de re-clave está de conformidad con la sección 4.4.1

4.7.6 Publicación de un Certificado de Re-clave por parte de la AC

El Certificado de re-clave está publicado en el depósito públicamente accesible del centro de procesamiento que lo expide.

4.7.7 Notificación de expedición de Certificados por parte de la AC a otras Entidades

Las ARs podrán recibir notificación de expedición de expedición de Certificado que ellos aprueban.

4.8 Modificación de Certificado

4.8.1 Circunstancia de Modificación y Certificado

La modificación de Certificado se refiere a la solicitud para la expedición de un nuevo Certificado debido a cambios en la información en un Certificado existente (otros que no sea la clave pública del Suscriptor)

La modificación del Certificado se considera una solicitud de Certificado en términos de la sección 4.1

4.8.2 ¿Quién puede solicitar una modificación de Certificado?

Véase la sección 4.1.1

4.8.3 Solicitudes de Proceso de Modificación de Certificado

Una AR llevará a cabo identificación y autentificación de toda la información del Suscriptor requerida en términos de la sección 3.2

4.8.4 Notificación de una Expedición de un Nuevo Certificado a Suscriptor

Véase la sección 4.3.2

4.8.5 Acciones que constituyen la Aceptación del Certificado Modificado

Véase la sección 4.4.1

4.8.6 Publicación del Certificado modificado por parte de la AC

Véase la sección 4.4.2

4.8.7 Notificación de la Expedición de Certificado por parte de la AC a otras Entidades

Véase la sección 4.4.3

4.9 Cancelación y Suspensión de Certificado

4.9.1 Circunstancias de Cancelación

Solamente en las circunstancias listadas a continuación un Certificado del Suscriptor de usuario final será revocado por un centro de Procesamiento (o por el Suscriptor) y publicado en una CRL. A la solicitud de un Suscriptor que no pueda utilizar más (o que no desee utilizar más) un Certificado por una razón que no sea la mencionada a continuación, Advantage Security pondrá un aviso en el Certificado como inactivo en su base de datos, pero no publicará el Certificado en una CRL.

Un Certificado del Suscriptor de usuario final se cancela así:

- Advantage Security, un cliente o un Suscriptor tiene razón para creer o sospecha fuertemente que ha habido una manipulación de la clave privada del Suscriptor.
- Advantage Security o un cliente tiene razones para creer que el Suscriptor ha violado de manera importante una obligación, manifestación o garantía importante de conformidad con el contrato de Suscriptor aplicable
- El contrato de Suscriptor con el Suscriptor ha sido terminado
- La Afiliación entre una Cliente compañía con un Suscriptor se da por terminado o ha terminado en contrario.
- La afiliación entre una organización que es un Suscriptor de un Certificado organizacional Clase 2 y el representante organizacional que controla la clave privada del Suscriptor se da por terminada o terminado en contrario
- Advantage Security o un cliente tiene razón para creer que el Certificado fue expedido de una manera que no está de conformidad con los procedimientos

requeridos pro la CPS aplicable, certificada fue expedido a una persona que no es la nombrada en el asunto de Certificado o el Certificado fue expedido sin la autorización de la persona nombrada el sujeto de dicho Certificado.

- Advantage Security o un cliente tiene razón para creer que un hecho importante en la solicitud del Certificado es falsa
- Advantage Security o un cliente determina que un requisito importante de una expedición de Certificado no fue satisfecha ni renunciada
- En el caso de los Certificados organizacionales, el nombre de la organización del Suscriptor cambia
- La información dentro del Certificado, que no sea la información del Suscriptor no verificado, es incorrecta o a cambiado, o
- El uso continuo de ese Certificado puede dañar la JSE

Cuando se considere que el uso del Certificado puede dañar a la JSE:

- La naturaleza y número de las quejas recibidas
- La identidad de las quejas
- La legislación relacionada vigente
- Respuestas al supuesto uso dañino del Suscriptor

Cuando se considere que el uso de un Certificado de Firma de Código puede dañar la JSE:

- El nombre del código que se firma
- El comportamiento del código
- Los métodos de distribución del código
- Las divulgaciones hechas a los receptores del código
- Cualquier alegato adicional hecho con respecto del código

Advantage Security también podrá cancelar un Certificado de Agente Certificador si la autoridad del administrador para actuar como administrador ha sido dada por terminada o en contrario ha finalizado.

Los contratos de Suscriptor de Advantage Security requieren que los Suscriptores de usuarios finales inmediatamente notifiquen a Advantage Security de una manipulación conocida o de la que se sospecha de su clave privada.

Advantage Security también puede cancelar un Certificado de Agente Certificador si la autoridad del administrador para actuar como administrador ha sido dada por terminada o ha finalizado en contrario.

Los Contratos del Suscriptor requieren que los Suscriptores usuarios finales inmediatamente notifiquen a Advantage Security una manipulación conocida de su clave o de la que se sospeche.

4.9.2 ¿Quién puede solicitar una Cancelación?

Los Suscriptores Individuales pueden solicitar la cancelación de sus propios Certificados individuales. En el caso de Certificados Organizacionales, un representante debidamente

autorizado de la organización tendrá la capacidad de solicitar la cancelación de los Certificados expedidos a la organización. Un representante debidamente autorizado de Advantage Security tendrá la capacidad de solicitar la cancelación de un Agente Certificador. La entidad que aprobó una Solicitud de Certificado de Suscriptor también podrá cancelar o solicitar la cancelación del Certificado de Suscriptor.

Solamente Advantage Security tiene la capacidad de solicitar o iniciar la cancelación de los Certificados expedidos para sus propias ACs. Los Centros de Procesamiento que no son Advantage Security, los Centros de Servicio y las ARs tienen la capacidad, a través de sus representantes debidamente autorizados de solicitar la cancelación de sus propios Certificados y sus Entidades Superiores podrán solicitar o iniciar la cancelación de sus Certificados.

4.9.3 Proceso para Solicitud de Cancelación

Antes de la cancelación de un Certificado, la AC verifica que la cancelación haya sido solicitada por el Suscriptor del Certificado o la entidad que aprobó la Solicitud de Certificado. Los procesos aceptables para autentificar las solicitudes de cancelación del Suscriptor incluyen:

- Que el Suscriptor presente para ciertos tipos de certificado la Challenge Phrase del Suscriptor (o el equivalente de la misma) y cancele el Certificado automáticamente si coincide la Challenge Phrase (o el equivalente de la misma) que se tiene en registros,
- Recibir un mensaje que se supone es del Suscriptor que solicita la cancelación y que contenga una firma digital verificable con referencia al Certificado que se cancelará, y
- Comunicación con el Suscriptor que proporcione aseguramiento razonable, basándose en la Clase de Certificado, que la persona u organización que solicita la cancelación es, de hecho el Suscriptor. Dependiendo de las circunstancias, dicha comunicación podrá incluir uno o más de lo siguiente: teléfono, fax, correo electrónico, dirección de correos o servicios de mensajería.

Los administradores AC/AR tienen la capacidad de solicitar la cancelación de Certificados de Suscriptor usuario final dentro del Sub-dominio de la CA/RA. Advantage Security autentificará la identidad de los Agentes Certificadores mediante los controles de acceso utilizando el SSL y la autentificación del cliente antes de permitirles que lleven a cabo funciones de cancelación.

4.9.4 Período de Gracia de la Solicitud de Cancelación

Las solicitudes de cancelación serán presentadas tan pronto como sea posible dentro de un tiempo comercialmente razonable.

4.9.5 Tiempo dentro del cual la AC Debe Procesar la Solicitud de Cancelación

Se toman los pasos comercialmente razonables para procesar sin retraso las solicitudes de cancelación.

4.9.6 Requerimientos de Revisión de Cancelación para las Partes Confiables

Las Partes Confiables revisarán el estado de los Certificados en los cuales desean confiar. Un método por el cual las Partes Confiables pueden revisar el estado del Certificado es consultando la CRL más reciente de Advantage Security en el cual la Parte Confiable desea confiar. Alternativamente, las Partes Confiables podrán cumplir con este requerimiento ya sea revisando el estado del Certificado utilizando el depósito basado en la Red aplicable o utilizando el OCSP. Las ACs proporcionarán a las Partes Confiables información de cómo encontrar la CRL adecuada, el depósito basado en la Red o el contestador OCSP para revisar el estado de cancelación.

- Para las ACs Cliente de PKI Administrada, las CRLs se indican en: http://onsitecrl.verisign.com/OnSitePublic/LatestCRL.crl

Una “Tabla de Referencia de CRL” también se indica en el Depósito de Advantage Security para dar la capacidad a las Partes Confiables de determinar la ubicación de la CRL para Advantage Security.

4.9.7 Frecuencia de Expedición de las CRLs

Las CRLs para Certificados de Suscriptor usuario final se expiden por lo menos una vez al día. Si un Certificado listado en una CRL vence, puede retirarse de las CRLs expedidas subsecuentemente después del vencimiento del Certificado.

4.9.8 Latencia Máxima para CRLs

Las CRL se indican en el depósito dentro de un tiempo comercialmente razonable después de su generación. Este se hace generalmente automáticamente dentro de los minutos de generación.

4.9.9 Cancelación En-Línea/Disponibilidad de Revisión de Estado

La cancelación en-línea y otra información del estado del Certificado están disponibles en un depósito vía un depósito con base en la Red y, en donde se ofrezca, en el OCSP. Advantage Security tendrá un depósito con base en la Red que permite a las Partes Confiables hacer solicitudes en-línea con relación a la cancelación y la información del estado de otro Certificado.

4.9.10 Requerimientos para Revisar la Cancelación En-Línea

Una parte confiable debe revisar el estado de un certificado en el que desee confiar. Si una Parte Confiable no revisa el estado de un Certificado en el cual la Parte Confiable

desea confiar consultando la CRL relacionada más reciente, la Parte Confiable revisará el estado del Certificado consultando el depósito aplicable o solicitando el estado del Certificado utilizando el contestador OCSP.

4.9.11 Requerimientos Especiales con relación a la Manipulación de Claves

Se les notificará a los Participantes de la JSE de una Manipulación real o que se sospecha de la clave privada AC utilizando los esfuerzos comercialmente razonables. Advantage Security utilizará los esfuerzos comercialmente razonables para notificar a las Partes Confiables si descubren, o tienen razones para creer, que ha habido una Manipulación de la clave privada de su propia AC o una de las ACs dentro de sus subdominios.

4.10 Servicios de Estado de Certificado

4.10.1 Características Operacionales

El Estado de los certificados públicos está disponible vía las CRLs a través de un Sitio Web del Centro de Procesamiento (en una URL especificada en ese CPS del Centro de Procesamiento), el directorio LDAP y vía un contestador OCSP.

4.10.2 Disponibilidad de Servicio

Los Servicios de Estado de Certificados estarán disponibles 24 x 7 sin interrupción programada.

4.10.3 Características Opcionales

El OCSP es una característica de servicio opcional del estado que no está disponible para todos los productos y debe estar específicamente activada para otros productos.

4.10.4 Final de la Suscripción

Un suscriptor puede terminar una suscripción de un certificado JSE:

- Dejando que su certificado venza sin renovar ese certificado o sin hacer otra clave del mismo.
- Cancelando su certificado antes del vencimiento del certificado sin reemplazar los certificados.

4.10.5 Depósito de la Clave y Recuperación

Advantage Security no podrá dar en depósito las claves de Suscriptor usuario final. Advantage Security no almacena copias de claves privadas de Suscriptores.

5 Instalaciones, Administración y Controles de Operación

5.1 Controles Físicos

Advantage Security tiene controles documentados físicos detallados y políticas de seguridad para las ACs y las ARs. El cumplimiento con estas políticas e incluye en los requerimientos de auditoria independientes de Advantage Security descritos en la Sección 8. Estos documentos contienen información confidencial de seguridad y solamente están disponibles mediante acuerdo con Advantage Security. A continuación se describe una revisión general de los requerimientos.

5.1.1 Ubicación y Construcción del Sitio

Todas las operaciones de la AC de Advantage Security serán llevadas a cabo dentro de un ambiente físicamente protegido que impida, prevenga y detecte uso no autorizado, acceso o divulgación de información y sistemas confidenciales. Para Advantage Security este ambiente cumplirá con los requerimientos de la Guía de Requerimientos de Seguridad y Auditoria de Advantage Security.

Dichos requerimientos se basan en parte en el establecimiento de escalones físicos de seguridad. Un escalón es una barrera tal como una puerta cerrada con llave que proporciona control de acceso obligatorio para personas y requiere una respuesta positiva (por ejemplo, una puerta se abre) de cada persona para proceder a la siguiente área. Cada escalón sucesivo proporciona más acceso restringido y mayor seguridad física contra la intrusión o acceso no autorizado. Además, cada escalón físico de seguridad encapsula el siguiente escalón interior, de manera que un escalón interno debe estar totalmente contenido dentro de un escalón exterior y no puede tener una pared exterior común con el escalón exterior, el último escalón es la pared exterior del edificio.

El nivel mínimo de seguridad física requerido por la AC o la AR se determina mediante la clase de certificados más alta que ellos procesan. Por ejemplo, Advantage Security procesa y expide Certificados Clase 2 y por lo tanto, opera al nivel de seguridad más alto requerido por la JSE. Se les requiere a las ACs o las ARs que procesen o expiden certificados Clase 2 que implementen un nivel de seguridad adecuado para la clase específica de certificado. Las ACs y las ARs describirán más a detalle su Ubicación y Construcción del Sitio en su CPS.

5.1.2 Acceso Físico

El acceso a cada escalón de seguridad física será auditable y controlado de manera que cada escalón puede ser accesado solamente por personal autorizado.

5.1.3 Energía y Aire Acondicionado

Para asegurar las instalaciones de la ACs y las ARs, se equipararán con sistemas de energía básicos y de respaldo para asegurar el acceso continuo, ininterrumpido a la energía eléctrica. Asimismo, estas instalaciones seguras se equiparán con sistemas básicos y de respaldo de calefacción/ventilación/aire acondicionado para controlar la temperatura y la humedad relativa.

5.1.4 Exposición al Agua

Las instalaciones seguras de la ACs y las ARs serán construidas y equipadas y se implementarán los procedimientos para prevenir inundaciones u otra exposición dañina al agua.

5.1.5 Prevención y Protección contra Incendio

Las instalaciones de seguridad de las ACs y las ARs se construirán y equipararán, y los procedimientos se implementarán para prevenir y extinguir incendios u otra exposición dañina al fuego o al humo. Estas medidas cumplirán con las regulaciones de seguridad aplicables locales.

5.1.6 Almacenamiento de Medios

Las ACs y las ARs protegerán a los medios magnéticos teniendo respaldos de los datos de sistemas críticos o de cualquier información delicada contra agua, fuego u otros peligros ambientales y utilizarán medidas de protección para impedir, detectar y prevenir el uso no autorizado, acceso o divulgación de dichos medios.

5.1.7 Disposición de Desperdicios

Las ACs y las ARs implementarán los procedimientos para la disposición de desperdicios (papel, medios o cualquier otro desperdicio) para prevenir el uso no autorizado, acceso o divulgación de desperdicios que contentan Información Confidencial/Privada.

5.1.8 Respaldos Fuera de Sitio

5.2 Puestos de Confianza

Los empleados, contratistas y consultores que estén designados para manejar la confianza infraestructural serán considerados como “Personas de Confianza” que sirven

en un “Puesto de Confianza”. Las personas que intentan llegar a ser Personas de Confianza obteniendo un Puesto de Confianza cumplirán con los requerimientos de monitoreo de esta CP.

Las Personas de Confianza incluyen a los empleados, contratistas y consultores que tienen acceso o autentificación de control u operaciones criptográficas que pueden afectar de manera importante:

- La validación de información en Solicitudes de Certificado;
- La aceptación, rechazo u otro procesamiento de Solicitudes de Certificado, solicitudes de cancelación o solicitudes de renovación o información de inscripción;
- La expedición o cancelación de Certificados, incluyendo (en el ACso de Centros de Procesamiento) personal que tenga acceso a partes restringidas de su depósito o el manejo de la información o solicitudes del Suscriptor.

Las Personas de Confianza incluyen mas no están limitadas a:

- Personal de servicio a clientes.
- Personal de sistema de administración
- Personal de ingeniería designado, y
- Ejecutivos que están designados para manejar la confianza infraestructural.

5.2.1 Número de Personas Requeridas por Tarea

Las ACs y ARs establecerán, mantendrán y ejercerán procesos de control estrictos para asegurar la segregación de obligaciones basadas en la responsabilidad de trabajo y para asegurar que se les requiera a las múltiples Personas de Confianza cumplir con las tareas delicadas.

Los procesos de políticas y control son para asegurar la segregación de obligaciones basadas en las responsabilidades de trabajo. Las tareas más delicadas, tales como el acceso y la administración del equipo de cómputo criptográfico de la AC (unidad de firma criptográfica o CSU) y el material clave asociado, requieren varias Personas de Confianza.

Estos procesos internos de control están diseñados para asegurar que por lo menos se necesiten dos personas de confianza del personal para tener ya sea acceso físico o lógico al dispositivo. El acceso al equipo criptográfico de la AC es estrictamente ejercido por varias Personas de Confianza a través de su ciclo de vida, desde la recepción que llega y la inspección a la destrucción final lógica y/o física. Una vez que un módulo está activado con claves operacionales, se invocan controles de acceso adicionales para mantener un control dividido sobre el acceso tanto físico como lógico al dispositivo. Las personas con acceso físico a los módulos no tienen “Partes Secretas” y viceversa.

Otras operaciones manuales tales como la validación y expedición de Certificados Clase 2, no expedidos por un sistema automatizado de validación y expedición, requieren la participación de por lo menos 2 Personas de Confianza o una combinación de por lo menos una persona de confianza y una validación automatizada y un proceso de expedición.

5.2.2 Identificación y Autentificación de Cada Puesto

Las ACs y ARs confirmarán la identidad y autorización de todo el personal que desea ser de Confianza antes de que a ese personal:

- Se le expidan sus dispositivos de acceso y se les otorgue acceso a las instalaciones requeridas;
- Se les den credenciales electrónicas para accesar y llevar a cabo funciones especificas sobre los Sistemas de Información y los sistemas de la AC y AR.

La autentificación de identidad incluirá la presencia (física) personal de dicho personal ante las Personas de Confianza que llevan a cabo funciones de recursos humanos o de seguridad dentro de una entidad y una revisión de formatos de identificación bien reconocidos, tales como pasaportes y licencias de conductor. La identidad será confirmada además a través de antecedentes y los procesos de revisión especificados en esta CP.

5.2.3 Puestos que Requieren Separación de Deberes

Los puestos que requieren Separación de deberes incluyen (mas no están limitados a):

- La validación de información en las Solicitudes de Certificado;
- La aceptación rechazo u otro proceso de Solicitudes de Certificado, solicitudes de cancelación o solicitudes de renovación o información de registro;
- La expedición o cancelación de Certificados, incluyendo el personal que tiene acceso a partes restringidas del depósito;
- El manejo de la información del Suscriptor o solicitudes;
- La cara de una AC en producción.

5.2.4 Controles de Personal

La JSE tiene políticas de control y seguridad de personal documentadas y detalladas para las ACs o las ARs a las cuales apegarse y contra las que se auditarán. El cumplimiento con estas políticas está incluido en los requerimientos independientes de auditoria descritos en la Sección 8. Estos documentos contienen información delicada de seguridad y solamente están disponibles para los participantes de la JSE conforme a contratos con Advantage Security. Una revisión general de los requerimientos se describe a continuación:

5.2.5 Requerimientos de Habilidades, Experiencia y Autorización

Las ACs y las ARs requieren que el personal que desea llegar a ser Personas de Confianza presenten evidencia de los antecedentes requeridos, de las habilidades y la experiencia que se necesita para cumplir con sus eventuales responsabilidades de trabajo de manera competente y satisfactoria, así como la prueba de cualquier autorización gubernamental, si hubiere, necesaria para llevar a cabo servicios de certificación de conforme a contratos con el gobierno.

5.2.6 Procesos de Revisión de Antecedentes

Las ACs y las ARs llevarán a cabo revisiones de antecedentes de personal que desea llegar a ser Personas de Confianza. Las revisiones de los antecedentes serán repetidas por el personal que tiene Puestos de Confianza por lo menos cada cinco (5) años. Estos procesos estarán sujetos a cualquier limitación de revisiones de antecedentes impuestos por la ley local. En la medida que uno de los requerimientos impuestos por esta sección no pueda cumplirse debido a una prohibición o limitación de ley local, la entidad investigadora utilizará una técnica de investigación substituta permitida por la ley que proporcione información substancialmente similar, incluyendo mas no limitada a obtener una revisión de antecedentes llevada a cabo por una agencia gubernamental aplicable.

Los factores revelados en una revisión de antecedentes que puedan ser considerados razones para rechazar a los candidatos de Puestos de Confianza o para tomar acción contra una Persona de Confianza ya existente, se discuten en la Guía de Requerimientos de Seguridad y Auditoria de Advantage Security y generalmente incluyen (mas no están limitados) a lo siguiente:

- Manifestaciones fraudulentas hechas por el candidato o por la Persona de Confianza.
- Referencias profesionales altamente desfavorables o no confiables.
- Ciertas convicciones criminales, e
- Indicciones de falta de responsabilidad financiera.

Los reportes que contienen dicha información se evaluarán por personal de recursos humanos y de seguridad, y dicho personal tomará las acciones que sean razonables con base en el tipo, magnitud y frecuencia del comportamiento descubierto por la revisión de antecedentes. Dichas acciones podrán incluir medidas hasta por e incluyendo la cancelación de ofertas de empleo hechas a los candidatos de Puestos de Confianza o la terminación de las Personas de Confianza existentes. El uso de la información revelada en una revisión de antecedentes para tomar dichas acciones estará sujeto a la ley aplicable.

La investigación de los antecedentes que desean ser una Persona de Confianza incluye:

- Una confirmación de empleos anteriores,
- Una revisión de referencias profesionales,
- Una confirmación del grado de escolaridad más alto o más importante obtenido,
- Una búsqueda de antecedentes penales (locales, estatales o municipales y nacionales), y
- Una revisión de registros créditos/financieros.

5.2.7 Requerimientos de Capacitación

Las ACs y las ARs proporcionarán a su personal con la capacitación necesaria para su personal para cumplir con sus responsabilidades laborales con relación a las operaciones de las ACs y las ARs de manera competente y satisfactoria. También revisarán periódicamente sus programas de capacitación y su capacitación tratará los elementos relacionados con las funciones llevadas a cabo por su personal. El personal de servicio de

un Agente Certificador externo cumplirá con los requerimientos de capacitación de Advantage Security, como una condición de las operaciones de inicio del Agente Certificador.

Los programas de capacitación deben trabar los elementos relacionados con el ambiente específico de la persona que se capacita, incluyendo:

- Principios de seguridad y mecanismos de la JSE,
- Equipo de cómputo y versiones de programas de cómputo en vigor,
- Todos los deberes que se espera la persona lleve a cabo,
- Reporte y manejo de incidentes y manipulaciones, y
- Procedimientos de recuperación en ACso de desastre y continuidad del negocio.

5.2.8 Frecuencia y Requerimientos de Nueva Capacitación

Advantage Security proporcionará capacitación nueva y actualizaciones a su personal en la medida y frecuencia requerida para asegurar que dicho personal mantiene el nivel requerido de eficiencia para cumplir con las responsabilidades de su trabajo de manera competente y satisfactoria.

5.2.9 Sanciones para Acciones No Autorizadas

Advantage Security mantendrá y ejercerá las políticas de empleo para la disciplina del personal que siga acciones no autorizadas. Las acciones disciplinarias podrán incluir medidas hasta por e incluyendo la terminación y serán proporcionales a la frecuencia y gravedad de las acciones no autorizadas.

5.2.10 Requerimientos de Contratistas Independientes

Las ACs y las ARs podrán permitir a los contratistas independientes o consultores como Personas de Confianza solamente en la medida necesaria para ajustarse a relaciones independientes claramente definidas y solamente conforme a las siguientes condiciones:

- Que la entidad que utilice los contratistas independientes o consultores como Personas de Confianza no tenga empleados adecuados disponibles para llenar los puestos de Personas de Confianza, y
- Que la entidad confíe en contratistas o consultores e la misma medida como si fueran empleados.

De lo contrario, los contratistas independientes y consultores tendrán acceso a las instalaciones de seguridad de Advantage Security, de una Afiliada o un Cliente Compañía solamente en la medida en que estén acompañados y directamente supervisados por las Personas de Confianza.

5.2.11 Documentación Proporcionada al Personal

Advantage Security, las Afiliadas y los Clientes Compañía proporcionarán a su personal (incluyendo las Personas de Confianza) la capacitación necesaria y el acceso a otra documentación que se necesite para cumplir con sus responsabilidades de trabajo de manera competente y satisfactoria.

5.3 Procesos de Bitácoras de Auditoria

5.3.1 Tipos de Eventos Registrados

Los tipos de eventos auditables que deben ser registrados por Advantage Security se establecen a continuación. Todas las bitácoras, ya sean electrónicas o manuales, contendrán la fecha y hora del evento, y la identidad de la entidad que causó el evento. Las ACs establecerán en sus CPS los registros y tipos de eventos que registren.

Los tipos de eventos auditables incluyen:

- Eventos operacionales incluyendo mas no limitados a (1) arranque y apagado de sistemas y aplicaciones, (2) cambios a los detalles o claves de la AC, (3) eventos de módulos criptográficos de administración de ciclo de vida relacionados (por ejemplo, recepción, uso, desinstalación y retiro), (4) posesión de datos de activación para las operaciones de clave privada de la AC, bitácoras de acceso físico, (5) cambios en el sistema de configuración y mantenimiento, (6) Registros de la destrucción de medios que contienen material clave, datos de activación o información personal del Suscriptor.
- Certificar eventos de ciclo de vida incluyendo mas no limitados a expedición inicial, reclave, renovación, cancelación, suspensión.
- Eventos de empleados de confianza incluyendo mas no limitados a (1) intentos de acceso y salida, (2) intentos de crear, quitar, establecer contraseñas o cambiar los privilegios del sistema de los usuarios con privilegios, (3) cambios de personal.
- Reportes de discrepancia y de manipulación incluyendo mas no limitados a intentos de acceso al sistema no así como de acceso a la red.
- Lecturas y operaciones fallidas en el Certificado y el depósito.
- Cambios a las políticas de creación de Certificados, por ejemplo, período de validez.

5.3.2 Frecuencia de Procesamiento de Bitácora

Las bitácoras de auditoria se revisarán en respuesta a las alertas basadas en irregularidades e incidentes dentro de sus sistemas AC/AR. Advantage Security comparará las bitácoras de auditoria con el manual de soporte y las bitácoras electrónicas de sus Clientes AR y de los Centros de Servicio cuando se considere que alguna acción es sospechosa.

El procesamiento de bitácoras de auditoria consistirá de una revisión de las bitácoras de auditoria y documentar las razones de todos los eventos importantes en un resumen de bitácoras de auditoria. Las revisiones de las bitácoras de auditoria incluyen una verificación de que la bitácora no ha sido alterada, una inspección de todos los registros de bitácora, y una investigación de cualquier alerta o irregularidades en las bitácoras. Las acciones tomadas basadas en las revisiones de bitácoras de auditoria se documentarán.

5.3.3 Período de Retención para Bitácora de Auditoria

Las bitácoras de auditoria serán retenidas en el sitio por lo menos dos (2) meses después del procesamiento y posteriormente se archivarán de conformidad con la Sección 5.5.2.

5.3.4 Protección de la Bitácora de Auditoria

Las bitácoras de auditoria se protegen con un sistema electrónico de bitácoras de auditoria que incluye los mecanismos para proteger los archivos de bitácoras contra vistas, modificación, supresión no autorizadas u otra alteración.

5.3.5 Procesos de Respaldo de Bitácoras de Auditoria

Diariamente se crean respaldos incrementados de bitácoras de auditoria y se realizan respaldos completos semanalmente.

5.3.6 Notificación al Sujeto que Causó el Evento

En el caso de que un evento se registre por el sistema de recolección de auditoria, no se requiere dar notificación a la persona, organización, dispositivo o aplicación que causó el evento.

5.3.7 Evaluaciones de Vulnerabilidad

Los eventos en el proceso de auditoria se registran, en parte para monitorear las vulnerabilidades del sistema. Se llevan a cabo evaluaciones de seguridad lógicas de vulnerabilidad se revisan, y se verifican después de un examen de estos eventos monitoreados. Las se basan en datos automatizados cargados en tiempo real y se llevan a cabo diaria, mensual y anualmente. Una anual será una entrada en una Auditoria de Cumplimiento anual de la entidad.

5.4 Registros de Archivos

5.4.1 Tipos de Registros Archivados

Las ARs y las ACs archivan:

- Todos los datos de auditoria reunidos conforme a la Sección 5.4.
- Información de solicitud de Certificado.
- Documentación soportando las aplicaciones de certificado.
- Información del ciclo de vida del certificado, por ejemplo, cancelación, reclave e información de solicitud de renovación.

5.4.2 Período de Retención de Archivos

Los registros serán retenidos por lo menos por los períodos de tiempo establecidos después de la fecha en que venza el Certificado o cuando sea cancelado.

- Diez (10) años y seis (6) meses para los Certificados Clase 2.

5.4.3 Protección de Archivos

Una entidad que mantiene un archivo de registros protegerá el archivo de manera que solamente las Personas de Confianza de la entidad puedan tener acceso al archivo. El archivo se protege contra vistas, modificación, supresión no autorizada u otra alteración mediante almacenamiento con un Sistema Confiable. Los medios que guardan los datos de archivos y las aplicaciones requeridas para procesar los datos de archivo se mantendrán para asegurar que los datos del archivo pueden ser accesados por el tiempo establecido en esta CP.

5.4.4 Procesos de Respaldo de Archivos

Las entidades que compilan información electrónica respaldarán de manera incrementada los archivos de sistemas de dicha información diariamente y llevarán a cabo respaldos totales semanalmente. Las copias de registros en papel se mantendrán en una instalación segura fuera del sitio.

5.4.5 Requerimientos para Sello de Hora de Recepción de los Registros

Los Certificados, las CRLs y otros registros de cancelación contendrán la información de hora y fecha. Dicha información de tiempo no necesita estar criptográficamente basada.

5.4.6 Sistema de Recolección de Archivos (Interno o Externo)

Los sistemas de recolección de archivos para las entidades dentro de Advantage Security serán internos. Los Centros de Procesamiento asistirán a sus compañías AR para mantener un registro de auditoria. Dicho sistema de recolección de archivos, por lo tanto, es externo a esa compañía AR. De lo contrario, las entidades dentro de la Advantage Security utilizarán sistemas internos de recolección de archivos.

5.4.7 Procesos para Obtener y Verificar Información de Archivos

Solamente Personal de Confianza autorizado puede obtener acceso al archivo. La integridad de la información se verifica cuando se restaura.

5.5 Conversión de Claves

Un Certificado AC de Advantage Security podrá ser renovado si la Secretaría de Economía. Después de esa reconfirmación, la Secretaría de Economía aprobará o rechazará la solicitud de renovación.

Después de la aprobación de una solicitud de renovación, la Secretaría de Economía y Advantage Security llevará a cabo una Ceremonia de Generación de Clave con el objeto de generar una nueva clave par para la AC. Durante dicha Ceremonia de Generación de Clave, la Entidad Superior firmará y expedirá a la AC un nuevo Certificado. Dicha Ceremonia de Generación de Clave cumplirá con los requerimientos de Ceremonia de Clave documentados en las políticas confidenciales de seguridad de la JSE. Los nuevos

Certificados AC que contengan las nuevas claves públicas AC generados durante dicha Ceremonia de Generación de Claves se pondrán a disposición de las Partes Confiables.

5.6 Manipulación y Recuperación en caso de Desastre

5.6.1 Procesos de Manejo de Incidentes y Manipulaciones

Los respaldos de la siguiente información de la AC se mantendrán en almacenamiento fuera del sitio y se pondrán a disposición en el caso de una Manipulación o desastre: los datos de la Solicitud del Certificado, datos de auditoria y registros de base de datos para todos los Certificados expedidos. Los respaldos de las claves privadas de AC se generarán y mantendrán de conformidad con la CP § 6.2.4. Los Centros de Procesamiento mantendrán respaldos de la información anteriormente especificada de la AC para sus propias ACs, así como las ACs de los Centros de Servicio y los Clientes Compañía dentro de sus Sub-dominios.

5.6.2 Los Recursos de Cómputo, Programas de Cómputo y/o Datos se Corrompen

Después de que haya una corrupción de recursos de cómputo, programas de cómputo, y/o datos, la AC o AR afectada preparará inmediatamente un reporte del incidente y una respuesta al evento de conformidad con los procesos de reporte y manejo de incidentes y Manipulaciones de Advantage Security documentados en la CPS aplicable y las políticas documentadas confidenciales de seguridad de la JSE.

5.6.3 Procesos de Manipulación de Clave Privada de Entidad

En el caso de manipulación de una clave privada esa AC será cancelada. Los Centros de Procesamiento utilizan los esfuerzos comercialmente razonables para notificar a las Partes Confiables potenciales si descubren o tienen razones para creer que hay una Manipulación de la clave privada de una AC en su sub-dominio en la JSE.

5.6.4 Capacidad de Continuidad de Negocios Después de un Desastre

Advantage Security desarrolla, prueba, mantiene e implementa un plan de recuperación en caso de desastre diseñado para mitigar los efectos de cualquier clase de desastre natural o provocado por el hombre. Los planes de recuperación en caso de desastre tratan la restauración de los servicios de sistemas de información y las funciones de negocio clave. Los sitios de recuperación en caso de desastre tienen las protecciones de seguridad física equivalentes especificadas por la JSE.

Advantage Security tiene la capacidad de restauración o de recuperación de operaciones esenciales en veinticuatro (24) horas después de un desastre con, por lo menos, soporte de las siguientes funciones: expedición de Certificados, cancelación de Certificados, publicación de información de cancelación. Una base de datos de recuperación en caso de desastre del Centro de Procesamiento estará sincronizada con la base de datos de producción dentro de los límites de tiempo establecidos en la Guía de Requerimientos de Seguridad y Auditoria. Un equipo de recuperación en caso de desastre de Advantage Security tendrá las protecciones de seguridad físicas documentadas en las políticas

confidenciales de seguridad, que incluyen el ejercimiento de escalones de seguridad físicos.

Un plan de recuperación en caso de desastre Advantage Security establece disposiciones para recuperación total en una semana después de que ocurra el desastre en el sitio básico Advantage Security. Advantage Security instalará y probará el equipo en su sitio básico para soportar las funciones AC/AR después de un desastre mayor que haría que todas las instalaciones fueran inoperables. Dicho equipo asegura la redundancia y la tolerancia de fallas.

5.7 Terminación de la AC o AR

La terminación de una AC o AR que no sea de Advantage Security (Afiliada, Cliente compañía) estará sujeta al contrato celebrado entre la AC que se dará por terminada y su Entidad Superior. Ambas partes, de buena fe, utilizarán sus esfuerzos razonablemente comerciales para convenir un plan de terminación que minimice la interrupción a los Clientes, Suscriptores y Partes Confiables. El plan de terminación puede cubrir aspectos tales como:

- Proporcionar notificación a las partes afectadas por la terminación, tales como Suscriptores, Partes Confiables y Clientes,
- Manejo del costo de dicha notificación,
- La cancelación del Certificado expedido por la Secretaría de Economía,
- La preservación de los archivos y registros de la AC durante los períodos de tiempo requeridos por esta CP.
- La continuación de los servicios de soporte del Suscriptor y del cliente,
- La continuación de los servicios de cancelación, tales como la expedición de CRLs o el mantenimiento de servicios de revisión de estado en línea,
- La cancelación de Certificados no vencidos y no cancelados de Suscriptores usuario final y ACs subordinadas, si es necesario,
- El reembolso (si es necesario) a Suscriptores cuyos Certificados no vencidos y no cancelados sean cancelados conforme al plan o disposición de terminación para la expedición de un sucesor de la AC de los Certificados sustituto.
- La disposición de la clave privada de la AC y el token que contienen dicha clave privada,
- Disposiciones que se necesitan para la transición de los servicios de la AC a un sucesor de la CA.

6 Controles Técnicos de Seguridad

6.1 Generación e Instalación de Par de Claves

6.1.1 Generación de Par de Claves

La generación de clave par se llevará a cabo utilizando los Sistemas de Confianza y los procesos que proporcionan la fuerza criptográfica requerida de las claves generadas y que previenen la pérdida, divulgación, modificación, o uso no autorizado de las claves privadas. Los suscriptores deben generar su par de claves confidencialmente. Este requerimiento aplica a los Suscriptores usuario final de persona moral o física.

Las Claves de AC se generan en una Ceremonia de Generación de Clave. Todas las Ceremonias de Generación de Claves se apegan a los requerimientos documentados en las políticas confidenciales de seguridad de la JSE.

6.1.2 Entrega de Clave Privada al Suscriptor

Las claves privadas del Suscriptor usuario final son generadas por los mismos Suscriptores usuario final, y por lo tanto, la entrega de la clave privada a un Suscriptor no es necesaria.

6.1.3 Entrega de Clave Pública al Emisor del Certificado

Cuando una clave pública se transfiera a la AC emisora para certificarse, se entregará a través de un mecanismo que asegure que la clave pública no ha sido alterada durante el tránsito y que el Solicitante del Certificado posee la clave privada correspondiente a la clave pública transferida. El mecanismo aceptable dentro de la JSE para la entrega de la clave pública es un paquete PKCS#10 de solicitud de Certificado de firma o un método equivalente que asegure:

- Que la clave pública no ha sido alterada durante el tránsito; y
- Que el Solicitante del Certificado posee la clave privada correspondiente a la clave pública transferida.

6.1.4 Entrega de Clave Pública a Partes Confiables

Las claves públicas de Advantage Security se incluyen en los Certificados raíz que no estén insertados dentro de las aplicaciones de las muchas aplicaciones populares de programas de cómputo, haciendo que los mecanismos especiales de distribución de las raíces sean innecesarios. También, en muchas instancias, la Parte Confiable que utiliza el protocolo S/MIME automáticamente recibirá, además del Certificado del Suscriptor, los Certificados (y por lo tanto las claves públicas) de Advantage Security y la Secretaría de Economía.

6.1.5 Tamaños de Clave

El par de claves serán de suficiente tamaño para evitar que otras determinen la clave privada par utilizando criptoanálisis durante el período de uso esperado de dichas claves par. El Estándar Actual de JSE para tamaños de clave mínimos es el uso de las claves par equivalentes en fuerza a 1024 bits RSA para los certificados de suscriptor y de 2048 bits para los certificados AC y AR.

6.1.6 Generación de Parámetros de Clave Pública y Revisión de Calidad

Advantage Security usa el estándar de Firma Digital FIPS 186-2 o un estándar equivalente aprobado por la JSE. Cuando Advantage Security utiliza el Estándar de Firma Digital, la calidad de los Parámetros Clave generados será verificada de conformidad con las FIPS 186-2 o un estándar equivalente aprobado.

6.1.7 Propósitos de Uso de Clave (según Campo de Uso de Clave X.509 v3)

Refiérase a la Sección 7.1.2.1.

6.1.8 Protección de Clave Privada y Controles de Ingeniería de Módulo Criptográfico

6.1.9 Estándares y Controles de Módulo Criptográfico

Las claves privadas dentro de Advantage Security se protegerán utilizando un Sistema Confiable y los propietarios de las claves privadas tomarán las precauciones necesarias para prevenir la pérdida, divulgación, modificación o uso no autorizado de dichas Claves Privadas de conformidad con esta CP, las obligaciones contractuales y los requerimientos documentados en las políticas confidenciales de seguridad de la JSE. Los Suscriptores Usuarios Finales tienen la opción de proteger sus claves privadas en tarjetas inteligentes u otro token criptográfico.

Advantage Security llevará a cabo todas las operaciones criptográficas AC en módulos criptográficos clasificados en un mínimo de FIPS 140-1 nivel 3. Los Centros de Servicio llevarán a cabo todas las operaciones criptográficas AR en un módulo criptográfico clasificado en FIPS 140-1 nivel 3.

6.1.10 Control de Clave Privada (m fuera de n) de Multi-persona

El control de multi-persona se ejerce para proteger los datos de activación necesitados para activar las claves privadas AC que tiene Advantage Security conforme a los estándares documentados en las políticas confidenciales de seguridad de la JSE. Los Centros de Procesamiento utilizan “Secretos Compartidos” para dividir la clave privada o los datos de activación necesitados para operar la clave privada en partes separadas llamadas “Partes Secretas” que tienen los individuos denominados los “Propietarios de las Partes”. Algún número mismo de Partes Secretas (m) del total de Partes Secretas (n) se requerirá para operar la clave privada.

Advantage Security utiliza Secretos compartidos para proteger los datos de activación necesitados para activar sus propias claves privadas y otras ACs dentro de sus respectivos Sub-dominios conforme a los estándares documentados en las políticas confidenciales de seguridad de la JSE. Advantage Security también utiliza secretos compartidos para proteger los datos de activación necesitados para activar las claves privadas localizadas en sus respectivos sitios de recuperación en caso de desastre.

El número mismo de partes necesitado para firmar un certificado AC es 3. Debe tomarse nota que el número de partes distribuido para tokens en caso de desastre puede ser menor que el número distribuido para tokens operacionales, mientras el número mismo de acciones requeridas sigue siendo el igual.

6.1.11 Clave Privada en Depósito

Las claves privadas no se depositan. El depósito de las claves privadas para suscriptores usuario final se explica más a detalle en la Sección 4.12.

6.2 Respaldo de Clave Privada

Las ACs respaldarán sus propias claves privadas de manera que puedan recuperarse de desastres y malfuncionamiento del equipo de conformidad con los estándares documentados en las políticas confidenciales de seguridad de la JSE. Advantage Security también respaldarán las claves privadas de las ACs dentro de sus sub-dominios. Los respaldos serán hechos de acuerdo con estas políticas documentadas. Los respaldos serán hechos copiando dichas claves privadas y registrándolas en los módulos criptográficos de respaldo conforme a la Sección 6.2.6 y 6.2.7.

Las claves privadas que se respaldan se protegen contra modificación y divulgación no autorizada a través de medios físicos o criptográficos. Los respaldos están protegidos contra un nivel de protección física y criptográfica igual o que excede la de los módulos criptográficos dentro del sitio AC, tales como un sitio de recuperación en caso de desastre o en otra instalación segura fuera de sitio, tal como una caja de seguridad bancaria.

Advantage Security recomienda que los certificados de persona moral y física respalden sus claves privadas y las protejan contra modificación o divulgación no autorizada mediante medios físicos o criptográficos.

6.2.1 Archivo de clave Privada

Cuando las claves par AC lleguen al final de su periodo de validez, dichas claves par AC se archivarán durante un período de por lo menos 5 años. Las claves par AC archivadas serán almacenadas de manera segura utilizando módulos de equipo criptográfico que cumpla con los requerimientos de esta CP. Los controles de procedimientos evitan que las claves par AC archivadas se devuelvan a producción para uso. Al momento del final del período archivado, las claves privadas AC archivadas serán destruidas de manera segura conforme a esta CP.

6.2.2 Transferencia de Clave Privada hacia o desde un Módulo Criptográfico

El registro de una clave privada en un módulo criptográfico utilizará los mecanismos para prevenir la pérdida, el robo, la modificación, la divulgación no autorizada o el uso no autorizado de dicha clave privada.

Cuando Advantage Security genera las claves privadas AC o AR en un módulo de equipo criptográfico y que las transfieren hacia otro, se transferirán de manera segura dichas claves privadas hacia el segundo módulo criptográfico en la medida necesaria para prevenir pérdida, robo, modificación, divulgación no autorizada, o uso no autorizado de dichas claves privadas. Dichas transferencias estarán limitadas a hacer copias de respaldo de las claves privadas en tokens de conformidad con los estándares

documentados en las políticas confidenciales de seguridad de la JSE. Las claves privadas serán encriptadas durante dicha transferencia.

6.2.3 Almacenamiento de Clave Privada en Módulo Criptográfico

Las claves privadas AC o AR que se tienen en módulos de equipo criptográfico se almacenan en formatos encriptados.

6.2.4 Método de Activación la Clave Privada

Advantage Security protegerá los datos de activación de sus claves privadas contra la pérdida, robo, modificación, divulgación no autorizada o uso no autorizado.

6.2.4.1 Certificados Clase 2

El Estándar JSE para protección de clave privada Clase 2 (que no sea la de Administradores) es para que los Suscriptores:

- Utilicen una tarjeta inteligente, dispositivo de acceso biométrico, o seguridad de fuerza equivalente para autentificar al Suscriptor antes de la activación de la clave privada; y
- Tomar las medidas razonables comercialmente para la protección física de la estación de trabajo del Suscriptor para prevenir el uso de la estación de trabajo y su clave privada asociada sin la autorización del Suscriptor.

Se recomienda el uso de una contraseña junto con una tarjeta inteligente o dispositivo de acceso biométrico de conformidad con la Sección 6.4.1. Cuando se desactiven, las claves privadas serán guardadas solamente en formato encriptado.

6.2.4.2 Claves Privadas del Agente Certificador

El estándar de Advantage Security para la protección de la clave privada de Agentes Certificadores requiere que ellos:

- Utilicen tarjetas inteligentes, dispositivos de acceso biométrico, contraseñas de conformidad con la Sección 6.4.1 o seguridad de fuerza equivalente para autentificar al Administrador antes de la activación de la clave privada, que incluye, por ejemplo, una contraseña para operar la clave privada, una contraseña de Windows o una contraseña de pantalla o una contraseña de acceso a la red; y
- Tomen las medidas razonables comercialmente para la protección física de la estación de trabajo del Agente Certificador para prevenir el uso de la estación de trabajo y su clave privada asociada sin la autorización del Agente Certificador.

Advantage Security recomienda que los Agentes Certificadores utilicen una tarjeta inteligente, dispositivos de acceso biométrico o seguridad de fuerza equivalente junto con el uso de una contraseña de conformidad con la Sección 6.4.1 para autentificar al Agente Certificador antes de la activación de la clave privada.

Cuando se desactiven, las claves privadas se guardarán solamente en formatos encriptados.

6.2.4.3 Claves Privadas en poder de Advantage Security

Se activará una clave privada AC en-línea por un mismo número de Propietarios de Partes, como se define en la Sección 6.2.2, que proporcionen sus datos de activación (almacenados en medios seguros). Una vez que la clave privada se active, la clave privada podrá estar activa por un período de tiempo indefinido hasta que se desactive cuando el AC salga de la línea. Asimismo, se les requerirá a un mismo número de Propietarios de las Partes sus datos de activación con el objeto de activar una clave privada AC fuera de línea. Una vez que la clave privada se active, estará activa solamente por una vez.

6.2.5 Método de Desactivación de Clave Privada

Los Suscriptores usuario final Clase 2 tienen la obligación de proteger sus claves privadas. Dichas obligaciones se extienden a la protección de clave privada después de que haya ocurrido la operación de una clave privada. La clave privada puede ser desactivada después de cada operación, al momento de salirse del sistema u al momento de retirar una tarjeta inteligente del lector de tarjetas inteligentes dependiendo del mecanismo de autentificación utilizado por el usuario.

Cuando un Advantage Security saca de línea a una AC en-línea, el personal de Advantage Security retirará el token que contiene la clave privada de la AC del lector con el objeto de desactivarlo. Con relación a las claves privadas de ACs fuera de línea, después de terminar una Ceremonia de Generación de Clave, en las cuales dichas claves privadas se utilicen para operaciones de clave privada, el personal del Centro de Procesamiento retirará el token que contiene dichas claves privadas de AC de lector con el objeto de desactivarlas. Una vez retiradas del lector, los tokens se protegerán de conformidad con la Guía de Requerimientos de Seguridad y Auditoria.

6.2.6 Método de Destrucción de Clave Privada

Al terminar las operaciones de una AC de un Centro de Procesamiento o una AC dentro de su Sub-dominio, o la pérdida, robo, modificación, divulgación no autorizada, o uso no autorizado de dicha clave privada, el personal del Centro de Procesamiento desactivará la clave privada de la AC eliminándola utilizando la funcionalidad del token que contiene dicha clave privada de AC para prevenir su recuperación después de la eliminación, sin afectar adversamente las claves privadas de otras ACs contenidas en el token. Este proceso será vigilado de conformidad con los estándares documentados en las políticas de seguridad confidencial en la JSE.

6.2.7 Clasificación de Módulo Criptográfico

Véase la Sección 6.2.1

6.3 Otros Aspectos de la Administración de la Clave Par

6.3.1 Archivo de Clave Pública

Las ACs archivarán sus propias claves públicas, así como las claves públicas de todas las ACs dentro de sus Subdominios de conformidad con la Sección 5.5.

6.3.2 Periodos Operacionales de Certificados y Periodos de Uso de Clave Par

El Período Operacional para los Certificados se establecerá conforme a los límites de tiempo establecidos e la Tabla 4 a continuación.

El período de uso para las claves par de Suscriptor usuario final es el mismo que el Período Operacional para sus Certificados, excepto que las claves privadas pueden continuar utilizándose después del Periodo Operacional para desencriptación y verificación de firma. El Período Operacional de un Certificado termina al momento de su vencimiento o cancelación. Advantage Security no expedirá Certificados si sus Períodos Operacionales se extienden más allá del período de uso de la clave par de la CA. Por lo tanto, el período de uso de la clave par AC es necesariamente más corto que el período operacional del Certificado AC. Específicamente, el período de uso es el Período Operacional del Certificado AC menos el Periodo Operacional de los Certificados que expide la AC. Al final del periodo de uso de un Suscriptor o una clave par CA, el Suscriptor o la AC cesarán posteriormente todo el uso de la clave par, excepto en la medida que una AC necesite firmar información de cancelación hasta el final del Período Operacional del último Certificado que haya expedido.

Certificado expedido por:	***Período de Validez***
AC auto-firmado (2048 bits)	Hasta 50 años
AC en línea	Generalmente 10 años después de la emisión y renovación
AC en-línea a Suscriptor usuario final individual	Generalmente 10 años después de la emisión y renovación

Tabla 4 – Períodos Operacionales de Certificado

Excepto como se estableció en esta Sección, Generalmente 10 años después de la renovación cesará todo uso de sus claves par después de que sus períodos de uso hayan vencido.

Los Certificados expedidos por Advantage Security a los Suscriptores usuario final individuales pueden tener Períodos Operacionales más largos de dos años, hasta cinco años, si se cumplen los siguientes requerimientos:

- Los Certificados son Certificados Individuales.
- Las claves par de los suscriptores residen en un token, tal como una tarjeta inteligente.
- Se les solicita a los suscriptores pasar por procedimientos de re-autentificación por lo menos cada 25 meses conforme a la Sección 3.2.3.
- Los suscriptores probarán la posesión de la clave privada correspondiente a la clave pública dentro del Certificado por lo menos cada 25 meses.

- Si un Suscriptor no puede completar los procedimientos de re-autentificación conforme a la Sección 3.2.3 exitosamente o no puede probar la posesión de dicha clave privada cuando se le requiera conforme a lo anterior, la AC automáticamente cancelará el Certificado de Suscriptor.

Los Certificados expedidos por las ACs a los Suscriptores usuarios finales Organizacionales Clase 2 podrán tener Períodos Operacionales más largos de dos años, hasta cinco años, siempre y cuando el contenido del certificado se re-autentificado por la AC o la AR por lo menos cada 25 meses.

6.4 Datos de Activación

6.4.1 Generación e Instalación de Datos de Activación

Advantage Security, al generar e instalar datos de activación de sus claves privadas utilizarán los métodos que protegen los datos de activación en la medida necesarias para prevenir la pérdida, robo, modificación, divulgación no autorizada o uso no autorizado de dichas claves privadas.

En la medida que se utilizan las contraseñas como datos de activación, los Suscriptores generarán contraseñas que no fácilmente pueden ser adivinadas o penetradas por ataques de directorios. Es posible que los Suscriptores usuarios finales Clase 2 no necesiten generar datos de activación, por ejemplo, si ellos utilizan dispositivos de acceso biométrico.

Advantage Security genera datos de activación para sus propias claves privadas de AC, y para las claves privadas de ACs y ARs dentro de sus Subdominios, de conformidad con los requerimientos de Secretos Compartidos de esta CP y los estándares documentados en la políticas confidenciales de seguridad de la JSE.

6.4.2 Protección de Datos de Activación

Advantage Security protegerá los datos de activación para sus claves privadas utilizando los métodos que protegen contra pérdida, robo, modificación, divulgación no autorizada o uso no autorizado de dichas claves privadas.

Los Suscriptores usuario final protegerán los datos de activación para sus claves privadas en la medida necesaria para prevenir pérdida, robo, modificación, divulgación no autorizada o uso no autorizado de dichas claves privadas.

Advantage Security utiliza Secretos Compartidos de conformidad con esta CP y los estándares documentados en las políticas confidenciales de seguridad de la JSE. Advantage Security proporciona los procesos y medios para dar la capacidad a los Propietarios de Partes de tomar las precauciones necesarias para prevenir pérdida, robo, modificación, divulgación no autorizada o uso no autorizado de las Partes Secretas que están en su poder. Los Propietarios de Partes no:

- Copiarán, divulgarán o pondrán a disposición de un tercero la Parte Secreta ni harán ningún uso no autorizado de ella; ni
- Divulgarán a ningún tercero su carácter o el carácter de otra persona como un Propietario de Parte.

Las Partes Secretas y cualquier información divulgada al Propietario de la Parte con relación a sus obligaciones como Propietario de la Parte constituyen Información Confidencial/Privada.

Advantage Security incluye en sus planes de recuperación en caso de desastre disposiciones para Propietarios de Partes que ponen a disposición sus Partes Secretas en un sitio de recuperación en caso de desastre después de un desastre. Advantage Security mantiene un registro de auditoria de Partes Secretas, y los Propietarios de Partes participarán en el mantenimiento de un registro de auditoria.

6.4.3 Otros Aspectos de Datos de Activación

6.4.3.1 Transmisión de Datos de Activación

En la medida en que se transmitan los datos de activación para sus claves privadas, Advantage Security protegerá la transmisión utilizando métodos que protejan contra pérdida, robo, modificación, divulgación no autorizada o uso no autorizado de dichas claves privadas. En la medida que la combinación de contraseñas de nombre del usuario de Windows o de red se utilicen como datos de activación para un Suscriptor usuario final, las contraseñas transferidas en una red estarán protegidas contra el acceso de usuarios no autorizados.

6.4.3.2 Destrucción de Datos de Activación

Los datos de activación para claves privadas AC serán desactivados utilizando métodos que protegen contra la pérdida, robo, modificación, divulgación no autorizada o uso no autorizado de dichas claves privadas protegidas por dichos datos de activación. Después de que venzan los períodos de retención de registros especificados en la Sección 5.5.2, Advantage Security desactivará los datos de activación mediante sobre-escritura y/o destrucción física.

6.5 Controles de Seguridad de Computadoras

Las funciones AC y AR ocurren en los Sistemas Confiables de conformidad con los estándares documentados en las políticas confidenciales de seguridad de la JSE (en el caso de Advantage Security).

6.5.1 Requerimientos Técnicos Específicos de Seguridad de Computadoras

Advantage Security asegurará que los sistemas que guardan los programas de cómputo y archivos de datos de la AC son Sistemas Confiables seguros contra acceso no autorizado, que puede demostrarse mediante el cumplimiento con el criterio de auditoria aplicable conforme a la Sección 4.5.1. Además, Advantage Security limita el acceso a los servidores de producción a aquellas personas con una razón de negocios válida para acceso. Los usuarios de aplicación general no tendrán cuentas en los servidores de producción.

Advantage Security tendrá las redes de producción lógicamente separadas de otros componentes. Esta separación previene el acceso a la red excepto a través de procesos de aplicación definidos. Los Centros de Procesamiento utilizarán sistemas de seguridad externos (firewalls) para proteger la red de producción de intrusiones internas y externas y limitar la naturaleza y fuente de las actividades de la red que puedan tener acceso a los sistemas de producción. Los Centros de Procesamiento requerirán del uso de contraseñas con un mínimo de tamaño de caracteres y una combinación de caracteres alfanuméricos y especiales, y requerirán que las contraseñas se cambien periódicamente y cuando sea necesario. El acceso directo a una base de datos de Advantage Security que guarda el depósito de Advantage Security estará limitado a las Personas de Confianza en el grupo de operaciones del Centro de Procesamiento que tengan una razón de negocios válida par dicho acceso.[6]

Las ARs se asegurarán de que los sistemas que mantienen programas de cómputo AR y archivos de datos sean Sistemas Confiables seguros contra acceso no autorizado, que puedan demostrarse mediante el cumplimiento con el criterio de auditoria aplicable conforme a la Sección 4.5.1.

Los ARs separarán, de manera lógica, el acceso a estos sistemas y a esta información de otros componentes. Esta separación previene el acceso excepto a través de procesos definidos. Las ARs utilizarán sistemas de seguridad externos para proteger la red de intrusiones internas y externas y limitarán la naturaleza y fuente de actividades que puedan tener acceso a dichos sistemas e información. Las ARs requerirán el uso de contraseñas con un mínimo de tamaño de caracteres y requerirán que las contraseñas se cambien periódicamente y según sea necesario. El acceso directo a la base de datos de la AR que guarda información del Suscriptor estará limitado a las Personas de Confianza en el grupo de operaciones de la AR que tenga una razón de negocios válida para dicho acceso.

6.5.2 Clasificación de Seguridad de Computadoras

Las áreas específicas de seguridad delicada de la funcionalidad de la AC y la AR del programa de cómputo que proporciona Advantage Security cumplirá con los requerimientos de aseguramiento EAL 3 (Criterio Común para Evaluación de Seguridad de la Tecnología de la Información, versión 2.1, Agosto, 1999).

6.6 Controles Técnicos de Ciclo de Vida

6.6.1 Controles de Desarrollo de Sistema

Advantage Security proporciona programas de cómputo para funciones AC y AR para. Dicho programa de cómputo, en la medida utilizada para manejar Certificados Clase 2 será desarrollado dentro de ambiente de desarrollo de sistemas que cumplan con los requerimientos de aseguramiento de desarrollo de Advantage Security. Advantage

[6] Los Servidores Gateway incluirán la siguiente funcionalidad:
Control de acceso a los servicios CA, identificación y autentificación de lanzamiento de servicios CA, re-uso de objeto para la memoria aleatoria de acceso de la CA, uso de criptografía para comunicación de sesión y seguridad de base de datos, archivos de historial de AC y de Suscriptor usuario final y de datos de auditoria, auditoria de seguridad relacionada con eventos, auto-prueba de seguridad relacionada con los servicios CA, y patrón Confiable para identificación de puestos de PKI e identidades asociadas.

Security utilizará un proceso de diseño y desarrollo que ejerza aseguramiento de calidad y corrección de procesos.

El programa proporcionado por Advantage Security, cuando se carga por primera vez, proporcionará un método para que la entidad verifique que el programa de cómputo en el sistema:

- Originado de Advantage Security,
- No haya sido modificado antes de la instalación, y
- Sea la versión que se intenta utilizar.

6.6.2 Controles de Administración de Seguridad

El programa de cómputo para funciones de AC y AR diseñado para administrar Certificados Clase 2 estará sujeto a revisiones para verificar su integridad. Advantage Security proporciona una mezcla de todos sus paquetes de programas de cómputo o actualizaciones de programas de cómputo. Esta mezcla puede utilizarse para verificar la integridad de dichos programas de cómputo de manera manual. Los Centros de Procesamiento también tendrán mecanismos y/o políticas para controlar y monitorear la configuración de sus sistemas AC. En el momento de la instalación y por lo menos una vez al día, Advantage Security validará la integridad del sistema AC.

6.7 Controles de Seguridad de Red

Las funciones AC y AR se llevan a cabo utilizando redes aseguradas de conformidad con los estándares documentados en las políticas confidenciales de Advantage Security para evitar el uso no autorizado, la falsificación y ataques de negación del servicio. Las comunicaciones de información delicada estarán protegidas utilizando encripción punto-a-punto para firmas de confidencialidad y digitales para no-rechazo y autentificación.

6.8 Sellos de Hora de Recepción

Los certificados, las CRLs y otros registros de cancelación de bases de datos contendrán información de la hora y la fecha. Dicho información de la hora no necesita ser criptográfica.

7 Certificado, CRL y Perfiles OCSP

7.1 Perfil de Certificado

Los Certificados JSE se apegan a (a) ITU-T Recomendación X.509 (1997): Tecnología de la Información – Interconexión de Sistemas Abiertos – El Directorio: Estructura de Autentificación, Junio 1997 y (b) RFC 3280: Internet X.509 Certificado de Infraestructura de Clave Pública y al Perfil CRL, Abril 2002 (“RFC 3280”).

Por lo menos, los Certificados X.509 Advantage Security contendrá los campos básicos y los valores indicados prescritos o las obligaciones de valor especificados en la Tabla 5 a continuación:

Campo	*Valor u Obligación de Valor*
Número de serie:	Valor único por Emisor DN
Algoritmo Firma	SHA-1 con RSA
Emisor DN	Véase Sección 7.1.4
Válido de	Base Universal de Tiempo Coordinado. Sincronizado al Reloj Maestro de la Secretaría de Economía. Codificado de acuerdo con la RFC 3280.
Válido para	Base Universal de Tiempo Coordinado. Sincronizado al Reloj Maestro de la Secretaría de Economía. Codificado de acuerdo con la RFC 3280.
Asunto DN	Véase CP § 7.1.4
Clave Pública	Codificado de acuerdo con la RFC 3280 Certificado de Suscriptor: 1024 bits Certificado de AC/AR: 2048 bits
Firma	Generado y codificado de conformidad con la RFC 3280.

Tabla 5 – Campos Básicos de Perfil de Certificado

7.1.1 Número(s) de Versión

Los Certificados Advantage Security serán Certificados X.509 Versión 3. Los Certificados AC serán Certificados AC X.509 Versión 3. Los Certificados de Suscriptor usuario final serán X.509 Versión 3.

7.1.2 Extensiones de Certificado

Advantage Security distribuirá Certificados X.509 Versión 3 con las extensiones requeridas por la Sección 7.1.2.-7.1.2.8.

7.1.2.1 Uso de la Clave

Generalmente se distribuyen Certificados X.509 Versión 3 de conformidad con la RFC 3280: Internet X.509 Certificado de Infraestructura Clave Pública X.509 y Perfil CRL, Abril 2002. La extensión de Uso de Clave en los Certificados X.509 Version 3 generalmente se configuran para establecer y autorizar datos y el campo crítico de conformidad con la Tabla 6 a continuación. El campo crítico en la extensión del Uso de la Clave generalmente se establece como falso.

		ACs	Suscriptores Usuario Final Clase 2
Criticalidad		FALSO	FALSO
0	digitalSignature	Autorizado	Establecido
1	nonRepudation	Autorizado	Autorizado
2	keyEncipherment	Autorizado	Establecido
3	dataEnchipherment	Autorizado	Autorizado

4	keyAgreement	Autorizado	Autorizado
5	keyCertSign	Establecido	Autorizado
6	CRLSign	Establecido	Autorizado
7	enchipherOnly	Autorizado	Autorizado
8	dicipherOnly	Autorizado	Autorizado

Tabla 6 – Aplicaciones para Extensión del Uso de Clave

Nota: Aunque el bit nonRepudation no está establecido en la extensión de Uso de Clave, Advantage Security sin embargo, soporta los servicios de nonRepudation para estos Certificados. No se requiere que el bit nonRepudation sea establecido en estos Certificados porque la industria de la PKI no ha alcanzado un consenso de lo que significa el bit nonRepudation. Hasta que surja tal consenso, el bit nonRepudation no será significativo para Partes Confiables potenciales. Además, las aplicaciones más comúnmente utilizadas no reconocen el bit nonRepudation. Por lo tanto, establecer el bit no ayudará a las Partes Confiables a tomar una decisión confiable. Consecuentemente, esta CP requiere que el bit nonRepudiation sea autorizado.

7.1.2.2 Extensión de Políticas de Certificado

La extensión de las Políticas de Certificado de Certificados X.509 Versión 3 se distribuye con el objeto identificador de esta CP de conformidad con la Sección 7.1.6 y con los calificadores de política establecidos en la Sección 7.1.8. El campo de criticalidad de esta extensión se establecerá en FALSO.

7.1.2.3 Nombres Alternativos de sujeto

La extensión subjectAltName de los Certificados X.509 Verisión 3 se distribuyen de acuerdo con la RFC 3280. El campo de criticalidad de esta extensión se establecerá en FALSO.

7.1.2.4 Obligaciones Básicas

La extensión de Obligaciones Básicas de Certificados AC X.509 Versión 3 tendrá el campo AC establecido en VERDADERO. La extensión de Obligación Básica de Certificados de Suscriptor Usuario Final se distribuirá con un valor de una secuencia vacía. El campo de criticalidad de esta extensión se establecerá en VERDADERO para los Certificados AC de lo contrario se establecerá en FALSO.

Los Certificados AC X.509 Versión 3 tendrán un campo “pathLenConstraint” de la extensión de Obligaciones Básicas establecido en el número máximo de certificados AC que pueden seguir a este Certificado en un patrón de certificación. Los Certificados AC expedidos a un Cliente Compañía en-línea que expide Certificados de Suscriptor usuario final tendrán un campo “pathLenConstraint” establecido en un valor “0” indicando que solamente un Certificado de Suscriptor usuario final podrá seguir en el patrón de certificación.

7.1.2.5 Puntos de Distribución de CRL

Certificados JSE X.509 Versión 3 se distribuyen con una extensión CrlDistribution que contine el URL de la ubicación donde una Parte Confiable puede obtener una CRL para verificar el estado del Certificado. El campo de criticalidad de esta extensión se establecerá en FALSO.

7.1.2.6 Identificador de Clave de Autoridad

Los Certificados JSE X.509 Versión 3 generalmente se distribuyen con una extensión authorityKeyIdentifier. El método para generar el keyIdentifier basado en la clave pública de la AC que expide el Certificado se calculará de acuerdo a uno de los métodos descritos en la RFC 3280. El campo de criticalidad de esta extensión se establecerá en FALSO.

7.1.2.7 Identificador de Clave de Sujeto

En los Certificados JSE X.509 Versión 3, el campo de criticalidad de esta extensión se establecerá en FALSO y el método para generar el keyIdentifier basado en la clave pública del Sujeto del Certificado será calculado de acuerdo con uno de los métodos descritos en la RFC 3280.

7.1.2.8 Identificadores Objeto Algoritmo

Los Certificados JSE se firman utilizando los siguientes algoritmos:

- Sha-1WithRSAEncription OBJECT IDENTIFIER ::={iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

Las firmas de Certificados producidas utilizando estos algoritmos cumplirán con la RFC 3279. El uso de sha-1WithRSAEncryption será el método de firma de Advantage Security.

7.1.3 Formas de Nombres

Los Certificados Advantage Security se distribuyen con el nombre requerido conforme a la Sección 3.1.1. Además, los Certificados de Suscriptor usuario final generalmente incluyen un campo de Unidad Organizacional adicional que contiene una notificación que establece que los términos de uso del Certificado se establecen en una URL, y el URL será un indicador para el Contrato de Parte Confiable aplicable. Las excepciones al requerimiento anterior se permitirán cuando el espacio, el formato o las limitaciones de inter-operabilidad dentro de los Certificados hagan que esa Unidad Organizacional sea imposible de usar junto con la aplicación de los Certificados.

7.1.4 Identificador de Objeto Política de Certificado

El identificador de objeto para la política de Certificado correspondiente a cada Clase de Certificado se establece en la Sección 1.2. La extensión CertificatePolicies en cada Certificado Advantage Security X.509 Versión 3 se distribuye de conformidad con la Sección 1.2.

7.1.5 Sintaxis y Semántica de Clasificadores de Política

Todos los Certificados Advantage Security X.509 Versión 3 incluyen un clasificador de política dentro de sus extensiones CertificatePolicies. Específicamente dichos Certificados contendrán un clasificador indicador CPS distribuido con una URL indicando el Contrato de Partes Confiable aplicable.

7.2 Perfil CRL

Los CRLs se apegan a la RFC 3280 y contienen los campos básicos y contenidos especificados en la Tabla 8 a continuación:

Campo	Valor o Obligación de Valor
Versión	Véase la Sección 7.2.1.
Algoritmo de Firma	Algoritmo utilizado para firmar la CRL. Las CRLs de Advantage Security se firman utilizando sha1WithRSAEncryption
Emisor	Advantage Security, S. de R.L. de C.V.
Fecha Efectiva.	La fecha de emisión de la CRL. Las CRLs son efectivas al momento de expedición.
Próxima Actualización:	La fecha mediante la cual se expedirá la próxima CRL. La frecuencia de expedición de la CRL es de conformidad con los requerimientos de la Sección 4.4.7.
Certificados Cancelados	El listado de los certificados cancelados, incluyendo el Número de Serie del Certificado cancelado y la Fecha de Cancelación.

Tabla 8 – Campos Básicos de Perfil de CRL

7.2.1 Número(s) de Versión

La Advantage Security soporta tanto CRLs X.509 Versión 1 como Versión 2.

7.3 Perfil OCSP

OSCP (Protocolo de Estado de Certificado En-Línea) es una forma de obtener información oportuna acerca del estado de cancelación de un certificado en especial. El OCSP puede utilizarse para validar:

- Certificados Persona Moral y Física Clase 2

Los contestadores OCSP se apegan a la RFC2560.

7.3.1 Número(s) de Versión

Se soporta la Versión 1 de la especificación del OCSP como se define por la RFC2560.

7.3.2 Extensiones OCSP

El Servicio Advantage Security utilizado para validar Certificados Organizacionales Clase 2 utiliza sellos de recepción seguros y período de validez para establecer el tiempo de cada respuesta del OCSP. Advantage Security no utiliza una ocasión para establecer el tiempo de cada respuesta del OCSP y los clientes no deben esperar una ocasión en la respuesta a una solicitud que contiene una ocasión. En vez de eso, los clientes deben utilizar el reloj local para verificar el tiempo de la respuesta.

8 Auditoria de Cumplimiento y Otras Evaluaciones

Advantage Security pasa por una auditoria de cumplimiento periódica ("Auditoria de Cumplimiento") para asegurar el cumplimiento con los Estándares JSE después de que comiencen las operaciones.

Además de estas auditorias de cumplimiento, Advantage Security tendrán la capacidad de llevar a cabo otras revisiones e investigaciones para asegurarse de la confiabilidad de la JSE, que incluye más no está limitada a:

- Una "Revisión de Seguridad y Prácticas". Una Revisión de Seguridad y Prácticas consiste de una revisión de una instalación segura, documentos de seguridad, CPS, contratos relacionados con la JSE, políticas de privacidad y planes de validación para asegurar que cumple con los Estándares JSE.
- Advantage Security tendrá la capacidad de llevar a cabo "Revisiones Complementarias de Administración de Riesgos" por si misma o un Cliente después de encontrar Auditorias de Cumplimiento incompletas o descubrimientos excepcionales o como parte del proceso general de administración de riesgos en el curso ordinario de operaciones.

Advantage Security tendrá la capacidad de delegar el llevar a cabo estas auditorias, revisiones e investigaciones a la Secretaría de Economía de la entidad que se esté auditando, revisando o investigando o a una compañía de auditoria. Las entidades que estén sujetas a una auditoria, revisión o investigación proporcionarán cooperación razonable a Advantage Security y al personal que lleve a cabo la auditoria, revisión o investigación.

8.1 Frecuencia y Circunstancias de Evaluación

Las Auditorias de Cumplimiento se llevan a cabo por lo menos anualmente por cuenta y gasto de la entidad auditada.

8.2 Identidad/Habilidades del Evaluador

Una compañía de auditoria llevará a cabo las Auditorias de Cumplimiento de Advantage Security dentro de un período de doce (12) meses.

Las revisiones y las auditorias llevadas a cabo por una empresa de auditoria serán realizadas por una compañía de contadores públicos certificada con experiencia demostrada en seguridad de computadoras o mediante profesionales en seguridad de computadoras empleados por un consultor competente de seguridad. Dicha empresa también habrá demostrado su experiencia en la realización de auditorias de seguridad IT y de cumplimiento de la PKI.

8.3 Relación del Evaluador con la Entidad Evaluada

Las Auditorias de Cumplimiento llevadas a cabo por empresas de auditoria serán realizadas por empresas independientes de la entidad auditada. Dichas empresas no tendrán un conflicto de intereses que entorpezca su capacidad de llevar a cabo servicios de auditoria.

8.4 Temas Cubiertos por la Evaluación

Los temas de auditoria para cada categoría de la entidad se establecen a continuación. La entidad auditada podrá hacer una Auditoria de Cumplimiento, un módulo que sea parte de una auditoria general anual de los sistemas de información de la entidad.

8.5 Auditoria de Advantage Security

Advantage Security será auditadas conforme a la Guía de Programa de Auditoria, la cual incorpora lineamientos proporcionados en la Declaración sobre Estándares de Auditoria (SAS *por sus siglas en* inglés) Número 770, del Instituto Americano de Contadores Públicos Certificados, *Reportes sobre* el Procesamiento de Operaciones de Organizaciones de Servicio. Sus Auditorias de Cumplimiento serán un WebTrust para las Autoridades de Certificación.

8.6 Acciones Tomadas como Resultado de Deficiencia

Después de recibir un reporte de Auditoria de Cumplimiento, la entidad de auditoria contactará a la parte auditada para discutir cualquier excepción o deficiencia mostrada por la Auditoria de Cumplimiento. Advantage Security también tendrá la capacidad de discutir dichas excepciones o deficiencias con la parte auditada. La entidad auditada y la Entidad Superior, de buena fe, utilizarán sus esfuerzos razonables comercialmente para convenir en un plan de acción correctivo para corregir los problemas que causan las excepciones o deficiencias y para implementar el plan.

En el caso de omisión de la entidad auditada en desarrollar un plan de acciones correctivas o implementarlo, o si el reporte revela excepciones o deficiencias que Advantage Security cree plantea una amenaza inmediata a la seguridad o integridad de la JSE, entonces:

(a) Advantage Security y/o la JSE determinarán si el reporte de cancelación y manipulación es necesario,
(b) Advantage Security y la JSE tendrán la capacidad de suspender los servicios a la entidad auditada, y
(c) Si es necesario, Advantage Security y la JSE podrán dar por terminados los servicios sujetos a esta CP y a los términos del contrato de la entidad auditada con su Entidad Superior.

8.7 Comunicaciones de Resultados

Después de cualquier Auditoria de Cumplimiento, la entidad auditada proporcionará a Advantage Security y a la Secretaría de Economía el reporte anual y los testimonios

basados en su auditoria o auto-auditoria dentro de los catorce (14) días después de terminar la auditoria y a más tardar cuarenta y cinco (45) días después de la fecha e aniversario del comienzo de operaciones.

9 Otros Negocios y Asuntos Jurídicos

9.1 Tarifas

9.1.1 Expedición de Certificado o Tarifas de Renovación

Advantage Security tiene la capacidad de cargar a los Suscriptores usuario final la expedición, administración y renovación de Certificados.

9.1.2 Tarifas de Acceso a Certificado

Advantage Security, las Afiliadas y los Clientes AR no cargarán una tarifa como condición para poner a disposición en un depósito un Certificado o en contrario poner a disposición de las Partes Confiables los Certificados.

9.1.3 Tarifas de Acceso a Cancelación o a Información de Estatus

Advantage Security no cargarán una tarifa como condición para poner a disposición en un depósito las CRLs o el servicios OCSP requeridas por esta CP o en contrario a disposición de las Partes Confiables. Advantage Security no permitirá el acceso a la información de cancelación, información de estatus de Certificado o el tiempo de recepción en sus depósitos, a terceros que proporcionen productos o servicios que utilicen dicha información de estatus de Certificado sin el previo consentimiento por escrito de Advantage Security.

9.1.4 Tarifas para Otros Servicios

Advantage Security no cargan una tarifa por acceso a esta CP o a sus respectivos CPS. Cualquier uso hecho con propósitos distintos a los de simplemente ver el documento, tal como la reproducción, redistribución, modificación o creación de trabajos derivados estarán sujetos a un contrato de licencia con la entidad que tiene los derechos de autor del documento.

9.1.5 Política de Reembolso

En la medida permitida por la ley aplicable, Advantage Security, las Afiliadas y las Revendedoras implementarán una política de reembolso. Establecerán sus políticas de reembolso dentro de sus sitios Web (incluyendo un listado en sus depósitos), en sus Contratos de Suscriptor y, en el caso de Advantage Security en sus CPSs.

9.2 Responsabilidad Financiera

9.2.1 Cobertura de Seguro

Advantage Security mantendrá un nivel comercialmente razonable de cobertura de seguro para errores y omisiones, ya sea a través de un programa de seguro de errores y omisiones con un corredor de seguros o una retención de auto-seguro. Este requerimiento de seguro no aplica para entidades gubernamentales.

9.2.2 Otros Activos

Advantage Security, las Afiliadas y los Clientes Compañía tendrán suficientes recursos financieros para mantener sus operaciones y cumplir con sus obligaciones, y ellos razonablemente deben poder soportar el riesgo de responsabilidad ante los Suscriptores y las Partes Confiables.

9.2.3 Cobertura de Seguro o Garantía para Entidades Finales

El Plan de Protección NetSure es un programa de garantía extendido que aplica dentro del Subdominio de Advantage Security de la JSE. En los casos que aplique, el Plan de Protección NetSure proporciona a los Suscriptores que reciben Certificados a Menudeo protección contra sucesos accidentales tales como robo, corrupción, pérdida o divulgación no intencional de la clave privada del Suscriptor (que corresponde ala clave pública en el Certificado), así como la impersonación y cierta pérdida de uso del Certificado del Suscriptor. El Plan de Protección NetSure también proporciona protección a las Partes Confiables cuando confían en Certificados cubiertos por el Plan de Protección NetSure. NetSure es un programa que proporciona Advantage Security y que está respaldado por el seguro contratado con corredores comerciales. Para información general con relación al Plan de Protección NetSure, y una explicación de que Certificados están cubiertos por dicho plan, visite **http://www.advantage-security.com/repositorio**.

Las protecciones del Plan de Protección NetSure también se ofrecen, por una tarifa, a los Clientes Compañía AR de Advantage Security. Pueden obtener protecciones conforme al Plan de Protección NetSure sujeto a los términos de un contrato adecuado por este servicio. Este servicio no solamente extiende las protecciones del Plan de Protección NetSure a los Suscriptores cuyas solicitudes de Certificado son aprobadas por el cliente compañía, también extiende estas protecciones al cliente compañía mismo.

Adicionalmente, Advantage Security cuenta con el seguro y fianza para fungir como Prestador de Servicios de Certificación, exigido por la Secretaría de Economía.

9.3 Confidencialidad de la Información de Negocio

9.3.1 Alcance de la Información Confidencial

Los siguientes registros de Suscriptores serán, conforme a las disposiciones de la Sección 9.3.2, mantenidos como confidenciales y privados (“Información Confidencial/Privada”):

- Registros de solicitud de AC, ya sea aprobados o rechazados,
- Registros de Solicitud de Certificado,

- Registros de operaciones (tanto registros totales como el registro de auditoria de las operaciones),
- Registros de auditoria a la JSE creados o retenidos por Advantage Security o un Cliente,
- Reportes de auditoria de la JSE creados por Advantage Security o un Cliente (en la medida que dichos reportes se mantengan), o por sus auditores respectivos (ya sea internos o públicos),
- Planeación de contingencia y planes de recuperación en caso de desastre, y
- Medidas de seguridad que controlan las operaciones de Advantage Security o el equipo y programas de cómputo de la Afiliada y la administración de servicios de Certificado y servicios designados de registro.

9.3.2 Información que No Está Dentro del Alcance de la Información Confidencial

Advantage Security reconoce que los Certificados, la cancelación de Certificado y otra información de estatus, depósitos de Advantage Security y la información contenida dentro ellos no es considerada Información Confidencial/Privada. La información no expresamente considerada Información Confidencial/Privada conforme a la Sección 9.3.1 no será considerada ni confidencial ni privada. Esta sección está sujeta a las leyes de privacidad aplicables.

9.3.3 Responsabilidad de Proteger la Información Confidencial

9.4 Privacidad de la Información Personal

9.4.1 Plan de Privacidad

Advantage Security establecerán una política de privacidad conforme a la Guía de Requerimientos Legales. Dichas políticas de privacidad se apegarán a las leyes aplicables de privacidad local. Advantage Security no divulgarán o venderán los nombres de los Solicitantes de Certificados u otra información de identificación acerca de ellos, de conformidad con las disposiciones de la Sección 9.3.2 y conforme al derecho de una AC final de transferir dicha información a una AC sucesora de conformidad con las disposiciones de la Sección 5.8.

9.4.2 Información Tratada como Privada

Cualquier información acerca de los Suscriptores que no esté disponible públicamente a través del contenido del certificado expedido, el directorio del certificado y las CRLs en-línea es tratada como privada.

9.4.3 Información No Considerada Como Privada

De acuerdo a las leyes locales, toda la información que se hace pública mediante un certificado no es considerada como privada.

9.4.4 Responsabilidad de Proteger la Información Privada

Los Participantes de la JSE que reciben información privada la asegurarán contra manipulaciones y divulgación a terceros y cumplirán con todas las leyes locales de privacidad en su jurisdicción.

9.4.5 Aviso y Consentimiento para Utilizar Información Privada

A menos que se establezca en contrario en esta CP, en la Política de Privacidad aplicable o mediante acuerdo, la información privada no se utilizará sin el consentimiento de la parte a quien dicha información aplique. Esta sección está sujeta a las leyes de privacidad aplicables.

9.4.6 Divulgación de Conformidad con los Procesos Judiciales o Administrativos

Advantage Security reconoce que tendrá la capacidad de divulgar Información Confidencial/Privada si, de buena fe, Advantage Security cree que:

- La divulgación es necesaria en respuesta a citación y a las garantías de búsqueda.
- La divulgación es necesaria en respuesta a procesos judiciales, administrativos o legales durante el proceso de averiguación en una acción civil o administrativa, tales como citaciones, interrogatorios, solicitudes de admisión y solicitudes de producción de documentos.

Esta sección está sujeta a las leyes de privacidad aplicables.

9.4.7 Otras Circunstancias de Divulgación de Información

Las políticas privadas contendrán disposiciones relacionadas con la divulgación de Información Confidencial/Privada a la persona que la divulgue a Advantage Security. Esta sección está sujeta a las leyes de privacidad aplicables.

9.5 Derechos de Propiedad Intelectual

9.5.1 Derechos de Propiedad en Información de Certificados y Cancelación

Las ACs retienen todos los Derechos de Propiedad Intelectual en la información de Certificados y de cancelación que ellos expiden. Advantage Security y los Clientes otorgarán permisos para reproducir y distribuir Certificados de manera no exclusiva libres de regalías, en la inteligencia que sean reproducidos completamente y que el uso de los Certificados esté sujeto al Contrato de Parte Confiable al que se hace referencia en el Certificado. Advantage Security y los Clientes otorgarán permiso para utilizar la información de cancelación para llevar a cabo las funciones de Parte Confiable conforme al Contrato de Uso de CRL aplicable, al Contrato de Parte Confiable o cualquier otro contrato aplicable.

9.5.2 Derechos de Propiedad en la CP

Los Participantes de la JSE reconoce que Advantage Security retiene todos los Derechos de Propiedad Intelectual de esta CP.

9.5.3 Derechos de Propiedad en Nombres

Un Solicitante de Certificado retiene todos los derechos que tiene (si hubiere) en cualquier marca, marca de servicio o nombre comercial contenidos en cualquier Solicitud de Certificado y nombre distinguido dentro de cualquier Certificado expedido para dicho Solicitante de Certificado.

9.5.4 Derechos de Propiedad en Claves y Material Clave

Las claves par que corresponden a los Certificados de las ACs y a los Suscriptores usuario final son propiedad de las ACs y de los Suscriptores usuario final que sean los respectivos Sujetos de estos Certificados, independientemente del medio físico dentro del cual se almacenan y protegen, y dichas personas retienen todos los Derechos de Propiedad Intelectual en esas claves par. Sin detrimento de lo anterior, las claves públicas raíz de Advantage Security y los Certificados raíz que las contienen, incluyendo todas las claves públicas y los Certificados auto-firmados, son propiedad de Advantage Security. Advantage Security otorga licencias a los fabricantes de programas y equipos de cómputo para reproducir dichos Certificados raíz para poner las copias en dispositivos o programas de cómputo confiables.

9.6 Manifestaciones y Garantías

9.6.1 Manifestaciones y Garantías de la CA

Las ACs de Advantage Security garantizan que:

- No hay ninguna alteración de hechos importante en el Certificado conocida por las entidades o que se origine de las entidades que aprueban la Solicitud de Certificado o que expiden el Certificado,
- No existen errores en la información en el Certificado que hayan sido introducidos por las entidades que aprueban la Solicitud de Certificado o que expiden el Certificado como resultado de una omisión en ejercer el cuidado razonable en el manejo de la Solicitud de Certificado o en la creación del Certificado,
- Sus Certificados cumplen con todos los requerimientos importantes de esta CP y la CPS aplicable, y
- Los servicios de cancelación y el uso de un depósito se apegan a todos los requerimientos importantes de esta CP y la CPS aplicable en todos los aspectos importantes.

9.6.2 Manifestaciones y Garantías de la AR

Las ARs de Advantage Security garantizan que:

- No hay ninguna alteración de hechos importante en el Certificado conocida por las entidades o que se origine de las entidades que aprueban la Solicitud de Certificado o que expiden el Certificado,

- No existen errores en la información en el Certificado que hayan sido introducidos por las entidades que aprueban la Solicitud de Certificado o que expiden el Certificado como resultado de una omisión en ejercer el cuidado razonable en el manejo de la Solicitud de Certificado.
- Sus Certificados cumplen con todos los requerimientos importantes de esta CP y la CPS aplicable, y
- Los servicios de cancelación (cuando apliquen) y el uso de un depósito se apegan a todos los requerimientos importantes de esta CP y la CPS aplicable en todos los aspectos importantes

Los Contratos de Suscriptor podrán incluir manifestaciones y garantías adicionales.

9.6.3 Manifestaciones y Garantías del Suscriptor

El Suscriptor garantiza que:

- Cada firma digital creada que utiliza la clave privada que corresponde a la clave pública listada en el Certificado es la firma digital del Suscriptor y que el Certificado ha sido aceptado y que está en operación (no vencido o cancelado) en el momento en que se crea la firma digital.
- Su clave privada está protegida y que ninguna persona no autorizada ha tenido nunca acceso a la clave privada del Suscriptor.
- Todas las manifestaciones hechas por el Suscriptor en la Solicitud de Certificado y presentadas por el Suscriptor son verdaderas.
- Toda la información proporcionada por el Suscriptor y contenida en el Certificado es verdadera.
- El Certificado está siendo utilizado exclusivamente para propósitos autorizados y legales, consistentes con todos los requerimientos importantes de esta CP y la CPS aplicable, y
- El Suscriptor es un Suscriptor usuario final y no una AC, y no está utilizando la clave privada que corresponde a ninguna clave pública listada en el Certificado para propósitos de firmar digitalmente ningún Certificado (o cualquier otro formato de clave pública certificada) o CRL, como una AC o en contrario.

Los Contratos de Suscriptor podrán incluir manifestaciones y garantías adicionales.

Manifestaciones y Garantías de la Parte Confiable

Los Contratos de Parte Confiable requieren a las Partes Confiables reconocer que tienen suficiente información para tomar una decisión informada con respecto a la medida en la cual ellos escogen confiar en la información en un Certificado, que son los únicos responsables por decidir si confiar o no en dicha información y que ellos soportarán todas las consecuencias legales por su omisión en cumplir con las obligaciones de Parte Confiable en términos de esta CP.

Los Contratos de Parte Confiable podrán incluir manifestaciones y garantías adicionales.

9.7 Renuncia de Garantías

En la medida permitida por la ley aplicable, los Contratos de Suscriptor y los Contratos de Parte Confiable renunciarán a las posibles garantías de Advantage Security y a las de las

Afiliadas, incluyendo cualquier garantía de mercantibilidad o adecuación a un propósito especial, fuera del contexto del plan de Protección NetSure.

9.8 Limitaciones de Responsabilidad

En la medida permitida por la ley aplicable, los Contratos de Suscriptor y los Contratos de Parte Confiable limitarán la responsabilidad de Advantage Security y la responsabilidad aplicable de las Afiliadas fuera del contexto del Plan de Protección NetSure. Las limitaciones de responsabilidad incluirán una exclusión de daños indirectos, especiales, incidentales y consecuenciales. También incluirán los siguientes topes de responsabilidad que limitan los daños de Advantage Security y de la Afiliada con relación a un Certificado específico:

Clase	Topes de Responsabilidad
Clase 2	Cinco mil dólares americanos (US $20,000.00)

Tabla 9 – Topes de Responsabilidad

Los topes de responsabilidad en la Tabla 5 limitan los daños recuperables fuera del contexto del Plan de Protección NetSure. Las cantidades pagadas conforme al Plan de Protección NetSure están sujetas a sus propios topes de responsabilidad. **http://www.advantage-security.com/repositorio/**.

La responsabilidad (y/o limite de la misma) de los Suscriptores será como se establece en los contratos aplicables de Suscriptor.

La responsabilidad (y/o límite de la misma) de los Agentes Certificadores externos será como se establece en los Contratos aplicables de Parte Confiable.

Indemnizaciones

9.8.1 Indemnización por parte de los Suscriptores

En la medida permitida por la ley aplicable, se le requiere al Suscriptor indemnizar a Advantage Security por:

- Falsedad o alteración de hechos por parte del Suscriptor en la Solicitud de Certificado del Suscriptor.
- Omisión por parte del Suscriptor en divulgar un hecho importante en la Solicitud de Certificado, si la alteración u omisión fue hecha de manera negligente o con la intención de engañar a alguna parte,
- La omisión del Suscriptor en proteger la clave privada del Suscriptor, para utilizar un Sistema Confiable, o en contrario tomar las precauciones necesarias para evitar la manipulación, pérdida, divulgación, modificación o uso no autorizado de la clave privada del Suscriptor, o
- El uso de un nombre del Suscriptor (incluyendo mas no limitado dentro de un nombre común, nombre de dominio, o dirección de correo electrónico) que infrinja los Derechos de Propiedad Intelectual de un tercero.

El Contrato de Suscriptor aplicable podrá incluir obligaciones de indemnización adicionales.

9.8.2 Indemnización por parte de las Partes Confiables

En la medida permitida por la ley aplicable, los Contratos de Parte Confiable requerirán a las Partes Confiables indemnizar a Advantage Security y a cualquier AC o AR que no sea de Advantage Security por:

- La omisión de la Parte Confiable en cumplir con las obligaciones de una Parte Confiable,
- La confianza de la Parte Confiable en un Certificado que no es razonable conforme a las circunstancias, o
- La omisión de la Parte Confiable en checar el estatus de dicho Certificado para determinar si el Certificado está vencido o cancelado.

El Contrato de Parte Confiable aplicable podrá incluir obligaciones de indemnización adicionales.

9.9 Vigencia y Terminación

9.9.1 Vigencia

La CP entra en vigor al momento de su publicación en el depósito de Advantage Security. Las modificaciones a esta CP son ejercibles al momento de su publicación en el depósito de Advantage Security.

9.9.2 Terminación

Esta CP según se modifique periódicamente permanecerá vigente hasta que sea reemplazada por una nueva versión.

9.9.3 Efecto de Terminación y Sobrevivencia

Sin embargo, al momento de la terminación de esta CP, Advantage Security está obligado conforme a sus términos para todos los certificados expedidos por el tiempo restante de los periodos de validez de dichos certificados.

9.9.4 Notificaciones Individuales y Comunicaciones con Participantes

A menos que se especifique en contrario mediante acuerdo entre las partes, los participantes de la JSE utilizarán los métodos razonables comercialmente para comunicarse entre sí, tomando en consideración la criticalidad y materia objeto de la comunicación.

Modificaciones

9.9.5 Procedimiento de Modificación

Las modificaciones a esta CP pueden hacerse mediante la Autoridad Administradora de la Política de Advantage Security. Las modificaciones serán ya sea en el formato de un documento que contenga un formato modificado de la CP o una actualización. Las versiones modificadas o actualizaciones estarán asociadas con la sección de Actualizaciones de Prácticas y Notificaciones del Depósito de Advantage Security ubicado en:
https://www.advantage-security.com/repositorio/ Las actualizaciones reemplazan cualquier disposición designada o en conflicto de la versión referenciada en la CP. La Gerencia de Prácticas y Políticas determinará si los cambios a la CP requieren un cambio en los identificadores de objeto de la política del Certificado de las políticas de Certificado que correspondan a cada Clase de Certificado.

9.9.6 Mecanismo y Período de Notificación

Advantage Security se reserva el derecho de modificar la CP sin notificación de las modificaciones que no son importantes, incluyendo mas no limitadas a correcciones de errores tipográficos, cambos a las URLs, y cambios a la información de contacto. La decisión de Advantage Security de designar modificaciones como importantes o no importantes será a la sola discreción de Advantage Security.

Independientemente de cualquier cosa en la CP en contrario, si Advantage Security cree que las modificaciones importantes a la CP son necesarias inmediatamente para detener o evitar una violación a la seguridad de la JSE o de cualquier parte de ella, Advantage Security tendrá la capacidad de hacer dichas modificaciones mediante su publicación en el Depósito de Advantage Security. Dichas modificaciones serán efectivas inmediatamente en el momento de su publicación. Dentro de un tiempo razonable después de la publicación, Advantage Security notificará dichas modificaciones a las Afiliadas.

9.9.6.1 Período de Comentarios

Excepto como se exprese en contrario, el período de comentarios para cualquier modificación importante a la CP será quince (15) días, a partir de la fecha en la cual se transmitan las modificaciones en el Depósito de Advantage Security. Cualquier Participante de la JSE tendrá la capacidad de presentar comentarios ante Advantage Security hasta el final del período de comentarios.

9.9.6.2 Mecanismo para Manejar los Comentarios

Advantage Security considerará cualquier comentario a las modificaciones propuestas. Advantage Security ya sea (a) permitirá que las modificaciones propuestas entren en vigor sin modificación, (b) cambiará las modificaciones propuestas y las republicará como una nueva modificación cuando se requiera, ó (c) retirará las modificaciones propuestas. Advantage Security tiene la capacidad de retirar modificaciones propuestas notificando a las Afiliadas y proporcionando notificación en la sección de Actualización de Prácticas y Notificaciones del Depósito de Advantage Security. A menos que las modificaciones

propuestas se cambien o retiren, serán efectivas al momento del vencimiento del período de comentarios.

9.9.7 Circunstancias conforme a las Cuales Debe Cambiarse el OID

Si Advantage Security determina que es necesario un cambio en el identificador de objeto que corresponde a una política de Certificado, la modificación contendrá nuevos identificadores de objeto para las políticas de Certificado que correspondan al Certificado. De lo contrario, las modificaciones no requerirán un cambio en el ìdentificador de objeto de la política del Certificado.

9.10 Disposiciones de Resolución de Disputas

9.10.1 Disputas entre Advantage Security, las Afiliadas y los Clientes

Las disputas entre uno o más de cualquiera de Advantage Security, las Afiliadas y/o los Clientes serán resueltas de conformidad con las disposiciones en los contratos aplicables entre las partes.

9.10.2 Disputas con Suscriptores Usuario Final o Partes Confiables

En la medida permitida por la ley aplicable, los Contratos de Suscriptor y los Contratos de Parte Confiable contendrán una cláusula de resolución de disputas. Los procedimientos en la Guía de Requerimientos Legales de Prácticas para resolver disputas que involucren a Advantage Security requieren un período de negociación inicial de sesenta (60) días después del litigio en el tribunal federal o estatal que comprenda el Condado del Distrito Federal, México, en el caso de los demandantes que sean residentes Mexicanos o, en el caso de todos los otros demandantes, arbitraje proporcionado por la Cámara Internacional de Comercio (“ICC” *por sus siglas en inglés*) de conformidad con los Reglamentos de la ICC de Conciliación y Arbitraje, a menos que Advantage Security apruebe lo contrario.

9.11 Ley Gobernante

Sujeto a cualquier límite que aparezca en la ley aplicable, las leyes del Distrito Federal, México, gobernarán la ejecutabilidad, interpretación y validez de esta CP, independientemente de contrato o de otra decisión de disposiciones de ley y sin el requerimiento de establecer un nexo comercial en Distrito Federal, México. Esta decisión de ley se toma para asegurar procesos e interpretación uniforme para todos los Participantes de la JSE, independientemente de donde se localizan.

Esta disposición de ley gobernante aplica solamente a esta CP. Los contratos que incorporan la CP mediante referencia podrán tener sus propias disposiciones de ley gobernante, en la inteligencia de que esta Sección 9.14 gobierna la ejecutabilidad, interpretación y validez de los términos de la CP separados y aparte de las disposiciones remanentes de cualquier dicho contrato, sujetas a cualquier limitación que aparezca en la ley aplicable.

Esta CP está sujeta a las leyes aplicables nacionales, estatales, locales y extranjeras, reglamentos, regulaciones, ordenanzas, decretos y ordenes incluyendo mas no limitadas a restricciones de exportación o importación de programas de cómputo, equipo de cómputo o información técnica.

9.12 Cumplimiento con la Ley Aplicable

Esta CP está sujeta a las leyes aplicables nacionales, estatales, locales y extranjeras, reglamentos, regulaciones, ordenanzas, decretos y ordenes incluyendo mas no limitadas a restricciones de exportación o importación de programas de cómputo, equipo de cómputo o información técnica.

9.12.1 Separabilidad

En el caso de que un tribunal de ley u otro tribunal que tenga autoridad considere que una cláusula o disposición de esta CP no es válida, las cláusulas o disposiciones remanentes de la CP permanecerán válidas.

9.12.2 Causas de Fuerza Mayor

En la medida permitida por la ley aplicable, los Contratos de Suscriptor y los Contratos de Parte Confiable incluirán una cláusula de casos de fuerza mayor que proteja a Advantage Security.