POLÍTICA DE CERTIFICACIÓN (CP)

E-SIGN S.A.

VERSION 1.2

Fecha: Marzo 2014

INDICE

1 INTRODUCCION

La **Comunidad de Confianza de E-Sign** (***E-SIGN CA NET***) es una PKI que agrupa una gran comunidad pública, organizada a través de distintas autoridades certificadoras digitales ampliamente distribuidas, y de usuarios con diversas necesidades de comunicación y de información segura.

E-Sign ofrece servicios de la E-SIGN CA NET en conjunto con una red global de Asociados ("Asociados") a través de todo el mundo.

Este documento, "POLÍTICA DE CERTIFICADOS DE E-SIGN CA NET" (CP) es la principal declaración de política que gobierna la E-SIGN CA NET. La CP cuida de los requerimientos de negocio y técnicos que permiten aprobar, proveer, administrar, usar, revocar y renovar Certificados digitales en la E-SIGN CA NET, y provee a todos los participantes de la E-SIGN CA NET, servicios confiables asociados. Estos requerimientos protegen la seguridad e integridad de la E-SIGN CA NET y comprenden un único conjunto de reglas que se aplican en forma consistente y transversal a toda la E-SIGN CA NET, sus CA raíz, CA subordinadas y certificados de usuario final. La CP no es un acuerdo legal entre E-Sign y los participantes de la E-SIGN CA NET; las obligaciones contractuales entre E-Sign y los participantes de la E-SIGN CA NET son establecidas por medio de acuerdos con dichos participantes.

Este documento está dirigido a:

- Proveedores de servicio PKI de la E-SIGN CA NET ("Asociados") quienes tienen que operar en términos de su propia CPS (Declaración de Prácticas de Certificación) que cumpla con los requisitos establecidos por la CP.
- Suscriptores de Certificados que necesiten entender como son autenticados y cuáles son sus obligaciones como Suscriptores de E-SIGN CA NET y cómo son protegidos bajo la E-SIGN CA NET
- Terceras partes que reciben los certificados digitales de la ESIGN CA, que necesitan saber cuánta confianza pueden depositar en un Certificado de la E-SIGN CA NET, o en un documento firmado utilizando ese Certificado.

La CP en todo caso no gobierna ningún servicio fuera de ella. Por lo tanto, E-Sign y Asociados pueden ofrecer servicios de creación de entidades certificadoras privadas, a través de los cuales algunas organizaciones creen su propia CA privada fuera de la E-SIGN CA NET, y puedan emitir certificados digitales; en el caso de las jerarquías privadas, las organizaciones externalizan a E-Sign o a algún Asociado las funciones de back-end para la entrega, administración, revocación y renovación de Certificados.

Dado que esta CP solo aplica a la E-SIGN CA NET, esta no aplica para estas jerarquías privadas.

Esta CP se ajusta a la Internet Engineering Task Force (IEFT) RFC 3647 en lo que respecta a Política de Certificados (CP Certificate Policy) y a la construcción de la Declaración de Práctica de Certificación (CPS Certification Practice Statement).

1.1 Resumen

Un resumen de la estructura de la E-SIGN CA NET se muestra en el Diagrama 1, más abajo. En la parte superior de la jerarquía se halla esta CP, que contiene las políticas bajo las cuales los participantes deben operar.

E-Sign, sus CA subordinadas y sus clientes con CA Subdordinadas (Asociados) operan como CAs bajo la CP de la E-SIGN CA NET, emitiendo Certificados de usuarios finales (Suscriptores).

Las Autoridades de Registro (RAs, Registration Authorities) son entidades que validan los requerimientos de Certificado bajo la E-SIGN CA NET. E-Sign y sus Asociados actúan como RAs para los Certificados que emiten.
E-Sign y los Asociados establecen relaciones contractuales con empresas que deseen administrar los requerimientos de sus propios Certificados, y que actúan como RAs, autentificando requerimientos de Certificado para ellos mismos y para sus Asociados individuales. E-Sign o el Asociado entonces podrán dar cumplimiento a la emisión de los Certificados autentificados.

Dependiendo de la clase y tipo de Certificado, los Certificados Digitales pueden ser usados por los Suscriptores paraasegurar sitios Web, firmar digitalmente código u otro contenido, firmar digitalmente documentos y/o correos electrónicos. La persona que finalmente recibe un documento o comunicación firmada, o bien accede un sitio Web seguro se conoce como el Tercero que Confía, es decir, él/ella está confiando en el Certificado y debe tomar una decisión de si confiar en él.

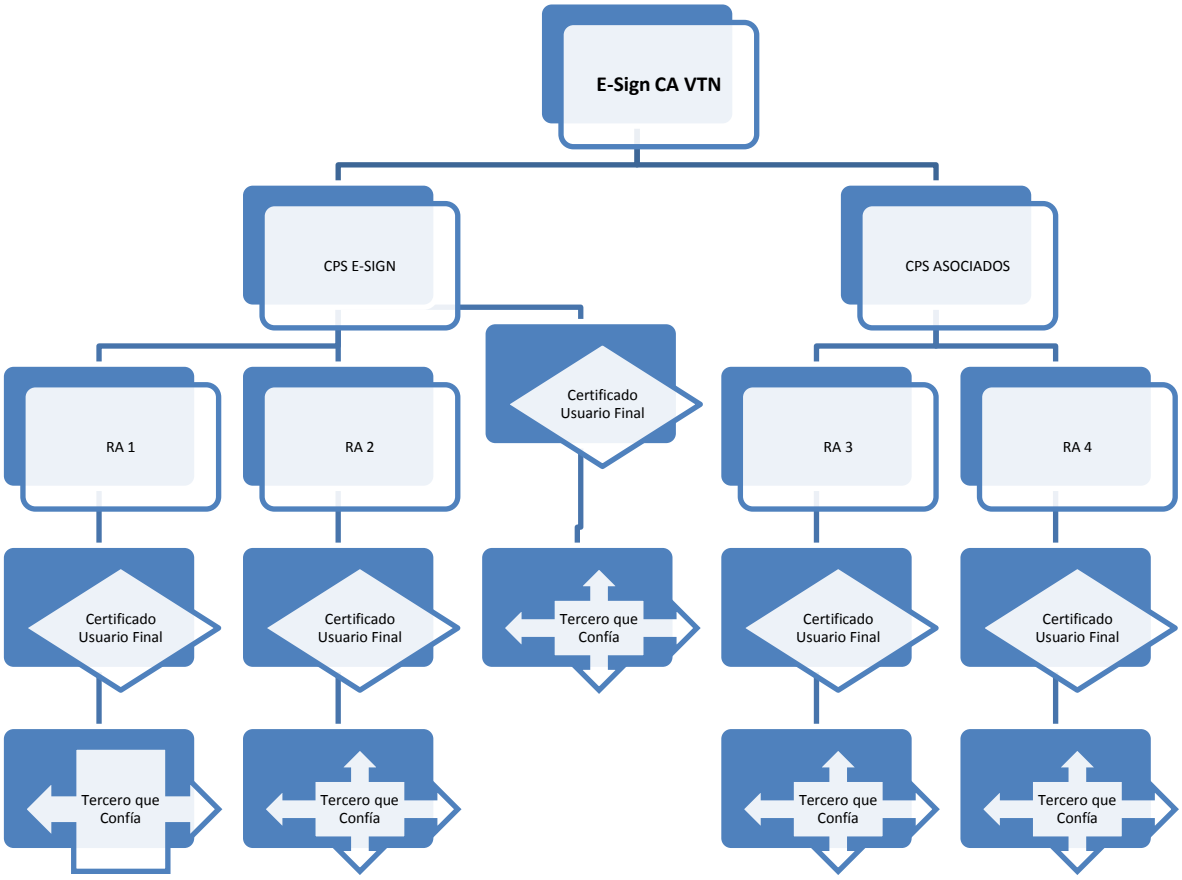

Diagrama 1. Estructura E-SIGN CA NET

El Diagrama 2 más abajo muestra en forma resumida las clases de Certificado bajo la E-SIGN CA NET, a quienes se les puede proveer y sus respectivos niveles de seguridad, basados en los procedimientos de identificación y autentificación requeridos para cada clase. Esta CP describe con más detalle cómo se hace la autenticación e identificación para cada Clase o Certificado.

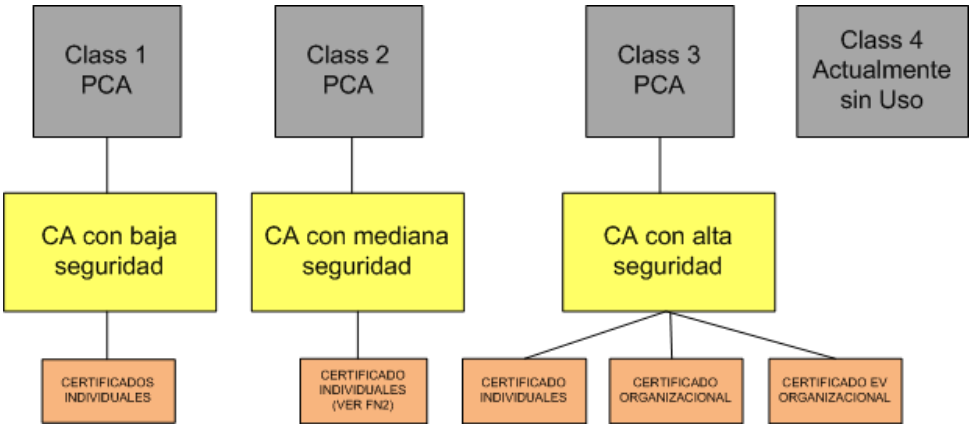

Diagrama 2. Clases de Certificados E-SIGN CA NET

1.2 Nombre e Identificación de este Documento

Este documento es la Política de Certificación (CP Certificate Policy) de E-SIGN CA NET. E-Sign, actuando como autoridad definidora de la política, ha asignado un objeto identificador de valor extendido para cada Clase de Certificado entregado bajo la E-SIGN CA NET. Los valores de los objetos identificadores utilizados para las Clases de usuarios de los Certificados Suscritos son:

- La Política de Certificado de la E-SIGN CA NET:

La OID indicada anteriormente puede ser extendida para definir políticas adicionales, que puedan cubrir un tipo particular de Certificado. El OID extendido debe ser definido en la CPS particular para ese producto.

1.3 Participantes de la PKI

1.3.1 Autoridades Certificadoras

El término Autoridad Certificadora o Autoridad de Certificación (CA) es el término genérico que se refiere a todas las entidades autorizadas para emitir Certificados de llave pública bajo la E-SIGN CA NET. El termino CA abarca una subcategoría de emisores llamadas Autoridades Certificadoras Primaria (PCA Primary Certification Authority). Las PCAs actúan como raíz de tres dominios, uno por cada clase de Certificado. Cada PCA es una entidad de E-Sign. Las Autoridades Certificadoras son subordinadas a las PCAs, y son las que emiten Certificados de usuario final o de otras Autoridades Certificadoras (CAs).

Los clientes empresariales (“Clientes Empresa”) de E-Sign pueden operar sus propias entidades emisoras como una CA subordinada a una PCA E-SIGN CA NET, para las personas que forman parte de su organización. Este cliente entra en una relación contractual con E-Sign para cumplir con todas las exigencias de la CP de E-SIGN CA NET. Estas CAs subordinadas pueden, sin embargo, poner en práctica una serie de prácticas más restrictivas sobre la base de sus necesidades internas.

1.3.2 Autoridades de Registro

Una Autoridad de Registro es una entidad que realiza la identificación y autenticación de solicitantes Certificados de Certificados de usuario final, envía solicitudes de revocación de Certificados de usuario final, y aprueba las solicitudes de renovación o de reemisión de Certificados en nombre de una CA de la E-SIGN CA NET. E-Sign y los Asociados pueden actuar como RA para los Certificados que emiten.

Los terceros que entran en una relación contractual con E-Sign o un Asociado, pueden operar su propia RA y autorizar la emisión de Certificados a través de una autoridad de la E-SIGN CA NET. Las RAs de terceros deben cumplir con todos los requisitos de la CP E-SIGN CA NET, la CPS pertinente y todo acuerdo contractual firmado con E-Sign. Las RAs pueden, sin embargo, poner en práctica una serie de prácticas más restrictivas sobre la base de sus necesidades internas. Un ejemplo de RA como tercera parte es un cliente de EGovSign.

1.3.3 Suscriptores

Son considerados Suscriptores bajo la E-SIGN CA NET todos los usuarios finales (incluidas las entidades) de Certificados emitidos por una CA E-SIGN CA NET. Un Suscriptor es la entidad nombrada como el usuario final Suscriptor de un Certificado. Usuarios finales Suscriptores pueden ser personas, organizaciones o, componentes de infraestructura, tales como firewalls, routers, servidores de seguridad u otros medios utilizados para asegurar las comunicaciones dentro de una organización.

En algunos casos, los Certificados son emitidos directamente a personas o entidades para su propio uso. Sin embargo, normalmente existen otras situaciones en que la parte que requiere un Certificado es diferente del sujeto al que le corresponde la credencial. Por ejemplo, una organización puede requerir Certificados para sus empleados de tal forma que puedan representar a la organización en transacciones electrónicas del negocio. En tal situación, la entidad que suscribe la emisión de Certificados (es decir, paga por ellos, ya sea a través de la suscripción a un servicio específico, o como emisor) es diferente a la entidad que es el sujeto del Certificado (por lo general, el titular de la credencial). Dos términos diferentes se utilizan en esta CP para distinguir estos dos roles: "Suscriptor", es la entidad que contrata con E-Sign la capacidad de emisión de credenciales y "Sujeto", es la persona a la que se le otorga la credencial. El Suscriptor tiene la responsabilidad última sobre el uso de la credencial, pero el sujeto es el individuo que se autentica cuando se presenta la credencial.
Cuando se utiliza “Sujeto”, es para indicar una distinción respecto del Suscriptor. Cuando se utiliza "Suscriptor", puede significar sólo el Suscriptor como una entidad distinta, pero también puede usar el término para abarcar a los dos. El contexto de su uso en esta CP invocará la comprensión correcta.
Las CAs son técnicamente también los Suscriptores de los Certificados dentro de la E-SIGN CA NET, ya sea como PCA que se emite un Certificado autofirmado a sí mismo, o como una CA a la cual una CA Superior le emite un Certificado. Las referencias a "entidades finales" y "Suscriptores" en esta CP, sin embargo, sólo se aplican a usuarios finales Suscriptores.

1.3.4 Terceros que Confían (Parte que Confía)

Los Terceros que Confían (Parte que Confía) es una persona o entidad que actúa confiando en un Certificado y / o una firma digital emitida bajo la E-SIGN CA NET. Los Terceros que Confían puede ser o no un Suscriptor dentro de la E-SIGN CA NET.

1.3.5 Otros Participantes

Un Asociado es un tercero de confianza de importancia, por ejemplo en la industria de las tecnologías, las telecomunicaciones o la industria de servicios financieros que ha llegado a un acuerdo con E-Sign para operar una Autoridad Certificadora bajo la E-SIGN CA NET dentro de un territorio específico.

Los Clientes Empresa son organizaciones que pueden operar sus propias entidades emisoras como una CA bajo E-SIGN CA NET, para las personas que forman parte de su organización.

1.4 Uso de los Certificados

1.4.1 Uso adecuado de los Certificados

1.4.1.1 Certificados Emitidos a Personas (Certificados Individuales)

Los Certificados individuales son utilizados normalmente por las personas para firmar y encriptar (cifrar) correos electrónicos y para la autenticación en aplicaciones (autenticación de cliente). No obstante que los usos más comunes de Certificados individuales se incluyen en la tabla indicada a continuación, un Certificado individual puede ser utilizado para otros fines, siempre que los Terceros que Confían sea capaces de confiar razonablemente en el Certificado y que ese uso no esté prohibido por la ley, por esta CP, por cualquier CPS bajo la cual haya sido emitido el Certificado y cualquier acuerdo con los Suscriptores.

Clase de Certificado	Nivel de Seguridad			Uso		
	Nivel de Seguridad Bajo	Nivel de Seguridad Medio	Nivel de Seguridad Alto	Firmado	Encriptación	Autenticación del Cliente
Certificados Class 1	✓			✓	✓	✓
Certificados Class 2		✓		✓	✓	✓
Certificados Class 3			✓	✓	✓	✓

Tabla 1. Usabilidad de Certificados Individuales

1.4.1.2 Certificados emitidos a Organizaciones

Los Certificados de Organización se emiten a organizaciones después de autenticar que la Organización tiene existencia legal y que los atributos de otra Organización incluidos en el Certificado (con exclusión de la información no verificada de Suscriptor) han sido autenticados. Por ejemplo, la propiedad de un dominio de Internet o e-mail. No es la intención de esta CP limitar los casos de usos de Certificados Organizacionales. Mientras que los usos más comunes se incluyen en la tabla que se muestra a continuación, un Certificado organizacional puede ser utilizados para otros fines, siempre que el usuario que confía sea capaz de confiar razonablemente en el Certificado y que su uso no esté prohibido por la ley, por la CP, por cualquier CPS bajo la cual haya sido expedido el Certificado y los acuerdos con los Suscriptores.

1.4.1.3 Niveles de Seguridad

Los Certificados de Nivel de Seguridad Bajo son Certificados que no deberían ser utilizados para propósitos de autentificación o para soportar el no repudio. Este certificado digital ofrece modestas garantías de que el correo electrónico fue originado a partir de un emisor con una determinada dirección de correo electrónico. El Certificado, sin embargo, no aporta prueba alguna de la identidad del Suscriptor. La aplicación de encriptación permite a un Tercero que Confía utilizar el Certificado del Suscriptor para cifrar los mensajes al Suscriptor, aunque el

Tercero que Confía remitente no puede estar seguro de que el receptor es de hecho la persona nombrada en el Certificado.

Los Certificados de Nivel de Seguridad Medio son aquellos Certificados útiles para garantizar la identidad del Suscriptor, y su correo electrónico, y que requieren un nivel medio de seguridad, en relación a la clase 1 y 3.

Los Certificados de alta seguridad son Certificados de Class 3 individuales y organizacionales de que proporcionan un alto nivel de seguridad de la identidad del Suscriptor, en comparación con los certificados Class 1 y 2.

1.4.2 Usos Prohibidos de Certificados

Los Certificados deben ser utilizados solo en la medida que su uso sea consistente con la ley aplicable, y en particular deberán ser utilizados sólo hasta el punto que ésta lo permita.

Los Certificados de E-SIGN CA NET no están diseñados, concebidos ni autorizados para su uso en equipos de control críticos o para usos que requieren un rendimiento a prueba de fallos, tales como la operación de instalaciones nucleares, control de sistemas de navegación o comunicación, sistemas de control de tráfico aéreo, o sistemas de control de armas, donde una falla podría acarrear la muerte, lesiones personales o daños medioambientales graves. Además, los Certificados de Class 1 no deberán ser utilizados como prueba de identidad o como soporte de no repudio de identidad o autoría. Los Certificados de cliente están destinados a aplicaciones de cliente y no deberán ser utilizados como Certificados de servidor o Certificados de la organización.

Los Certificados de CA no se pueden utilizar para cualquier función, excepto las funciones propias de CA. Por otra parte, los Certificados de Suscriptor de usuario final no deberán ser utilizados como Certificados de CA.

1.5 Política de Administración

1.5.1 Organización que Administra la Documentación

E-Sign S.A.
Avenida Andrés Bello 2.777, Oficina 1503
Las Condes
Santiago
Chile

1.5.2 Contacto

Administrador de la Política de Certificados
E-Sign S.A.
Avenida Andrés Bello 2.777, Oficina 1503
Las Condes
Santiago
Chile
+56 (2) 24331500
+56 (2) 24331501
practicas@esign-la.com

1.5.3 Persona que determina la CP Adecuada para la Política

La Autoridad de Administración de la Política E-SIGN CA NET (PMA Policy Management Authority) determina la propiedad y aplicabilidad de esta CP.

1.5.4 Procedimiento de Aprobación de la CP

La aprobación de esta CP y posteriores modificaciones serán realizados por el PMA. Las modificaciones podrán estar en forma de un documento conteniendo una modificación de la CP o bien en un aviso de actualización. Las versiones modificadas o actualizaciones estarán vinculadas a la Sección Actualizaciones y Avisos de las Prácticas del repositorio E-SIGN ubicado en: *https://www.ESIGN-LA.com*

Las actualizaciones sustituyen cualquier disposición designada o conflictiva de la versión de referencia de la CP. El PMA deberá determinar si los cambios a la CP requieren un cambio en los objetos identificadores de políticas de Certificados de las Políticas de Certificado correspondientes a cada Clase de Certificado.

1.6 Definiciones y Siglas

Para una mejor comprensión de los términos y siglas utilizados en este documento, ver Anexo A, Definiciones y Siglas

2 Responsabilidades de Publicación y Repositorio

2.1 Repositorios

E-Sign y los Asociados son responsables de mantener un repositorio en línea de acceso público, donde se publican los Certificados aprobados por E-Sign, los Asociados o sus RAs, así como la información relativa a la revocación de tales Certificados.

2.2 Publicación de Información de Certificados

E-Sign y los Asociados mantienen un repositorio, publicado en Web, que permite a los Terceros que Confían hacer consultas en línea sobre la revocación y demás información del estado del Certificado. Cualquier excepción a esta regla deberá ser aprobada por el PMA y debe ser documentado en la CPS apropiada. E-Sign y sus Asociados ofrecen a los Terceros que Confían, información sobre cómo encontrar el repositorio adecuado para comprobar el estado del Certificado y, si el protocolo OCSP (Online Certificate Status Protocol) está disponible, la forma como encontrar el servidor OCSP.

E-Sign y los Asociados publican los certificados que emiten en nombre de sus propias CAs y de las CAs en sus subdominios. En caso de la revocación de un Certificado de Suscriptor usuario final, la CA que emitió el Certificado deberá publicar un aviso de tal revocación en el repositorio. Además, E-Sign y los Asociados deberán emitir Listas de Revocación de Certificados (CRLs) y, si están disponibles, proporcionar servicios OCSP para sus propias CAs y las CAs en sus subdominios.

E-Sign y sus Asociados en todo momento deben publicar una versión actualizada de:

- Esta CP de la E-SIGN CA NET
- Su CPS
- Acuerdos de Suscriptor
- Otros acuerdos específicos aplicables

2.3 Tiempo y Frecuencia de Publicación

La información de la CA es publicada prontamente después de que está disponible para la CA. La E-SIGN CA NET ofrece CRLs que muestran la revocación de los Certificados de la CA, y ofrece servicios de verificación de estado a través del Repositorio de E-SIGN y los repositorios de los Asociados.

Las CRLs de Certificados de usuario final deben ser emitidas al menos una vez por día.

Las CRLs de las CA que sólo emiten Certificados de CA se publicarán a lo menos trimestralmente, y también cada vez que un Certificado de CA sea revocado.

Si un Certificado que está en una CRL caduca, puede ser removido de las CRL publicadas con posterioridad a la expiración del Certificado.

2.4 Control de Acceso a Repositorios

E-Sign y sus Asociados no deben utilizar intencionalmente medios técnicos para limitar el acceso a esta CP, a la CPS, a Certificados, información del estado de Certificados o CRLs. E-Sign y sus Asociados podrán, sin embargo, exigir a las personas a aceptar un Acuerdo de Usuario de Confianza o Contrato de uso de la CRL como condición para acceder a los Certificados, la información del estado de Certificados o CRLs. E-Sign y sus Asociados deberán implementar controles para prevenir que personas no autorizadas puedan, puedan agregar, eliminar o modificar contenidos del repositorio.

3 Identificación y Autenticación

3.1 Identificación (Naming)

A menos que se indique lo contrario en esta CP, la CPS pertinente o el contenido de los Certificados digitales, los nombres que aparecen en los Certificados emitidos bajo la E-SIGN CA NET son autenticados.

3.1.1 Tipos de Nombre

Los Certificados de usuario final contienen un Distinguished Name (DN) X.501 en el campo nombre del Asunto (Subject).
El DN del Subject de los Certificados de Suscriptor de Usuario Final incluye un componente denominado Nombre Común (CN =).
El valor autenticado del nombre común incluido en el DN del Asunto de los Certificados de organización debe ser un nombre de dominio, dirección e-mail de la organización, el nombre legal de la organización dentro de la organización, o el nombre del representante de la organización autorizado para utilizar el llave privada de la organización.
El componente (O=) debe ser el nombre legal de la organización.
El valor del nombre común incluido en el DN del Asunto de los Certificados individuales representará el nombre generalmente aceptado de la persona.
Los nombres comunes deben estar debidamente autenticados en el caso de Certificados de Class 2-3.
Los Certificados E-SIGN CA NET también pueden contener una referencia al Acuerdo de Partes Confiadas en sus DNs.

3.1.2 Necesidad de que los Nombres sean Significativos

Los Certificados de Suscriptor Usuario Final de Class 2-3 deberán incluir nombres significativos, en el sentido siguiente: En Certificados de Class 2 y 3 de Suscriptor Usuario Final el Suscriptor deberá contener los nombres con la semántica comúnmente entendible, permitiendo la determinación de la identidad de la persona u organización del Certificado.

3.1.3 Anonimato o Seudónimos de Suscriptores

La identidad de los Suscriptores individuales Class 1 no se ha autenticado, por lo que los Suscriptores de Certificados Class 1 pueden usar seudónimos (nombres distintos al verdadero nombre personal o de organización de un Suscriptor). Los Suscriptores de Certificados Class 2 y 3 no están autorizados a utilizar seudónimos.

Cuando sea requerido por ley o solicitado por una autoridad del Estado o de Gobierno para proteger la identidad de ciertos Suscriptores del usuario final (por ejemplo, los menores de edad, o información confidencial de empleados del gobierno), un Certificado puede ser emitido indicando que la identidad ha sido autenticada, pero está protegida. Cada solicitud de anonimato en un Certificado serán evaluados por sus méritos por el PMA.

3.1.4 Reglas para Interpretar Formas Variadas de Nombres

No se estipulan reglas específicas

3.1.5 Unicidad de los Nombres

Los nombres de los Suscriptores (DN) dentro de la E-SIGN CA NET serán únicos dentro de un Sub-dominio de Asociados y clientes para una clase específica de Certificado. Es posible para un Suscriptor tener dos o más Certificados, emitidos por CA distintas, con el mismo nombre distinguido del sujeto.

3.1.6 Reconocimiento, Autenticación, y Rol de Marcas Registradas

Los solicitantes de Certificados no podrán utilizar en su solicitud de Certificado nombres que infrinjan los derechos de propiedad intelectual de otros. Ni E-Sign ni el Asociado estarán obligados a determinar si un Solicitante de Certificado tiene derechos de propiedad intelectual en el nombre que aparece en una Solicitud de Certificado, ni a mediar respecto de cualquier controversia relativa a la propiedad de cualquier nombre de dominio, nombres comerciales, marcas, o marca de servicio. E-Sign y el Asociado respectivo no tendrá derecho alguno de rechazar o suspender cualquier Solicitud de Certificado, debido a ese conflicto, a menos que haya una decisión de una autoridad competente sobre la materia.

3.2 Validación Inicial de Identidad

3.2.1 Método Probatorio de la Posesión de Llave Privada

El solicitante del Certificado debe demostrar que legítimamente posee la llave privada correspondiente a la llave pública que se incluye en el Certificado.
El método para probar la posesión de una llave privada es PKCS # 10, otra demostración criptográficamente equivalente, u otro método aprobado por E-Sign. Este requisito no se aplica cuando un par de llaves es generado por una CA en nombre de un Suscriptor, por ejemplo, cuando las llaves pre-generadas se colocan en tarjetas inteligentes o dispositivos criptográficos seguros.

3.2.2 Autenticación de la Identidad de la Organización

Cada vez que un Certificado contenga el nombre de la organización, la identidad de la organización e información de inscripción proporcionados por los solicitantes de Certificados (a excepción de la información del Suscriptor no verificada) se confirma de acuerdo con los procedimientos establecidos en los Procedimientos de Validación documentados por E-Sign.
Como mínimo, E-Sign o Asociado deberá:

- determinar que existe la organización mediante el uso de al menos una tercera parte proveedora de servicios de pruebas o base de datos, o, alternativamente, la documentación de la organización emitida por o inscrita en el organismo de gobierno o autoridad reconocida competentes y que confirme la existencia de la organización,
- confirmar por teléfono, correo de confirmación, o un procedimiento comparable al Solicitante del Certificado la información de la organización, que la organización ha autorizado la Solicitud de Certificado, y que la persona que presenta la Solicitud de Certificado en nombre del Solicitante de Certificado está autorizado para hacerlo. Cuando un Certificado incluye el nombre de una persona como representante autorizado de la Organización, la calidad de empleado de esa persona y su autoridad para actuar en nombre de la Organización, también debe ser confirmada.

Cada vez que un nombre de dominio o dirección de correo electrónico esté incluido en el Certificado, E-Sign o el Asociado autenticarán el derecho de la Organización para usar ese nombre de dominio, ya sea como un nombre de dominio completo o de correo electrónico.

3.2.3 Autenticación de Identidad Individual

Los procedimientos de autenticación de identidad individual difieren de acuerdo a la Clase de Certificado. El estándar de autentificación mínimo para cada clase de Certificado E-SIGN CA NET se explica en la Tabla 3.

Clase de Certificado	Autenticación de Identidad

Class 1	Sin autenticación de identidad. Hay una confirmación limitada de la dirección de correo electrónico del Suscriptor, al exigir que el Suscriptor responda un e-mail a esa dirección.

.....

Class 2	Autenticar la identidad, validando la identidad proporcionada por el Suscriptor de alguna de las siguientes formas: • Información que reside en la base de datos de un servicio de identidad aprobado por E-Sign, tales como bases de datos del Estado, bases de datos de instituciones financieras u otra fuente confiable de información en el país o territorio en el que se emite el Certificado, • información generada por E-Sign • información contenida en los registros de negocios o en bases de datos de información comercial (directorios de empleados o clientes) de una RA que aprueba Certificados a sus propios Asociados individuales • información obtenida presencialmente del Suscriptor a través de un canal autorizado por E-Sign • información obtenida desde dispositivos seguros que utilicen medios biométricos • información proporcionada por entidades públicas
Class 3	La autenticación de los Certificados Individuales de Class 3 se basan en la presencia personal (física) del Solicitante del Certificado ante un agente de la CA o RA, o ante un notario público u otros oficiales con autoridad comparable en la jurisdicción del Solicitante del Certificado. El agente, notario u otro funcionario comprobará la identidad del Solicitante del Certificado contra una forma conocida de identificación oficial fotográfica, como pasaporte o licencia de conducir y otra credencial de identificación. Los Certificados de Class 3 de administrador también deberán incluir la autenticación de la organización y una confirmación por parte de la organización de la identidad de la persona para que actúe como administrador. E-Sign y sus Asociados también pueden tener la ocasión de aprobar las solicitudes de Certificados para sus propios administradores. Los administradores son "personas de confianza" dentro de una organización. En este caso, la autenticación de las Suscripciones de Certificado se basa en los procedimientos para la confirmación de su identidad en relación con su empleo y la comprobación de antecedentes.

Tabla 3. Autenticación de Identidad Individual

3.2.4 Información No-Verificada del Suscriptor

La Información No-Verificada del Suscriptor incluye:

- Unidad Organizacional (OU)
- Nombre del Suscriptor en Certificados de Class 1
- Cualquier otra información designada como no-verificada en el Certificado

3.2.5 Validación de Autorización

Cada vez que el nombre de una persona se asocia con un nombre de la organización en un Certificado de tal manera de indicar la afiliación de la persona o la autorización para actuar en nombre de la Organización, la CA o RA:

- determina que existe la organización mediante el uso de al menos un tercero proveedor de servicios de identificación probatoria o de base de datos, o, alternativamente, la documentación emitida por la organización o ante la agencia del gobierno o autoridad reconocida que confirma la existencia de la organización, y
- utiliza información contenida en los registros de negocios o de bases de datos de información comercial (directorios de empleados o clientes) de una RA que aprueba Certificados a sus propios individuos, o confirma por teléfono, correo o un procedimiento similar, el vínculo de la persona de la Organización que presenta la Solicitud de Certificado y, en su caso, su autoridad para actuar en nombre de la Organización.

3.2.6 Criterio de Interoperabilidad

La E-SIGN CA NET (Comunidad de Confianza de E-Sign) puede proporcionar servicios de interoperabilidad que permitan a una CA no E-SIGN CA NET poder interactuar con la red E-SIGN CA NET certificando la CA en forma unilateral. Las CAs capacitadas para interoperar de esta forma cumplen con esta CP, complementado por políticas adicionales cuando sea necesario.
E-Sign sólo permitirá la interoperabilidad con la red E-SIGN CA NET de una CA fuera de la E-SIGN CA NET cuando se cumplan los siguientes requisitos:

- Tener un acuerdo contractual con E-Sign o un Asociado
- Operar bajo una CPS que cumpla con los requisitos de E-SIGN CA NET para las clases de Certificados que emitirá
- Pasar por una evaluación de cumplimiento antes de poder interoperar
- Pasar por una evaluación anual de cumplimiento de operación continua para interoperar.

3.3 Identificación y Autenticación en caso de Requerimientos de Cambio de Llaves

Antes de la expiración de un Certificado de Suscriptor existente, es necesario que el Suscriptor obtenga un nuevo Certificado para mantener la continuidad de uso del Certificado. Las CAs y RAs generalmente requieren que el Suscriptor generar un nuevo par de llaves de tal forma de sustituir el par de llaves que expira (procedimiento definido técnicamente como "cambio de llaves"). Sin embargo, en algunos casos (es decir, para los Certificados de servidor Web) los Suscriptores podrán solicitar un nuevo Certificado para un par de llaves existente (procedimiento definido técnicamente como "renovación").

En términos generales, tanto el "Cambio de Llaves" como la "Renovación" se describen habitualmente como "Renovación de Certificados", destacando el hecho de que el antiguo Certificado está siendo sustituido por un nuevo Certificado y no enfatizando si se trata o no de la generación de un nuevo par de Llaves.

Para todas las clases y tipos de Certificados de E-Sign, a excepción de los Certificados Clase 3 de Servidor, esta distinción no es importante dado que siempre un nuevo par de llaves es generado como parte del proceso de reemplazo del Certificado de usuario final de E-Sign. Sin embargo, para los Certificados Clase 3 de Servidor, debido a que el par de llaves del Suscriptor es generado

en el servidor web y la mayoría de servidores web tienen herramientas de generación de llaves que permiten la creación de una nueva solicitud de Certificado para un par de llaves existente, existe una distinción entre "Cambio de Llaves" y "Renovación".

3.3.1 Identificación y Autenticación para Cambio Rutinario de Llave

La entidad que aprueba una Solicitud de Certificado para el Suscriptor de un Certificado de Suscriptor de Usuario Final será responsable de la autenticación de la solicitud de cambio de llaves o renovación. Los procedimientos de cambio de llaves aseguran que la persona u organización que desea renovar / cambiar llaves del Certificado del Suscriptor de Usuario Final es, de hecho, el Suscriptor del Certificado.
Un procedimiento aceptable es mediante el uso de una Frase Secreta (o su equivalente), o la prueba de la posesión de la llave privada. Los Suscriptores eligen y presentan junto con su información de enrolamiento una Frase Secreta; al momento de renovación de un Certificado, si un Suscriptor ingresa acertadamente la Frase Secreta (o su equivalente), con la información de enrolamiento del Suscriptor (incluyendo la información del contacto) y la información no ha cambiado, el Certificado es renovado automáticamente.
Después de cambiar llaves o renovar de esta manera, y al menos en instancias alternativas de cambios de llaves o renovaciones posteriores a partir de entonces, la CA o RA re-confirma la identidad del Suscriptor de acuerdo con los requisitos de identificación y autenticación de una Solicitud de Certificado original.

3.3.2 Identificación y Autenticación para cambio de Llaves Después de Revocación

El Cambio de Llaves/Renovación después de la revocación, no está permitida si la revocación se produjo debido a que:

- el Certificado (que no sea un Certificado de Class 1) fue emitido a una persona distinta de la que se identifica en el Asunto del Certificado, o
- el Certificado (que no sea un Certificado de Class 1) fue publicado sin la autorización de la persona o entidad nombrada como el Asunto de dicho Certificado, o
- la entidad que aprueba la Solicitud del Certificado del Suscriptor descubre o tiene razones para creer que un hecho material en la Solicitud de Certificado es falso
- el Certificado se considera perjudicial para la E-SIGN CA NET.
- Existe compromiso de la llave privada.

En relación al párrafo anterior, la renovación de un Certificado de Organización o Certificado de CA que siga a una revocación del Certificado es permitido en la medida que los procedimientos de renovación aseguren que la Organización o CA que requiere la renovación sea de hecho el Solicitante del Certificado.
Los Certificados de organización renovados deberán contener igual DN del Asunto que el DN del Asunto del Certificado de Organización que está siendo renovado.

La renovación de un Certificado Individual luego de su revocación debe asegurar que la persona que solicita la renovación es de hecho, el Suscriptor.
Un procedimiento aceptable es el uso de una Frase Secreta (o su equivalente). Con excepción de este procedimiento u otro procedimiento aprobado por E-Sign, para la identificación y autenticación de una renovación de un Certificado luego de su revocación deben ser utilizados los mismos requisitos utilizados en la identificación y autenticación de la Solicitud de Certificado original.

3.4 *Identificación y Autentificación Para la Solicitud de Revocación*

Los procedimientos de revocación garantizan previo a cualquier revocación de cualquier Certificado que la revocación de hecho, haya sido solicitada por el Suscriptor del Certificado, la entidad que aprobó la emisión del Certificado, o E-Sign y sus Asociados.

Los procedimientos aceptables para la autenticación de las Solicitudes de Revocación de un Suscriptor incluyen:

- Que el Suscriptor, para ciertos tipos de Certificados, haya ingresado la Frase Llave del Suscriptor (o su equivalente), y procediendo a revocar el Certificado en forma automática, siempre que coincida con la Frase Secreta (o su equivalente) en el registro
- El haber recibido un mensaje del Suscriptor que solicita la revocación conteniendo una firma digital verificable con referencia al Certificado de que se está revocando,
- La comunicación con el Suscriptor proveyendo garantías razonables a la luz de la clase de Certificado que se revoca, que la persona o entidad solicitante, sea de hecho el Suscriptor. Esta comunicación, dependiendo de las circunstancias, puede incluir uno o más de los siguientes datos: teléfono, fax, e-mail, correo postal o servicio de mensajería.

Los administradores de CA/RA tienen derecho a solicitar la revocación de Certificados de Suscriptor de usuario final dentro del Sub Dominio Sub de la CA/RA. E-Sign y Asociados autentican la identidad de los Administradores a través de control de acceso usando SSL y autenticación del cliente antes de permitirles realizar funciones de revocación u otro procedimiento aprobado por la E-SIGN CA NET.

Las RAs que utilicen un módulo de software de administración automatizada podrán presentar solicitudes de revocación por lotes a la E-SIGN CA NET. Dichas solicitudes deberán ser autenticadas a través de una petición firmada digitalmente y firmada con la llave privada en el token de hardware de administración automatizada de la RA.

Las solicitudes para revocar un Certificado de CA deberá estar autenticada por la entidad Superior para asegurar que la revocación de hecho, ha sido solicitada por la CA.

4 Requerimientos Operacionales del Ciclo de Vida de los Certificados

4.1 Solicitud de Certificado

4.1.1 Quien puede enviar una Solicitud de Certificado

A continuación se muestra una lista de personas que pueden presentar solicitudes de Certificado:

- Cualquier persona que sea el asunto del Certificado,
- Cualquier representante de una organización o entidad,
- Cualquier representante autorizado de una CA,
- Cualquier representante autorizado de una RA.

4.1.2 Proceso y responsabilidades del Enrolamiento

4.1.2.1 Suscriptores de Certificado de Usuario Final

Todos los Suscriptores de Certificados de usuario final deben manifestar explícita o tácitamente su consentimiento con el Acuerdo de Suscripción que contiene las declaraciones y garantías descritas en la Sección 9.6.3 y se someten a un proceso de enrolamiento, que considera las siguientes obligaciones:

- completar la Solicitud de Certificado y aportar información veraz y correcta,
- generar, o aceptar la generación, del par de llaves
- entregar su, o sus llaves públicas, directamente o a través de la RA, a E-Sign o sus Asociados,
- demostrar la posesión y / o el control exclusivo de la llave privada, físicamente o por medios lógicos, correspondiente a la llave pública entregada a E-Sign y sus Asociados.

4.1.2.2 Certificados de CA y RA

Los Suscriptores de Certificados de CA y RA celebran un contrato con E-Sign o sus Asociados. Los Solicitantes de la CA y RA deben proporcionar sus credenciales para demostrar su identidad y proporcionar información de contacto durante el proceso de contratación. Durante este proceso de contratación o, a más tardar antes de la Ceremonia de Generación de Llaves para crear un par de llaves de CA o RA, el solicitante debe proporcionar a E-Sign o sus Asociados los elementos para determinar el nombre completo y adecuado del contenido de los Certificados que deban otorgarse al solicitante.

4.2 Procesamiento de la Solicitud de Certificado

4.2.1 Funciones de Identificación y Autenticación

Una RA debe realizar la identificación y autenticación de información de los Suscriptores según lo indicado en la sección 3.2.

4.2.2 Aprobación o Rechazo de Solicitudes de Certificado

Una RA aprobará una solicitud de Certificado si se cumplen los siguientes criterios:

- Identificación y autenticación exitosa de la información del Suscriptor que se requiere en términos de la sección 3.2
- Que el pago haya sido recibido (si procede)

Una RA rechazará una solicitud de Certificado si:

- la identificación y autenticación de toda la información del Suscriptor que se requiere en términos de la Sección3.2 no se puede completar o
- el Suscriptor no presenta la documentación de apoyo,
- el Suscriptor no responde a los avisos en un plazo determinado
- el pago (si aplica) no ha sido recibido,
- la RA cree que la emisión de un Certificado al Suscriptor puede acarrear descredito a la E-SIGN CA NET

4.2.3 Tiempo para procesar las Solicitudes de Certificado

Las CAs y RAs comienzan la tramitación de Solicitudes de Certificado en un plazo razonable luego de la recepción de dichas solicitudes. No existe ninguna estipulación de tiempo para completar la tramitación de una solicitud, a menos que se indique lo contrario en el acuerdo de suscriptor pertinente, CPS u otro acuerdo entre los participantes de la E-SIGN CA NET.
La Solicitud del Certificado se mantiene activa hasta que es rechazada, o transcurra un plazo razonable sin que el solicitante envíe los antecedentes necesarios para su aprobación.

4.3 Entrega de Certificados

4.3.1 Acciones de la CA durante la Entrega de Certificados

El Certificado es creado y entregado luego de la aprobación de la Solicitud de Certificado por la CA, o bien, luego de la recepción de un requerimiento de la RA, para que se emita el Certificado. La CA crea y envía al Solicitante, o a la persona o entidad que éste haya indicado, su Certificado emitido basándose en la información contenida en la Solicitud de Certificado luego de la aprobación de tal Solicitud.

4.3.2 Notificación de entrega del Certificado al Suscriptor por parte de la CA

Las CA emisoras de Certificados a los Suscriptores, ya sea directamente o a través de un RA, notificarán a los Suscriptores, que se han creado los Certificados, y ofrecerán a los Suscriptores el acceso a estos, notificándoles que sus Certificados están disponibles y los medios para su obtención. Los Certificados deberán estar disponibles para los Suscriptores, ya sea permitiéndoles descargarlos desde un sitio web, a través de un mensaje conteniendo el Certificado o a través de la entrega de los medios físicos en los cuales se el certificado. Los certificados pueden ser descargados en forma individual en dispositivos individuales, o de manera centralizada y segura.

4.4 Aceptación del Certificado

4.4.1 Conducta Constitutiva de la Aceptación del Certificado

Son conductas constitutivas de aceptación del Certificado, y del respectivo acuerdo de suscriptor:

- Descargar, instalar o usar el Certificado.
- No oponerse expresamente al Certificado o a su contenido.

4.4.2 Publicación del Certificado por parte de la CA

E-Sign o su Asociado respectivo publica los Certificados emitidos en un repositorio de acceso público.

4.4.3 Notificación de la emisión del Certificado por la CA a otras entidades

Las RAs pueden recibir la notificación de la emisión de Certificados que han aprobado.

4.5 Uso del Par de Llaves y del Certificado

4.5.1 Uso de la Llave Privada y del Certificado por el Suscriptor

El uso de la llave privada correspondiente a la llave pública del Certificado sólo será permitido una vez que el Suscriptor ha aceptado el Acuerdo de Suscriptor y aceptado el Certificado. El Certificado deberá ser utilizado legalmente en conformidad con el Acuerdo del Suscriptor de E-Sign, los términos de esta CP y la CPS correspondientes. El uso de Certificados debe ser consistente con la extensión del campo *KeyUsage*, incluido en el Certificado (por ejemplo, si la firma digital no está habilitada, el Certificado no debe ser utilizado para la firma).
Los Suscriptores deben proteger sus llaves privadas de uso no autorizado y se debe dejar de utilizar luego de la expiración o revocación del Certificado.

4.5.2 Uso de Certificado y la Llave Pública por parte del Tercero que Confía

Los Terceros que Confían podrán revisar los términos de uso del Certificado, revisando las CPS específicas indicadas en el contenido del Certificado mismo, y el Acuerdo de Tercera Parte que Confía.

La confianza en un Certificado debe ser razonable bajo las circunstancias. Si las circunstancias indican la necesidad de garantías adicionales, los Terceros que Confían debe obtener tales garantías para que tal confianza se considere razonable.

Antes de realizar cualquier acto de confianza, las partes que confían evaluarán de forma independiente:

- la conveniencia de la utilización de un Certificado para cualquier propósito determinado y determinar que el Certificado, de hecho, ser utilizará para un propósito adecuado que no esté prohibido o restringido por la CP. E-Sign, CA y RA no son responsables de evaluar la conveniencia de la utilización de un Certificado.
- Que el Certificado este siendo utilizado de acuerdo con las extensiones del campo *KeyUsage* incluido en el Certificado (por ejemplo, si la firma digital no está habilitada, el Certificado no puede ser invocado para validar la firma de un Suscriptor).
- El estado del Certificado y todas las CAs en la cadena del el Certificado. Si alguno de los Certificados en la Cadena de Certificados ha sido revocado, los Terceros que Confían son los únicos responsables de investigar si la dependencia de una firma digital realizada por un Certificado de Suscriptor antes de la revocación de un Certificado en la cadena de Certificados es razonable. Dicha dependencia se realiza únicamente a riesgo de los Terceros que Confían.

Suponiendo que el uso del Certificado es apropiado, las partes que confían utilizarán el software y/o hardware apropiado para realizar la verificación de firma digital u otras operaciones criptográficas que deseen realizar, como condición para confiar en Certificados que tengan relación con cada operación de este tipo. Dichas operaciones incluyen la identificación de la

Cadena de Certificados y la verificación de las firmas digitales en todos los Certificados de la Cadena de Certificados.

4.6 Renovación del Certificado

La renovación del Certificado es la emisión de un nuevo Certificado al Suscriptor sin tener que cambiar la llave pública o cualquier otra información en el Certificado. La Renovación del Certificado esta soportada para Certificados de Class 3, donde se genera el par de llaves en un servidor web.

4.6.1 Circunstancias para la Renovación de Certificados

Antes de la expiración de un Certificado de Suscriptor, es necesario que éste haga su renovación de tal forma de mantener la continuidad del uso del Certificado. Un Certificado puede ser renovado después de su expiración.

4.6.2 Quién puede solicitar la Renovación

Sólo el Suscriptor de un Certificado individual o un representante autorizado de una organización puede solicitar la renovación de Certificados

4.6.3 Procesamiento de Solicitudes de Renovación de Certificados

Los procedimientos de renovación aseguran que la persona u organización que persigue la renovación del Certificado sea de hecho sea el Suscriptor del Certificado o la persona autorizada por el Suscriptor.

Un procedimiento aceptable es el uso de una Frase Secreta (o su equivalente), o la prueba de posesión de la llave privada.

Los Suscriptores eligen y envían junto con su información de enrolamiento una Frase Secreta (o su equivalente). En el momento de la renovación de un Certificado, si el Suscriptor envía acertadamente la Frase Secreta (o su equivalente) con información de reinscripción del Suscriptor, y la información de enrolamiento (incluyendo la información del contacto) no ha cambiado, el Certificado renovado se emite automáticamente. Luego de ser renovado el certificado, o al menos luego de la renovación posterior, la CA o RA confirmará la identidad del Suscriptor de acuerdo con los requisitos especificados en la presente CP para la autenticación de una Solicitud de Certificado original.

Aparte de este procedimiento u otro procedimiento aprobado por E-Sign, los requerimientos para la autenticación de una Solicitud de Certificado original se deben utilizar para la renovación de un Certificado de Suscriptor de usuario final.

4.6.4 Notificación de la Emisión de nuevos Certificados de Suscriptor

La notificación de expedición de la Renovación del Certificado al Suscriptor se realiza de acuerdo a lo indicado en la Sección 4.3.2

4.6.5 Conducta Constitutiva de la Aceptación de la Renovación de un Certificado

La conducta que constituye la Aceptación de la renovación de un Certificado se señala en la Sección 4.4.1

4.6.6 Publicación de la Renovación del Certificado por la CA

El Certificado renovado se publica en un repositorio de acceso público de E-Sign o el Asociado que lo emite.

4.6.7 Notificación de Emisión del Certificado de la CA a otras entidades

Las RAs podrán recibir la notificación de la emisión de los Certificados que aprueben.

4.7 Cambio de Llaves de un Certificado

El cambio de llaves de un Certificado es la solicitud para la emisión de un nuevo Certificado que acredita la nueva llave pública. El cambio de llaves del Certificado es válido para todas las clases de Certificados.

4.7.1 Circunstancias para el Cambio de Llaves de un Certificado

Antes de la expiración de un Certificado de Suscriptor, es necesario que el Suscriptor cambie las llaves del certificado de tal forma de mantener la continuidad de uso del Certificado.

4.7.2 Quién puede Solicitar la Certificación de una nueva Llave Pública

Sólo el Suscriptor de un Certificado individual o un representante autorizado de un Certificado de la Organización puede solicitar la renovación de Certificados

4.7.3 Procesamiento de Requerimientos de Cambio de Llaves del Certificado

Los procedimientos para cambio de llaves aseguran que la persona u organización que solicita la renovación de un Certificado de Suscriptor sea de hecho el suscriptor (o el autorizado por el suscriptor) del Certificado.

Un procedimiento aceptable es a través del uso de una Frase Secreta (o su equivalente), o la prueba de la posesión de la llave privada. Los Suscriptores eligen y envían junto con su información de enrolamiento una Frase Secreta (o su equivalente). En el momento de la renovación de un Certificado, si el Suscriptor envía acertadamente la Frase Secreta (o su equivalente) con información de reinscripción del Suscriptor, y la información de enrolamiento (incluyendo la información del contacto) no ha cambiado, el Certificado de renovación se emite automáticamente. Luego de dos cambios de llaves, la CA o RA confirmará la identidad del Suscriptor de acuerdo con los requisitos especificados en la presente CP para la autenticación de una Solicitud de Certificado original.

Aparte de este procedimiento u otro procedimiento aprobado por E-Sign, requerimientos para la autenticación de una Solicitud de Certificado original se deben utilizar para el cambio de llaves de un Certificado de Suscriptor de usuario final.

4.7.4 Notificación de la emisión de nuevos Certificados de Suscriptor

La notificación al Suscriptor de la emisión de un Certificado con cambio de llaves se hace de acuerdo con la Sección 4.3.2

4.7.5 Conducta Constitutiva de la Aceptación de un Certificado con Cambio de Llaves

La Conducta constitutiva de la Aceptación de un Certificado con cambio de llaves se señala en la Sección 4.4.1

4.7.6 Publicación del Certificado con cambio de Llaves por la CA

El Certificado con cambio de Llaves se publica en el repositorio de acceso público de E-Sign o el Asociado que lo ha emitido.

4.7.7 Notificación de Emisión del Certificado de la CA a otras entidades

Las RA pueden recibir la notificación de la emisión de Certificados que aprueban.

4.8 Modificación de Certificado

4.8.1 Circunstancias para la Modificación de Certificados

Modificación de Certificado se refiere a la solicitud de la emisión de un nuevo Certificado debido a los cambios en la información contenida en el Certificado (que no sea la llave pública del Suscriptor).

La Modificación de Certificado se considera como una Solicitud de Certificado en términos de la Sección 4.1.

4.8.2 Quién pueden solicitar la Modificación de Certificados

Ver Sección 4.1.1

4.8.3 Procesamiento de Solicitudes de Modificación de Certificados

Una RA realizará la identificación y autenticación de toda la información requerida del Suscriptor en términos de la sección 3.2

4.8.4 Notificación de la emisión de nuevos Certificados de Suscriptor

Ver Sección 4.3.2

4.8.5 Conducta Constitutiva de Aceptación de la Modificación del Certificado

Ver Sección 4.4.1

4.8.6 Publicación del Certificado Modificado por la CA

Ver Sección 4.4.2

4.8.7 Notificación de emisión del Certificado de la CA a otras entidades

Ver Sección 4.4.3

4.9 Revocación y Suspensión de Certificado

4.9.1 Circunstancias para la Revocación

Sólo en las circunstancias enumeradas a continuación un Certificado de Suscriptor puede ser revocado y publicado en una CRL. A solicitud de un Suscriptor que ya no pueda usar (o no quiera usar) un Certificado por un motivo distinto de los mencionados a continuación, E-Sign marcará el Certificado como inactivo en su base de datos, sin embargo no publicará el Certificado en una CRL.

Un Certificado de Suscriptor es revocado si:

- E-Sign, un Asociado, un Cliente Empresa, o un Suscriptor tiene razones para creer o tiene fundadas sospechas de que ha habido un compromiso de la llave privada, de un Suscriptor,
- E-Sign, un Asociado, un Cliente Empresa tiene motivos para creer que el Suscriptor ha incumplido materialmente una obligación material, declaración o garantía de acuerdo al Acuerdo de Suscripción vigente,
- El Acuerdo de Suscriptor con el Suscriptor ha terminado,
- La relación entre un Cliente Empresa con un Suscriptor se termina o simplemente finaliza de otra forma,
- La asociación entre una organización, que es un Suscriptor de un Certificado Organizacional de Class 3 y el representante de la organización que tiene el control de la llave privada del Suscriptor se termina o simplemente finaliza de otra forma,
- E-Sign, un Asociado, un Cliente Empresa tiene motivos para creer que el Certificado fue emitido de manera que no está de acuerdo con los procedimientos requeridos por la CPS, el Certificado (que no sea un Certificado de Class 1) fue emitido a una persona que no sea el que es Asunto del Certificado o el (que no sean Certificado de Class 1) se emitió sin la autorización de la persona que es Asunto de dicho Certificado,
- E-Sign, un Asociado, un Cliente Empresa tiene motivos para creer que un hecho material en la Solicitud del Certificado es falso,
- E-Sign, un Asociado, un Cliente Empresa determina que un prerrequisito material para la emisión del Certificado no estaba satisfecho,
- En el caso en que en Certificados de Organización de Class 3, el nombre del suscriptor cambia,
- La información contenida en el Certificado, excepto la información no verificada del Suscriptor, es incorrecta o ha cambiado,

- La identidad del Suscriptor, no se ha logrado re-verificar de acuerdo con lo establecido en la sección 6.3.2,
- El Suscriptor no ha presentado el pago a su vencimiento, o
- El uso continuado de este Certificado es perjudicial para la E-SIGN CA NET.

Se considera que el uso del Certificado es perjudicial para, la E-SIGN CA NET, entre otras cosas, lo siguiente:

- La naturaleza y el número de quejas recibidas
- La identidad del denunciante (s)
- La legislación vigente en la materia
- Las respuestas a la presunta utilización perjudicial del Suscriptor

Al considerar si el uso de un Certificado de firma de código es perjudicial para la E-SIGN CA NET, además, considera entre otras cosas, lo siguiente:

- El nombre del código que se está firmando
- El comportamiento del código
- Métodos de distribución del código
- Revelaciones hechas a los destinatarios del código
- Cualquier alegato adicional sobre el código

E-Sign también puede revocar un Certificado de Administrador si la autoridad que actúa como Administrador se ha terminado.

E-Sign, un Asociado o un Cliente Empresa puede revocar un Certificado de Administrador si la autoridad que actúa como Administrador se ha terminado.

Los Acuerdos de Suscriptor requieren que los usuarios finales notifiquen inmediatamente a E-Sign, un Asociado o un Cliente Empresa si sabe o sospecha de un compromiso de su llave privada.

4.9.2 Quién puede Solicitar la Revocación

Suscriptores Individuales pueden solicitar la Revocación de sus propios Certificados Individuales. En el caso de los Certificados Organizacionales, un representante debidamente autorizado de la organización tendrá derecho a solicitar la revocación de los Certificados emitidos a la organización. Un representante debidamente autorizado de E-Sign, un Asociado o una RA tendrá derecho a solicitar la revocación de un Certificado de Administrador de la RA. La entidad que aprobó la solicitud de un Suscriptor de Certificados también tendrá derecho a revocar o solicitar la revocación del Certificado del Suscriptor.

Sólo E-Sign tiene derecho a solicitar o iniciar la revocación de los Certificados expedidos a sus propias entidades emisoras.

Las RAs tienen derecho, a través de sus representantes debidamente autorizados, a solicitar la revocación de sus propios Certificados, y sus entidades superiores tendrán derecho a solicitar o iniciar la revocación de sus Certificados.

4.9.3 Procedimiento para la Solicitud de Revocación

Antes de la revocación de un Certificado, la CA verifica que la revocación haya sido solicitada por el Suscriptor del Certificado, o la entidad que aprobó la Solicitud de Certificado. Los procedimientos aceptables para la autenticación de las solicitudes de revocación del Suscriptor incluyen:

- El Suscriptor, tiene que, para ciertos tipos de Certificados enviar la Frase Secreta del Suscriptor (o su equivalente) y la revocación del Certificado se materializa en forma automática, sólo si coincide con la Frase Secreta (o su equivalente) en el registro,
- Habiendo recibido un mensaje del Suscriptor que solicita la revocación y contiene una firma digital verificable con referencia al Certificado que se desea revocar, y la comunicación con el Suscriptor proporciona garantías razonables a la luz de la clase de Certificado que la persona o la organización que solicita la revocación es, de hecho, el Suscriptor. Dependiendo de las circunstancias, dicha comunicación puede incluir uno o más de los siguientes datos: teléfono, fax, e-mail, correo postal o servicio de mensajería.

Los Administradores de CA/RA tienen derecho a solicitar la revocación de los Certificados de Suscriptor dentro del Subdominio de la CA/RA. E-Sign y los Asociados deben autenticar la identidad de los administradores a través de control de acceso utilizando SSL y la autenticación cliente antes de permitirles realizar funciones de revocación.

RAs utilizando el Módulo de Administración de Software Automatizado podrán presentar solicitudes de revocación masivas a E-Sign. Dichas solicitudes se autentican a través de una petición firmada digitalmente con la llave privada del token del Administrador.

Las solicitudes de CAs para revocar un Certificado de CA deben estar autenticadas por las entidades superiores para asegurarse de que la revocación de hecho, ha sido solicitada por la CA.

4.9.4 Período de Gracia para la Solicitud de Revocación

Las solicitudes de revocación se deben presentar tan pronto como sea posible dentro de un plazo comercialmente razonable.

4.9.5 El plazo en el que la CA debe procesar la Solicitud de Revocación

Pasos comercialmente razonables de tramitación de solicitudes de revocación son adoptados para no provocar demoras.

4.9.6 Requisitos de Comprobación de Revocación para Partes que Confían

Las Partes que Confían deberán comprobar el status de los Certificados en los cuales desean confiar. Un método a través cual las Partes que Confían pueden comprobar el estado del Certificado es consultando la CRL más reciente de la CA que emitió el Certificado. Alternativamente, las partes que confían pueden cumplir con este requisito, ya sea comprobando el estado de Certificado a través de una consulta en la web del repositorio o mediante el uso de OCSP (si está disponible).

Las CAs deben proporcionar a las Partes que Confían, información sobre cómo encontrar la CRL, repositorio basado en web o servidor OCSP (donde esté disponible) correspondientes para comprobar el estado de revocación.

- Para las E-SIGN CA NET PCAs y Autoridades Certificadoras de Class 3, las CRL se publican en el repositorio E-SIGN, en *http://crl.E-SIGN.com*
- Para CAs Clientes (Asociados), las CRL se publican en repositorios específicos del cliente, cuya ubicación se comunica a los clientes PKI.

Una "tabla de referencia de CRL" también se publica en el repositorio de E-SIGN para permitir a las partes que confían determinar la ubicación de la CRL de la CA correspondiente.

4.9.7 Frecuencia de Emisión de CRL

Las CRL para Certificados de Suscriptor de usuario final se emiten por lo menos una vez al día. Las CRL para los Certificados de CA se publicará por lo menos una vez al año, y también cada vez que un Certificado de CA se revoca. Las CRL para CA raíces para firma de contenido autentificado (Authenticated Content Signing, ACS) son publicadas anualmente y también cada vez que un certificado de CA es revocado.

Si un Certificado que figura en una CRL caduca, puede ser removido posteriormente de la CRL emitida después de la expiración del Certificado.

Cualquier desviación de esta política general debe obtener la aprobación del PMA y se publicará en el CPS apropiada.

4.9.8 Latencia Máxima de las CRLs

La CRL se publica en el repositorio de E-SIGN dentro de un plazo comercialmente razonable después de la generación. Esto se hace automáticamente en pocos minutos después de la generación.

4.9.9 Disponibilidad de Comprobación de Revocación / Estado en Línea

La información en línea de revocación y otra de estado del Certificado está disponible a través de un repositorio en la Web y, OCSP cuando es ofrecido. Los Asociados tendrán un repositorio basado en web que permite a las Partes que Confían poder hacer consultas en línea sobre la revocación y demás información del estado del Certificado.

4.9.10 Requerimientos para Comprobación de la Revocación en Línea

Una Parte que Confía, debe verificar el estado de un Certificado en el que desea confiar. Si una Parte que Confía no comprueba el estado de un Certificado en el que desea confiar consultando la CRL pertinente más reciente, deberá comprobar el estado del Certificado mediante la consulta en el repositorio respectivo o mediante la solicitud de Status del Certificado usando el respondedor OCSP que corresponda (donde los servicios de OCSP está disponibles).

4.9.11 Otras formas de Publicación de Revocación Disponibles

No aplica.

4.9.12 Requerimientos Especiales para Llaves Comprometidas

Los participantes de E-SIGN CA NET serán notificados cuando exista o se sospeche de compromiso en llaves privadas de la CA, utilizando esfuerzos comercialmente razonables.

Los Asociados deben hacer todos los esfuerzos comerciales razonables para notificar a las partes que confíen si se descubre o tiene razones para creer que ha habido un compromiso de la llave privada de una de sus propias Autoridades Certificadoras o de una de las Autoridades Certificadoras dentro de sus sub-dominios.

4.9.13 Circunstancias para la Suspensión

No aplica.

4.9.14 Quién puede solicitar la Suspensión

No aplica.

4.9.15 Procedimiento para la solicitud de suspensión

No aplica.

4.9.16 Límites del período de suspensión

No aplica.

4.10 Servicios de Estado de Certificados

4.10.1 Características Operacionales

El Estado de los Certificados públicos está disponible en CRL vía un sitio web de E-Sign o un Asociado (en una URL especifica contenida en la C PS), el directorio LDAP y a través de un servicio OCSP (donde esté disponible).

4.10.2 Disponibilidad del Servicio

E-Sign hará los mayores esfuerzos para que los Servicios de Estado de Certificados estén siempre disponibles, salvo interrupciones programadas.

4.10.3 Características Opcionales

OCSP es una función de estado de servicio opcional que no está disponible para todos los productos y debe estar específicamente habilitado para otros productos

4.11 Termino de la vigencia de un Certificado

Un Suscriptor poner término a la vigencia de un Certificado de E-SIGN CA NET:

- Permitiendo que su Certificado expire sin renovación o cambio de llaves del mismo
- Revocando el Certificado antes de su expiración sin solicitar su reemplazo

4.12 Custodia y Recuperación de Llaves

Las CA participantes bajo la E-SIGN CA NET que deseen custodiar llaves privadas de Suscriptor de usuario final, deben adoptar todos los resguardos necesarios para que el respectivo Suscriptor mantenga el control de dichas llaves, al menos por medios lógicos.

Los Clientes que utilizan un Servicio de Administración de llaves aprobado por E-Sign pueden custodiar las llaves privadas de Suscriptores cuyas Solicitudes de Certificados hayan sido aprobadas por ellos.

4.12.1 Política y Prácticas de Custodia y Recuperación de Llaves

A los Clientes Empresa mediante el Servicio de Administración de Llaves (o un servicio equivalente aprobado por E-Sign) se les permite custodiar las llaves privadas de los Suscriptores. Las llaves privadas custodiadas se deben almacenar encriptadas, utilizando el software autorizado por E-Sign.

Con excepción de los Clientes Empresa que utilizan el Servicio de Administración de Llaves (o un servicio equivalente aprobado por E-Sign), las llaves privadas de la CA o Suscriptores usuarios finales no podrán ser custodiados.

Las Llaves Privadas de usuario final Suscriptor sólo se podrán recuperar bajo las circunstancias permitidas por éste en el respectivo acuerdo de suscriptor, según el cual:

- Se deberá confirmar la identidad de cualquier persona que se presente como Suscriptor de tal forma de asegurarse que el Suscriptor solicitante de la llave privada del Suscriptor, sea quien dice ser y no sea un impostor.
- Los Clientes Empresa deberán recuperarán la Llave privada del Suscriptor sin la autorización del Suscriptor sólo para propósitos legítimos y legales, como por ejemplo cumplir con un procedimiento judicial o administrativo o una orden de registro, y no para fines ilícitos ilegales, fraudulentos, o de otro tipo, y
- Estos Clientes Empresa deberán tener controles personales para evitar que los Administradores de Servicios de Gestión y otras personas puedan obtener acceso no autorizado a las llaves privadas.

Se recomienda que un cliente empresa que utilice DEI:

- Notifique a los Suscriptores que sus llaves privadas están en custodia
- Proteger las llaves de los Suscriptores en custodia de intromisiones no autorizadas,
- Proteger toda la información, incluida la propia llave del Administrador (s), utilizada para recuperar las llaves de los Suscriptores, en custodia.

- Liberar las llaves custodiadas de los Suscriptores sólo para las solicitudes de recuperación debidamente autenticadas y autorizadas.
- Revocar par de Llaves del Suscriptor previo a recuperar la llave de cifrado.
- No estar obligado a comunicar ninguna información relativa a la recuperación de llaves del suscriptor, excepto cuando el mismo Suscriptor ha solicitado la recuperación.
- No divulgar o permitir que se divulgue las llaves en custodia o información relativa a custodia de llaves a ninguna tercera parte, a menos que sea requerido por la ley, regulación gubernamental, política de la empresa, o por orden de un tribunal de jurisdicción competente.

4.12.2 Política y Prácticas de Encapsulamiento y de Recuperación de Llaves de Sesión

Las llaves privadas se almacenan en un repositorio del Administrador de Llaves, en forma encriptada. Cada llave privada del Suscriptor individual es encriptada con su propia llave simétrica. Un registro de custodia de llaves es generado, luego la llave simétrica es combinada con una llave de sesión aleatoria para formar una llave de máscara de sesión.

La llave de máscara de sesión resultante junto con la información de la solicitud de Certificado se enviada de forma segura y almacenada en la base de datos del software de E-Sign.

La llave privada del usuario final y la llave de sesión individual se almacenan en la base de datos Administrador de Llaves.

La base de datos se opera fuera del centro de datos seguro de E-Sign. El cliente empresa puede optar por operar la base de datos del Administrador de Llaves, ya sea en instalaciones de la empresa o del centro de datos seguro de E-Sign.

La recuperación de una llave privada y el Certificado digital requiere que el Administrador del Cliente Empresa acceda con seguridad al centro de control del software de E-Sign, seleccione el par de llaves apropiado para la recuperación y haga clic en un hipervínculo "recuperar".

Sólo después que un administrador aprobado haya hecho clic en el vínculo "recuperar", se recupera la llaves de máscara de sesión para ese par de llaves desde la base de datos. El programa recupera la llave de sesión y lo combina con la llave de máscara de sesión para regenerar la llave simétrica que se usó originalmente para cifrar la llave privada, lo que permite la recuperación de la llave privada del usuario final. Como un paso final, un archivo PKCS # 12 encriptado es devuelto al administrador y, finalmente, distribuido al usuario final.

4.13 Controles Físicos

La E-SIGN CA ha documentado controles físicos detallados y políticas de seguridad de CA y RA a las que es necesario adherir. El cumplimiento de estas políticas se incluye en los requisitos de auditoría independiente E-SIGN CA descritos en la Sección 8. Estos documentos contienen información confidencial y sólo están disponibles bajo un acuerdo con E-Sign. Un resumen de los requisitos es descrito en los siguientes apartados.

4.13.1 Localización del Sitio y Construcción e

Todas las operaciones de una CA o RA E-SIGN CA se deben llevar a cabo dentro de un ambiente protegido físicamente, que permita disuadir, prevenir y detectar usos no autorizados de, acceso a, o divulgación de información sensible y sistemas. Para E-Sign y Asociados, este entorno debe cumplir con los requisitos de Seguridad de E-Sign y los requerimientos ISO/IEC 27001.

Tales requerimientos se basan en parte en el establecimiento de niveles de seguridad física.

Un nivel es una barrera, tal como una puerta cerrada o puerta que exige control de acceso obligatorio para las personas y requiere una respuesta positiva para cada persona, que desea pasar a la siguiente zona. Cada nivel sucesivo proporciona un acceso más restringido y mayor seguridad física contra la intrusión o acceso no autorizado. Además, cada nivel de seguridad física encapsula el siguiente nivel interno, de tal manera que una capa interna debe estar completamente contenida en una capa exterior y no puede tener una pared común con el mundo exterior fuera de nivel, siendo el nivel más exterior la pared exterior del edificio.

El nivel mínimo de seguridad física que requiere una CA o RA está determinado por la clase más alta de Certificados que procese. Por ejemplo, E-Sign procesa y entrega certificados de Class1, 2 y 3 y por lo tanto, opera al más alto nivel de seguridad requerido por E-SIGN CA.

Las CAs o RAs que procesan y emiten certificados Class 1 o Class 2 requieren tener un nivel de seguridad adecuado para el tipo específico de Certificado. Las CAs y RAs deben especificar su ubicación y construcción del Site en más detalle en su CPS.

4.13.2 Acceso Físico

El acceso a cada nivel de seguridad física será auditable y controlado de modo tal que cada nivel pueda ser accedido sólo por personal autorizado.

4.13.3 Energía y Aire Acondicionado

Las instalaciones de seguridad de las CAs y RAs deben estar equipadas con sistemas de energía principal y de respaldo para asegurar la disponibilidad continua e ininterrumpida de energía eléctrica. Además, estas instalaciones de seguridad deben estar equipadas con sistema primario y de respaldo de calefacción, ventilación y aire acondicionado para controlar la temperatura y la humedad relativa.

4.13.4 Exposición al Agua

Las instalaciones de seguridad de CAs y RAs deben estar construidas y equipadas, de tal forma de evitar inundaciones u otras exposiciones dañinas provocadas por el agua. A su vez se deben tener implementados los procedimientos necesarios para prevenir y evitar los efectos nocivos del agua en las instalaciones.

4.13.5 Prevención de Incendios y Protección

Las instalaciones seguras de CAs y RAs deben estar construidas y equipadas, de tal forma de prevenir y extinguir incendios y otras exposiciones dañinas a las llamas o el humo. Estas medidas deben cumplir todas las regulaciones locales de seguridad aplicables.

4.13.6 Almacenamiento de Medios

Las CAs y RAs deberán proteger los medios magnéticos que contienen copias de seguridad de datos de sistemas críticos o cualquier otra información sensible al agua, fuego, u otros peligros ambientales, y utilizará las medidas de protección para disuadir, detectar y prevenir el uso no autorizado, el acceso a, o la divulgación de tales medios.

4.13.7 Eliminación de Desechos

Las CAs y RAs deberán implementar procedimientos para la eliminación de desechos (papel, medios de comunicación, o cualquier otro desecho) para prevenir el uso no autorizado, el acceso o la divulgación de los desechos que contengan información confidencial / privado.

4.13.8 Respaldo Fuera de las Instalaciones

Las CAs y RAs deberán mantener copias de seguridad de los datos críticos del sistema o cualquier otra información confidencial, incluyendo los datos de auditoría, en un lugar seguro fuera del sitio.

4.14 Procedimientos de Control

4.14.1 Roles de Confianza

Empleados, contratistas y consultores que han sido designados para administrar la infraestructura confiable serán consideradas las "Personas de Confianza", las cuales sirven en una "Posición de Confianza." Las personas que deseen convertirse en Personas de Confianza para obtener una Posición de Confianza, deberán cumplir los requisitos de investigación incluidos en esta CP.

Las Personas de Confianza incluyen a todos los empleados, contratistas y consultores que tengan acceso a o controlen operaciones de autenticación o criptográficas que puedan afectar materialmente a:

- la validación de la información en las solicitudes de Certificado;
- la aprobación, rechazo, u otro procesamiento de solicitudes de certificado, solicitudes de revocación, o solicitudes de renovación, o la información de solicitudes;
- la emisión o revocación de los Certificados, incluyendo (en el caso de los Asociados) personal que tiene acceso a áreas restringidas de su repositorio o el manejo de la información o solicitudes del Suscriptor.

Personas de confianza incluyen, pero no se limitan a:

- personal de servicio al cliente,
- personal de administración del sistema,
- personal de ingeniería designado, y
- ejecutivos que han sido designados para administrar confiabilidad de la infraestructura.

4.14.2 Número de Personas Requeridas por Tarea

Las CAs y RAs deberán establecer, mantener y hacer cumplir rigurosos procedimientos de control de tal forma de asegurar la segregación de funciones sobre la base de la responsabilidad del

trabajo y asegurar que múltiples Personas de Confianza son necesarias para realizar tareas delicadas.

Las políticas y procedimientos de control deben garantizar la segregación de funciones sobre la base de responsabilidades del trabajo. Las tareas más sensibles, tales como el acceso y manejo de hardware criptográfico CA (unidad de la firma criptográfica o CSU) y el material clave asociado, requieren varias Personas de Confianza.

Estos procedimientos de control interno están diseñados para asegurar que, como mínimo, dos miembros del personal de confianza tienen que tener acceso físico o lógico en el dispositivo. El acceso al hardware criptográfico de la CA es estrictamente cumplido por varias Personas de Confianza a lo largo de su ciclo de vida, desde la recepción inicial y la inspección, hasta la lógica final y/o la destrucción física. Una vez que un módulo se activa con las llaves operacionales, nuevos controles adicionales de acceso son utilizados para mantener dividido el control en acceso físico y lógico a los dispositivos. Las personas con acceso físico a los módulos no tienen "partes secretas" o “secretos compartidos” y viceversa.

Otras operaciones manuales, tales como la validación y emisión de los Certificados de Class 3, no emitidas por un sistema de validación y de emisión automática, requieren de la participación de al menos dos Personas de Confianza, o una combinación de al menos una persona de confianza y un proceso de validación y emisión automática . Las operaciones manuales para la recuperación de llaves, opcionalmente, puede requerir la validación de los dos (2) Administradores autorizados.

4.14.3 Identificación y Autenticación para Cada Rol

Las CAs y RAs deberá confirmar la identidad y la autorización de todo el personal que postula a ser de confianza previo a que:

- Se les haya entregado sus dispositivos de acceso y se les permita acceder a las instalaciones requeridas;
  Se les haya emitido sus credenciales electrónicas para acceder y realizar funciones específicas en los sistemas de Información y sistemas de la CA o RA.

La autentificación de identidad deberá incluir la presencia personal (física) ante Personas de Confianza que realizan funciones de Recursos Humanos o de seguridad dentro de una entidad, y una verificación de formas de identificación bien reconocidas, tales como pasaporte y licencias de conducir. La identidad deberá ser confirmada, posteriormente, a través de procedimientos de verificación de antecedentes especificados en la presente CP.

4.14.4 Roles que Requieren Segregación de Tareas

Los roles que requieren Separación o Segregación de tareas incluyen (no estando limitados a):

- La validación de información en las Solicitudes de Certificado;
- La aceptación, rechazo, u otro procesamiento de Solicitudes de Certificados, Solicitudes de Revocación, Solicitudes de Recuperación de Llaves o Solicitudes de Renovación, o Información de Enrolamiento;
- La emisión o revocación de Certificados, incluyendo personal con acceso a áreas restringidas del repositorio;
- El manejo de la información del Suscriptor o de las Solicitudes
- La generación, emisión o destrucción de un Certificado de CA

- La carga de una CA en ambiente de producción

4.15 Controles sobre el Personal

La E-SIGN CA ha documentado detalladas políticas de control y seguridad de personal para CAs y RAs, a las cuales adherir y bajo las cuales ser auditadas. El cumplimiento de estas políticas está incluido en los requisitos de auditoría independiente en la sección 8. Estos documentos contienen información confidencial y sólo están disponibles para los participantes de la E-SIGN CA que tienen acuerdo con E-Sign. Un resumen de los requisitos se describe en los siguientes apartados.

4.15.1 Requerimientos de Calificaciones, Experiencia y Autorización

Las CAs y RAs, deben exigir que personal que postula a convertirse en Personas de Confianza presenten pruebas de los antecedentes, calificaciones y la experiencia necesarias para llevar a cabo sus responsabilidades de trabajo en forma competente y satisfactoria, así como las pruebas de autorización gubernamentales, si fuera el caso, necesarias para realizar los servicios de certificación en contratos con el gobierno.

4.15.2 Procedimientos de Verificación de Antecedentes

Las ACs y RAs llevarán a cabo revisiones de antecedentes del personal que postula a convertirse en Personas de Confianza.

La verificación de antecedentes se replicará para el personal que ocupa Posicionesde Confianza, al menos cada cinco (5) años. Estos procedimientos estarán sujetos a las limitaciones impuestas por la ley local. En la medida en que uno de los requerimientos impuestos por esta sección no se puede llevar a cabo a causa de una prohibición o limitación en la legislación local, la entidad investigadora deberá utilizar una técnica de investigación permitida por la ley, que proporcione información sustancialmente similar, incluyendo pero no limitado, a la obtención de una verificación de antecedentes realizada por la agencia gubernamental correspondiente.

Los factores revelados en una revisión de antecedentes que pueden ser considerados motivos de rechazo de los candidatos para las Posiciones de Confianza o para tomar medidas contra una Persona de Confianza existente se discuten en la Comité de de Seguridad de E-Sign e incluyen por lo general (pero no se limitan a) lo siguiente:

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

Los informes que contienen dicha información deben ser evaluados por recursos humanos y personal de seguridad, y ese personal debe tomar acciones que sean razonables en función de la naturaleza, magnitud y frecuencia de la conducta descubierta por la verificación de antecedentes.

Estas acciones pueden incluir medidas que pueden llegar incluso hasta la cancelación de las ofertas de empleo hechas a candidatos para los Puestos de Confianza o el despido de Personas de Confianza existentes. El uso de la información revelada en una investigación de antecedentes para tomar tales acciones estará sujeto a la legislación aplicable.

La investigación de antecedentes de las personas que buscan convertirse en una Persona de Confianza incluye lo siguiente:

- Una confirmación de empleos previos,
- Una verificación de referencias profesionales,
- Una confirmación del grado académico más alto o más relevante obtenido,
- Una búsqueda de antecedentes penales (local, regional, estatal, y nacional),
- Una revisión de registros financieros

Los Asociados se encargarán de las investigaciones adicionales:

- Una búsqueda de los registros de licencia de conducir, y
- Una búsqueda de documentos oficiales emitidos por gobiernos, instituciones públicas o instituciones privadas que cumplan funciones públicas (similar a los servicios de Registro Civil en Latinoamérica o del Seguro Social, en Estados Unidos).

4.15.3 Requisitos de Capacitación (Entrenamiento)

Las CAs y RAs deberán proporcionar a su personal la formación necesaria para llevar a cabo sus responsabilidades de trabajo, en relación con las operaciones de CA o RA, en forma competente y satisfactoria.

Asimismo, periódicamente se deberán revisar los programas de capacitación, y la capacitación se referirá a los elementos relevantes para las funciones desempeñadas por el personal.

El personal de servicio al cliente del Asociado deberán satisfacer los requisitos de entrenamiento de E-Sign, como condición de inicio de las operaciones de Asociados.

Los programas de capacitación deben abordar los elementos relevantes para el medio ambiente particular de la persona que está siendo entrenada, incluyendo:

- Principios y mecanismos de seguridad de la E-SIGN CA
- Versiones, de hardware y software en uso,
- Todas las tareas que se espera la persona realice,
- Presentación y manejo de informes de Incidentes y Compromisos, y
- Procedimientos recuperación de desastres y continuidad de negocio.

4.15.4 Frecuencia y Requerimientos de Reforzamiento

Las CAs y RAs proporcionarán cursos de actualización y reforzamiento a su personal en la medida y la frecuencia necesaria para garantizar que dicho personal mantenga el nivel necesario de competencia para llevar a cabo sus responsabilidades de trabajo en forma competente y satisfactoria.

4.15.5 Frecuencia y Secuencia de Rotación de Trabajo

No aplica.

4.15.6 Sanciones por Acciones no Autorizadas

Las CAs y RAs deberán establecer, mantener y hacer cumplir políticas de empleo para la disciplina del personal que siga acciones no autorizadas.

Las acciones disciplinarias pueden incluir medidas que pueden llegar incluso al despido y deberán ser proporcionales a la frecuencia y severidad de las acciones no autorizadas realizadas.

4.15.7 Requisitos de Contratista Independiente

Las CAs y RAs pueden permitir que contratistas o consultores independientes puedan convertirse en Personas de Confianza sólo en la medida necesaria para acomodar relaciones de subcontratación adecuadas y sólo bajo las siguientes condiciones:

- la entidad que utiliza contratistas o consultores independientes como Personas de Confianza no tiene empleados adecuados disponibles para llenar los roles de las Personas de Confianza y,
- los contratistas o consultores son de confianza para la entidad en la misma medida como si fueran empleados.

De lo contrario, los contratistas y consultores independientes tendrán acceso a dependencias seguras de E-Sign, de un Asociados, o de un Cliente Empresa, sólo en la medida en que son acompañados y supervisados directamente por Personas de Confianza.

4.15.8 Documentación Proporcionada al Personal

E-Sign, Asociados y Clientes Empresas deberán proporcionar a su personal (incluidas las Personas de Confianza) la formación necesaria y el acceso a documentación necesaria para llevar a cabo sus responsabilidades de trabajo en forma competente y satisfactoria.

4.16 Procedimientos de Registro de Auditoría

4.16.1 Tipos de Eventos Registrados

Los tipos de incidentes comprobables que deben ser registrados por las CAs y RAs son expuestos a continuación. Todos los registros, electrónicos y manuales, deberán contener la fecha y hora del incidente, y la identidad de la entidad que causó el incidente. Las CAs deberán indicar en su CPS los registros y los tipos de eventos que se deben registrar.

Los tipos de eventos auditables incluyen:

- Eventos operacionales (incluyendo pero no limitado a (1) la generación de llaves propias de una CA y las llaves de CAs subordinadas, (2) la puesta en marcha y detención de los sistemas y aplicaciones, (3) cambio en los datos de CA o claves, (4) eventos relacionados con el ciclo de vida del módulo criptográfico (por *ejemplo,* uso, des-instalación, y retiro), (5) la posesión de data para activación de las operaciones de llave privada de la CA, los registros de acceso físico, (6) cambios de la configuración y mantenimiento del sistema, (7) registros de la destrucción de medios que contenienen material de claves, datos de activación o información personal del Suscriptor)
- Eventos relacionados con el ciclo de vida de Certificados (incluyendo pero no limitado a la emisión inicial, cambio de llaves, renovación, revocación, suspensión)

- Eventos de empleados confiables (incluyendo pero no limitado a (1) intentos de inicio y cierre de sesión, (2) intentos para crear, eliminar, configurar contraseñas o cambiar los privilegios del sistema de los usuarios privilegiados, (3) cambios de personal)
- Informes de discrepancia y compromiso (incluyendo pero no limitado a intentos de inicio de sesión no autorizado al sistema o a la red)
- Operaciones de lectura y escritura fallidas en el Certificados y repositorio
- Cambios en la políticas de creación de Certificado por ejemplo, período de validez

4.16.2 Frecuencia de Procesamiento de Registros (Logs)

Los registros de auditoría deben ser revisados, como respuesta a las alertas basadas en irregularidades e incidentes dentro de los sistemas de la CA / RA. Los Asociados deberán comparar sus registros de auditoría con los registros manuales o electrónicos de sus Clientes RA Servicio cuando una acción sea considerada sospechosa. Cuando una acción sea considerada sospechosa, las CAs deberán comparar sus registros de auditoría con los registros manuales o electrónicos de sus RAs clientes.

El procesamiento de los registros de auditoría consistirá en una revisión de los registros de auditoría y la documentación de la causa de todos los eventos significativos, en un resumen del registro de auditoría. Las revisiones de registros de auditoría deberán incluir, la verificación de que el registro no ha sido manipulado, inspección de todas las entradas del registro y una investigación de cualquier alerta o irregularidad en los registros. Las medidas adoptadas, sobre la base de revisiones de registro de auditoría, deberán ser documentadas.

4.16.3 Período de Retención de Registro de Auditoría

Los registros de auditoría se conservarán en el lugar por lo menos dos (2) meses después del procesamiento y, posteriormente, archivados, de conformidad con la Sección 5.5.2.

4.16.4 Protección del Registro de Auditoría

Los registros de auditoría estarán protegidos con un por medios electrónicos, que incluye, mecanismos para proteger los archivos de registro; de personas no autorizadas, modificaciones, eliminación, u otra manipulación.

4.16.5 Procedimientos de Auditoría Log Backup

Se deben hacer respaldos de seguridad incrementales de los registros de auditoría y, semanalmente se crearan respaldos de seguridad completos.

4.16.6 Sistema de Recolección de Auditoría (Interno vs Externo)

No hay estipulación

4.16.7 Notificación al Sujeto Causante del Evento

Cuando un evento es registrado por el sistema de recolección de auditoría, no se requiere dar un aviso a la persona, organización, dispositivo o aplicación que causó el evento.

4.16.8 Evaluación de Vulnerabilidades

Los eventos en el proceso de auditoría se registran, en parte, para monitorear vulnerabilidades del sistema. Las evaluaciones de vulnerabilidad de seguridad lógica ("LSVAs") son ejecutados, revisitados y, revisados siguiendo un examen de estos eventos monitoreados. Las LSVAs se basan en datos registrados automáticamente en tiempo real y se llevan a cabo sobre una base de tiempo diaria, mensual y anual. Una evaluación de vulnerabilidad de seguridad lógica LSVA anual será un aporte a la Auditoria de Cumplimiento anual de la entidad.

4.17 Archivo de Registros

4.17.1 Tipos de Registros Archivados

Archivos de CAs y RAs:

- Todos los datos de auditoría recopilados en términos de la Sección 5.4
- Información de Suscripción de Certificados
- Documentación de apoyo de solicitudes de Certificados
- Información del Ciclo de Vida de Certificados, por ejemplo, revocación, cambio de llaves y la información de solicitud de renovación

4.17.2 Periodo de Retención de Archivos

Los registros se conservarán durante al menos los plazos establecidos a continuación, después de la fecha de la expiración o revocación del Certificado:

- Un (1) años para los Certificados de Class 1,
- Seis (6) años y seis (6) meses para Certificados de Class 2 y Class 3,
- Veinte (20) años y seis (6) meses para Certificados de Class 4

4.17.3 Protección del Archivo

Una entidad que mantiene un archivo de registros, debe proteger el archivo para que sólo las Personas de Confianza de la entidad puedan tener acceso al archivo.

El archivo debe estar protegido contra accesos no autorizados, modificaciones, eliminaciones, o manipulación, bajo un Sistema Confiable de almacenamiento.

Los medios que contienen los archivos de datos y las aplicaciones necesarias para procesarlos se mantendrán para asegurar que los datos del archivo puedan ser accesibles durante el período de tiempo establecido en la presente CP.

4.17.4 Procedimientos de Respaldo de Archivos

Las entidades recopiladoras de información electrónica deberán hacer respaldos incrementales de los archivos de información del sistema diariamente, y hacer respaldos completos semanalmente. Las copias de los registros realizados en papel se mantendrán en una instalación segura fuera del sitio.

4.17.5 Requisitos para el Sellado de Tiempo de los Registros

Los Certificados, CRLs y otras entradas a la base de datos de revocación deberá tener información de fecha y hora. Tal información de tiempo, no necesita tener base criptográfica.

4.17.6 Sistema de Recolección de Archivo (Interno o Externo)

Los Sistemas de Recolección de Archivo de las entidades serán internos a la E-SIGN CA, con excepción de los Clientes RA. ~~Los Asociados~~ Las CAs deberán ayudar a sus RAs clientes a preservar ~~las pistas~~ un registro de auditoría. Tal sistema de recolección de archivos es entonces externo a la RA. De lo contrario, las entidades dentro de la E-SIGN CA deberán utilizar sistemas de recolección de archivos internos.

4.17.7 Procedimientos para Obtener y Verificar Información Archivada

Sólo personal de confianza autorizado puede obtener acceso al archivo. La integridad de la información es verificada cuando el archivo se restaura.

4.18 Cambio de Llaves

Un Certificado de CA puede ser renovado si la Entidad Superior de la CA reconfirma la identidad de la CA. Después de la reconfirmación, la entidad superior deberá aprobar o rechazar la solicitud de renovación. Después de la aprobación de la solicitud de renovación, la Entidad Superior deberá llevar a cabo una Ceremonia de Generación de Llaves con el fin de generar un nuevo par de llaves para la CA. Durante la Ceremonia de Generación de Llaves, la Entidad Superior deberá firmar y emitir un nuevo Certificado a la CA. Tal Ceremonia de Generación de Llaves deberá cumplir los requisitos documentados en las políticas de seguridad confidenciales de E-SIGN CA. Los nuevos Certificados de CA que contienen las nuevas llaves públicas generadas durante la Ceremonia de Generación de Llaves se pondrá a disposición de las Partes que Confían.

4.19 Compromiso y Recuperación de Desastres

4.19.1 Procedimientos de Manejo de Incidentes y Compromisos

Copias de seguridad de la siguiente información de la CAs se mantendrá almacenada fuera del sitio y puesto a disposición en el caso de un Compromiso o un desastre: Los datos de Solicitudes de Certificado, los datos de auditoría y registros de la base de todos los Certificados emitidos. Se debe generar y mantener Copias de seguridad de las llaves privadas de la CA de acuerdo con CP § 6.2.4. Los Asociados deberán mantener copias de seguridad de la anterior información de la CA de sus propias Autoridades Certificadoras y Clientes Empresas dentro de sus sub-dominios.

4.19.2 Recursos Computacionales, Software, y/o los Datos están Dañados

Luego de la corrupción de los recursos informáticos, software y / o datos, la CA o RA afectada debe perparar un informe del incidente y una respuesta al evento, de acuerdo con los procedimientos documentados de E-Sign para incidentes y compromisos establecidos en la CPS correspondiente y las políticas confidenciales de seguridad de E-SIGN CA.

4.19.3 Procedimientos de Compromiso de Llaves Privadas de la Entidad

En el caso de un compromiso de la llave privada de la CA, tal CA será revocada. Los Asociados harán todos los esfuerzos comerciales razonables para notificar a las partes que confían si, se descubre o tiene razones para creer que ha habido un compromiso de la llave privada de una CA dentro de los sub-dominios de la E-SIGN CA.

4.19.4 Capacidad de Continuidad de Negocio Luego de un Desastre

Las entidades E-SIGN CA que operen instalaciones seguras de CA y RA deben desarrollar, probar, mantener y, si es necesario, implementar un Plan de Recuperación de Desastres (DRP) para mitigar los efectos de cualquier tipo de desastre natural o provocado por el hombre.

Los planes de recuperación de desastres se hacen cargo de la restauración de los sistemas de información de servicios y las funciones claves de negocio.

Los sitios de recuperación de desastre tienen seguridad física equivalente a las especificadas por la E-SIGN CA.

La base de datos de recuperación de desastres se debe sincronizar con la base de datos de producción dentro de los plazos establecidos en el Sistema General de Seguridad de la Información (SGSI).

Los equipos de recuperación de desastres deben tener las protecciones de seguridad física de acuerdo a lo documentado en las políticas de la E-SIGN CA de seguridad confidencial, que incluye la aplicación de niveles (tiers) de seguridad física.

4.20 Terminación de la CA o RA

La terminación de una CA o RA no E-SIGN CA (Asociado, Clientes Empresa) estará sujeta al acuerdo celebrado entre la CA que será terminada y la Entidad Superior.

Ambas partes, de buena fe, harán los esfuerzos comercialmente razonables para ponerse de acuerdo sobre un plan de terminación que minimice la interrupción de servicio a los clientes, Suscriptores y partes que confían.

El plan de terminación puede cubrir temas tales como:

- La notificación a las partes afectadas por la terminación, tales como Suscriptores, Partes Confiadas, y Clientes,
- Manejo del costo de dicha notificación,
- La revocación del Certificado emitido a la CA por la Entidad Superior,
- La preservación de los archivos de la CA y los registros para los plazos exigidos en el presente CP
- La continuación de los servicios de soporte a Suscriptores y clientes,
- La continuación de los servicios de revocación, tales como la emisión de la CRL o el mantenimiento de los servicios en línea de verificación de estado,
- La revocación de Certificados no vencidos sin revocar, de Suscriptores y de CAs subordinadas, si es necesario,

- El reembolso (si es necesario) a los Suscriptores cuyos certificados no expirados, ni revocados se revocan durante el plan de terminación o la disposición, para la emisión de los Certificados de reemplazo a través de CAs sucesoras,
- Disposición de la llave privada de la CA y el token de hardware que contiene dicha llave privada,
- Disposiciones necesarias para la transición de los servicios de la CA a una CA sucesora

5 Controles de Instalación, Administración y Operacionales

5.1 Controles Físicos

La E-SIGN CA ha documentado controles físicos detallados y políticas de seguridad de CA y RA a las que es necesario adherir. El cumplimiento de estas políticas se incluye en los requisitos de auditoría independiente E-SIGN CA descritos en la Sección 8. Estos documentos contienen información confidencial y sólo están disponibles bajo un acuerdo con E-Sign. Un resumen de los requisitos es descrito en los siguientes apartados.

5.1.1 Ubicación y Construcción del Site

Todas las operaciones de una CA o RA E-SIGN CA se deben llevar a cabo dentro de un ambiente protegido físicamente, que permita disuadir, prevenir y detectar usos no autorizados de, acceso a, o divulgación de información sensible y sistemas. Para E-Sign y Asociados, este entorno debe cumplir con los requisitos de Seguridad de E-Sign y los documentos de la Política General de Seguridad de E-Sign.

Tales requerimientos se basan en parte en el establecimiento de niveles de seguridad física.

Un nivel es una barrera, tal como una puerta cerrada o puerta que exige control de acceso obligatorio para las personas y requiere una respuesta positiva para cada persona, que desea pasar a la siguiente zona. Cada nivel sucesivo proporciona un acceso más restringido y mayor seguridad física contra la intrusión o acceso no autorizado. Además, cada nivel de seguridad física encapsula el siguiente nivel interno, de tal manera que una capa interna debe estar completamente contenida en una capa exterior y no puede tener una pared común con el mundo exterior fuera de nivel, siendo el nivel más exterior la pared exterior del edificio.

El nivel mínimo de seguridad física que requiere una CA o RA está determinado por la clase más alta de Certificados que procese. Por ejemplo, E-Sign procesa y entrega certificados de Class1, 2 y 3 y por lo tanto, opera al más alto nivel de seguridad requerido por E-SIGN CA.

Las CAs o RAs que procesan y emiten certificados Class 1 o Class 2 requieren tener un nivel de seguridad adecuado para el tipo específico de Certificado. Las CAs y RAs deben especificar su ubicación y construcción del Site en más detalle en su CPS.

5.1.2 Acceso Físico

El acceso a cada nivel de seguridad física será auditable y controlado de modo tal que cada nivel pueda ser accedido sólo por personal autorizado.

5.1.3 Energía y Aire Acondicionado

Las instalaciones de seguridad de las CAs y RAs deben estar equipadas con sistemas de energía principal y de respaldo para asegurar la disponibilidad continua e ininterrumpida de energía eléctrica. Además, estas instalaciones de seguridad deben estar equipadas con sistema primario y de respaldo de calefacción, ventilación y aire acondicionado para controlar la temperatura y la humedad relativa.

5.1.4 Exposición al Agua

Las instalaciones de seguridad de CAs y RAs deben estar construidas y equipadas, de tal forma de evitar inundaciones u otras exposiciones dañinas provocadas por el agua. A su vez se deben tener implementados los procedimientos necesarios para prevenir y evitar los efectos nocivos del agua en las instalaciones.

5.1.5 Prevención de Incendios y Protección

Las instalaciones seguras de CAs y RAs deben estar construidas y equipadas, de tal forma de prevenir y extinguir incendios y otras exposiciones dañinas a las llamas o el humo. Estas medidas deben cumplir todas las regulaciones locales de seguridad aplicables.

5.1.6 Almacenamiento de Medios

Las CAs y RAs deberán proteger los medios magnéticos que contienen copias de seguridad de datos de sistemas críticos o cualquier otra información sensible al agua, fuego, u otros peligros ambientales, y utilizará las medidas de protección para disuadir, detectar y prevenir el uso no autorizado, el acceso a, o la divulgación de tales medios.

5.1.7 Eliminación de Desechos

Las CAs y RAs deberán implementar procedimientos para la eliminación de desechos (papel, medios de comunicación, o cualquier otro desecho) para prevenir el uso no autorizado, el acceso o la divulgación de los desechos que contengan información confidencial / privado.

5.1.8 Respaldo Fuera de las Instalaciones

Las CAs y RAs deberán mantener copias de seguridad de los datos críticos del sistema o cualquier otra información confidencial, incluyendo los datos de auditoría, en un lugar seguro fuera del sitio.

5.2 Procedimientos de Control

5.2.1 Roles de Confianza

Empleados, contratistas y consultores que han sido designados para administrar la infraestructura confiable serán consideradas las "Personas de Confianza", las cuales sirven en una "Posición de Confianza." Las personas que deseen convertirse en Personas de Confianza para obtener una Posición de Confianza, deberán cumplir los requisitos de investigación incluidos en esta CP.

Las Personas de Confianza incluyen a todos los empleados, contratistas y consultores que tengan acceso a o controlen operaciones de autenticación o criptográficas que puedan afectar materialmente a:

- la validación de la información en las solicitudes de Certificado;
- la aprobación, rechazo, u otro procesamiento de solicitudes de certificado, solicitudes de revocación, o solicitudes de renovación, o la información de solicitudes;

- la emisión o revocación de los Certificados, incluyendoel personal que tiene acceso a áreas restringidas de su repositorio o el manejo de la información o solicitudes del Suscriptor.

Personas de confianza incluyen, pero no se limitan a:

- personal de servicio al cliente,
- personal de administración del sistema,
- personal de ingeniería designado, y
- ejecutivos que han sido designados para administrar confiabilidad de la infraestructura.

5.2.2 Número de Personas Requeridas por Tarea

Las CAs y RAs deberán establecer, mantener y hacer cumplir rigurosos procedimientos de control de tal forma de asegurar la segregación de funciones sobre la base de la responsabilidad del trabajo y asegurar que múltiples Personas de Confianza son necesarias para realizar tareas delicadas.

Las políticas y procedimientos de control deben garantizar la segregación de funciones sobre la base de responsabilidades del trabajo. Las tareas más sensibles, tales como el acceso y manejo de hardware criptográfico CA (unidad de la firma criptográfica o CSU) y el material clave asociado, requieren varias Personas de Confianza.

Estos procedimientos de control interno están diseñados para asegurar que, como mínimo, dos miembros del personal de confianza tienen que tener acceso físico o lógico en el dispositivo. El acceso al hardware criptográfico de la CA es cumplido por varias Personas de Confianza a lo largo de su ciclo de vida, desde la recepción inicial y la inspección, hasta la lógica final y/o la destrucción física. Una vez que un módulo se activa con las llaves operacionales, nuevos controles adicionales de acceso son utilizados para mantener dividido el control en acceso físico y lógico a los dispositivos. Las personas con acceso físico a los módulos no tienen "secretos compartidos" y viceversa.

Otras operaciones manuales, tales como la validación y emisión de los Certificados de Class 3, no emitidas por un sistema de validación y de emisión automática, requieren de la participación de al menos dos Personas de Confianza, o una combinación de al menos una persona de confianza y un proceso de validación y emisión automática . Las operaciones manuales para la recuperación de llaves, opcionalmente, puede requerir la validación de los dos (2) Administradores autorizados.

5.2.3 Identificación y Autenticación para Cada Rol

Las CAs y RAs deberá confirmar la identidad y la autorización de todo el personal que postula a ser de confianza previo a que:

- Se les haya entregado sus dispositivos de acceso y se les permita acceder a las instalaciones requeridas;
  Se les haya emitido sus credenciales electrónicas para acceder y realizar funciones específicas en los sistemas de Información y sistemas de la CA o RA.

La autentificación de identidad deberá incluir la presencia personal (física) ante Personas de Confianza que realizan funciones de Recursos Humanos o de seguridad dentro de una entidad, y una verificación de formas de identificación bien reconocidas, tales como pasaporte y licencias

de conducir. La identidad deberá ser confirmada, posteriormente, a través de procedimientos de verificación de antecedentes especificados en la presente CP.

5.2.4 Roles que Requieren Segregación de Tareas

Los roles que requieren Separación o Segregación de tareas incluyen (no estando limitados a):

- La validación de información en las Solicitudes de Certificado;
- La aceptación, rechazo, u otro procesamiento de Solicitudes de Certificados, Solicitudes de Revocación, Solicitudes de Recuperación de Llaves o Solicitudes de Renovación, o Información de Enrolamiento;
- La emisión o revocación de Certificados, incluyendo personal con acceso a áreas restringidas del repositorio;
- El manejo de la información del Suscriptor o de las Solicitudes
- La generación, emisión o destrucción de un Certificado de CA
- La carga de una CA en ambiente de producción

5.3 Controles sobre el Personal

La E-SIGN CA ha documentado detalladas políticas de control y seguridad de personal para CAs y RAs, a las cuales adherir y bajo las cuales ser auditadas. El cumplimiento de estas políticas está incluido en los requisitos de auditoría independiente en la sección 8. Estos documentos contienen información confidencial y sólo están disponibles para los participantes de la E-SIGN CA que tienen acuerdo con E-Sign. Un resumen de los requisitos se describe en los siguientes apartados.

5.3.1 Requerimientos de Calificaciones, Experiencia y Autorización

Las CAs y RAs, deben exigir que personal que postula a convertirse en Personas de Confianza presenten pruebas de los antecedentes, calificaciones y la experiencia necesarias para llevar a cabo sus responsabilidades de trabajo en forma competente y satisfactoria, así como las pruebas de autorización gubernamentales, si fuera el caso, necesarias para realizar los servicios de certificación en contratos con el gobierno.

5.3.2 Procedimientos de Verificación de Antecedentes

Las ACs y RAs llevarán a cabo revisiones de antecedentes del personal que postula a convertirse en Personas de Confianza.

La verificación de antecedentes se replicará para el personal que ocupa Posicionesde Confianza, al menos cada cinco (5) años. Estos procedimientos estarán sujetos a las limitaciones impuestas por la ley local. En la medida en que uno de los requerimientos impuestos por esta sección no se puede llevar a cabo a causa de una prohibición o limitación en la legislación local, la entidad investigadora deberá utilizar una técnica de investigación permitida por la ley, que proporcione información sustancialmente similar, incluyendo pero no limitado, a la obtención de una verificación de antecedentes realizada por la agencia gubernamental correspondiente.

Los factores revelados en una revisión de antecedentes que pueden ser considerados motivos de rechazo de los candidatos para los Posicionesde Confianza o para tomar medidas contra una Persona de Confianza existente se discuten en el Comité de Seguridad de E-Sign e incluyen por lo general (pero no se limitan a) lo siguiente:

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

Los informes que contienen dicha información deben ser evaluados por recursos humanos y personal de seguridad, y ese personal debe tomar acciones que sean razonables en función de la naturaleza, magnitud y frecuencia de la conducta descubierta por la verificación de antecedentes.

Estas acciones pueden incluir medidas que pueden llegar incluso hasta la cancelación de las ofertas de empleo hechas a candidatos para los Puestos de Confianza o el despido de Personas de Confianza existentes. El uso de la información revelada en una investigación de antecedentes para tomar tales acciones estará sujeto a la legislación aplicable.

La investigación de antecedentes de las personas que buscan convertirse en una Persona de Confianza incluye lo siguiente:

- Una confirmación de empleos previos,
- Una verificación de referencias profesionales,
- Una confirmación del grado académico más alto o más relevante obtenido,
- Una búsqueda de antecedentes penales (local, regional, estatal, y nacional),
- Una revisión de registros financieros

Los Asociados se encargarán de las investigaciones adicionales:

- Una búsqueda de los registros de licencia de conducir, y
- Una búsqueda de de documentos oficiales emitidos por gobiernos, instituciones públicas o instituciones privadas que cumplan funciones públicas (similar a los servicios de Registro Civil en Latinoamérica o del Seguro Social, en Estados Unidos).

5.3.3 Requisitos de Capacitación (Entrenamiento)

Las CAs y RAs deberán proporcionar a su personal la formación necesaria para llevar a cabo sus responsabilidades de trabajo, en relación con las operaciones de CA o RA, en forma competente y satisfactoria.

Asimismo, periódicamente se deberán revisar los programas de capacitación, y la capacitación se referirá a los elementos relevantes para las funciones desempeñadas por el personal.

El personal de servicio al cliente del Asociado deberán satisfacer los requisitos de entrenamiento de E-Sign, como condición de inicio de las operaciones de Asociados.

Los programas de capacitación deben abordar los elementos relevantes para el medio ambiente particular de la persona que está siendo entrenada, incluyendo:

- Principios y mecanismos de seguridad de la E-SIGN CA
- Versiones, de hardware y software en uso,
- Todas las tareas que se espera la persona realice,
- Presentación y manejo de informes de Incidentes y Compromisos, y
- Procedimientos recuperación de desastres y continuidad de negocio.

5.3.4 Frecuencia y Requerimientos de Reforzamiento

Las CAs y RAs proporcionarán cursos de actualización y reforzamiento a su personal en la medida y la frecuencia necesaria para garantizar que dicho personal mantenga el nivel necesario de competencia para llevar a cabo sus responsabilidades de trabajo en forma competente y satisfactoria.

5.3.5 Frecuencia y Secuencia de Rotación de Trabajo

No aplica.

5.3.6 Sanciones por Acciones no Autorizadas

Las CAs y RAs deberán establecer, mantener y hacer cumplir políticas de empleo para la disciplina del personal que siga acciones no autorizadas.

Las acciones disciplinarias pueden incluir medidas que pueden llegar incluso al despido y deberán ser proporcionales a la frecuencia y severidad de las acciones no autorizadas realizadas.

5.3.7 Requisitos de Contratista Independiente

Las CAs y RAs pueden permitir que contratistas o consultores independientes puedan convertirse en Personas de Confianza sólo en la medida necesaria para acomodar relaciones de subcontratación adecuadas y sólo bajo las siguientes condiciones:

- la entidad que utiliza contratistas o consultores independientes como Personas de Confianza no tiene empleados adecuados disponibles para llenar los roles de las Personas de Confianza y,
- los contratistas o consultores son de confianza para la entidad en la misma medida como si fueran empleados.

De lo contrario, los contratistas y consultores independientes tendrán acceso a dependencias seguras de E-Sign, de un Asociados, o de un Cliente Empresa, sólo en la medida en que son acompañados y supervisados directamente por Personas de Confianza.

5.3.8 Documentación Proporcionada al Personal

E-Sign, Asociados y Clientes Empresas deberán proporcionar a su personal (incluidas las Personas de Confianza) la formación necesaria y el acceso a documentación necesaria para llevar a cabo sus responsabilidades de trabajo en forma competente y satisfactoria.

5.4 Procedimientos de Registro de Auditoría

5.4.1 Tipos de Eventos Registrados

Los tipos de incidentes comprobables que deben ser registrados por las CAs y RAs son expuestos a continuación. Todos los registros, electrónicos y manuales, deberán contener la fecha y hora del incidente, y la identidad de la entidad que causó el incidente. Las CAs deberán indicar en su CPS los registros y los tipos de eventos que se deben registrar.

Los tipos de eventos auditables incluyen:

- Eventos operacionales (incluyendo pero no limitado a (1) la generación de llaves propias de una CA y las llaves de CAs subordinadas, (2) la puesta en marcha y detención de los sistemas y aplicaciones, (3) cambio en los datos de CA o claves, (4) eventos relacionados con el ciclo de vida del módulo criptográfico (por *ejemplo,* uso, des-instalación, y retiro), (5) la posesión de data para activación de las operaciones de llave privada de la CA, los registros de acceso físico, (6) cambios de la configuración y mantenimiento del sistema, (7) registros de la destrucción de medios que contenienen material de claves, datos de activación o información personal del Suscriptor)
- Eventos relacionados con el ciclo de vida de Certificados (incluyendo pero no limitado a la emisión inicial, cambio de llaves, renovación, revocación, suspensión)
- Eventos de empleados confiables (incluyendo pero no limitado a (1) intentos de inicio y cierre de sesión, (2) intentos para crear, eliminar, configurar contraseñas o cambiar los privilegios del sistema de los usuarios privilegiados, (3) cambios de personal)
- Informes de discrepancia y compromiso (incluyendo pero no limitado a intentos de inicio de sesión no autorizado al sistema o a la red)
- Operaciones de lectura y escritura fallidas en el Certificados y repositorio
- Cambios en la políticas de creación de Certificado por ejemplo, período de validez

5.4.2 Frecuencia de Procesamiento de Registros (Logs)

Los registros de auditoría deben ser revisados, como respuesta a las alertas basadas en irregularidades e incidentes dentro de los sistemas de la CA / RA. Los Asociados deberán comparar sus registros de auditoría con los registros manuales o electrónicos de sus Clientes RA Servicio cuando una acción sea considerada sospechosa. Cuando una acción sea considerada sospechosa, las CAs deberán comparar sus registros de auditoría con los registros manuales o electrónicos de sus RAs clientes.

El procesamiento de los registros de auditoría consistirá en una revisión de los registros de auditoría y la documentación de la causa de todos los eventos significativos, en un resumen del registro de auditoría. Las revisiones de registros de auditoría deberán incluir, la verificación de que el registro no ha sido manipulado, inspección de todas las entradas del registro y una investigación de cualquier alerta o irregularidad en los registros. Las medidas adoptadas, sobre la base de revisiones de registro de auditoría, deberán ser documentadas.

5.4.3 Período de Retención de Registro de Auditoría

Los registros de auditoría se conservarán en el lugar por lo menos dos (2) meses después del procesamiento y, posteriormente, archivados, de conformidad con la Sección 5.5.2.

5.4.4 Protección del Registro de Auditoría

Los registros de auditoría estarán protegidos con medidas electrónicas que incluye, mecanismos para proteger los archivos de registro; de personas no autorizadas, modificaciones, eliminación, u otra manipulación.

5.4.5 Procedimientos de Auditoría Log Backup

Periódicamente, según lo señalado en la Política General de Seguridad de E-Sign, se deben hacer respaldos de seguridad incrementales de los registros de auditoría y, semanalmente se crearan respaldos de seguridad completos.

5.4.6 Sistema de Recolección de Auditoría (Interno vs Externo)

No hay estipulación

5.4.7 Notificación al Sujeto Causante del Evento

Cuando un evento es registrado por el sistema de recolección de auditoría, no se requiere dar un aviso a la persona, organización, dispositivo o aplicación que causó el evento.

5.4.8 Evaluación de Vulnerabilidades

Los eventos en el proceso de auditoría se registran, en parte, para monitorear vulnerabilidades del sistema. Las evaluaciones de vulnerabilidad de seguridad lógica ("LSVAs") son ejecutados, revisitados y, revisados siguiendo un examen de estos eventos monitoreados. Las LSVAs se basan en datos registrados automáticamente en tiempo real y se llevan a cabo sobre una base de tiempo diaria, mensual y anual. Una evaluación de vulnerabilidad de seguridad lógica LSVA anual será un aporte a la Auditoria de Cumplimiento anual de la entidad.

5.5 Archivo de Registros

5.5.1 Tipos de Registros Archivados

Archivos de CAs y RAs:

- Todos los datos de auditoría recopilados en términos de la Sección 5.4
- Información de Suscripción de Certificados
- Documentación de apoyo de solicitudes de Certificados
- Información del Ciclo de Vida de Certificados, por ejemplo, revocación, cambio de llaves y la información de solicitud de renovación

5.5.2 Periodo de Retención de Archivos

Los registros se conservarán durante al menos los plazos establecidos a continuación, después de la fecha de la expiración o revocación del Certificado:

- Un (1) año para los Certificados de Class 1,
- Seis (6) años y seis (6) meses para Certificados de Class 2 y Class 3,
- Veinte (20) años y seis (6) meses para Certificados de Class 4

5.5.3 Protección del Archivo

Una entidad que mantiene un archivo de registros, debe proteger el archivo para que sólo las Personas de Confianza de la entidad puedan tener acceso al archivo.

El archivo debe estar protegido contra accesos no autorizados, modificaciones, eliminaciones, o manipulación, bajo un sistema de almacenamiento.

Los medios que contienen los archivos de datos y las aplicaciones necesarias para procesarlos se mantendrán para asegurar que los datos del archivo puedan ser accesibles durante el período de tiempo establecido en la presente CP.

5.5.4 Procedimientos de Respaldo de Archivos

Las entidades recopiladoras de información electrónica deberán hacer respaldos incrementales de los archivos de información del sistema diariamente, y hacer respaldos completos semanalmente. Las copias de los registros realizados en papel se mantendrán en una instalación segura fuera del sitio.

5.5.5 Requisitos para el Sellado de Tiempo de los Registros

Los Certificados, CRLs y otras entradas a la base de datos de revocación deberá tener información de fecha y hora. Tal información de tiempo, no necesita tener base criptográfica.

5.5.6 Sistema de Recolección de Archivo (Interno o Externo)

Los Sistemas de Recolección de Archivo de las entidades serán internos a la E-SIGN CA, con excepción de los Clientes RA. ~~Los Centros de Procesamiento~~ Las CAs deberán ayudar a sus RAs clientes a preservar ~~las pistas~~ un registro de auditoría. Tal sistema de recolección de archivos es entonces externo a la RA. De lo contrario, las entidades dentro de la E-SIGN CA deberán utilizar sistemas de recolección de archivos internos.

5.5.7 Procedimientos para Obtener y Verificar Información Archivada

Sólo personal de confianza autorizado puede obtener acceso al archivo. La integridad de la información es verificada cuando el archivo se restaura.

5.6 Cambio de Llaves

Un Certificado de CA puede ser renovado si la Entidad Superior de la CA reconfirma la identidad de la CA. Después de la reconfirmación, la entidad superior deberá aprobar o rechazar la solicitud de renovación. Después de la aprobación de la solicitud de renovación, la Entidad Superior deberá llevar a cabo una Ceremonia de Generación de Llaves con el fin de generar un nuevo par de llaves para la CA. Durante la Ceremonia de Generación de Llaves, la Entidad Superior deberá firmar y emitir un nuevo Certificado a la CA. Tal Ceremonia de Generación de Llaves deberá cumplir los requisitos documentados en las políticas de seguridad confidenciales de E-SIGN CA. Los nuevos Certificados de CA que contienen las nuevas llaves públicas generadas durante la Ceremonia de Generación de Llaves se pondrá a disposición de las Partes que Confían.

5.7 Compromiso y Recuperación de Desastres

5.7.1 Procedimientos de Manejo de Incidentes y Compromisos

Copias de seguridad de la siguiente información de la CAs se mantendrá almacenada fuera del sitio y puesto a disposición en el caso de un Compromiso o un desastre: Los datos de Solicitudes de Certificado, los datos de auditoría y registros de la base de todos los Certificados emitidos. Se debe generar y mantener Copias de seguridad de las llaves privadas de la CA de acuerdo con CP §

6.2.4. Los Asociados deberán mantener copias de seguridad de la anterior información de la CA de sus propias Autoridades Certificadoras y Clientes Empresas dentro de sus sub-dominios.

5.7.2 Recursos Computacionales, Software, y/o los Datos están Dañados

Luego de la corrupción de los recursos informáticos, software y / o datos, la CA o RA afectada debe perparar un informe del incidente y una respuesta al evento, de acuerdo con los procedimientos documentados de E-Sign para incidentes y compromisos establecidos en la CPS correspondiente y las políticas confidenciales de seguridad de E-SIGN CA.

5.7.3 Procedimientos de Compromiso de Llaves Privadas de la Entidad

En el caso de un compromiso de la llave privada de la CA, tal CA será revocada. Los Asociados harán todos los esfuerzos comerciales razonables para notificar a las partes que confían si, se descubre o tiene razones para creer que ha habido un compromiso de la llave privada de una CA dentro de los sub-dominios de la E-SIGN CA.

5.7.4 Capacidad de Continuidad de Negocio Luego de un Desastre

Las entidades E-SIGN CA que operen instalaciones seguras de CA y RA deben desarrollar, probar, mantener y, si es necesario, implementar un Plan de Recuperación de Desastres (DRP) para mitigar los efectos de cualquier tipo de desastre natural o provocado por el hombre.

Los planes de recuperación de desastres se hacen cargo de la restauración de los sistemas de información de servicios y las funciones claves de negocio.

Los sitios de recuperación de desastre tienen seguridad física equivalente a las especificadas por la E-SIGN CA.

Los Asociados tienen la capacidad de restaurar o recuperar las operaciones esenciales dentro de las veinticuatro (24) horas después de un desastre con, como mínimo, el soporte a las siguientes funciones: revocación de Certificados, publicación de información de revocación, y la entrega de información de recuperación de llaves para Clientes Empresa utilizando el Administrador de Llaves .

La base de datos de recuperación de desastres se debe sincronizar con la base de datos de producción dentro de los plazos establecidos en el Sistema General de Seguridad de la Información (SGSI).

Los equipos de recuperación de desastres deben tener las protecciones de seguridad física de acuerdo a lo documentado en las políticas de la E-SIGN CA de seguridad confidencial, que incluye la aplicación de niveles (tiers) de seguridad física.

El Plan de recuperación de desastres prevé una recuperación completa dentro de una semana después de ocurrido el desastre en el site principal de E-Sign o un Asociado.

E-Sign o el Asociado deberá instalar y probar el equipo en el sitio principal para soportar las funcionalidades de la CA/RA, luego de cualquier desastre excepto aquel de una magnitud que pudiera hacer que toda la instalación deje de funcionar. Terminación de la CA o RA

La terminación de una CA o RA no E-SIGN CA (Asociado, Clientes Empresa) estará sujeta al acuerdo celebrado entre la CA que será terminada y la Entidad Superior.

Ambas partes, de buena fe, harán los esfuerzos comercialmente razonables para ponerse de acuerdo sobre un plan de terminación que minimice la interrupción de servicio a los clientes, Suscriptores y partes que confían.

El plan de terminación puede cubrir temas tales como:

- La notificación a las partes afectadas por la terminación, tales como Suscriptores, Partes Confiadas, y Clientes,
- Manejo del costo de dicha notificación,
- La revocación del Certificado emitido a la CA por la Entidad Superior,
- La preservación de los archivos de la CA y los registros para los plazos exigidos en el presente CP
- La continuación de los servicios de soporte a Suscriptores y clientes,
- La continuación de los servicios de revocación, tales como la emisión de la CRL o el mantenimiento de los servicios en línea de verificación de estado,
- La revocación de Certificados no vencidos sin revocar, de Suscriptores y de CAs subordinadas, si es necesario,
- El reembolso (si es necesario) a los Suscriptores cuyos certificados no expirados, ni revocados se revocan durante el plan de terminación o la disposición, para la emisión de los Certificados de reemplazo a través de CAs sucesoras,
- Disposición de la llave privada de la CA y el token de hardware que contiene dicha llave privada,
- Disposiciones necesarias para la transición de los servicios de la CA a una CA sucesora

6 Controles técnicos de seguridad

6.1 Generación e instalación del par de llaves

6.1.1 Generación del par de llaves

La generación del par de llaves se llevará a cabo utilizando medios electrónicos, físicos y lógicos y procesos que proporcionen la robustez criptográfica requerida, para así evitar la pérdida, divulgación, modificación o uso no autorizado de las llaves privadas.

Este requisito se aplica a los Suscriptores, Clientes Empresa que utilizan el Administrador de Llaves, CAs que pre-generen pares de llaves en tokens de hardware de Suscriptores y Asociados.

Las Llaves de CA se generan en una Ceremonia de Generación de Llaves.

Todas las ceremonias de generación de llaves se ajustan a los requerimientos indicados en las políticas confidenciales de seguridad de E-SIGN CA.

6.1.2 Entrega de la Llave Privada al Suscriptor

Las llaves privadas de los Suscriptores son generalmente generadas por los Suscriptores, y por lo tanto, la entrega de llaves privadas al Suscriptor no es necesaria.

Las llaves privadas se entregan a los Suscriptores sólo cuando:

- Sus Solicitudes de Certificados son aprobadas por un Cliente Empresa que utiliza Administrador de Llaves de sesión, o
- Su par de llaves es generado previamente en tokens de hardware, que son distribuidas a los solicitantes de acuerdo con el proceso de enrolamiento.

Los Clientes Empresa que utilizan un software de encriptación aprobado por E-Sign deberán utilizar dicho software y sistemas confiables para entregar las llaves privadas a Suscriptores, y deberán garantizar la entrega a través del uso de PKCS # 12 o a través de cualquier otro medio comparable equivalente (por ejemplo, cifrado) con el fin de evitar la pérdida, divulgación, modificación o uso no autorizado de tales llaves privadas.

Cuando los pares de llaves son generadas previamente en tokens de hardware, las entidades que distribuyen deben hacer esfuerzos comercialmente razonables para garantizar la seguridad física de los tokens de tal forma de evitar la pérdida, divulgación, modificación o uso no autorizado de las llaves privadas en ellos.

6.1.3 Entrega de Llave Pública al Emisor del Certificado

Cuando una llave pública se transfiere a la CA emisora para ser certificada, debe ser entregada a través de un mecanismo que garantice que la llave pública no ha sido alterada durante el tránsito y que el Solicitante del Certificado posea la llave privada correspondiente a la llave pública transferida.

El mecanismo aceptable dentro de la E-SIGN CA, para la entrega de llave pública, es un mensaje de solicitud de firma de Certificado PKCS#10 o un método equivalente que garantice que:

- La llave pública no ha sido alterada durante el tránsito, y que
- El solicitante del Certificado posea la llave privada correspondiente a la llave pública transferida.

Los Asociados que realizan Ceremonias de Generación de Llaves transfieren la llave pública desde el módulo criptográfico en el que fue creada hacia el módulo criptográfico de la CA Superior (mismo módulo criptográfico si es PCA), incorporándola en una solicitud PKCS#10 firmada.

6.1.4 Entrega de Llave Pública de CA a Partes Confiadas

Las llaves públicas de las PCAs están incluidas en los Certificados raíz, por lo que un usuario de confianza que utilice protocolo S/MIME recibirá automáticamente, además del Certificado del Suscriptor, los Certificados (y por lo tanto las llaves públicas) de todas las CAs subordinadas a los correspondientes PCA.

6.1.5 Tamaños de Llave

Los pares de llaves deben ser de longitud suficiente para evitar que se descubra la llave privada del par de llaves utilizando criptoanálisis durante el período de la utilización esperada de dicho par de llaves.

El estándar E-SIGN CA para el mínimo tamaño de llaves es el uso de pares de llaves con robustez equivalente a lo que define RSA para 2048 bits en PCAs y CAs.

Para certificados para llaves de certificados de RAs y entidades finales con un tamaño mínimo equivalente en robustez a RSA 2048 bits.

E-Sign recomienda, para PCAs y CAs, el uso de un tamaño mínimo de llaves equivalente en robustez a ECC 256 bit.

La norma E-SIGN CA para el algoritmo de hash de firma digital es SHA-1 o SHA-2.

6.1.6 Generación y Verificación de Calidad de Parámetros de Llave Pública

Los partícipes de E-SIGN CA que utilizan el Estándar de Firma Digital deberán generar los parámetros de llave requeridos en conformidad con el estándar FIPS 186-2 o una norma equivalente - aprobada por PMA.

Cuando los partícipes de E-SIGN CA utilicen el Estándar de Firma Digital, la calidad de los parámetros de llave generados se deben verificar en conformidad con FIPS 186-2 o una norma equivalente - aprobada por PMA.

6.1.7 Propósitos de Uso de Llave (de acuerdo al campo X.509 v3 Campo Uso de la Llave {Usage Field})

Consultar Sección 7.1.2.1.

6.2 Protección de la Llave Privada y Controles de Ingeniería del Módulo Criptográfico

6.2.1 Estándares y Controles del Módulo Criptográfico

Las llaves privadas dentro de la E-SIGN CA deben estar protegidas con un sistema confiable, y los usuarios de llave privada deben tomar las precauciones necesarias para evitar la pérdida, divulgación, modificación o uso no autorizado de acuerdo con, las obligaciones contractuales y requisitos indicados en las políticas de confidencialidad de la seguridad, de esta CP. Los Suscriptores tienen la opción de proteger sus llaves privadas en una tarjeta inteligente o un token de hardware. E-Sign y los clientes de RA deben proteger los segmentos de llave privada en estos servidores utilizando un sistema de confianza.

Los Asociados deberán realizar todas las operaciones criptográficas de la CA en módulos criptográficos con un estándar mínimo de FIPS 140-1 nivel 3.

Las RA deberán realizar todas las operaciones criptográficas en un módulo criptográfico clasificado en FIPS 140-1 nivel 2.

Los requisitos para calificaciones en esta sección están sujetos a los requisitos locales aplicables a calificaciones más elevadas.

6.2.2 Control de Llave Privada (m de n) para Varias Personas

El Control Multi Personal se aplica para proteger los datos de activación necesarios para que los Asociados puedan activar las llaves privadas de CA siguiendo las normas documentadas en las políticas confidenciales de seguridad de la E-SIGN CA. Los Asociados utilizan un procedimiento llamado "Compartición de Secreto" para dividir la llave privada o los datos de activación necesarios para operar la llave privada, en partes separadas llamadas "Secretos Compartidos" que quedan a cargo de individuos llamados "Shareholders", custodiadas en cajas de seguridad.

Los Asociados utilizan Compartición de Secreto para proteger los datos de activación necesarios para activar sus propias llaves privadas y otras CA dentro de sus respectivos subdominios de acuerdo con las normas documentadas en las políticas confidenciales de seguridad de la E-SIGN CA. Los Asociados también usan Compartición de Secreto para proteger los datos de activación necesarios para activar las llaves privadas ubicadas en sus respectivos sitios de recuperación de desastres.

El número mínimo de partes separadas necesarias para firmar un Certificado de CA es 2.Cabe señalar que el número de comparticiones distribuidas para tokens de recuperación de desastres puede ser menor que el número distribuido para tokens operacionales, mientras que el número mínimo de comparticiones necesarias sigue siendo el mismo.

6.2.3 Custodia de la Llave Privada

Las llaves privadas de la CA no son custodiadas. La Custodia de las llaves privadas de Suscriptores se explica con más detalle en la Sección 4.12.

6.2.4 Copia de Seguridad de la Llave Privada

Las CAs deben custodiar sus propias llaves privadas con el fin de ser capaz de recuperarse de desastres y daños en el equipamiento de acuerdo con las normas documentadas en las políticas confidenciales de Seguridad de la E-SIGN CA.

Los Asociados deben a su vez tener copia de seguridad de las llaves privadas de las CA dentro de sus subdominios.

Las copias de seguridad se deben realizar de acuerdo con estas políticas y procedimientos documentados.

Las copias de seguridad se harán mediante la copia de las llaves privadas e ingresándolas cifradas en medios de almacenamiento, de acuerdo con lo indicado en la Sección 6.2.6 y 6.2.7.

Las llaves privadas respaldadas deben ser protegidas de la modificación o divulgación no autorizados a través de medios físicos o medios de encriptación.

Las copias de seguridad deben estar protegidas con un nivel de protección física y de cifrado igual o superior a la de los módulos criptográficos en el sitio de la CA, tal como en un sitio de

recuperación ante desastres o en cualquier otro sitio externo seguro, tal como una caja fuerte de un banco.

La copia de seguridad de llaves privadas de usuario final Suscriptor sujetas a los de Servicios del Administrador de Llaves de sesión, se rige por lo indicado en la Sección 4.12.

6.2.5 Archivo de Llaves privadas

Al momento de expiración de un Certificado de CA E-SIGN CA, el par de llaves asociadas con el Certificado será retenido en forma segura por un período de al menos 5 años utilizando módulos de hardware criptográfico que cumple los requisitos de esta CP.

Estos pares de llaves de CA no se utilizarán para los eventos de firma después de la fecha de vencimiento del correspondiente Certificado de CA, a menos que el Certificado de CA haya sido renovado en los términos que se expresan en esta CP.

6.2.6 Transferencia de la Llave Privada hacia o desde un Módulo Criptográfico

El ingreso de una llave privada a un módulo criptográfico deberá usar mecanismos para prevenir la pérdida, robo, modificación, revelación no autorizada o uso no autorizado de dicha llave privada.

Los Asociados, que generan llaves privadas de CA o RA en un módulo de hardware criptográfico y las transfieran a otro de forma segura, deberán hacer la transferencia en forma segura al segundo módulo criptográfico, tomando todas las medidas necesaria para evitar la pérdida, robo, modificación, revelación no autorizada o uso no autorizado de tales llaves privadas. Tales transferencias estarán limitadas a realizar copias de seguridad de las llaves privadas en tokens de acuerdo con las normas documentadas en las políticas confidenciales de seguridad de la E-SIGN CA. Las llaves privadas deberán ser cifradas durante la transferencia.

Los participantes E-SIGN CA que pre-generen llaves privadas y transfieran las mismas a un token de hardware, por ejemplo, al transferir llaves privadas generadas de un usuario final Suscriptor en una tarjeta inteligente, deberán transferir en forma segura tales llaves privadas al token en la medida necesaria de tal forma de evitar pérdida, robo, modificación, la divulgación no autorizada o uso no autorizado de tales llaves privadas.

6.2.7 Almacenamiento de la Llave Privada en el Módulo Criptográfico

Las llaves privadas de CAs o RAs deben almacenarse en forma encriptada en los módulos de hardware criptográfico.

6.2.8 Método de Activación de la Llave Privada

Todos los participantes E-SIGN CA deberán proteger los datos de activación de sus llaves privadas contra pérdida, robo, modificación, divulgación no autorizada o uso no autorizado.

6.2.8.1 Certificados de Class 1

El estándar E-SIGN CA para la protección de llave privada de Class 1 para los Suscriptores es que adopten medidas comercialmente razonables de tal forma de proteger físicamente la estación de

trabajo del Suscriptor y así prevenir el uso de la estación de trabajo y su llave privada asociada sin la autorización previa del Suscriptor.

Además, E-Sign recomienda que los Suscriptores usen una contraseña, de acuerdo con la Sección 6.4.1 o seguridad equivalente para autentificar al Suscriptor antes de la activación de la llave privada, lo que incluye, por ejemplo, una contraseña para operar la llave privada, un equipo con inicio de sesión Windows o contraseña del protector de pantalla, o una contraseña de inicio de sesión de red.

6.2.8.2 Certificados de Class 2

El estándar E-SIGN CA para la protección de la llave privada de Class 2 para Suscriptores es:

- Utilice una contraseña de acuerdo con la Sección 6.4.1 o la seguridad equivalente para autentificar al Suscriptor antes de la activación de la llave privada, lo por ejemplo incluye, una contraseña para operar la llave privada, o un logon de Windows o una contraseña de protector de pantalla; y
- Tomar las medidas comercialmente razonables para la protección física de la estación de trabajo del Suscriptor de tal forma de prevenir el uso de la estación de trabajo y su llave privada asociada sin la autorización del Suscriptor.

Cuando estén desactivadas, las llaves privadas se mantendrán en forma encriptada.

6.2.8.3 Certificados de Class 3 que no sean Certificados de Administrador

El estándar E-SIGN CA para la protección de llave privada de Class 3 (que no sea de administrador) es para que los Suscriptores:

- Utilicen una tarjeta inteligente, un dispositivo de acceso biométrico, o seguridad equivalente para autentificar al Suscriptor antes de la activación de la llave privada, y
- Tomen las medidas comercialmente razonables que permitan, la protección física de la estación de trabajo del Suscriptor y prevenir el uso de la estación de trabajo y su llave privada asociada sin la autorización del Suscriptor.
- Se recomienda el uso de una contraseña, junto con una tarjeta inteligente u otro dispositivo de acceso biométrico, de acuerdo con la Sección 6.4.1.

Cuando estén desactivadas, las llaves privadas se mantendrán en forma encriptada.

6.2.8.4 Llaves Privadas de Administrador (Class 3)

El estándar E-SIGN CA para la protección de llave privada de Administrador les obliga a:

- Utilizar una tarjeta inteligente, un dispositivo de acceso biométrico, contraseña de acuerdo con la sección 6.4.1, o seguridad equivalente para autentificar al administrador antes de la activación de la llave privada, que por ejemplo incluyen, una contraseña para operar la llave privada, un inicio de sesión o contraseña de protector de pantalla, o una contraseña de inicio de sesión de red, y
- Tomar las medidas comercialmente razonables para la protección física de la estación de trabajo del administrador para evitar el uso de la estación de trabajo y su llave privada asociada sin la autorización del administrador.

E-Sign recomienda a los administradores utilizar una tarjeta inteligente, un dispositivo de acceso biométrico, o seguridad equivalente, junto con el uso de una contraseña, de acuerdo con la Sección 6.4.1, y así autenticar al administrador antes de la activación de la llave privada.

Cuando estén desactivadas, las llaves privadas se mantendrán en forma encriptada.

6.2.8.5 RAs que utilicen Módulo Criptográfico (con Administrador de Servicios de Llave de sesión)

El estándar E-SIGN CA para la protección de llaves privadas de administradores que utilizan módulo criptográfico requiere que:

- Use el módulo criptográfico con una contraseña, de acuerdo con la Sección 6.4.1, para autenticar al administrador antes de la activación de la llave privada, y
- Adoptar las medidas comercialmente razonables para la protección física del lugar en que se encuentra el lector del módulo criptográfico, y así prevenir el uso de la estación de trabajo y la llave privada asociada con el módulo criptográfico sin la autorización del administrador.

6.2.8.6 Llaves Privadas que poseen los Asociados (Class 1-3)

La Llave privada de una CA en línea debe ser activada por un número mínimo de Participantes (Shareholders), tal como se define en la sección 6.2.2, que suministren sus datos de activación (almacenados en medios seguros).

Una vez que la llave privada está activada, la llave privada puede estar activa por un período indefinido hasta que se desactiva cuando el CA se va fuera de línea.

Del mismo modo, un número mínimo de Participantes (Shareholders) estarán obligados a suministrar sus datos de activación para activar la llave privada de una CA fuera de línea. Una vez que la llave privada está activada, se activa sólo por un tiempo.

6.2.9 Método de Desactivación de la Llave Privada

Los Suscriptores usuarios finales Class 3, tienen la obligación de proteger sus llaves privadas.

Estas obligaciones se extienden a la protección de la llave privada después que una operación llave privada haya tenido lugar.

La llave privada se puede desactivar después de cada operación, al cerrar la sesión en su sistema, o después del retiro de la tarjeta inteligente del lector de tarjetas inteligentes en función del mecanismo de autenticación utilizado por el usuario

Cuando una CA en línea es desconectada, el personal debe remover el token que contiene la llave privada de CA del lector con el fin de desactivarlo.

Con respecto a las llaves privadas de las CA fuera de línea, después realizar la Ceremonia de Generación de Llaves, en el que tales llaves privadas se utilizan para operaciones de llave privada, el personal debe remover el token que contiene las llaves privadas de CA desde el lector para desactivarlas.

Una vez retirado del lector, los tokens deben ser protegidos en forma segura.

6.2.10 Método de Destrucción de la Llave Privada

Cuando sea necesario, las llaves privadas de la CA son destruidas de una manera que razonablemente se asegure de que no hay restos de la llave que pudieran conducir a la reconstrucción de esta.

El personal de la CA desactiva la llave privada de la CA borrándola utilizando funcionalidad del token que contiene dicha llave privada de CA a fin de evitar su posible recuperación, todo esto mientras no se afecten negativamente el contenido de otras llaves privadas de CAs contenidas en el token.

Este proceso será atestiguado de acuerdo con las normas documentadas en las políticas de seguridad confidenciales de la E-SIGN CA.

6.2.11 Calificación Módulo Criptográfico

Véase la sección 6.2.1

6.3 Otros aspectos de la Gestión del Par de Llaves

6.3.1 Archivo de Llaves Públicas

La CA deberá archivar sus propias llaves públicas, así como las llaves públicas de todas las CAs dentro de sus sub-dominios, de acuerdo a lo indicado en la sección 5.5.

6.3.2 Período Operacional de Certificados y Períodos de Uso del Par de Llaves

El período operacional de los Certificados se fijará de acuerdo con los plazos establecidos en la tabla 4 siguiente. Los Certificados de Suscriptor que son renovaciones de Certificados de Suscriptor ya existentes pueden tener un período de validez más largo (hasta 3 meses). El periodo de uso del par de llave de Suscriptor es el mismo que el período de validez de sus Certificados, con la salvedad de que las llaves privadas puedan seguir siendo utilizadas después del período de funcionamiento para el descifrado y verificación de firmas. El período operacional de un Certificado finaliza a su vencimiento o revocación. Una CA no emitirá Certificados si sus períodos de funcionamiento se extienden más allá del periodo de uso del par de llaves de la CA. Por lo tanto, el período de uso del par de llaves de CA es necesariamente más corto que el período de validez del Certificado de CA.

En concreto, el periodo de uso es igual al período de validez del Certificado de CA menos el período de validez de los Certificados emitidos por la CA.

Al final del periodo de uso para un Suscriptor o para un par de llaves de CA, el Suscriptor o CA a partir de entonces se deja de utilizar el par de llaves, a menos que la CA necesite firmar la información de revocación hasta el final del período de operación del último Certificado emitido.

Certificado emitido por:	*Período de validez*
PCA auto-firmada (1024 bits RSA)	Hasta 30 años
PCA auto-firmada (2048 bits RSA)	Hasta 50 años
PCA auto-firmada (256 bit ECC)	Hasta 30 años

PCA auto-firmada (384 bit ECC)	Hasta 30 años
PCA para CA intermedia offline	Generalmente 10 años, pero hasta 15 años después de la renovación
PCA para CA en línea	Por lo general 5 años, pero hasta 10 años después de la renovación
CA intermedia offline para CA en línea	Por lo general 5 años, pero hasta 10 años después de la renovación
CA en línea para suscriptor usuario final individual	Normalmente hasta 2 años, pero en las condiciones descritas a continuación, hasta 6 años en las condiciones descritas a continuación, sin opción de renovar o re codificación. Después de 6 años se requiere nuevo enrolamiento.
CA en línea para Suscriptor Entidad final Organizacional.	Normalmente hasta 3 años. NOTA: Los Certificados SSL pueden ser válidos por un máximo de 6 años. Como mínimo, el nombre completo de los Certificados SSL con una validez de más de 3 años se vuelve a verificar después de tres años desde la fecha de emisión del Certificado.

Tabla 4 – Períodos Operacionales de Certificados

Excepto como se indica en esta sección, los participantes E-SIGN CA deberán dejar de utilizar sus pares de llaves después del período de uso expirado.

Los Certificados emitidos por CAs para Suscriptores usuarios finales pueden tener Períodos Operacionales de más de dos años, hasta seis años, si se cumplen las siguientes condiciones:

- Protección del par de llaves de Suscriptor en relación con su entorno operativo para los Certificados de Organización, operación con un centro de datos protegido y para Certificados individuales, el par de llaves de suscriptor reside en un token de hardware, como una tarjeta inteligente,
- Los Suscriptores están obligados a someterse a los procedimientos, de re-autenticación por lo menos cada 3 años, de acuerdo a lo indicado en la Sección 3.2.3,
- Si un Suscriptor no puede completar con éxito la re-autenticación de acuerdo a los procedimientos previstos en la Sección 3.2.3 o no es capaz de demostrar la posesión de la llave privada cuando sea requerido, la CA automáticamente revocará el Certificado del Suscriptor.

Cualquier excepción con este procedimiento requiere la aprobación del PMA y debe ser documentado en la correspondiente CPS.

6.4 Datos de Activación

6.4.1 Generación e Instalación de Datos de Activación

Los participantes E-SIGN CA que generan e instalan datos de activación de sus llaves privadas deben utilizar métodos que protejan los datos de activación en la medida necesaria para evitar la

pérdida, robo, modificación, revelación no autorizada o uso no autorizado de tales llaves privadas.

En el caso en que sean utilizadas contraseñas como datos de activación, los Suscriptores deberán generar contraseñas que no sean fáciles de adivinar o de quebrar por ataques por diccionario. Los suscriptores de Class 3 pueden no necesitar la generación de datos de activación, por ejemplo, si utilizan dispositivos de acceso biométrico.

Los Asociados generan los datos de activación para sus propias llaves privadas de CA, y para las llaves privadas de las CAs y RAs dentro de sus sub-dominios, de acuerdo con los requisitos de Secreto Compartido de esta CP y los estándares documentados en las políticas de seguridad confidencial de la E-SIGN CA.

6.4.2 Protección de Datos de Activación

Los participantes E-SIGN CA deberán proteger los datos de activación de sus llaves privadas usando métodos de protección contra la pérdida, robo, modificación, revelación no autorizada o uso no autorizado de tales llaves privadas.

Los Suscriptores tendrán que proteger los datos de activación de sus llaves privadas, en la medida necesaria para evitar la pérdida, robo, modificación, revelación no autorizada o uso no autorizado de tales llaves privadas

Los Asociados deben utilizar Secreto Compartido, de acuerdo con esta CP y de acuerdo con los estándares documentados en las políticas de seguridad confidencial de la E-SIGN CA.

Los Asociados proporcionan los procedimientos y medios para permitir a las Personas Involucradas (Shareholders) a tomar las precauciones necesarias para evitar la pérdida, robo, modificación, divulgación no autorizada o uso no autorizado de los Secretos Compartidos que poseen.

Los Participantes (Shareholders) no deberán:

- Copiar, divulgar, o hacer disponible el Secreto Compartido a un tercero, o hacer cualquier uso no autorizado de el en absoluto, o
- revelar el estado de cualquier persona como Participante (Shareholder) a un tercero.

Los Secretos Compartidos y cualquier información revelada a los Participantes (Shareholders) en relación con sus funciones como Participanteconstituyen información confidencial y privada.

6.4.3 Otros Aspectos de los Datos de Activación

6.4.3.1 Transmisión de Datos de Activación

En la medida en que los datos de activación de llaves privadas se transmitan, los participantes E-SIGN CA deberán proteger la transmisión utilizando los métodos que permitan protegen contra la pérdida, robo, modificación, revelación no autorizada o uso no autorizado de tales llaves privadas.

En la medida en que se utilice una combinación, nombre de usuario / contraseña para inicio de sesión en Windows o en red como datos de activación de un Suscriptor, las contraseñas transferidas a través de la red deben estar protegidas contra el acceso de usuarios no autorizados.

6.4.3.2 Destrucción de los Datos de Activación

Los datos de activación de las llaves privadas de la CA serán retirados del servicio utilizando métodos que protegen contra la pérdida, robo, modificación, divulgación no autorizada o uso no autorizado de las llaves privadas protegidas por los datos de dicha activación.

Después de los períodos de retención de registros indicados en la sección 5.5.2 , los Asociados de datos deberán desactivar los datos de activación a través de sobre-escritura y/o destrucción física.

6.5 Controles de Seguridad Informática

Las funciones de CAs y RAs tienen lugar en Sistemas Confiables, de acuerdo con las normas documentadas en las políticas de seguridad confidenciales de la E-SIGN CA (en el caso de E-Sign y sus Asociados).

6.5.1 Requerimientos Técnicos Específicos de Seguridad Computacional

Los Asociados se asegurarán de que los sistemas de mantenimiento de software de la CA y archivos de datos son sistemas Confiables y seguros al acceso no autorizado, lo que puede ser demostrado por el cumplimiento de los criterios de auditoría aplicables en virtud de Sección 5.4.1.

Además, los Asociados deben limitar el acceso a servidores de producción a aquellos individuos con una razón de negocios válida. Los usuarios de aplicaciones generales no tienen cuentas en los servidores de producción.

Los Asociados deberán tener redes de producción separadas lógicamente de otros componentes.

Esta separación previene el acceso a la red, excepto a través de procesos de aplicación definida. Los Asociados deben utilizar cortafuegos para proteger la red de intrusión interna y externa y limitar la naturaleza y fuente de actividades de red que pudieran acceder a los sistemas de producción.

Los Asociados deben requerir el uso de contraseñas con una longitud mínima de caracteres y una combinación de caracteres alfanuméricos y especiales, y deberán requerir que las contraseñas cambien en forma periódica y cuando sea necesario. El acceso directo a bases de datos de mantenimiento del repositorio se limitará a personas de confianza del grupo de Operaciones que tengan una razón válida para dicho acceso.

Las RAs deberán asegurar que los sistemas de mantenimiento del software y de archivos de datos de la RA son sistemas Confiables y seguros contra el acceso no autorizado, lo que debe ser demostrado por el cumplimiento de los criterios de auditoría aplicables en virtud de Sección 5.4.1.

Las RAs deberán separar lógicamente el acceso a estos sistemas e información, de cualquier otro componente. Esta separación impedirá el acceso excepto a través de procesos definidos. Las RAs deberán utilizar cortafuegos para proteger la red contra la intrusión interna y externa y limitar la naturaleza y la fuente de actividades que puedan acceder a estos sistemas e información. Las RAs deberán requerir la utilización de contraseñas con una longitud mínima de caracteres y una

combinación de caracteres alfanuméricos y especiales, y deberán requerir que las contraseñas sean cambiadas en forma periódica y cuando sea necesario. El acceso directo a las bases de datos que mantienen información de Suscriptores deberá ser limitada a Personas de Confianza del grupo de operaciones de la RA en la medida en que tengan una razón válida para dicho acceso.

6.5.2 Calificación de Seguridad Informática

Las áreas específicas de seguridad sensible, de la funcionalidad de la CA y RA de software suministrado por E-Sign deberá cumplir con requisitos de garantía y seguridad.

6.6 Controles Técnicos del Ciclo de Vida

6.6.1 Control de Desarrollo de Sistemas

El software de funcionalidad CA y RA, utilizado para gestionar los Certificados de Class 2 o 3, se debe desarrollar dentro de un entorno de desarrollo de sistemas que satisfagan los requerimientos de desarrollo seguro de E-Sign. E-Sign utilizará un proceso de diseño y desarrollo que exige el aseguramiento de calidad y la corrección del proceso.

El software proporcionado por E-Sign, cuando se carga por primera vez, deberá proporcionar un método para que la entidad pueda verificar que el software en el sistema:

- se originó a partir de E-Sign,
- no ha sido modificado antes de la instalación, y
- es la versión utilizable

6.6.2 Administración de Controles de Seguridad

El software para funcionalidades de CAs y RAs diseñado para administrar los Certificados de Class 2 o 3 será sometido a controles para verificar su integridad. Los Asociados deben contar con mecanismos y/o políticas para controlar y supervisar la configuración de sus sistemas de CA. Tras la instalación, y por lo menos una vez al día, los Asociados deberán validar la integridad del sistema de CA.

6.6.3 Controles de Seguridad del Ciclo de Vida

Ninguna estipulación

6.7 Controles de Seguridad de la Red

Las funciones para CA y RA se realizan en redes seguras de acuerdo con las normas documentadas en las políticas de seguridad confidencial de la E-SIGN CA, de forma tal de evitar el acceso no autorizado, alteración, y ataques de denegación de servicio. Las comunicaciones de información sensible serán protegidas mediante encriptación punto a punto para la confidencialidad y firmas digitales para el no repudio y autenticación.

6.8 Sellado de Tiempo

Los certificados, CRLs y otros registros de la base de revocación deberán contener información de fecha y hora. Tal Información de tiempo no necesita tener base criptográfica.

7 Perfiles de Certificado, CRL y OCSP

7.1 Perfil de Certificado

Los Certificados E-SIGN CA generalmente se ajustan a (a) ITU-T Recommendation X.509 (1997): Information Technology – Open Systems Interconnection – The Directory Authentication Framework, June 1997 y (b) RFC 5280: Internet X.509 Public Key Infrastructure Certificate y CRL Profile, April 2002 ("RFC 5280").

Como mínimo, los Certificados X.509 de E-SIGN CA deberán contener los campos básicos y los valores prescritos o las limitaciones de valor en la tabla 5 siguiente:

Campo	*El valor o la restricción de valor*
Número de serie	Valor único por DN Emisor
Algoritmo de firma	Identificador de objeto del algoritmo utilizado para firmar el Certificado (ver CP § 7.1.3)
Emisor DN	Vea la Sección 7.1.4
Válido desde	Base de Tiempo Coordinado Universal. Sincronizado con un reloj atómico. Codificado de acuerdo con la RFC 5280.
Válido hasta	Base de Tiempo Coordinado Universal. Sincronizado con un reloj atómico. Codificado de acuerdo con la RFC 5280.
Asunto DN (Subject)	Ver CP § 7.1.4
Asunto Llave Pública (Subject Public Key)	Codificados de acuerdo con RFC 5280
Firma	Generado y codificado de acuerdo con RFC 5280

Tabla 5 - Campos del Perfil Básico de Certificado

7.1.1 Número (s) de Versión

Los certificados de E-SIGN CA serán Certificados X.509 Versión 3 Los certificados de CA serán Certificados X.509 versión 3. Los certificados de Suscriptor usuario final deberán ser Certificados X.509 Versión 3.

7.1.2 Extensiones de Certificado

Los Asociados deberán poblar los Certificados X.509 Versión 3 con las extensiones requeridas por la Sección 7.1.2.1-7.1.2.8. Las extensiones privadas son permitidas, pero el uso de una extensión privada (s) no se justifica en virtud de esta CP y CPS salvo que se incluyan específicamente como referencia.

7.1.2.1 Utilización de Llaves

Los certificados X.509 Versión 3 son generalmente poblados de acuerdo con RFC 5280: Internet X.509 Public Key Infrastructure and CRL Profile, Abril de 2002. El campo criticidad de la extensión KeyUsage generalmente se establece en FALSE para certificados de Suscriptor entidad final, pero, en TRUE para los Certificados de CA.

Nota: El bit de No Repudio no requiere estar encendido en estos Certificados porque la industria PKI todavía no ha llegado a un consenso en cuanto a lo que el bit de No Repudio significa.

Hasta que no exista un consenso al respecto, el bit de No Repudio, no será significativo para las Partes que Confían. Por otra parte, la mayoría de las aplicaciones de uso común no siempre respetan el bit de No Repudio. Por lo tanto, encender el bit no ayuda a las Partes que Confían a tomar una decisión de confianza. En consecuencia, esta CP no requiere que el bit de No Repudio sea encendido. Puede estar encendido en el caso de Certificados de firma con par de llaves dual emitidos a través de Administrador de Llave de sesión, o por requerimiento. Cualquier controversia relativa al no repudio derivado de la utilización de un Certificado digital es un asunto exclusivo entre el Suscriptor y los Terceros que Confían. E-Sign no incurrirá en responsabilidad en relación con ello.

7.1.2.2 Extensión de Políticas de Certificado

La Extensión de Políticas de Certificado de Certificados X.509 Versión 3 se completa con el identificador de esta CP, de conformidad con la Sección 7.1.6 y con calificadores de políticas establecidos en la Sección 7.1.8. El campo de criticidad de esta extensión se establece en FALSO.

7.1.2.3 Nombres Alternativos del Sujeto

La extensión subjectAltName de Certificados X.509 Versión 3 son poblados de acuerdo con RFC 5280. El campo de criticidad de esta extensión se establece en FALSO.

7.1.2.4 Restricciones Básicas

La extensión BasicConstrains de los Certificados X.509 versión 3 de CA tendrá el campo CA establecido con valor VERDADERO. La extensión BasicConstrains de los Certificados de Suscriptor Final, tendrá el campo CA establecido con valor FALSO. El campo de criticidad de esta extensión se establece en VERDADEROpara los Certificados de CA, pero para los demás se establece en FALSO.

Los Certificados X.509 Versión 3 CA deben tener un campo "pathLenConstraint" de la extensión BasicConstraints indicando el número máximo de Certificados de CA que pueden seguir a este Certificado en una ruta de certificación. Los Certificados de CA que emite Certificados de Suscriptor usuario final deberán tener un campo "pathLenConstraint" con valor en "0". Esto indica que sólo un Certificado de Suscriptor usuario final puede seguir en la ruta de certificación.

7.1.2.5 Uso de Llave Extendida

Por defecto, ExtendedKeyUsage se establece como una extensión no críticas. Los Certificados E-SIGN CA de CA no incluyen la extensión ExtendedKeyUsage.

	Certificados de cliente Class 1-3, Certificados RA expedidos a Administración Automatizada de Tokens, y Certificados Organizacionales ASB Class 3	Certificados Organizacionales de Objeto de Firma Class 3	Otros Certificados Organizacionales Class 3 (por ejemplo, IDs de Servidor Seguro y IDs Servidor Global)
ServerAuth (1.3.6.1.5.5.7.3.1)	No está incluido	No está incluido	Incluido
ClientAuth (1.3.6.1.5.5.7.3.2)	Incluido	No está incluido	Incluido
CodeSigning (1.3.6.1.5.5.7.3.3)	No está incluido	Incluido	No está incluido
EmailProtection (1.3.6.1.5.5.7.3.4)	Incluido	No está incluido	No está incluido
TimeStamping (1.3.6.1.5.5.7.3.8)	No está incluido	No está incluido	No está incluido

Tabla 7 - Tipos de Propósitos Clave incluidos en la extensión ExtendedKeyUsage

7.1.2.6 Puntos de Distribución de CRL

Los Certificados de E-SIGN CA X.509 Versión 3 se completan con una extensión de cRLDistributionPoints conteniendo la dirección URL de la ubicación donde una Parte que Confía puede obtener una CRL para comprobar el estado del Certificado. El campo criticidad de esta extensión se establece en FALSO.

7.1.2.7 Identificador de la Llave de Autoridad

Los Certificados E-SIGN CA X.509 Versión 3 son generalmente poblados con una extensión authorityKeyIdentifier. El valor de keyIdentifier estará basado en la llave pública de la entidad emisora del Certificado y será calculado de acuerdo con uno de los métodos descritos en el RFC 5280. El campo de criticidad de esta extensión se establece en FALSO.

7.1.2.8 Identificador de la Llave del Sujeto

Si está presente en los Certificados E-SIGN CA X.509 Versión 3, el campo de criticidad de esta extensión se establece en FALSO y el valor de keyIdentifier estará basado en la llave pública del Sujeto del Certificado y será calculado de acuerdo con uno de los métodos descritos en la RFC 5280.

7.1.3 Identificadores de Objeto de Algoritmo

Los Certificados E-SIGN CA son firmados con uno de los siguientes algoritmos.

- ***sha256withRSAEncryption*** OBJECT IDENTIFIER:: = {iso (1) member-body (2) us (840) rsadsi (113549) pkcs (1) PKCS-1 (1) 11}
- ***ECDSA-con-SHA256*** OBJECT IDENTIFIER:: = {iso (1) member-body (2) us (840) ansi-X9-62 (10045) signatures (4) ECDSA-con-SHA2 (3) 2}
- ***ECDSA-con-SHA384*** OBJECT IDENTIFIER:: = {iso (1) member-body (2) us (840) ansi-X9-62 (10045) signatures (4) ECDSA-con-SHA2 (3) 3}
- ***sha-1WithRSAEncryption*** OBJECT IDENTIFIER:: = {iso (1) member-body (2) us (840) rsadsi (113549) pkcs (1) PKCS-1 (1) 5}
- ***md5WithRSAEncryption*** OBJECT IDENTIFIER:: = {iso (1) member-body (2) us (840) rsadsi (113549) pkcs (1) PKCS-1 (1) 4}

Las firmas de Certificado de producidas utilizando estos algoritmos deben cumplir con RFC 3279. En lugar de md5WithRSAEncryption se usa ya sea sha-1WithRSAEncryption o sha-256WithRSAEncryption .

Algunas CAs soportan el uso de algoritmo de cifrado SHA-256, SHA-384 y SHA-512 en los Certificados de Suscriptor entidad final.

7.1.4 Formas de Nombre

Los Certificados E-SIGN CA se completan con el nombre Issuer Name y Subject Distinguished Name requerido según está definido en la Sección 3.1.1. En cada Certificado emitido el nombre Issuer Name será poblado incluyendo los valores de campos Country, Organization Name y Common Name de la CA emisora. Además, los Certificados de Suscriptor usuario final por lo general incluyen adicionalmente un campo Organizational Unit que contiene un aviso indicando que las condiciones de uso del Certificado se establecen en una URL, y la URL es un puntero al Acuerdo del Tercero que Confía. Excepciones a la regla anterior se permitirán cuando las limitaciones de espacio, el formato, o la interoperabilidad dentro de Certificados hagan que tal campo Organizational Unit sea imposible de usar en conjunto con la aplicación para la cual los Certificados están destinados, o si el puntero a la parte correspondiente del Acuerdo del Tercero que Confía se incluye en la extensión de la política de certificación.

7.1.5 Restricciones de Nombres

Ninguna estipulación

7.1.6 Identificador de Objeto de Política de Certificado

El identificador de objeto de la política de Certificado correspondiente a cada clase de Certificado se establece en la Sección 1.2. La extensión CertificatePolicies de cada Certificado E-SIGN CA X.509 versión 3 está poblado de acuerdo con la Sección 1.2.

7.1.7 Uso de la Extensión Limitaciones de Política

Ninguna estipulación

7.1.8 Sintaxis y Semántica de Calificadores de Política

Los Certificados E-SIGN CA X.509 Versión 3 contienen un calificador de política dentro de la extensión Políticas de Certificados. Por lo general, dichos Certificados contienen un calificador del tipo puntero a CPS que apunta al Acuerdo de las Partes que Confían o a la CPS aplicables.

Además, algunos Certificados contienen un calificador Aviso de Usuario que apunta al Acuerdo de las Partes que Confían aplicable.

7.1.9 Semántica de Procesamiento para las Extensiones Críticas de Políticas de Certificado

Ninguna estipulación

7.2 Perfil de la CRL

Las CRL se ajustan a la RFC 5280 y contienen los campos básicos y contenidos especificados en la Tabla 8 a continuación:

Campo	El Valor o Restricción de Valor
Versión	Ver Sección 7.2.1.
Algoritmo de Firma	Algoritmo utilizado para firmar la CRL, de acuerdo con RFC 3279.(Ver CP § 7.1.3)
Emisor	Entidad que ha firmado y emitido la CRL.
Fecha de vigencia	Fecha de emisión de la CRL. Las CRLs son efectivas desde la emisión.
Próxima actualización	Fecha en la que la próxima CRL será publicada. Frecuencia de emisión de la CRL está de acuerdo con los requisitos de la Sección 4.9.7.
Certificados Revocados	Lista de Certificados revocados, incluyendo el Número de Serie del Certificado revocado y la Fecha de Revocación.

Tabla 8 - Campos básicos de la CRL

7.2.1 Número (s) de Versión

La E-SIGN CA soporta las CRLs X.509, tanto Versión 1 como Versión 2.

7.2.2 Extensiones de CRL y de Registros CRL

Ninguna estipulación

7.3 Perfil OCSP

OCSP (Online Certificate Status Protocol) es una forma de obtener información oportuna sobre el estado de revocación de un Certificado en particular. E-Sign valida:

- Certificados de Class 2 Enterprise utilizando el OCSP de Empresa que cumple con RFC 2560, y
- Certificados de Empresa Class 2 y Certificados Organizacionales Class 3 utilizando el protocolo E-SIGN, el cual cumple con RFC 5019.

7.3.1 Número(s) de Versión

La versión 1 de la especificación de OCSP según se define en RFC2560 y la versión 1 de las especificaciones de OCSP definidas por RFC 5019 son compatibles.

7.3.2 Extensiones OCSP

E-Sign no utiliza un hápax para establecer la vigencia actual de cada respuesta OCSP y los clientes no deben esperar un hápax en la respuesta a una solicitud que contenga un hápax. En lugar de ello, los clientes deben utilizar el reloj local para comprobar la vigencia de la respuesta.

8 Auditorías de Cumplimiento y Otras Evaluaciones

E-Sign y sus Asociados deben someterse a una auditoría de cumplimiento periódico ("Auditoría de Cumplimiento") para asegurar el cumplimiento con las Normas E-SIGN CA NET después de que comiencen las operaciones.

Además de estas auditorías de cumplimiento, E-Sign y sus Asociados empoderados para realizar otros exámenes e investigaciones para garantizar la confiabilidad de la E-SIGN CA NET E-SIGN CA NET, que incluyen, pero no se limitan a:

- Una "Revisión de Seguridad y Prácticas" del Asociado antes de que inicie sus operaciones. Una "Revisión de Seguridad y Prácticas" consiste en una revisión de la instalación segura del Asociado, de los documentos de seguridad, CPS, los acuerdos de E-SIGN CA NET relacionados con la política de privacidad, y los planes de validación para asegurarse de que el Asociado cumple con los Estándares E-SIGN CA NET.
- E-Sign tendrá el derecho, a su discreción única y exclusiva para llevar a cabo en cualquier momento una "Auditoria / Investigación Exigente" de sí misma, a un Asociado o a un Cliente Empresa en el caso que E-Sign tenga razón fundada para creer que la entidad fiscalizada no ha cumplido con las normas E-SIGN CA NET, ha experimentado un incidente o un compromiso, o ha actuado o dejado de actuar, de manera que el fracaso de la entidad auditada, el incidente o compromiso, o el acto u omisión de actuar constituyen una verdadera, o son una amenaza potencial para la seguridad o integridad de la E-SIGN CA NET E-SIGN CA NET.

E-Sign tendrá derecho a realizar "Revisiones Suplementarias de Administración de Riesgos" en sí misma, a un Asociado, o a un Cliente después de los resultados incompletos o excepcionales en una auditoría de cumplimiento, o como parte del proceso de administración de riesgos global en el curso ordinario del negocio.

E-Sign podrá delegar la realización de estas auditorías, revisiones e investigaciones a la Entidad Superior de la entidad que está siendo auditada, revisada, o investigada, o a una firma de auditoría de terceros. Las entidades que están sujetas a una auditoría, revisión o investigación, deberán prestar debida cooperación con E-Sign y el personal que realiza la auditoría, revisión o investigación.

8.1 Frecuencia y Circunstancias de la Evaluación

Las auditorías de cumplimiento se llevan a cabo al menos una vez al año con cargo exclusivo de la entidad auditada.

8.2 Identidad / Calificaciones del Asesor

Una firma de auditoría de terceros realizará las auditorías de cumplimiento de E-Sign y sus Asociados.

Las revisiones y auditorías realizadas por una firma de auditoría de terceros deberán ser realizadas por una firma contable pública Certificada con experiencia demostrada en seguridad informática o por profesionales de informática acreditados en seguridad empleados por una consultora de seguridad competente. Estas empresas, también deben haber demostrado pericia en el desempeño de la seguridad de TI y auditorías de cumplimiento PKI.

8.3 Relacionamiento del Asesor con Entidades Evaluadas

Las auditorías de cumplimiento realizadas por empresas de auditoría de terceros se llevarán a cabo por firmas independientes a la entidad auditada. Estas empresas no deben tener conflicto de intereses que obstaculicen su capacidad para realizar servicios de auditoría.

8.4 Temas Cubiertos por la Evaluación

Los temas de auditoría para cada categoría de entidad se exponen a continuación. La entidad auditada puede hacer de la auditoría de cumplimiento un módulo que forma parte de una auditoría anual global de los sistemas de información de la entidad.

Auditorías de RA (Class 1-2)

Se recomienda que los Clientes Empresa que aprueban Certificados de Class 1 y 2 se sometan a una auditoría de cumplimiento anual. A solicitud de E-Sign y / o una entidad superior (si la Entidad Superior no es de E-Sign), los Clientes Empresa deberán someterse a una auditoría señalando las excepciones o irregularidades a las políticas de E-SIGN CA NET y las medidas adoptadas para corregir las irregularidades.

Auditoría de RA (Class 3)

Se recomienda que los Clientes Empresa que autorizan la emisión de Certificados SSL Class 3 se sometan a una auditoría anual de cumplimiento de sus obligaciones. A solicitud de E-Sign y / o una entidad superior (si la Entidad Superior no es de E-Sign) los clientes de empresa se sometan a una auditoría señalando las excepciones o irregularidades a las políticas E-SIGN CA NET y las medidas adoptadas para corregir las irregularidades.

Auditoría de E-Sign o de un Asociado (Class 1-3)

E-Sign y cada Asociado serán auditados de conformidad con las directrices establecidas en el American Institute of Certificate Public Accounts Statement en la Auditing Standards (SAS) Numero 70, Informes sobre el Procesamiento de Transacciones por Organizaciones de Servicios. Sus auditorías de cumplimiento serán un estándar WebTrust para Autoridades Certificadoras o una norma equivalente de auditoría aprobada por E-Sign, que incluye: un informe de políticas y procedimientos de operación y prueba de la eficacia operativa.

8.5 Acciones Tomadas como Resultado de Deficiencias

Después de recibir el informe de auditoría de cumplimiento, la Entidad Superior de la entidad auditada se pondrá en contacto con el auditado para discutir excepciones o deficiencias demostradas por la Auditoría de Cumplimiento. E-Sign también tendrá derecho a discutir las excepciones o deficiencias de la parte auditada. La entidad auditada y la Entidad Superior deberán, de buena fe, hacer los esfuerzos comercialmente razonables para acordar un plan de acción correctiva de los problemas que causan las excepciones o deficiencias y para implementar el plan.

En caso de falla de la entidad auditada para desarrollar un plan de acciones correctivas o ponerlo en práctica, o si el informe revela excepciones o deficiencias que E-Sign y la Entidad Superior de la entidad auditada razonablemente suponen una amenaza inmediata para la seguridad o integridad de la E-SIGN CA NET E-SIGN CA NET, entonces:

(a) E-Sign y / o la Entidad Superior determinarán si son necesarios los reportes de revocación y compromiso,

(b) E-Sign y la Entidad Superior tendrán derecho a suspender los servicios a la entidad auditada, y

(c) Si es necesario, E-Sign y la Entidad Superior podrán dar por terminado, tales servicios sujetos a esta CP y los términos del contrato de la entidad auditada con su Entidad Superior

8.6 Comunicación de Resultados

Después de cualquier auditoría de cumplimiento, la entidad auditada deberá proporcionar a E-Sign y su entidad superior (si la Entidad Superior no es de E-Sign), el informe anual y los testimonios sobre la base de su auditoría o auto-auditoría dentro de los catorce (14) días después de la finalización de la auditoría y no más tarde de cuarenta y cinco (45) días después de la fecha aniversario del inicio de las operaciones.

9 Otros Asuntos y Materias Legales

9.1 Honorarios

9.1.1 Tarifas de Emisión de Certificado de Emisión o Renovación

E-Sign, Asociados y Clientes RA tienen derecho a cobrar al usuario final suscriptor por la emisión, gestión y renovación de Certificados.

9.1.2 Tarifas de Acceso a Certificados

E-Sign, Asociados y Clientes RA no podrá cobrar una tarifa como condición para tener un Certificado disponible en un repositorio.

9.1.3 Tarifas Acceso a Información de Revocaciones o Estado

E-Sign y sus Asociados no podrán cobrar una tarifa como condición para que la CRL requerida por esta CP este disponible en un repositorio para las partes que confían. Tendrán, sin embargo, derecho a cobrar una cuota por proporcionar CRL personalizada, servicios de OCSP, u otros servicios de información de revocaciones y estado. E-Sign y sus Asociados no permitirán el acceso a información de revocación, información de estado de Certificados o sellado de tiempo en sus repositorios por terceros que ofrecen productos o servicios que utilizan la información de estado de Certificados sin el consentimiento previo de E-Sign, consentimiento expreso y por escrito.

9.1.4 Tarifas de Otros Servicios

E-Sign y Asociados no cobran una cuota por el acceso a esta CP o de sus respectivas CPS. Cualquier uso que se haga para otros fines que la simple visualización del documento, como la reproducción, distribución, modificación o creación de trabajos derivados, estará sujeto a un contrato de licencia con la entidad titular de los derechos en el documento.

9.1.5 Política de Devoluciones

En la medida permitida por la ley aplicable, E-Sign, los Asociados y Resellers deberán implementar una política de reembolso. Publicarán sus políticas de reembolso dentro de sus sitios web (incluyendo una lista en sus repositorios), en sus acuerdos de Suscriptor y, en el caso de E-Sign y sus Asociados, en su CPS.

9.2 Responsabilidad Financiera

9.2.1 Cobertura de Seguros

E-Sign, Asociados y Clientes Empresa (cuando sea necesario) deberá mantener un nivel comercialmente razonables de cobertura de seguro por errores y omisiones, ya sea a través de un programa de errores y omisiones de seguros con una compañía de seguros o de una retención auto-asegurada. Este requisito de seguro no se aplica a las entidades gubernamentales.

9.2.2 Otros activos

E-Sign, Asociados y Clientes Empresa tendrán suficientes recursos financieros para mantener sus operaciones y cumplir con sus obligaciones, y deben ser razonablemente capaces de soportar el riesgo de responsabilidad a los Suscriptores y partes que confían.

9.2.3 Cobertura de Garantía Adicional

Algunos participantes E-SIGN CA NET ofrecen programas de garantía extendida a suscriptores de Certificados SSL y de code signing con protección contra la pérdida o daño que se deba a un defecto en la emisión del Certificado o malversación causada por negligencia del participante o de incumplimiento de sus obligaciones, siempre que el Suscriptor del Certificado haya cumplido con sus obligaciones en virtud del contrato de servicio aplicable. Participantes E-SIGN CA NET que ofrecen programas de garantía extendida están obligados a incluir la información del programa en su CPS.

9.3 Confidencialidad de la Información de Negocios

9.3.1 Alcance de la Información Confidencial

Los siguientes registros de Suscriptores, sujetos a la Sección 9.3.2, debe mantenerse en forma confidencial y privada:

- registros de suscripción CA, ya sea aprobados o rechazados,
- registros de Solicitud de Certificado,
- llaves privadas en manos de clientes RA que utilicen Managed PKI KEY Manager y la información necesaria para recuperar tales llaves privadas,
- Registros transaccionales (tanto registros completos, como las pistas de auditoría de las operaciones),
- registros de auditoría creados o retenidos por E-Sign, un Asociado, o un cliente,
- Reportes de auditoría creados por E-Sign, un Asociado, o un cliente (en la medida de esos informes se mantienen), o sus respectivos auditores (internos o públicos) , Planes de contingencia y los planes de recuperación de desastres, y
- Medidas de seguridad que controlen las operaciones de hardware de E-Sign o de Asociados y software y la administración de los servicios de Certificado y los servicios de enrolamiento.

9.3.2 Información no incluida en el Alcance de la Información Confidencial

Los participantes reconocen que los Certificados E-SIGN CA NET, la revocación de Certificados y otra información de estado, los repositorios de los participantes E-SIGN CA NET, y la información contenida en ellos no se consideran Información Confidencial Privada.

Información que no esté expresamente considerada Información Confidencial Privada bajo la Sección 9.3.1 no se considerarán confidenciales ni privados. Esta sección está sujeta a las leyes de privacidad aplicables.

9.3.3 Responsabilidad de Proteger la Información Confidencial

Participantes E-SIGN CA NET que reciben información privada la asegurarán de compromiso y de divulgación a terceros.

9.4 Confidencialidad de la Información Personal

9.4.1 Plan de Privacidad

E-Sign y Asociados desarrollarán una política de privacidad de acuerdo con las Guías de Requerimientos de Prácticas Legales. Estas políticas de privacidad se ajustarán a las leyes de privacidad locales. E-Sign y sus Asociados no podrá divulgar ni vender los nombres de los solicitantes de Certificados u otra información de identificación acerca de ellos, sujeto a la Sección 9.3.2.

9.4.2 Información Tratada como Privada

Cualquier información sobre los Suscriptores que no está disponible públicamente a través del contenido del Certificado emitido, el directorio de Certificados y la CRL en línea se trata como información privada.

9.4.3 La Información no Considerada Privada

Sujeto a las leyes locales, toda la información pública en un Certificado se considera no privado.

9.4.4 Responsabilidad de Protección de la Información Privada

Los participantes E-SIGN CA NET que reciban información privada deben asegurarla de compromiso y su divulgación a terceros y deberá cumplir con todas las leyes de privacidad locales de su jurisdicción.

9.4.5 Notificación y Consentimiento para el uso de Información Privada

A menos que se indique lo contrario en esta CP, la política de privacidad aplicable o por acuerdo, la información privada no será utilizada sin el consentimiento de la parte a quien aplica esta información. Esta sección está sujeta a las leyes de privacidad aplicables

9.4.6 Divulgación de Conformidad con el Procedimiento Judicial o Administrativo

Los participantes reconocen que la E-SIGN CA NET E-Sign y el Asociado tendrán derecho a conocer Información Confidencial / Privada si, de buena fe, E-Sign o el Asociado consideran que:

- la revelación es necesaria en respuesta a citaciones y órdenes de registro.
- la revelación es necesaria en respuesta a un proceso legal, judicial, administrativo u otra durante el proceso de descubrimiento en una acción civil o administrativa, tales como citaciones, interrogatorios, las solicitudes de admisión, y las solicitudes de presentación de documentos.

Esta sección está sujeta a las leyes de privacidad aplicables.

9.4.7 Otras circunstancias de divulgación de información

Las Políticas de privacidad deben contener disposiciones relativas a la divulgación de información confidencial / privado para la persona que está divulgando esta información a E-Sign o al Asociado. Esta sección está sujeta a las leyes de privacidad aplicables.

9.5 Derechos de Propiedad Intelectual

La asignación de derechos de propiedad intelectual entre los participantes que no sean Suscriptores E-SIGN CA NET y partes de confianza se regirá por los acuerdos aplicables entre los participantes como E-SIGN CA NET. Las siguientes subsecciones de la sección 9.5 aplican a los derechos de propiedad intelectual en relación a los Suscriptores y partes que confían.

9.5.1 Derechos de Propiedad en los Certificados e Información de Revocación

Las CAs retienen todos los derechos de propiedad intelectual en y de los Certificados y la información de revocación emitidos. E-Sign, los Asociados y Clientes otorgarán permiso para reproducir y distribuir Certificados en una modalidad no exclusiva sin costo de royalties, siempre que se reproduzcan en su totalidad y que el uso de Certificados este sujeto al Acuerdo de usuario de confianza que se hace referencia en el Certificado.

E-Sign, Asociados, y Clientes otorgarán permiso de uso de información de revocación para llevar a cabo funciones, sujetas al Acuerdo de Uso de CRL.

9.5.2 Derechos de Propiedad en la CP

Los participantes reconocen que la E-SIGN CA NET E-Sign se reserva todos los derechos de propiedad intelectual en y para esta CP.

9.5.3 Derechos de Propiedad en los Nombres

Un Solicitante de Certificado retiene todos los derechos que tiene (en su caso) de cualquier marca comercial, marca de servicio o nombres comerciales contenidos en cualquier Solicitud de Certificado y nombre distinguido dentro de cualquier Certificado emitido al solicitante de Certificado.

9.5.4 Derechos de propiedad en llaves y de material de llaves

Los pares de llaves correspondientes a los Certificados de CA y Suscriptores usuarios finales son propiedad de la CA y de los Suscriptores usuario final y que son los asuntos (Subjects) respectivos de estos Certificados, sujetos a los derechos de los Clientes Empresa que utilizan Managed PKI Key Manager, independiente del medio físico en el que están almacenados y protegidos. Sin limitar la generalidad de lo anterior, las llaves públicas raíz de E-Sign y los Certificados raíz que las contienen, incluyendo todas las llaves públicas y Certificados PCA auto-firmado, son propiedad de E-Sign. Las licencias de software E-Sign y fabricantes de hardware para reproducir dichos Certificados raíz, y poner copias en dispositivos de hardware o software de confianza. Por último, los Secretos Compartidos de la llave privada de CA son propiedad de la CA, y la CA se

reserva todos los derechos de propiedad intelectual en y hacia tales Secretos Compartidos a pesar de que no se puede obtener la posesión física.

9.6 Declaraciones y Garantías

9.6.1 Declaraciones y Garantías de la CA

E-SIGN CA NET CA garantiza que:

- No hay declaraciones falsas de hechos en el Certificado conocidas o procedentes de las entidades que aprueban la Solicitud de Certificado o emisión de los Certificados,
- No hay errores en la información contenida en el Certificado introducida por las entidades que dan la aprobación de la Solicitud de Certificado o emisión de los Certificados, como resultado de la falta de cuidado razonable en la gestión de la Solicitud de Certificado o la creación del Certificado,
- Sus Certificados cumplen todos los requisitos materiales de esta CP y la CPS respectiva, y
- los servicios de revocación y el uso de un repositorio se ajustan a todas las necesidades materiales de la CP y la CPS respectiva en todos los aspectos materiales.

Acuerdos con los Suscriptores pueden incluir representaciones y garantías adicionales

9.6.2 Declaraciones y Garantías de la RA

E-SIGN CA NET RA garantiza que:

- No hay declaraciones falsas de hechos en el Certificado conocidas o procedentes de las entidades que aprueban la Solicitud de Certificado o emisión de los Certificados,
- No hay errores en la información contenida en el Certificado introducida por las entidades que dan la aprobación de la Solicitud de Certificado o emisión de los Certificados, como resultado de la falta de cuidado razonable en la gestión de la Solicitud de Certificado o la creación del Certificado,
- Sus Certificados cumplen todos los requisitos materiales de esta CP y la CPS respectiva, y
- los servicios de revocación (cuando corresponda) y el uso de un repositorio se ajustan a todas las necesidades materiales de la CP y la CPS aplicable en todos los aspectos materiales.

Acuerdos con los Suscriptores pueden incluir representaciones y garantías adicionales

9.6.3 Declaraciones y Garantías del Suscriptor

Suscriptores garantizan que:

- Cada firma digital creada utilizando la llave privada correspondiente a la llave pública incluida en el Certificado es la firma digital del Suscriptor y el Certificado ha sido aceptado y está en funcionamiento (no caducado o revocado) en el momento de crear la firma digital,
- Su llave privada está protegida y que ninguna persona no autorizada ha tenido nunca acceso a la llave privada del Suscriptor,
- Todas las declaraciones hechas por el Suscriptor en la Solicitud de Certificado del Suscriptor suministrados son verdaderos,
- Toda la información suministrada por el Suscriptor y contenida en el Certificado es verdadera,

- El Certificado se utiliza exclusivamente para propósitos autorizados y legales, en consonancia con todos los requisitos materiales de la PC y la CPS aplicables, y
- El Suscriptor es un Suscriptor usuario final y no una CA, y no está usando la llave privada que corresponde a cualquier llave pública incluida en el Certificado a los efectos de la firma digital de cualquier Certificado (o cualquier otro formato de llave pública certificada) o CRL, como una entidad de certificación o de otra manera.

Acuerdos con los Suscriptores pueden incluir representaciones y garantías adicionales

9.6.4 Declaraciones y Garantías de los Terceros que Confían

Acuerdos de Partes que confían requieren Partes que Confían para reconocer que tienen la información suficiente para tomar una decisión informada en cuanto a en que eligen confiar de la información contenida en un Certificado, que son el único responsable de decidir si debe o no confiar en dicha información, y que asumirá las consecuencias legales del incumplimiento de las obligaciones en términos de este CP.

Los Acuerdos de las Partes que Confían podrán incluir representaciones y garantías adicionales.

9.6.5 Declaraciones y garantías de los demás participantes

No hay estipulación.

9.7 Exclusión de garantías

En la medida permitida por la legislación aplicable, los acuerdos de suscripción y Acuerdos de las Partes que Confían renuncian a garantías posibles de E-Sign y posibles del Asociado, incluyendo cualquier garantía de comercialización o aptitud para un propósito particular, fuera del contexto del Plan de Protección NetSure

9.8 Limitaciones de Responsabilidad

En la medida permitida por la legislación aplicable, los Acuerdos de Suscriptor y Acuerdos de partes que Confían limitarán a E-Sign y Asociados cuando aplique, la responsabilidad de E-Sign y sus Asociados quedará limitada a las siguientes cifras.

Clase	Protecciones de responsabilidad
Class 1	Cien Dólares EE.UU. ($ 100.00 EE.UU.)
Class 2	Mil Dólares EE.UU. ($ 1,000.00 EE.UU.)
Class 3	Diez Mil Dólares EE.UU. ($ 10,000.00 EE.UU.)

Tabla 9 – Protecciones de Responsabilidad

La responsabilidad (y / o limitación de la misma) de los Suscriptores serán los establecidos en la normativa Acuerdos de Suscriptor.

La responsabilidad (y / o limitación de la misma) de la empresa RA y la CA se establecerán en el acuerdo (s) entre ellos.

La responsabilidad (y / o limitación de la misma) de las partes que confían serán las establecidas en el Acuerdo de Partes que Confían.

9.9 Indemnizaciones

9.9.1 Indemnización por Suscriptores

En la medida permitida por la legislación vigente, los Suscriptores tienen la obligación de indemnizar a CAs o RAs (Tanto E-SIGN CA NET y no E-SIGN CA NET) por:

- Falsedad o tergiversación de los hechos del Suscriptor en la Solicitud del Certificado del Suscriptor
- Incumplimiento por parte del Suscriptor de revelar un hecho relevante en la Solicitud de Certificado, si la falsedad u omisión es consecuencia de negligencia o con intención de engañar a cualquiera de las partes,
- el fracaso del Suscriptor para proteger la llave privada, y de tomar precauciones necesarias para evitar perjuicios, la pérdida, divulgación, modificación o uso no autorizado de la llave privada del Suscriptor, o
- El uso del nombre del Suscriptor que infrinja los derechos de propiedad intelectual de un tercero.

El Acuerdo de Suscripción puede incluir nuevas obligaciones de indemnización

9.9.2 Indemnización por las Partes que Confían

En la medida permitida por la legislación vigente, el Acuerdo de las Partes que Confían debe requerir a las Partes que Confían compensaciones a la CA o RA (tanto E-SIGN CA NET y no E-SIGN CA NET) por:

- Las Parte que Confía fallan en cumplir las obligaciones de una de las Partes que Confían,
- Las Parte que Confían confía en un Certificado que no es razonable dadas las circunstancias, o
- Las Parte que Confía fallan en comprobar el estado de dicho Certificado para determinar si el Certificado ha caducado o revocado.

El Acuerdo de Partes que Confían pueden incluir nuevas obligaciones de indemnización.

9.10 Duración y Terminación

9.10.1 Plazo

La CP queda vigente luego de su publicación en el repositorio de E-SIGN. Las enmiendas a esta CP entrarán en vigencia tras su publicación en el repositorio de E-SIGN

9.10.2 Terminación

Esta CP modificada de vez en cuando permanecerá vigente hasta que sea reemplazado por una nueva versión.

9.10.3 Efecto de la Terminación y la Supervivencia

Al término de esta CP, los participantes E-SIGN CA NET son, sin embargo responsables por todos los Certificados emitidos por el resto de los períodos de validez de dichos Certificados.

9.11 Avisos individuales y Comunicaciones con los Participantes

A menos que se especifique lo contrario por acuerdo entre las partes, los participantes deberán utilizar métodos comercialmente razonables para comunicarse entre sí, teniendo en cuenta la cuestión de la criticidad y objeto de la comunicación.

9.12 Modificaciones

9.12.1 Procedimiento para la enmienda

Las enmiendas a esta CP pueden ser hechas por la Autoridad de Administración de la Política E-SIGN CA NET E-SIGN CA NET. Las modificaciones deben ser hechas o bien dentro de la forma de un documento que contenga una modificación de la CP o una actualización. Las versiones modificadas o actualizaciones estarán vinculadas a las actualizaciones de las prácticas y en la sección Avisos del Repositorio de E-SIGN que se encuentra en:

https:// www.ESIGN-LA.com.

9.12.2 Mecanismo de Notificación y Período

E-Sign y el PMA se reservan el derecho de modificar la CP sin notificación de modificaciones que no son materiales, incluyendo sin limitación las correcciones de errores tipográficos, cambios de direcciones URL, y los cambios en la información de contacto. La decisión del PMA de designar las enmiendas como materiales o inmateriales-son a sola discreción del PMA

El PMA enviará aviso de Asociados de las modificaciones materiales a la CP propuestas por el PMA. La notificación debe incluir el texto de las enmiendas propuestas y el plazo para comentarios. Las enmiendas propuestas a la CP deberán figurar también en las actualizaciones de prácticas y en la sección Avisos del Repositorio de E-SIGN que se encuentra en: *https:// www.ESIGN-LA.com*. Los Asociados deberán publicar o proporcionar un enlace a las enmiendas propuestas por su propia cuenta en los sitios web en que encuentran los repositorios en un plazo razonable después de recibir la notificación de tales enmiendas.

No obstante, cualquier disposición en la CP, si el PMA considera que las enmiendas materiales a la CP son necesarias de inmediato para detener o prevenir una violación de la seguridad de la E-SIGN CA NET E-SIGN CA NET o cualquier parte de ella, E-Sign y el PMA tendrán derecho a hacer tales modificaciones publicándolas en el repositorio de E-SIGN. Los cambios se harán efectivos inmediatamente después de su publicación.

En un plazo razonable después de la publicación, E-Sign deberá informar a los Asociados de tales enmiendas.

9.12.2.1 Período de Comentarios

Salvo que se indique lo contrario, el plazo para las enmiendas materiales a la CP será de quince (15) días, a partir de la fecha en que las modificaciones se publican en el repositorio de E-SIGN. Cualquier participante E-SIGN CA NET tendrá derecho a presentar sus comentarios al PMA hasta el final del período de comentarios.

9.12.2.2 Mecanismo de Tramitar las Observaciones

El PMA tendrá en cuenta los comentarios sobre las enmiendas propuestas. El PMA podrá optar por (a) permitir que las enmiendas propuestas entren en vigor sin modificaciones, (b) modificar las propuestas de enmienda y volver con una nueva modificación cuando sea necesario, o (c) retirar las enmiendas propuestas. El PMA tiene derecho a retirar las enmiendas propuestas notificando a los Asociados y dando aviso en la Sección Avisos de Actualizaciones de Prácticas en el repositorio de E-SIGN. A menos que las enmiendas propuestas sean modificadas o retiradas, entrarán en vigor a la expiración del período de comentarios.

9.12.3 Circunstancias en las que el OID debe ser Cambiado

Si el PMA determina que es necesario un cambio en el identificador de objeto que corresponde a una política de Certificados, la enmienda deberá contener los nuevos identificadores de objeto de las políticas de Certificados correspondientes a cada Clase de Certificado. De lo contrario, las enmiendas no requieren un cambio en el identificador de objeto de la política de Certificado.

9.13 Disposiciones de Resolución de Disputas

9.13.1 Las Disputas entre E-Sign, Asociados y Clientes

Las disputas entre uno o más de cualquier miembro E-Sign, Asociados y / o de Clientes se resolverán de conformidad con lo dispuesto en los acuerdos pertinentes entre las partes.

9.13.2 Conflictos con Suscriptores Usuarios Finales o Partes que Confían

En la medida permitida por la legislación vigente, los Acuerdos de Suscriptor y Acuerdos de Partes que Confían deberán contener una cláusula de resolución de conflictos. Los procedimientos en la Guía de Requerimientos Legales Prácticos de Asociado para solucionar controversias relativas E-Sign requieren un período de negociación inicial de sesenta (60) días, seguido de un litigio en el tribunal federal o estatal que abarca el Condado de Santa Clara, California, en el caso de los demandantes que son residentes de los EE.UU., o, en el caso de todos los demás demandantes, el arbitraje administrado por la Cámara de Comercio Internacional ("CPI"), de conformidad con el Reglamento de la CCI de Conciliación y Arbitraje, a menos que sea aprobado por E-Sign.

9.14 Legislación Aplicable

Sujeto a los límites que aparecen en la legislación vigente, las leyes del Estado de California, EE.UU., se aplicará a: la ejecución, la construcción, la interpretación y validez de esta CP, independientemente de su contrato o otra opción de las disposiciones de la ley y sin el requisito de establecer un nexo comercial en California, EE.UU.. Esta elección de la ley se hace para

asegurar la uniformidad de los procedimientos y la interpretación para todos los participantes E-SIGN CA NET, sin importar dónde se encuentren.

Esta disposición legal rige sólo a este CP. Los acuerdos de incorporación de la CP por referencia pueden tener sus propias disposiciones legales, previsto que esta Sección 9.14 regule la obligatoriedad, la construcción, la interpretación y validez de los términos de la CP por separado y aparte de las restantes disposiciones de estos acuerdos, con sujeción a las limitaciones que aparecen en la legislación aplicable.

Esta CP está sujeta a la aplicación de leyes nacionales, estatales, locales y extranjeras, normas, reglamentos, ordenanzas, decretos y órdenes, incluyendo pero no limitado a, las restricciones a la exportación o importación de software, hardware, o información técnica.

9.15 Cumplimiento con la Ley Vigente

Esta CP está sujeta a las leyes nacionales, estatales, locales y extranjeras, normas, reglamentos, ordenanzas, decretos y órdenes, incluyendo pero no limitado a, las restricciones a la exportación o importación de software, hardware, o información técnica.

9.16 Disposiciones Varias

9.16.1 Acuerdo Completo

No aplicable

9.16.2 Asignación

No aplicable

9.16.3 Divisibilidad

En el caso de que una cláusula o disposición de esta CP se considere inaplicable por un tribunal de justicia o tribunal que tenga autoridad, el resto de la CP seguirá siendo válida.

9.16.4 Aplicación (honorarios de abogado y renuncia de derechos)

No aplicable

9.16.5 Fuerza Mayor

En la medida de lo permitid por la legislación aplicable, los Acuerdos de Suscriptor y Acuerdos de Partes que Confían se deberá incluir una cláusula de fuerza mayor que de protección a E-Sign y el Asociado.

9.17 Otras Disposiciones

No aplicable

Apéndice A. Tabla de siglas y definiciones

Tabla de siglas

Plazo	Definición
ANSI	El American National Standards Institute.
ACS	Autenticado Signing.
BIS	Los Estados Unidos Oficina de Industria y Ciencia de los Estados Unidos Departamento de Comercio.
California	Autoridad Certificadora.
CP	Certificado de la póliza.
CPS	Declaración de Prácticas de Certificación.
CRL	La lista de revocación de Certificados.
EAL	Evaluación de nivel de seguridad (de conformidad con los criterios comunes).
FIPS	Estado Unidos Federal Information Processing Standards.
Corte Penal Internacional	Cámara de Comercio Internacional.
KRB	Bloque de recuperación de llaves.
LSVA	Evaluación de vulnerabilidad de la seguridad lógica.
OCSP	Certificado Protocolo línea de estado.
PCA	Autoridad Certificadora de Primaria.
PIN	Número de identificación personal.
PKCS	De llave pública estándar de criptografía.
PKI	Infraestructura de Llave Pública.
PMA	Política de Autoridad de Gestión.
RA	Autoridad de Registro.
RFC	Solicitud de comentarios.
SAR	Requerimientos de Auditoria de Seguridad
SAS	Declaración sobre Normas de Auditoría (promulgada por el Instituto Americano de Contadores Públicos Certificados).
S / MIME	Seguro Multipurpose Internet Mail Extensions.
SSL	Secure Sockets Layer.
E-SIGN CA NET	E-SIGN CA NET.

Definiciones

Plazo	Definición
Administrador	Una persona de confianza dentro de la organización, Cliente Empresa, o Cliente de puerta de enlace que realiza la validación y otras funciones de CA o RA.
Administrador Certificado	Todo Certificado expedido a un administrador que sólo podrá ser utilizada para realizar funciones de CA o RA.
Filial	Uno de los principales tercero de confianza, por ejemplo en la tecnología, las telecomunicaciones o la industria de servicios financieros, que ha llegado a un acuerdo con E-Sign para una distribución E-SIGN CA NET y el canal de servicios dentro de un territorio específico.
Asociado Legal Prácticas *Los requisitos de la Guía*	Un documento que establece los requisitos de E-Sign para CPSes Asociados, convenios, procedimientos de validación y políticas de privacidad, así como otros requisitos que los Asociados deben cumplir.
Particular Asociado	Una persona natural que se relaciona con un cliente administrado PKI, Managed PKI Lite del cliente, o la entidad al cliente de Gateway (i) como un funcionario, director, empleado, socio, contratista, interno, o cualquier otra persona dentro de la entidad, (ii) como un miembro de un E-Sign registró comunidad de intereses, o (iii) como una persona que mantiene una relación con la entidad donde la entidad tiene negocio u otros registros que ofrecen garantías adecuadas de la identidad de dicha persona.
Automatizado de Administración	Un procedimiento por el que se aprueban las Solicitudes de Certificados de forma automática si la información de inscripción coincide con la información contenida en una base de datos.

Automatizado de Administración ***Módulo de software***	Software proporcionado por E-Sign que lleva a cabo procedimientos de administración automatizada.
Certificado	Un mensaje que, al menos, según un nombre o identifica a la entidad emisora, identifica al Suscriptor, contiene la llave pública del Suscriptor, identifica el Período Operativo del Certificado, contiene un número de serie del Certificado y está firmado digitalmente por la CA.
Certificado del solicitante	Una persona u organización que solicite la emisión de un Certificado por una CA.
Solicitud de Certificado	A petición de un Solicitante de Certificado (o agente autorizado de la Solicitud de Certificado) a una CA la emisión de un Certificado.

Plazo	Definición
Certificado de Cadena de	Una lista ordenada de Certificados que contiene un Certificado de Suscriptor usuario final y Certificados de CA, el cual termina en un Certificado raíz.
Certificado de gestión de ***Objetivos de Control***	Criterios que debe cumplir una entidad para satisfacer una auditoría de cumplimiento.
Las políticas de certificación (CP)	Este documento, que lleva por título "Políticas de Certificado E-SIGN CA NET" y es la principal declaración de política que rige la E-SIGN CA NET.
La lista de revocación de Certificados ***(CRL)***	Un periódicamente (o exigently) publicó la lista, la firma digital de una CA, de los Certificados identificados que han sido revocados antes de su fecha de vencimiento de acuerdo con CP § 3.4. La lista generalmente indica el nombre del emisor de CRL, la fecha de emisión, la fecha de la emisión de CRL programada siguiente, los números de los Certificados revocados "de serie, y los tiempos específicos y las razones para la revocación.
Solicitud de Certificado de firma	Un mensaje de transmitir una petición para que un Certificado emitido.
Autoridad Certificadora (CA)	Una entidad autorizada para emitir, gestionar, revocar y renovar Certificados en la red E-SIGN CA NET.
Prácticas de Certificación ***Declaración (CPS)***	Una declaración de las prácticas que E-Sign o un Asociado emplea al aprobar o rechazar Solicitudes de Certificados y emitir, administrar y revocar Certificados, y exige a sus Clientes de Managed PKI y los Clientes de puerta de enlace a emplear.
Frase desafío	Una frase secreta elegida por un Solicitante de Certificado durante la inscripción de un Certificado. Cuando se emite un Certificado, el Solicitante del Certificado se convierte en un abonado y un CA o RA puede usar la Frase para autenticar al Suscriptor cuando el Suscriptor tiene por objeto revocar o renovar el Certificado del Suscriptor.
Clase	A nivel específico de garantías tal como se define en el PP. Ver CP § 1.1.1.
Auditoría de Cumplimiento	Una auditoría periódica a la RA, CA, Asociado, Cliente Empresa o puerta de enlace El Cliente será auditado para determinar su conformidad con las Normas E-SIGN CA NET que se le aplican.
Compromiso	Una violación (o supuesta violación) de una política de seguridad, en el que una divulgación no autorizada de la pérdida de control sobre la información pueden haber ocurrido. Con respecto a las llaves privadas, un compromiso es una pérdida, robo, divulgación, modificación, uso no autorizado, u otro compromiso de la seguridad de la llave privada.
Confidencial / Privada ***Información***	Información que debe ser confidencial y privada de conformidad con CP § 2.8.1.
Contrato de uso del CRL	Un acuerdo que establece los términos y condiciones en que puede ser una CRL o la información de lo que solía.
Cliente	Una organización que puede ser un cliente administrado PKI, el cliente de puerta de enlace, o al Cliente ASB.
Empresa, como en la empresa	Una línea de negocios que entra en un Asociado de proporcionar servicios de gestión de PKI a los Clientes de Managed PKI.

Centro de Servicio	
Certificado EV	Un Certificado digital que contenga la información especificada en las Directrices de VE y que ha sido validado en conformidad con las Directrices
Auditoría exigentes / Investigación	Una auditoría o investigación por parte de E-Sign en E-Sign razones para creer que la falta de una entidad para cumplir con las Normas E-SIGN CA NET, un incidente o un compromiso en relación con la entidad, o una amenaza real o potencial para la seguridad de la E-SIGN CA NET planteado por la entidad se ha producido.
Derechos de Propiedad Intelectual	Los derechos de uno o más de los siguientes: derechos de autor, patentes, secretos comerciales, marcas registradas y otros derechos de propiedad intelectual.
Intermedio de certificación *Autoridad (CA intermedia)*	Una Autoridad Certificadora, cuyo Certificado se encuentra dentro de una cadena de Certificados entre el Certificado de la CA raíz y el Certificado de la Autoridad Certificadora que emitió el Certificado del Suscriptor usuario final.
Ceremonia de Generación de Llaves	Un procedimiento por el que una CA o RA par de llaves se genera, su llave privada se transfiere a un módulo criptográfico, su llave privada es una copia de seguridad, y / o su llave pública certificada es.
Administrador de Key Manager	Un administrador que realiza las funciones de generación de llaves y recuperación de un cliente administrado PKI utilizando administrado Administrador PKI Key.
Bloque de recuperación de llaves (KRB)	Una estructura de datos que contiene la llave privada de un Suscriptor que estén cifrados con una llave de cifrado. KRBS se generan usando software Managed PKI Key Manager.
Servicio de recuperación de llaves	Un servicio de E-Sign que ofrece las llaves de cifrado necesario para recuperar un bloque de llave de recuperación como parte del uso de un cliente administrado de PKI de Managed PKI Gerente llave para recuperar la llave privada del Suscriptor.
Administrador de Managed PKI	Un administrador que realiza la validación y otras funciones RA de un cliente administrado PKI.
Managed PKI de control	Una interfaz basada en web que permite a los administradores de PKI administrada para realizar la autenticación manual de

Plazo	Definición
Centro	Las solicitudes de Certificados
Guía DEI	Un documento que establece los requisitos operacionales y prácticas para los Clientes de DEI con el Administrador de llaves DEI administrada.
Manual de autenticación	Un procedimiento mediante el cual las Solicitudes de Certificados son revisados y aprobados manualmente uno por uno por uno Administrador mediante una interfaz basada en web.
Plan de Protección NetSure	Un programa de garantía extendida, que se describe en la CP § 9.2.3.
No verificada del Suscriptor *Información*	Información presentada por un Solicitante de Certificado a una CA o RA, e incluida en un Certificado, que no ha sido confirmado por la CA o RA y para el cual aplica CA y RA no ofrecen garantías de que no sea que la información fue presentada por el Solicitante del Certificado .
No repudio	Un atributo de una comunicación que proporciona protección contra una parte en una comunicación negar falsamente su origen, negando que se haya presentado, o negar su entrega. La negación de origen incluye la negación de que la comunicación se originó de la misma fuente como una secuencia de uno o más mensajes anteriores, aun cuando la identidad asociada con el remitente es desconocido. Nota: sólo un fallo de un tribunal, panel arbitral, u otro tribunal en última instancia, puede evitar el repudio. Por ejemplo, una firma digital verificada con referencia a un Certificado E-SIGN CA NET puede proporcionar la prueba en apoyo de una determinación de no repudio por un tribunal, pero no constituye en sí misma no repudio.

CA sin conexión	E-SIGN CA NET PCA, CA emisoras de raíz y otros designados CA intermedias que se mantienen en línea por razones de seguridad con el fin de protegerlos de posibles ataques de intrusos a través de la red. Estas emisoras no directamente señal de fin de Certificados de Suscriptor usuario.
Línea CA	CA que firman Certificados de Suscriptor usuario final se mantienen en línea con el fin de brindar un servicio continuo de firma.
De estado de Certificados en línea ***Protocolo (OCSP)***	Un protocolo para proporcionar a las Partes Basándose en tiempo real la información de estado de Certificados.
Período de funcionamiento	La temporada comienza con la fecha y hora se emite un Certificado (o en una fecha posterior y hora confirmadas en el Certificado) y termina con la fecha y la hora en que dicho Certificado expira o se revoca prematuramente.
PKCS # 10	Criptografía de llave pública estándar # 10, desarrollado por RSA Security Inc., que define una estructura para una solicitud de firma de Certificados.
PKCS # 12	Criptografía de llave pública Norma # 12, desarrollado por RSA Security Inc., que define un medio seguro para la transferencia de las llaves privadas.
La política de gestión ***Autoridad (PMA)***	La organización dentro de E-Sign la responsabilidad de promulgar esta política a lo largo de la E-SIGN CA NET.
Certificación de primaria ***Autoridad (PCA)***	Una CA que actúa como una entidad de certificación raíz de una clase específica de los Certificados, y Certificados de entidades emisoras de Certificados a los problemas de ella dependientes.
Centro de Procesamiento de	Una organización (E-Sign o algunos Asociados) que crea una instalación de vivienda segura, entre otras cosas, los módulos criptográficos utilizados para la expedición de Certificados. En las líneas del Sitio Web del consumidor y de negocios, Asociados de actuar como entidades emisoras de Certificados dentro de la E-SIGN CA NET y realizar todos los servicios de ciclo de vida del Certificado de emisión, manejo, revocación y renovación de Certificados.
Infraestructura de Llave Pública ***(PKI)***	La arquitectura, organización, técnicas, prácticas y procedimientos que, en conjunto apoyar la implementación y operación de un sistema basado en Certificados criptográfico de llave pública. La PKI E-SIGN CA NET consiste en sistemas que colaboran para proporcionar e implementar la E-SIGN CA NET.
Autoridad de Registro (RA)	Una entidad aprobada por una CA para asistir a los Solicitantes de Certificados en la solicitud de Certificados y aprobar o rechazar Solicitudes de Certificados, revocar Certificados o renovar Certificados.
Tercera Parte Confiada	Una persona u organización que actúa confiando en un Certificado y / o una firma digital.
Parte Confiada Acuerdo	Un acuerdo utilizado por una entidad de certificación que establece los términos y condiciones en que actúa un individuo o una organización como un usuario de confianza.
Distribuidor	Una entidad de servicios de marketing en nombre de E-Sign o de un Asociado a mercados específicos.
Certificado de venta al por menor	Un Certificado emitido por E-Sign o un Asociado, que actúa como CA, a los individuos o las organizaciones que aplican una a una a E-Sign o de un Asociado en su sitio web.
RSA	Un sistema criptográfico de llave pública inventado por Rivest, Shamir y Adelman.
RSA Secure Server CA	La Autoridad Certificadora que emite ID Servidor Seguro.
RSA Secure Server ***Jerarquía***	La jerarquía PKI compuesta por la Autoridad de Seguridad RSA de certificación del servidor.
Compartir secretos	Una parte de la llave privada de la CA o de una parte de los datos de activación necesaria para hacer funcionar una llave privada CA virtud de un acuerdo de Secreto Compartido.
Secreto Compartido	La práctica de la división de una llave privada de la CA o de los datos de activación para operar una llave privada de la CA con el fin de cumplir con varias personas el control sobre las operaciones llave de la CA privada en CP § 6.2.2.

Plazo	**Definición**
Secure Server ID	A la Class 3 Certificado de organización para apoyar sesiones SSL entre navegadores web y servidores web.

Secure Sockets Layer (SSL)	El método estándar para proteger las comunicaciones Web desarrollado por Netscape Communications Corporation. El protocolo de seguridad SSL proporciona cifrado de datos, autenticación de servidores, integridad de mensajes y autenticación de cliente opcional para una conexión de Protocolo de Control de Transmisión / Protocolo de Internet.
SGSI	Un conjunto de documentos de E-Sign, que establecen los requisitos de seguridad, auditoría y prácticas de seguridad.
Y prácticas de seguridad Revisión	Una revisión de un Asociado a cabo por E-Sign antes de que un Asociado se le permite entrar en funcionamiento.
Centro de Servicio	Un Asociado que no unidades de vivienda Certificado de firma para la expedición de Certificados con el propósito de la expedición de Certificados de una clase o tipo, sino más bien se basa en un Centro de Procesamiento para llevar a cabo la emisión, administración, revocación y renovación de los Certificados.
Sub-dominio	La parte de la E-SIGN CA NET bajo el control de una entidad y todas las entidades de ella dependientes dentro de la E-SIGN CA NET jerarquía.
Tema	El titular de una llave privada que corresponde a una llave pública. El término "sujeto" puede, en el caso de un Certificado de organización, se refieren al equipo o dispositivo que posee una llave privada. Un Sujeto recibe un nombre inequívoco, que se une a la llave pública contenida en el Certificado del Sujeto.
Suscriptor	En el caso de un Certificado individual, una persona que es objeto de, y se ha emitido un Certificado. En el caso de un Certificado de organización, una organización que posee el equipo o dispositivo que es el tema de, y que ha sido emitido, el Certificado. Un Suscriptor es capaz de utilizar, y está autorizado para utilizar la llave privada que corresponde a la llave pública incluida en el Certificado.
Acuerdo de Suscriptor de	Un acuerdo utilizado por una CA o RA establecen los términos y condiciones en que actúa un individuo o una organización como Suscriptor.
Entidad Superior	Una entidad por encima de una cierta entidad dentro de una jerarquía E-SIGN CA NET (la Class 1, 2, o la jerarquía de 3).
Riesgo suplementario Revisión de gestión	Una revisión de una entidad por E-Sign siguientes resultados incompletos o excepcionales en una Auditoría de Cumplimiento de la entidad o como parte del proceso de administración de riesgos global en el curso ordinario del negocio.
E-Sign	Significa, con respecto a cada uno partes pertinentes de esta CP, E-Sign S.A. y / o cualquier subsidiaria de propiedad absoluta de E-Sign responsable de las operaciones concretas en litigio.
E-SIGN ® Repositorio	Base de datos de E-Sign de proveedores de Certificados y otras E-SIGN CA NET información accesible en línea.
Persona de confianza	Un empleado, contratista o consultor de una entidad dentro de la E-SIGN CA NET responsable de la gestión de infraestructura confiabilidad de la entidad, sus productos, sus servicios, sus instalaciones y / o sus prácticas tal como se definen en la CP § 5.2.1.
Posición de confianza	Las posiciones dentro de una entidad E-SIGN CA NET que debe ser ejercido por una persona de confianza.
Sistema de confianza	Hardware, software y procedimientos que son razonablemente a salvo de intrusos y el mal uso, proporcionar un nivel razonable de disponibilidad, confiabilidad y buen funcionamiento, son razonablemente adecuados para el desempeño de sus funciones previstas y hacer cumplir la política de seguridad aplicables. Un sistema confiable no es necesariamente un "sistema fiable" como se reconoce en la nomenclatura gubernamental clasificada.
E-SIGN CA NET (E-SIGN CA NET)	El Certificado basado en infraestructura de llave pública regirá por las políticas de Certificados de confianza de E-SIGN Network, que permite el despliegue en todo el mundo y el uso de Certificados por parte de E-Sign y sus Asociados, y sus respectivos clientes, Suscriptores y partes que confían.
E-SIGN CA NET Participante	Una persona u organización que es uno o más de los siguientes dentro de la E-SIGN CA NET: E-Sign, una Asociado, un cliente, un Centro de Servicio Universal, un distribuidor, Suscriptor o un usuario de confianza.
Normas E-SIGN CA NET	El negocio, los requisitos legales y técnicos para la emisión, manejo, revocación, renovación y uso de Certificados dentro de la E-SIGN CA NET.

Apéndice B

Historial de cambios

Historia de cambios: la versión

Descripción	Sección y cambios realizados