PRÁCTICAS DE CERTIFICACIÓN (CPS)

E-SIGN S.A.

VERSION 2.4

Fecha: junio 2023

INDICE

1 INTRODUCCION

La **Comunidad de Confianza de E-Sign S.A.** (***ESIGN CA***) es una PKI organizada a través de distintas autoridades certificadoras digitales, y de usuarios con diversas necesidades de comunicación y de información segura.

Este documento, "PRACTICAS DE CERTIFICADOS DE ESIGN CA" (CPS) es la descripción detallada de las políticas procedimientos y mecanismos que nos obligamos a cumplir en la prestación de nuestros servicios de certificación de firma electrónica. La CPS cuida de los requerimientos de negocio y técnicos que permiten aprobar, proveer, administrar, usar, revocar y renovar certificados digitales en la ESIGN CA, y provee a todos los participantes de la ESIGN CA, servicios confiables. Estos requerimientos protegen la seguridad e integridad de la ESIGN CA y comprenden un único conjunto de reglas que se aplican en forma consistente y transversal a toda la ESIGN CA, sus CA raíz, CA subordinadas y certificados de usuario final. La CPS no es un acuerdo legal entre E-Sign y los participantes de la ESIGN CA; las obligaciones contractuales entre E-Sign y los participantes de la ESIGN CA son establecidas por medio de acuerdos con dichos participantes.

Este documento está dirigido a:

- Suscriptores de Certificados que necesiten entender como son autenticados y cuáles son sus obligaciones como Suscriptores de ESIGN CA y cómo son protegidos bajo la ESIGN CA
- Terceras partes que reciben los certificados digitales de la ESIGN CA, que necesitan saber cuánta confianza pueden depositar en un Certificado de la ESIGN CA, o en un documento firmado utilizando ese Certificado.

La CPS en todo caso no gobierna ningún servicio fuera de ella. Por lo tanto, E-Sign puede ofrecer servicios de creación de entidades certificadoras privadas, a través de los cuales algunas organizaciones creen su propia CA privada fuera de la ESIGN CA, y puedan emitir certificados digitales; en el caso de las jerarquías privadas, las organizaciones externalizan a E-Sign las funciones de back-end para la emisión, administración, revocación y renovación de certificados.

Dado que la CPS solo aplica a la ESIGN CA, esta no aplica para estas jerarquías privadas.

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

1.1 Resumen

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

E-Sign, sus CA subordinadas operan como CAs bajo la CP de la ESIGN CA, emitiendo Certificados de usuarios finales (Suscriptores).

Las Autoridades de Registro (RAs, Registration Authorities) son entidades que validan los requerimientos de Certificado bajo la ESIGN CA. E-Sign actúan como RAs para los Certificados que emiten.

Dependiendo de la Clase y tipo de Certificado, los Certificados Digitales pueden ser usados por los Suscriptores para asegurar 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 la Parte que Confía, es decir, él/ella está confiando en el Certificado y debe tomar una decisión de si confiar en él.

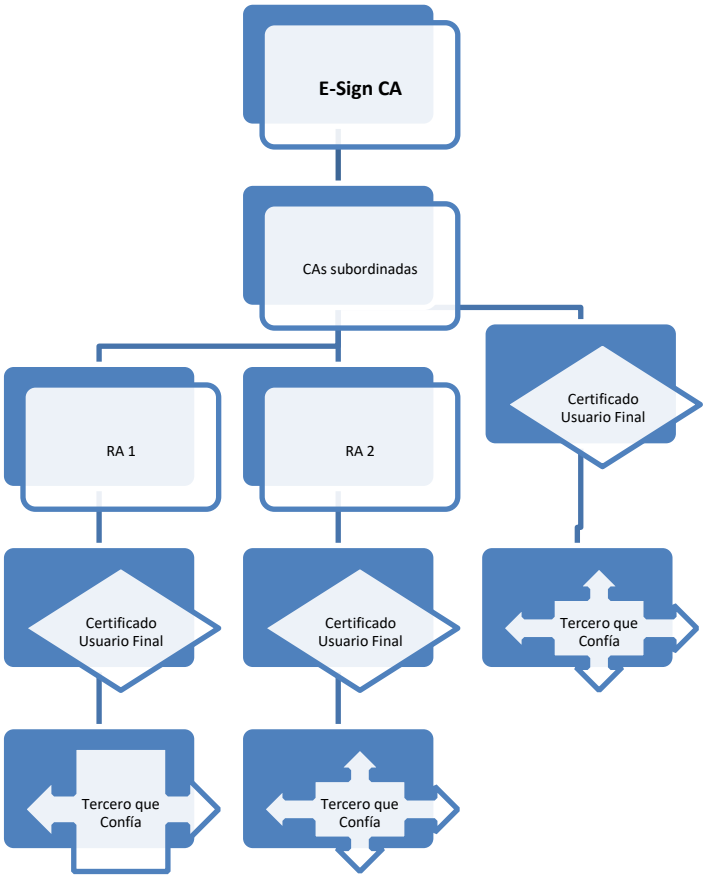

Diagrama 1. Estructura ESIGN CA

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

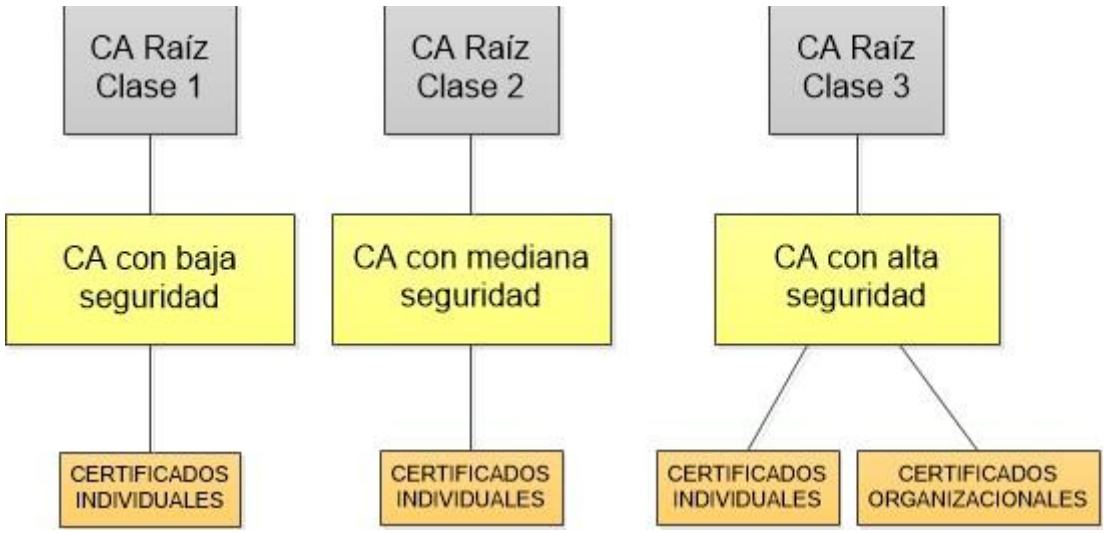

Diagrama 2. Clases de Certificados ESIGN CA

1.2 Nombre e Identificación de este Documento

Este documento es la Política de Certificación (CP Certificate Policy) de ESIGN CA. 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 ESIGN CA. Los valores de los objetos identificadores utilizados para las Clases de usuarios de los Certificados Suscritos son:

- Política de Certificado Clase 1: 1.3.6.1.4.1.42346.1.4.1.1
- Política de Certificado Clase 2: 1.3.6.1.4.1.42346.1.4.1.2
- Política de Certificado Clase 3: 1.3.6.1.4.1.42346.1.4.1.3

1.3 Participantes de la PKI

1.3.1 Autoridades Certificadoras

El término Autoridad Certificadora (CA) es el término genérico que se refiere a todas las entidades autorizadas para emitir Certificados de llave pública bajo la ESIGN CA. El término CA abarca una subcategoría de emisores llamadas Autoridades Certificadoras Raíz. Las CA raíz actúan como raíz de tres dominios, uno por cada Clase de Certificado. Cada CA Raíz es una entidad de E-Sign. Las Autoridades Certificadoras son subordinadas a las CA Raíz respectivas, y son las que emiten Certificados de usuario final o de otras Autoridades Certificadoras (CAs).

1.3.2 Autoridades de Registro

Una Autoridad de Registro (RA) es una entidad que realiza la identificación y autenticación de solicitantes 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 ESIGN CA. E-Sign puede actuar como RA para los Certificados que emite.

Los terceros que entran en una relación contractual con E-Sign, pueden operar su propia RA y autorizar la emisión de Certificados a través de una autoridad de la ESIGN CA. Las RAs de terceros deben cumplir con todos los requisitos de la CP ESIGN CA, 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.

1.3.3 Suscriptores

Son considerados Suscriptores bajo la ESIGN CA todos los usuarios finales (incluidas las entidades) de Certificados emitidos por una CA ESIGN CA. Un Suscriptor es la entidad nombrada como el usuario final de un Certificado. Usuarios finales, o Suscriptores, pueden ser personas, organizaciones o, componentes de infraestructura, tales como firewalls, routers, servidores de aplicaciones, servidores web 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. En tal situación, la entidad que suscribe la emisión de Certificados (a través de la suscripción a un servicio específico, o como emisor) es diferente a la entidad que es el sujeto del Certificado (el titular del certificado). Dos términos diferentes se utilizan en la CP para distinguir estos dos roles: "Suscriptor", es la entidad que contrata con ESign 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 del certificado digital, pero el sujeto es el individuo que se autentica cuando se presenta el certificado digital.

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 la CP invocará la comprensión correcta.

Las CAs son técnicamente también los Suscriptores de los Certificados dentro de la ESIGN CA, ya sea como CA raíz o como CA subordinada. Certificado Raíz es el certificado autofirmado por la misma ESIGN CA, que firma los demás certificados de CA. Las referencias a "entidades finales" y "Suscriptores" en la CP, sin embargo, sólo se aplican a usuarios finales Suscriptores.

1.3.4 Terceros que Confían (Parte que Confía)

Las Partes que Confían son personas o entidades que actúan confiando en un Certificado y/o una firma digital emitida bajo la ESIGN CA. Una Parte que Confía puede ser o no un Suscriptor dentro de la ESIGN CA.

1.3.5 Otros Participantes

No aplica.

1.4 Obligaciones

1.4.1 Esign

Se obliga a:

- Ofrecer y mantener instalaciones, sistemas, programas informáticos y los recursos humanos necesarios para otorgar los certificados en los términos establecidos en la Ley 19.799, el Decreto supremo 181, de 2002, del Ministerio de Economía, Fomento y Turismo y las normas técnicas conforme a éste, especialmente el Decreto Supremo 24, de 2019, que aprueba norma técnica para la prestación del servicio de firma electrónica avanzada (clave única Registro Civil).
- Cumplir y respetar los procedimientos establecidos en la Política de Certificación ESIGN(CP) y en estas Prácticas de Certificación (CPS) para la emisión de certificados.
- Comprobar fehacientemente la identidad del solicitante, a través de la comparecencia personal y directa ante www.firma.cl a través de la clave única que le otorgó el Registro Civil e Identificación.
- Aprobar o rechazar las solicitudes de certificados de conformidad con la Práctica de Certificación ESIGN.
- Emitir los certificados en conformidad al procedimiento establecido en la Práctica de Certificación ESIGN.
- Comunicar al suscriptor de la emisión de su certificado.
- Proveer al suscriptor de custodia para los datos de creación de firma en un dispositivo masivo criptográfico de ESIGN.
- Proveer al suscriptor de las técnicas y medios que le permitan generar y descargar los datos de creación de firma en el dispositivo masivo criptográfico de custodia de ESIGN.
- Configurar y mantener un Registro de Acceso Público de Certificados, con expresa indicación del estado de éstos (vigente, suspendido o revocado).
- Revocar o suspender los certificados, notificando de ello al suscriptor.
- Realizar razonables esfuerzos para comunicar a los suscriptores cualquier hecho conocido por ESIGNque pudiera afectar la validez del certificado.
- Mantener los canales de comunicación para atención de suscriptores y reclamos que se indican en el Procedimiento de Atención de Reclamos Casos y satisfacción de Clientes:
  - ✓ Presencial en nuestra oficina de Avda. Apoquindo 6550, oficina 501, Las Condes.
  - ✓ Call Center +56 2 24331500 o 600 360 0065
  - ✓ Correo Electrónico: Servicioalcliente@esign-la.com.
  - ✓ Formulario Web: contacto.firma.cl o www.esign-la.com opción contacto.

1.4.2 Suscriptor

Antes de la emisión del certificado se obliga a:

- Ser persona natural mayor de 18 años.
- Solicitar la emisión del certificado aceptando los términos y condiciones descritos en la Política de Certificación ESIGN (CP) y estas Prácticas de Certificados (CPS).

- Comparecer personal y directamente ante ESIGN en www.esign-la.com utilizando la clave única que le hubiere sido otorgada por el Registro Civil y responder verazmente las preguntas que se le disponibilidad como segundo factor digital de comprobación de su identidad.
- Proveer a ESIGN toda la información que de acuerdo con esta Política de Certificados (CP) es requerida para verificar su identidad.
- Crear y descargar el certificado en el dispositivo masivo criptográfico custodiado por ESIGN.
- Pagar las tarifas convenidas por concepto de los servicios de certificación, aun cuando no se acepten o no se ocupen los certificados emitidos.

Una vez emitido el certificado se obliga a:

- Aceptar el certificado. Se entiende que un certificado es aceptado por el suscriptor cuando:
  - ✓ Haya sido emitido por ESIGN, aun cuando el certificado no haya entrado en vigor por contener una fecha de inicio de operación posterior a su fecha de emisión.
  - ✓ No se haya formulado un reclamo por error o inexactitud en la emisión al momento de su recepción.
  - ✓ Se haya utilizado la clave de confirmación comunicada por ESIGN para retirar el certificado o se haya instalado éste en el dispositivo masivo criptográfico de custodia de ESIGN.
- Comunicar a ESIGN cualquier error o inexactitud en el certificado que reciba. Si no lo hace al momento de su recepción todas las declaraciones se tendrán por verdaderas.
- Usar los datos de creación de firma asociados al certificado para fines legales y autorizados, de conformidad con lo previsto en la Ley 19.799, la Práctica de Certificación ESIGN (CPS) y en esta Prácticas de Certificado (CP).
- Utilizar correctamente el certificado.
- Ser un usuario final, y no usar el certificado para actuar como certificador de firma electrónica.
- Comunicar inmediatamente a ESIGN el compromiso, pérdida, hurto, robo, acceso no autorizado o extravío, falsificación de sus datos de creación de firma o certificado o cualquier circunstancia que pudiera ser causal de suspensión o revocación de su certificado.
- Custodiar los datos de creación de firma, tomando precauciones razonables para evitar su pérdida, modificación y uso no autorizado.
- No revelar el PIN o el segundo factor de seguridad con el decidió proteger los datos de creación de firma almacenados en el dispositivo masivo criptográfico con custodia.
- Solicitar la suspensión o revocación del certificado cuando se presente alguna de las causales indicadas para este efecto en la Práctica de Certificación ESIGN (CPS).
- No usar los datos de creación de firma una vez que el certificado haya expirado o haya sido solicitada la suspensión o revocación.
- Realizar la comunicación o reclamos a ESIGN como se indica en Proceso de Atención de Reclamos Casos y satisfacción de Clientes a través de los siguientes canales:
  - ✓ Presencial en nuestra oficina de Avda. Apoquindo 6550, oficina 501, Las Condes.
  - ✓ Call Center +56 2 24331500 o 600 360 0065
  - ✓ Correo Electrónico: Servicioalcliente@esign-la.com.
  - ✓ Formulario Web: contacto.firma.cl o www.esign-la.com opción contacto.

1.4.3 Usuarios

Se obliga a:

- Verificar la validez del certificado mediante una consulta al registro de acceso público de certificados.
- Verificar la firma del suscriptor.
- Comprobar cualquier limitación funcional que incorpore el certificado.

- Validar el uso de certificado para propósitos autorizados de conformidad con la legislación vigente.

1.5 Uso de los Certificados

1.5.1 Uso adecuado de los Certificados

1.5.1.1 Certificados Emitidos a Personas (Certificados Individuales)

Los Certificados individuales son utilizados normalmente por las personas para firmar y encriptar y 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 presentada a continuación, un Certificado individual puede ser utilizado para otros fines, siempre que las Partes que Confían sea capaces de confiar razonablemente en el Certificado y que ese uso no esté prohibido por la ley, 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 Clase 1	✓			✓		✓
Certificados Clase 2		✓		✓		✓
Certificados Clase 3			✓	✓		✓

Tabla 1. Usabilidad de Certificados Individuales

1.5.1.2 Certificados emitidos a Organizaciones

Los Certificados de Organización se emiten a organizaciones después de autenticar que la Organización tiene existencia legal y que otros atributos de la Organización – que son 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.

1.5.1.3 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 remitente con una determinada dirección de correo electrónico. El Certificado, sin embargo, no aporta prueba alguna de la identidad del Suscriptor

Los Certificados de Nivel de Seguridad Medio son aquellos Certificados útiles para verificar 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 Clase 3 individuales y organizacionales que proporcionan un alto nivel de seguridad de la identidad del suscriptor, en comparación con los certificados Clase 1 y 2.

1.5.2 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 Clase 1 no deberán ser utilizados como prueba de identidad o como soporte de no repudio de identidad o autoría. Los Certificados Individuales están destinados a aplicaciones de cliente y no deberán ser utilizados como Certificados de servidor u organizacionales.

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.

1.5.3 Plataformas por las que se emiten los Certificados

Esign emite certificados a suscriptores de manera directa o a través de terceros:

1.5.3.1 Emisión directa desde la PSC al Suscriptor

- A través de sus sucursales de atención presencial ubicada en Apoquindo 6550, oficina 501, comuna de Las Condes.
- A treves de su sitio web www.firma.cl.

1.5.3.2 Emisión a través de terceros al Suscriptor

A través de partner o clientes corporativos que utilizan los servicios de validación y emisión de certificados que posee Esign.

Al existir cláusulas de confidencialidad exigidas por estos partner y clientes, la identidad de estos es considerada reservada/estratégica, por ende, esta información solo puede ser solicitada de manera formal enviando un correo a la dirección de correo servicioalcliente@esign-la.com, en donde se evaluará su entrega.

1.6 Administración de la Política

1.6.1 Organización que Administra el Documento

E-Sign S.A.
Avenida Apoquindo 6550, oficina 501
Las Condes
Santiago
Chile

1.6.2 Contacto

Oficial de Seguridad E-Sign S.A.
Avenida Apoquindo 6550, Oficina 501
Las Condes
Santiago
Chile
+56 (2) 24331500
+56 (2) 24331501 *practicas@esign-la.com*

1.6.3 Persona que Determina la Idoneidad de la CPS para la Política

La Autoridad de Administración de la Política ESIGN CA (PMA Policy Management Authority) determina la propiedad y aplicabilidad de esta CPS.

1.6.4 Procedimiento de Aprobación de la CPS

La aprobación de esta CPS y posteriores modificaciones serán realizados por el PMA. Las modificaciones podrán estar en forma de un documento conteniendo una modificación de la CPS 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.

Las actualizaciones sustituyen cualquier disposición designada o conflictiva de la versión de referencia de la CPS. 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.

1.7 Definiciones y Siglas

Para una mejor comprensión de los términos y siglas utilizados en este documento, ver "Apéndice A. Tabla de siglas y definiciones"

2 Responsabilidades de Publicación y Repositorio

2.1 Repositorios

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

2.2 Publicación de Información de Certificados

E-Sign mantiene un repositorio, publicado en Web, que permite a las Partes 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 documentada en la CPS apropiada. E-Sign ofrece a las Partes 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 publica los certificados que emite en nombre de sus propias CAs y de las CAs en sus subdominios. En caso de la revocación de un Certificado de usuario final, la CA que emitió el Certificado deberá publicar un aviso de tal revocación en el repositorio. Además, E-Sign deberá 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 en todo momento publica una versión actualizada de:

- Su CP de la ESIGN CA
- Su CPS
- Acuerdos de Suscriptor
- Otros acuerdos específicos aplicables tales como Política de Privacidad, Política de Precios, etc.

2.3 Tiempo o Frecuencia de Publicación

La información de la CA es publicada prontamente después de que está disponible para la CA. La ESIGN CA 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.

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 no debe utilizar intencionalmente medios técnicos para limitar el acceso a la CP, a esta CPS, a Certificados, información del estado de Certificados o CRLs. E-Sign podrá, sin embargo, exigir a

las personas aceptar un Acuerdo de Tercera Parte que Confía o Contrato de uso de la CRL como condición para acceder a los Certificados, la información del estado de Certificados o CRLs. E-Sign implementa controles para prevenir que personas no autorizadas puedan agregar, eliminar o modificar contenidos del repositorio.

3 Identificación y Autenticación

3.1 Identificación (Naming)

A menos que se indique lo contrario en la CP, la CPS pertinente o el contenido de los Certificados digitales, los nombres que aparecen en los Certificados emitidos bajo la ESIGN CA son autenticados, a excepción de los certificados Clase 1.

3.1.1 Tipos de Nombre

Los Certificados de usuario final contienen un Distinguished Name (DN) X.501 en el campo nombre del Sujeto (Subject).
El DN del Sujeto 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 Sujeto de los Certificados de organización debe ser un nombre de dominio, el nombre legal de la organización, o el nombre del representante de la organización autorizado para utilizar la 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 Sujeto 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 Clase 2 y 3.
Los Certificados ESIGN CA también pueden contener una referencia al Acuerdo de Tercera Parte que Confía en sus DNs.

3.1.2 Necesidad de que los Nombres sean Significativos

Los Certificados de Suscriptor Usuario Final de Clase 2 y 3 deberán incluir nombres significativos, en el sentido siguiente: los Certificados de Clase 2 y 3 de Usuario Final, deberán contener nombres con semántica comúnmente entendible, que permitan 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 Clase 1 no se autentica, por lo que los Suscriptores de Certificados Clase 1 pueden usar seudónimos (nombres distintos al verdadero nombre personal o de organización de un Suscriptor). Los Suscriptores de Certificados Clase 2 y 3 no están autorizados a utilizar seudónimos.

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 ESIGN CA no necesariamente son únicos dentro de un Sub-dominio de clientes para una Clase específica de Certificado, sin perjuicio de que cada Certificado puede ser distinguido en forma única. Es posible para un Suscriptor tener dos o más Certificados, 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. E-Sign no está obligado 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 no tendrá derecho alguno de rechazar 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 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 autorizada 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 autenticará 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 ESIGN CA se explica a continuación:

CLASE 1

Sin autenticación de identidad. Hay una confirmación limitada de la dirección de correo electrónico del Suscriptor.

CLASE 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 clientes.
- 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

CLASE 3

La autenticación de los Certificados Individuales de Clase 3 se da en las siguientes situaciones:

a. La presencia personal (física) del Solicitante del Certificado:
   - ante un agente de la CA o RA.
   - ante un notario público u otros oficiales con autoridad comparable en la jurisdicción del Solicitante del Certificado.

   En estos casos 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.

b. A través de un portal Web con autenticación con Clave Única, en cumplimiento con el Decreto N° 24 de abril de 2019, de la Subsecretaría de Economía del Gobierno de Chile.

   Para el caso de autenticación con Clave Única, E-Sign reconoce el sistema denominado "ClaveÚnica", como medio de comprobación fehaciente de la identidad del solicitante de un certificado de firma electrónica avanzada, junto a un mecanismo complementario de verificación de Identidad, para este caso se contempla lo siguiente:
   - Primer paso: autenticación con Clave Única exitoso
   - Segundo paso: presentación de datos registrados en Clave Única (datos parcialmente ofuscados), ingreso de número de documento (número único de la cédula de identidad), más enrolamiento de su número de teléfono celular.

- Tercer paso: Challenge, que es utilizado como mecanismo complementario digital de comprobación de identidad del solicitante, este consiste en un desafío de 4 preguntas personales, (dependiendo de la cantidad de información con la que se cuente de la persona) con alternativas, el sistema exige que 3 de las 4 respuestas sean correctas.
- Cuarto paso: creación de Pin de firma por parte del cliente/usuario, equivalente al segundo factor de seguridad, para ser utilizado al momento de realizar una firma y que será almacenado en el dispositivo criptográfico, lo que permitirá al titular controlar que el acceso y utilización de sus datos, pueda ser realizado únicamente por él.
- Luego de que los pasos antes mencionados sean realizados de manera exitosa, el certificado es generado, quedando almacenado en la plataforma Criptográfica HSM "Esigner", mientras que la llave privada respectiva quedará almacenada en un módulo criptográfico HSM, certificado FIPS PUB 140-2.
- Al momento de realizar la firma el suscriptor deberá ingresar el pin generado junto al certificado (Segundo factor de seguridad) y además un SMS (OTP) que será enviado al número telefónico declarado al inicio del proceso.

En esta modalidad el tercer paso corresponde al mecanismo complementario digital de comprobación de identidad del solicitante exigido en el artículo N°3 del decreto N°24 de abril de 2019. El pin solicitado en el cuarto paso corresponde al Segundo factor de Seguridad exigido en el artículo 5 del decreto N°24 de abril de 2019.

Los Certificados de Clase 3 de administrador también deberán incluir la autenticación de la organización y una confirmación por parte de la organización de la autorización a la persona para que actúe como administrador.

E-Sign también puede 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.

3.2.4 Información No-Verificada del Suscriptor

La Información No-Verificada del Suscriptor incluye:

- Unidad Organizacional (OU)
- Nombre del Suscriptor en Certificados de Clase 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 ESIGN CA puede proporcionar servicios de interoperabilidad que permitan a una CA no ESIGN CA poder interactuar con la red ESIGN CA certificando la CA en forma unilateral. Las CAs capacitadas para interoperar de esta forma cumplen con la CP, complementado por políticas adicionales cuando sea necesario.
E-Sign sólo permitirá la interoperabilidad con la red ESIGN CA de una CA fuera de la ESIGN CA cuando se cumplan los siguientes requisitos:

- Tener un acuerdo contractual con E-Sign
- Operar bajo una CPS que cumpla con los requisitos de ESIGN CA 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 Recambio de Llaves

En términos generales, tanto el "Recambio 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 "Recambio de Llaves" y "Renovación".

3.3.1 Identificación y Autenticación para Recambio Rutinario de Llave

La entidad que aprueba una Solicitud de Certificado para un Certificado de Usuario Final será responsable de la autenticación de la solicitud de recambio de llaves o renovación. Los procedimientos de recambio de llaves aseguran que la persona u organización que desea renovar/cambiar llaves del Certificado de Usuario Final es, de hecho, el Suscriptor del Certificado. Un procedimiento aceptable es mediante el uso de una Frase Secreta (o su equivalente). 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 recambio de Llaves Después de Revocación

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

- el Certificado (que no sea un Certificado de Clase1) fue emitido a una persona distinta de la que se identifica en el Sujeto del Certificado, o
- el Certificado (que no sea un Certificado de Clase 1) fue publicado sin la autorización de la persona o entidad nombrada como el Sujeto 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 ESIGN CA.
- 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 Sujeto que el DN del Sujeto 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.
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 Secreta/Contraseña 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 ser enviado por e-mail, correo postal o entregado presencialmente.

Los administradores de CA/RA tienen derecho a solicitar la revocación de Certificados de usuario final dentro del Sub Dominio de la CA/RA. E-Sign autentica la identidad de los Administradores a

través de control de acceso usando autenticación del cliente antes de permitirles realizar funciones de revocación u otro procedimiento aprobado por la ESIGN CA.
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 sujeto 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.
- demostrar la posesión de la llave privada, físicamente o por medios lógicos, correspondiente a la llave pública entregada a E-Sign.

4.1.2.2 Certificados de CA y RA

Los Suscriptores de Certificados de CA y RA celebran un contrato con E-Sign. 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 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

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
- la RA cree que la emisión de un Certificado al Suscriptor puede acarrear descredito a la ESIGN CA

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.

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 Emisión de los Certificados

4.3.1 Acciones de la CA durante la Emisión de los 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.

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 almacena el certificado. Los certificados pueden ser descargados en forma individual en dispositivos individuales, o de manera centralizada y segura.

4.3.2 Notificación de la emisión 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.

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 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 la 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 de la Parte que Confía

Las Partes 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, las Partes que Confían deben 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, se 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 esté siendo utilizado de acuerdo con las extensiones del campo KeyUsage incluido en el Certificado (por ejemplo, si digitalSignature no está habilitado, 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, las Partes 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 las Partes que Confían.

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 Clase 3, donde se genera el par de llaves en un servidor web.

La renovación es equivalente al recambio de llaves.

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 no 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 el Suscriptor del Certificado o la persona autorizada por el Suscriptor.

Un procedimiento aceptable es el uso de una Frase Secreta (o su equivalente).

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. El certificado no podrá ser renovado por más allá de 24 meses, sin que 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 usuario final.

4.6.4 Notificación de Nueva Emisión de Certificado al 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 4.5.

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.

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

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

4.7 Recambio 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 recambio 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 Recambio de Llaves del Certificado

Los procedimientos para recambio 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). 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 se emite. El certificado no podrá ser renovado por más allá de 24 meses, sin que 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 recambio de llaves de un Certificado de Suscriptor de usuario final.

4.7.4 Notificación de Nueva Emisión de Certificado al Suscriptor

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

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

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

4.7.6 Publicación del Certificado con recambio de Llaves por la CA

El Certificado con recambio de Llaves se publica en el repositorio de acceso público de E-Sign.

4.7.7 Notificación de Emisión del Certificado por parte 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 puede 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 Nueva Emisión de Certificado al Suscriptor

Ver Sección 4.3.2

4.8.5 Conducta Constitutiva de Aceptación de la Modificación del Certificado

Ver Sección 4.5.

4.8.6 Publicación del Certificado Modificado por la CA

Ver Sección 4.4.

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

Ver Sección 4.4

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.

Un Certificado de Suscriptor es revocado si:

- E-Sign, una organización 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, o una organización 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 su vigencia, por ejemplo por incumplimiento por parte del suscriptor de sus obligaciones.
- La relación entre una organización 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 Clase 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 o una organización 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 Clase 1) fue emitido a una persona que no sea la que es Sujeto del Certificado o el certificado (que no sea un Certificado de Clase 1) fue emitido sin la autorización de la persona que es Sujeto de dicho Certificado,
- E-Sign o una organización tiene motivos para creer que un hecho material en la Solicitud del Certificado es falso,
- E-Sign o 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 Clase 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 uso continuado de este Certificado es perjudicial para la ESIGN CA.

Al evaluar si el uso del certificado es perjudicial para la ESIGN CA, E-Sign considera, 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

E-Sign también puede revocar un Certificado de Administrador si el Administrador deja de tener autoridad como tal.

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

4.9.2 Quién puede Solicitar la Revocación

Los 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 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: e-mail, correo postal o presencialidad.

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 debe autenticar la identidad de los administradores a través de control de acceso utilizando SSL y la autenticación de cliente antes de permitirle realizar funciones de revocación.

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 Plazo en el que la CA Debe Procesar la Solicitud de Revocación

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

4.9.6 Requerimiento de Comprobación de Revocación para Terceros 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) correspondiente para comprobar el estado de revocación.

- Para los Certificados Raíz de la ESIGN CA y Autoridades Certificadoras de Clase 3, las CRL se publican en el repositorio E-SIGN, en http://pki.esign-la.com.

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.

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 razonable después de la generación. Esto se hace automáticamente en pocos minutos después de la generación.

4.9.9 Disponibilidad de Comprobación en Línea de Revocación/Estado

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.

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 ESIGN CA serán notificados cuando exista o se sospeche de compromiso en llaves privadas de la CA, utilizando esfuerzos comercialmente razonables.

4.9.13 Circunstancias para la Suspensión

No aplica, ya que la ESIGN CA no implementa suspensión de certificados.

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 (en una URL especifica contenida en el certificado), 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 Fin de la Suscripción

Un Suscriptor puede poner término a la vigencia de un Certificado de ESIGN CA:

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

4.12 Custodia y Recuperación de Llaves

ESIGN CA no custodia ni recupera llaves de Suscriptor usuario final.

4.12.1 Política y Prácticas de Custodia y Recuperación de Llaves

No aplica.

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

No aplica.

5 Controles de Instalación, Administración y Operacionales

5.1 Controles Físicos

La ESIGN 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 ESIGN CA descritos en la Sección 8. Estos documentos contienen información confidencial y sólo están disponibles previo acuerdo con E-Sign. Un resumen de los requisitos es descrito en los siguientes apartados.

5.1.1 Localización y Construcción del Sitio

Todas las operaciones de una CA o RA ESIGN 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.

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.

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 Clase1, 2 y 3 y por lo tanto, opera al más alto nivel de seguridad requerido por ESIGN CA.

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 y Protección contra Incendios

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, físicos y electrónicos 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 Controles Procedimentales

5.2.1 Roles de Confianza

Los empleados, contratistas y consultores que han sido designados para administrar la infraestructura serán considerados "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 la política de Empleado Confiable.

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 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 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 y el material de llaves asociado, requieren varias Personas de Confianza.

Estos procedimientos de control interno están diseñados para asegurar que, como mínimo, dos miembros del personal de confianza son requeridos para tener acceso físico o lógico al 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 acceso a "partes secretas" o “secretos compartidos” y viceversa.

5.2.3 Identificación y Autenticación para Cada Rol

Las CAs y RAs deberán 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.

5.2.4 Roles que Requieren Segregación de Tareas

Los roles que requieren Segregación de Funciones 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 activación de una CA en ambiente de producción

5.3 Controles sobre el Personal

La ESIGN 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 ESIGN 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 necesaria 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 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 Posiciones de Confianza, al menos cada tres (3) 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 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, y
- Conductas de riesgo repetitivas

Los informes que contienen dicha información deben ser evaluados por el Oficial de Seguridad, quien 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.

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 deberá abordar los elementos relevantes para las funciones desempeñadas por el personal.

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

- Principios y mecanismos de seguridad de la ESIGN 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
- 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 frecuencia necesarias 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.
Las Sanciones, amonestaciones, término del contrato, se deberán ejercer, de acuerdo a lo establecido en el Reglamento Interno de E-SIGN, específicamente en su Título XXI “De las sanciones y las multas”.

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, o de una organización, sólo en la medida en que son acompañados y supervisados directamente por Personas de Confianza.

5.3.8 Documentación Proporcionada al Personal

E-Sign y Organizaciones 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, o persona, 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 contienen 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)
- 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 erróneas en los Certificados y en el repositorio
- Cambios en las 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.

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 por medios electrónicos, para validar la integridad, la identificación temporal y el seguimiento de las actividades, incluyendo mecanismos para proteger los archivos de registro contra modificaciones, eliminación no autorizadas, u otro tipo de manipulación. Tal mecanismo de protección no necesita tener base criptográfica.

5.4.5 Procedimientos de Respaldo de Registros de Auditoría

Se deben hacer diariamente respaldos de seguridad incrementales de los registros de auditoría y, semanalmente se crearán 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

De acuerdo a lo establecido en el procedimiento de gestión de vulnerabilidades.

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

5.5.2 Periodo de Retención del Archivo

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 Clase 1,
- Seis (6) años y seis (6) meses para Certificados de Clase 2 y Clase 3,
- Veinte (20) años y seis (6) meses para Certificados de Clase 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 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.

5.5.4 Procedimientos de Respaldo de Archivo

E-Sign deberá 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 ESIGN CA, con excepción de los Clientes RA. Las CAs deberán ayudar a sus RAs clientes a preservar un registro de auditoría. Tal sistema de recolección de archivos es entonces externo a la RA. De lo contrario, las entidades dentro de la ESIGN 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 de CA

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 ESIGN 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 Recuperación de Compromisos y 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.

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 preparar 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 ESIGN 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.

5.7.4 Capacidad de Continuidad de Negocio Luego de un Desastre

Las entidades ESIGN 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 la especificada por la ESIGN CA.

Los equipos computacionales de recuperación de desastres deben tener las protecciones de seguridad física de acuerdo a lo documentado en las políticas confidenciales de seguridad de la ESIGN CA, que incluye la aplicación de niveles de seguridad física.

5.8 Terminación de la CA o RA

Las partes involucradas, 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 terceros que confían.

El plan de terminación puede cubrir temas tales como:

- La notificación a las partes afectadas por la terminación, tales como Suscriptores, Terceros que Confían, 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, 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 que utilizan CAs que pre-generen pares de llaves en tokens de hardware de Suscriptores.

Las Llaves de CA se generan en una Ceremonia de Generación de Llaves que es llevada a cabo por múltiples Personas de Confianza y que requiere la utilización de sistemas de confianza y módulos criptográficos que cumplen con los requerimientos de FIPS 140-2 nivel 3.

Todas las ceremonias de generación de llaves se ajustan a los requerimientos indicados en las políticas confidenciales de seguridad de ESIGN 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:

- Su par de llaves es generado previamente en tokens de hardware, que son distribuidas a los solicitantes de acuerdo con el proceso de solicitud de certificado.

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 ESIGN 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.

6.1.4 Entrega de Llave Pública de CA a Terceros que Confían

Los certificados de CA raíz y CAs intermedias son distribuidos a través de la publicación en un sitio web de la ESIGN CA. Los certificados de CA raíz y CAs son distribuidos a través de la publicación en el directorio.

La distribución de las llaves de CA a terceros que confían también es realizada indirectamente por los suscriptores en la medida que los documentos firmados que distribuyen incluyan los certificados de CA.

6.1.5 Tamaños de Llave

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

El estándar ESIGN CA para el mínimo tamaño de llaves es el uso de pares de llaves con robustez equivalente a 2048 bits RSA en Certificados Raíz y CAs.

Para llaves de certificados de RAs y entidades finales el tamaño mínimo es equivalente en robustez a 2048 bits RSA.

La norma ESIGN CA para el algoritmo de hash de firma digital es SHA-2.

6.1.6 Generación y Verificación de Calidad de Parámetros de Llave Pública

No aplicable.

6.1.7 Propósitos de Uso de Llave (de acuerdo al campo X.509 v3 Key Usage)

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 ESIGN 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 la ESIGN CA. Los Suscriptores tienen la opción de proteger sus llaves privadas en una tarjeta inteligente o un token de hardware.

Las RA deberán realizar todas las operaciones criptográficas en un módulo criptográfico clasificado en FIPS 140-2 nivel 3.

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

6.2.2 Control multi-personal de Llave Privada (n de m)

El número mínimo de partes separadas necesarias para respaldar o recuperar el respaldo de una llave privada de CA es 2. Cabe señalar que el número de partes distribuidas para tokens de recuperación de desastres puede ser menor que el número distribuido para tokens operacionales, mientras que el número mínimo de partes necesarias sigue siendo el mismo.

6.2.3 Custodia de la Llave Privada

Las llaves privadas de la CA no son custodiadas.

6.2.4 Copia de Seguridad de la Llave Privada

Las CAs deben crear copias de seguridad de sus propias llaves privadas con el fin de ser capaces de recuperarse de desastres y daños en el equipamiento de acuerdo con las normas documentadas en las políticas confidenciales de Seguridad de la ESIGN CA.

Las copias de seguridad de las llaves privadas de una CA son creadas mediante la copia de las llaves privadas y su transferencia cifrada en medios de almacenamiento, en un proceso que requiere la participación de al menos dos Personas de Confianza, de acuerdo con lo indicado en las Secciones

6.2.6 y 6.2.7. Además, 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 sujeto de los de Servicios del Administrador de Llaves, 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 ESIGN 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 cumplan los requisitos de la 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 la CP.

E-Sign no archiva copias de llaves privadas de RA ni de entidades finales.

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

La transferencia 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 participantes ESIGN 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 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 de la ESIGN 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 Clase 1

El estándar ESIGN CA para la protección de llave privada de Clase 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 Clase 2

El estándar ESIGN CA para la protección de la llave privada de Clase 2 es que los Suscriptores:

- Utilicen 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,
- Tomen las medidas comercialmente razonables para la protección física de la estación de trabajo del Suscriptor.

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

6.2.8.3 Certificados de Clase 3 que no sean Certificados de Administrador

El estándar ESIGN CA para la protección de llave privada de Clase 3 (que no sea de administrador) es 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

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 (Clase 3)

El estándar ESIGN CA para la protección de llave privada de Clase 3 de Administrador es que los Suscriptores:

- Utilicen una tarjeta inteligente, un dispositivo de acceso biométrico, que cumpla con la norma FIPS 140-2 L3, para autentificar al Administrador 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 Administrador

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.

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

No aplica.

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

No aplica.

6.2.9 Método de Desactivación de la Llave Privada

Los Suscriptores usuarios finales Clase 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

Para desactivar la llave privada de una CA en línea, un Administrador de la CA debe utilizar las herramientas de gestión que provee el módulo criptográfico a través del sistema.

Para desactivar la llave privada de una 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, un Administrador de la CA debe eliminar la llave del módulo criptográfico que la contiene, y remover el módulo criptográfico del sistema.

Los módulos criptográficos removidos de los sistemas de la CA deben ser almacenados 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 mediante las herramientas de gestión del módulo criptográfico 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 módulo.

Este proceso será atestiguado de acuerdo con las normas documentadas en las políticas de seguridad confidenciales de la ESIGN 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 Períodos Operacionales de Certificados y Períodos de Uso del Par de Llaves

El período operacional de un Certificado finaliza a su vencimiento o revocación. El máximo período operacional de los Certificados ESIGN CA se fijará de acuerdo con los plazos establecidos en la tabla 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 operacional del par de llave de Suscriptor es el mismo que el período operacional de sus Certificados, con la salvedad de que las llaves privadas pueden seguir siendo utilizadas después del período operacional para el descifrado y verificación de firmas. Una CA no emitirá Certificados si sus períodos operacionales se extienden más allá del periodo operacional del par de llaves de la CA. Por lo tanto, el período operacional del par de llaves de CA es necesariamente más corto que el período de validez del Certificado de CA.

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

Al final del periodo operacional de un par de llaves de un Suscriptor o de una CA, el Suscriptor o la CA 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*
CA Raíz auto-firmada	Hasta 30 años
CA Raíz para CA intermedia fuera de línea	Generalmente 10 años, pero hasta 15 años en caso de ser renovada.

CA Raíz para CA en línea	Por lo general 7 años, pero hasta 14 años en caso de ser renovada.
CA intermedia fuera de línea para CA en línea	Por lo general 5 años, pero hasta 10 años en caso de ser renovada
CA en línea para suscriptor usuario final individual	Normalmente hasta 3 años.
CA en línea para Suscriptor Entidad final Organizacional.	Normalmente hasta 3 años. NOTA: Los Certificados SSL pueden ser válidos por un máximo de 27 meses.

Tabla 2 – Períodos Operacionales de Certificados

Excepto como se indica en esta sección, los participantes ESIGN CA deberán dejar de utilizar sus pares de llaves después de expirado el período de uso.

Los Certificados emitidos por CAs para Suscriptores usuarios finales pueden tener Períodos Operacionales de más de dos 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 ESIGN 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.

6.4.2 Protección de Datos de Activación

Los participantes ESIGN CA, y los suscriptores, 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.

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 ESIGN CA deberán proteger la transmisión utilizando los métodos que permitan proteger contra la pérdida, robo, modificación, revelación no autorizada o uso no autorizado de tales llaves privadas.

En la medida en que se utilice 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 tales datos de activación.

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 ESIGN CA.

6.5.1 Requerimientos Técnicos Específicos de Seguridad Computacional

Las CAs deberán asegurar que los sistemas de mantenimiento del software y de archivos de datos de la CA son sistemas Confiables y seguros contra el acceso no autorizado.

Las CAs 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 limitado a Personas de Confianza del grupo de operaciones de la CA 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 Controles de Desarrollo de Sistemas

El software de funcionalidad de CA y RA, utilizado para gestionar los Certificados, 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.

6.6.2 Controles de Gestión de Seguridad

Ninguna estipulación

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 confidenciales de la ESIGN CA, de forma tal de evitar el acceso no autorizado, alteración, y ataques de denegación de servicio

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 ESIGN 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, May 2008 (“RFC 5280”).

Como mínimo, los Certificados X.509 de ESIGN CA deberán contener los campos básicos y los valores prescritos o las limitaciones de valor en la tabla 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)
DN de Emisor	Vea la Sección 7.1.4
Válido desde	Base de Tiempo Coordinado Universal. Codificado de acuerdo con RFC 5280.
Válido hasta	Base de Tiempo Coordinado Universal. Codificado de acuerdo con RFC 5280.
DN de Sujeto	Ver CP § 7.1.4
Llave Pública de Sujeto	Codificados de acuerdo con RFC 5280
Firma	Generado y codificado de acuerdo con RFC 5280

Tabla 3 - Campos del Perfil Básico de Certificado

7.1.1 Número (s) de Versión

Los certificados de CA serán Certificados X.509 versión 3, al igual que los certificados de usuario final.

7.1.2 Extensiones de Certificado

Las extensiones privadas son permitidas, pero el uso de una extensión privada (s) no se justifica en virtud de la CP y CPS salvo que se incluyan específicamente por referencia.

7.1.2.1 Utilización de Llaves

Los certificados X.509 Versión 3 son generalmente poblados de acuerdo con RFC 5280. El campo criticidad de la extensión KeyUsage generalmente se establece en VERDADERO para los Certificados de CA y en VERDADERO o FALSO para certificados de Suscriptor entidad final.

7.1.2.2 Extensión de Políticas de Certificado

La Extensión de Políticas de Certificado X.509 Versión 3 se completa con el identificador de la 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 BasicConstraints de los Certificados de CA X.509 versión 3 tendrá el campo CA establecido con valor VERDADERO. La extensión BasicConstraints de los Certificados de entidad

final, tendrá el campo CA establecido con valor FALSO. El campo de criticidad de esta extensión se establece en VERDADERO para los Certificados de CA, y para los certificados de Suscriptor puede ser establecido en VERDADERO o en FALSO.
Los Certificados de CA, X.509 Versión 3, 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 Extendido de la Llave

Por defecto, ExtendedKeyUsage se establece como una extensión no crítica. Los Certificados de CA de la ESIGN CA no incluyen la extensión ExtendedKeyUsage.

7.1.2.6 Puntos de Distribución de CRL

Los Certificados de ESIGN 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 ESIGN 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 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 ESIGN 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 RFC 5280.

7.1.3 Identificadores de Objeto de Algoritmo

Los Certificados ESIGN 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}
- ***sha384withRSAEncryption*** OBJECT IDENTIFIER:: = {iso (1) member-body (2) us (840) rsadsi (113549) pkcs (1) PKCS-1 (1) 12}
- ***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}

7.1.4 Formas de Nombre

Los Certificados ESIGN 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 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 de Tercera Parte 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 de Tercera Parte 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 ESIGN 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 ESIGN 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 Tercera Parte que Confía o a la CPS aplicables. Además, algunos certificados contienen un calificador - UserNotice- que apunta al Acuerdo de Tercera Parte que Confía aplicable.

7.1.9 Semántica de Procesamiento para la Extensión Crítica Políticas de Certificado

Ninguna estipulación

7.2 Perfil de la CRL

Las CRL se ajustan a RFC 5280 y contienen los campos básicos y contenidos especificados en la Tabla 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 4 - Campos básicos de la CRL

7.2.1 Número (s) de Versión

La ESIGN CA soporta CRLs X.509 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 Clase 1, Clase 2 y Clase 3 utilizando el OCSP que cumple con RFC 2560

7.3.1 Número(s) de Versión

La versión 1 de la especificación de OCSP según se define en RFC2560 y RFC 5019 es compatible.

7.3.2 Extensiones OCSP

E-Sign no utiliza un código aleatorio para establecer la vigencia actual de cada respuesta OCSP y los clientes no deben esperar un código aleatorio en la respuesta a una solicitud que contenga un código aleatorio. 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 se somete a una auditoría de cumplimiento periódico ("Auditoría de Cumplimiento") para asegurar el cumplimiento con las Normas ESIGN CA después de que comiencen las operaciones.

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 Evaluador

Una firma de auditoría de terceros realizará las auditorías de cumplimiento de E-Sign.
Las revisiones y auditorías deberán ser realizadas por una firma auditora 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 Evaluador con Entidad Evaluada

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.

E-Sign será auditado de conformidad con alguna de las mejores prácticas vigentes a la fecha, tales como AICPA WEBTRUST, ISO 27.001, 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, u otras.

8.5 Acciones Tomadas como Resultado de Deficiencia

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 ESIGN CA, 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 a 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 diez (10) días hábiles después de la finalización de la auditoría y no más tarde de cuarenta y cinco (45) días después de la fecha de inicio de las operaciones.

9 Otras Materias de Negocio y Legales

9.1 Honorarios

9.1.1 Tarifas de Emisión o Renovación de Certificados

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

9.1.3 Tarifas de Acceso a Información de Revocación o Estado

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

9.1.4 Tarifas de Otros Servicios

E-Sign no cobra una cuota por el acceso a esta CP o de sus respectivas CPS. Cualquier uso que se haga para otros fines que no sean 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 Reembolso

En la medida permitida por la ley aplicable, E-Sign deberá 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, en su CPS.

9.2 Responsabilidad Financiera

9.2.1 Cobertura de Seguros

E-Sign deberá mantener un nivel comercialmente razonable de cobertura de seguro por errores y omisiones, ya sea a través de un programa de seguros contra errores y omisiones 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 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 Terceros que Confían.

9.2.3 Cobertura de Garantía Adicional

Algunos participantes ESIGN CA ofrecen programas de garantía extendida a suscriptores de Certificados SSL 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. Los participantes ESIGN CA 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, deben mantenerse en forma confidencial y privada:

- registros de solicitudes de creación de CA, ya sea aprobados o rechazados,
- registros de Solicitud de Certificado,

- Registros transaccionales (tanto registros completos, como las pistas de auditoría de las operaciones),
- registros de auditoría creados o retenidos por E-Sign o un cliente,
- Reportes de auditoría creados por E-Sign 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, el software, 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 ESIGN CA, la revocación de Certificados y otra información de estado, los repositorios de los participantes ESIGN CA, 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

Los participantes ESIGN CA que reciben información privada la asegurarán contra compromisos y divulgación a terceros.

9.4 Privacidad de la Información Personal

9.4.1 Plan de Privacidad

E-Sign desarrollará una política de privacidad de acuerdo, la que se ajustará a las leyes de privacidad locales. E-Sign no podrá 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 publicada en un Certificado se considera no privada.

9.4.4 Responsabilidad de Protección de la Información Privada

Los participantes ESIGN CA que reciban información privada deben asegurarla contra compromisos y divulgación a terceros y deberán 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 Procedimientos Judiciales o Administrativos

Los participantes reconocen que la ESIGN CA tendrá derecho a conocer Información Confidencial/Privada si, de buena fe, E-Sign considera que:

- la revelación es necesaria en respuesta a citaciones y órdenes de registro.
- la revelación es necesaria en respuesta a un proceso judicial, administrativo o de otra índole legal durante el proceso de descubrimiento en una acción civil o administrativa, tales como citaciones, interrogatorios, las solicitudes de admisión, y 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/privada para la persona que está divulgando esta información a E-Sign. 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 ESIGN CA y Partes que Confían se regirá por los acuerdos aplicables entre los participantes como ESIGN CA. Las siguientes subsecciones de la Sección 9.5 aplican a los derechos de propiedad intelectual en relación a los Suscriptores y las 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 y sus 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 esté sujeto al Acuerdo de Tercera Parte que Confía al que se hace referencia en el Certificado.

E-Sign y sus Clientes otorgarán permiso de uso de información de revocación para llevar a cabo las funciones de Parte que Confía, sujetas al Acuerdo de Suscriptor, Acuerdo de Tercera Parte que Confía o cualquier otro acuerdo aplicable.

9.5.2 Derechos de Propiedad en la CP & CPS

Los participantes reconocen que la ESIGN CA se reserva todos los derechos de propiedad intelectual en y para esta CP, y la respectiva CPS.

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 en 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 sujetos respectivos de estos Certificados, 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 raíz auto-firmados, son propiedad de E-Sign. 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

ESIGN 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 que emiten 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 que emiten 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

Las RAs de ESIGN CA garantizan que:

- No hay declaraciones falsas de hechos en el Certificado conocidas o procedentes de las entidades que aprueban la Solicitud de Certificado o que emiten 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, como resultado de la falta de cuidado razonable en la gestión de la Solicitud de 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

Los 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 suministradas por el Suscriptor en la Solicitud de Certificado son verdaderas,
- 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 CP 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 las Partes que Confían

Los Acuerdos de Tercera Parte que Confía requieren que las Partes que Confían reconozcan que tienen la información suficiente para tomar una decisión informada en cuanto a que eligen confiar en la información contenida en un Certificado, que son los únicos responsables de decidir si deben o no confiar en dicha información, y que asumirán las consecuencias legales del incumplimiento de las obligaciones en términos de este CP.

Los Acuerdos de Tercera Parte que Confía podrán incluir representaciones y garantías adicionales.

9.6.5 Declaraciones y garantías de otros participantes

No hay estipulación.

9.7 Exclusión de garantías

En la medida permitida por la legislación aplicable, los acuerdos de suscripción y Acuerdos de Tercera Parte que Confía renuncian a garantías posibles de E-Sign, fuera del contexto de la normativa legal vigente.

9.8 Limitaciones de Responsabilidad

En la medida permitida por la legislación aplicable, los Acuerdos de Suscriptor y Acuerdos de Tercera Parte que Confía limitan la responsabilidad de E-Sign.

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

La responsabilidad (y/o limitación de la misma) de las partes que confían será la establecida en el Acuerdo de Tercera Parte que Confía.

9.9 Indemnizaciones

9.9.1 Indemnización por parte de los Suscriptores

En la medida permitida por la legislación vigente, los Suscriptores tienen la obligación de indemnizar a CAs o RAs (tanto ESIGN CA y no ESIGN CA) 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,
- la falla del Suscriptor para proteger la llave privada, o para tomar precauciones necesarias para evitar perjuicios, la pérdida, divulgación, modificación o uso no autorizado de la llave privada del Suscriptor, o
- El uso por parte del Suscriptor de un nombre 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 parte de las Partes que Confían

En la medida permitida por la legislación vigente, el Acuerdo de Tercera Parte que Confía debe requerir a las Partes que Confían compensaciones a la CA o RA (tanto ESIGN CA y no ESIGN CA) por:

- La falla de las Partes que Confían en cumplir las obligaciones de una Parte que Confía,
- La confianza de las Partes que Confían en un Certificado, cuando dicha confianza no es razonable dadas las circunstancias, o
- La falta de diligencia de las Partes que Confían en comprobar el estado de dicho Certificado para determinar si el Certificado ha caducado o revocado.

El Acuerdo de Tercera Parte que Confía pueden incluir nuevas obligaciones de indemnización.

9.10 Duración y Terminación

9.10.1 Duración

La CPS 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 CPS modificada de vez en cuando permanecerá vigente hasta que sea reemplazada por una nueva versión.

9.10.3 Efecto de la Terminación y la Supervivencia

Al término de esta CPS, los participantes ESIGN CA estarán, sin embargo, sujetos a sus disposiciones para todos los certificados emitidos por el resto de los períodos de validez de dichos certificados.

9.11 Avisos y Comunicaciones Individuales 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 Enmiendas

9.12.1 Procedimiento para la enmienda

Las enmiendas a esta CPS pueden ser hechas por la Autoridad de Administración de la Política ESIGN CA. Las modificaciones deben ser hechas o bien dentro de la forma de un documento que contenga una modificación de la CPS 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 publicada en su página web.

9.12.2 Mecanismo y Período de Notificación

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.

9.12.2.1 Período de Comentarios

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

9.12.2.2 Mecanismo de Tramitación de 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. 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 Disputas entre E-Sign y Clientes

Las disputas entre uno o más de cualquier miembro de la ESIGN CA 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 los Acuerdos de Tercera Parte que Confía deberán contener una cláusula de resolución de conflictos.

9.14 Legislación Aplicable

Sujeto a los límites que aparecen en la legislación vigente, las leyes de la República de Chile se aplicarán a: la ejecución, interpretación, ejecución y validez de esta CPS.

Esta disposición legal rige sólo a esta CPS.

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 CPS se considere inaplicable por un tribunal de justicia o tribunal que tenga autoridad, el resto de la CPS 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 permitido por la legislación aplicable, los Acuerdos de Suscriptor y Acuerdos de Tercera Parte que Confía deberán incluir una cláusula de fuerza mayor que proporcione protección a E-Sign.

9.17 Otras Disposiciones

No aplicable

Apéndice A - Tabla de siglas y definiciones

Tabla de siglas

Plazo	*Definición*
ANSI	*El American National Standards Institute.*
CP	*Certificate Policy, o Políticas de Certificado*
CPS	*Certificate Pratice Statement, o Declaración de Prácticas de Certificación.*
CRL	*Certificate Revocation List, o Lista de revocación de Certificados.*
FIPS	*Federal Information Processing Standards.*
OCSP	*Online Certificate Status Protocol, o Protocolo de estado en línea de Certificado.*
PKCS	Public-Key Cryptography Standards, *o Estándar de criptografía de llave pública.*
PKI	*Public Key Infraestructure, o Infraestructura de Llave Pública.*
RA	*Registration Authority, o Autoridad de Registro.*
RFC	*Request for Comments, o Solicitud de comentarios.*
S/MIME	*Secure Multipurpose Internet Mail Extensions.*
SSL	*Secure Sockets Layer.*
ESIGN CA	*ESIGN CA.*

Definiciones

Término	*Definición*
Administrador	*Una persona de confianza dentro de la organización, que realiza la validación y otras funciones de CA o RA.*
Certificado de Administrador	*Todo Certificado expedido a un administrador que sólo podrá ser utilizada para realizar funciones de CA o RA.*
Certificado	*Un mensaje que, al menos, establece 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.*
Solicitante de Certificado	*Una persona u organización que solicite la emisión de un Certificado por una CA.*
Solicitud de Certificado	*Una petición de un Solicitante de Certificado (o agente autorizado dl Solicitante del Certificado) a una CA para la emisión de un Certificado.*

Término	*Definición*
Cadena de Certificados	*Una lista ordenada de Certificados que contiene un Certificado de Suscriptor usuario final y Certificados de CA, el cual termina en un Certificado raíz.*
Políticas de certificación (CP)	*Este documento, que lleva por título "Políticas de Certificado ESIGN CA" y es la principal declaración de política que rige la ESIGN CA.*

Lista de revocación de Certificados (CRL)	*Listado, firmado digitalmente por una CA, de los Certificados que han sido identificados como 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 programada de la siguiente emisión de CRL , los números de serie de los Certificados revocados , y los tiempos específicos y las razones para la revocación.*
Solicitud de firma de Certificado	
Autoridad Certificadora (CA)	*Una entidad autorizada para emitir, gestionar, revocar y renovar Certificados en la red ESIGN CA.*
Prácticas de Certificación Declaración (CPS)	*Una declaración de las prácticas que E-Sign emplea al aprobar o rechazar Solicitudes de Certificados y al emitir, administrar y revocar Certificados, y exige a sus Clientes emplear.*
Frase Secreta	*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 Suscriptor y una CA o RA puede usar la Frase para autenticar al Suscriptor cuando el Suscriptor requiere revocar o renovar el Certificado del Suscriptor.*
Clase	*Un nivel específico de garantías tal como se define en la CP. Ver CP § 1.1.1.*
Auditoría de Cumplimiento	*Una auditoría periódica a la que la RA o CA se somete para determinar su conformidad con las Normas ESIGN CA que le aplican.*
Compromiso	*Una violación (o supuesta violación) de una política de seguridad, en el que una divulgación no autorizada de, o la pérdida de control sobre, la información puede 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.*
Información Confidencial/Privada	*Información que debe ser confidencial y privada de conformidad con CP § 2.8.1.*
Acuerdo de uso de CRL	*Un acuerdo que establece los términos y condiciones bajo las cuales puede ser usada una CRL o la información que ésta contiene.*
Autoridad Intermedia de certificación (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 es generado el par de llaves de una CA o RA , su llave privada es transferida a un módulo criptográfico, es generada una copia de seguridad de su llave privada, y/o su llave pública es certificada.*

Término	*Definición*
Información No verificada del Suscriptor	*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 las CA y RA aplicables no ofrecen otras garantías que no sean 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 que niegue falsamente su origen, niegue que se haya enviado, o niegue su entrega. La negación de origen incluye la negación de que la comunicación se originó de la misma fuente que una secuencia de uno o más mensajes anteriores, aun cuando la identidad asociada con el remitente es desconocida. 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 ESIGN CA puede proporcionar la prueba en apoyo de una determinación de no repudio por un tribunal, pero no constituye en sí misma no repudio.*
CA fuera de línea	*CA emisoras de raíz y otros CA intermedias designadas que se mantienen fuera de línea por razones de seguridad con el fin de protegerlos de posibles ataques de intrusos a través de la red. Estas emisoras no firman directamente Certificados de Suscriptor usuario final.*
CA en Línea	*CA que firman Certificados de Suscriptor usuario final se mantienen en línea con el fin de brindar un servicio de firma continuo.*
Protocolo de estado de Certificados en línea (OCSP)	*Un protocolo para proporcionar a las Partes que Confían la información de estado de Certificados en tiempo real.*
Período operacional	*Período que comienza con la fecha y hora en que se emite un Certificado (o en una fecha y hora posterior confirmadas en el Certificado) y termina con la fecha y la hora en que dicho Certificado expira o se revoca prematuramente.*
PKCS # 10	*Estándar de Criptografía de llave pública # 10, desarrollado por RSA Security Inc., que define una estructura para una solicitud de firma de Certificados.*
PKCS # 12	*Estándar de Criptografía de llave pública # 12, desarrollado por RSA Security Inc., que define un medio seguro para la transferencia de las llaves privadas.*
Infraestructura de Llave Pública (PKI)	*La arquitectura, organización, técnicas, prácticas y procedimientos que, en conjunto soportan la implementación y operación de un sistema criptográfico de llave pública basado en Certificados. La PKI ESIGN CA consiste en sistemas que colaboran para proporcionar e implementar la ESIGN CA.*
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 que Confía	*Una persona u organización que actúa confiando en un Certificado y/o en una firma digital.*
RSA	*Un sistema criptográfico de llave pública inventado por Rivest, Shamir y Adleman.*
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 el control multi personal sobre las operaciones llave privada de la CA en CP § 6.2.2.*

Término	*Definición*
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.*
Sub-dominio	*La parte de la ESIGN CA bajo el control de una entidad y todas las entidades de ella dependientes dentro de la jerarquía ESIGN CA.*
Sujeto	*El titular de una llave privada que corresponde a una llave pública. El término "sujeto" puede, en el caso de un Certificado de organización, referirse 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 sujeto de, y a quien 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	*Un acuerdo utilizado por una CA o RA que establece 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 ESIGN CA (la jerarquía Clase 1, 2, o 3).*
E-Sign	*E-Sign S.A., empresa con domicilio en la República de Chile y/o cualquier subsidiaria de propiedad de E-Sign responsable de las operaciones concretas en cuestión.*
Repositorio E-SIGN	*Base de datos de Certificados y otra información relevante de E-Sign accesible en línea.*
Persona de confianza	*Un empleado, contratista o consultor de una entidad dentro de la ESIGN CA responsable de la gestión de confiabilidad de la infraestructura 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 ESIGN CA que debe ser ejercido por una persona de confianza.*
Sistema de confianza	*Hardware, software y procedimientos que están razonablemente a salvo de intrusos y mal uso, proporcionan un nivel razonable de disponibilidad, confiabilidad y buen funcionamiento, son razonablemente adecuados para el desempeño de sus funciones previstas y hacen cumplir la política de seguridad aplicable. Un sistema confiable no es necesariamente un "sistema fiable" como se reconoce en la nomenclatura gubernamental clasificada.*
Participante ESIGN CA	*Una persona u organización que es uno o más de los siguientes dentro de la ESIGN CA: E-Sign, un cliente empresarial, un distribuidor o Suscriptor.*

Control de Documento

N°	Motivo	Fecha Modificación	Página	Realizado por	Fecha Aprobación	Revisado y aprobado
1.0	Creación de de Política	10/02/2020	Todo		10/02/2018	Comité de Seguridad
1.3	• Se eliminan referencias a productos no existentes Se actualiza tabla de duración de certificados. • Se reemplaza concepto PCA por Certificado raíz. • Se actualiza Apéndice A					Comité de Seguridad
2.0	• Se retira el concepto de Asociado • Se eliminan referencias a acciones u operaciones que no realiza E-Sign S.A. • Se señala el período máximo de vigencia de un certificado sin que sea autenticada nuevamente la identidad del titular • Se actualiza Apéndice A. Tabla de siglas y definiciones.	Enero-2019			Enero-2019	Comité de Seguridad
2.1	Se agrega hoja de vida Se agrega identificación del documento.	Febrero 2020	Todo	Ronald Pérez	Febrero 2020	Comité de Seguridad
2.2	Se agrega modelo de autenticación individual mediante Clave Única	Junio 2020	73	Ronald Pérez	Junio 2020	Comité de Seguridad
2.3	Se Divide documento CP/CPS, generando un documento independiente CPS	Marzo 2021	Todo	Ronald Pérez	Abril 2020	Comité de Seguridad
2.3a	Se normaliza estructura del documento	Julio 2021	Todo	Juan A. Pizarro	Julio 2021	Comité de Seguridad
2.3b	Se actualiza documento por procedimiento de validación y punto 5.4.8	Marzo 2022	23 - 44	Ronald Pérez	Marzo 2022	Comité de Seguridad
2.4	• Se incorpora punto 1.4, 1.5.3 • Se actualiza punto 3.2.3	Marzo 2023	16,19 y 24	Ronald Pérez	Marzo 2023	Comité de Seguridad
2.4	Se actualiza punto 3.2.3	Junio 2023	24	Ronald Pérez	Junio 2023	Comité de Seguridad