
Declaración de Prácticas de Certificación E-Sign S.A.

Versión 3.8.8.1

Fecha efectiva: 8 de febrero de 2013



E-Sign S.A.
Av. Andrés Bello 2777, Of. 1503
Las Condes
Santiago - Chile
+56 2 433.1501
<http://www.e-sign.cl>

Declaración de Prácticas de Certificación E-Sign S.A.

© 2010 Symantec Corporation. Todos los derechos reservados.

Fecha de publicación: Julio, 2012

Importante – Aviso de Adquisición

El 9 de Agosto, de 2010, Symantec Corporation completó la adquisición de la división de autenticación de VeriSign Inc. Como resultado Symantec es ahora el propietario registrado de este documento de Declaración de Prácticas de Certificación y de los Servicios de PKI descritos en este documento.

Sin embargo, un híbrido de referencias a ambos "VeriSign" y "Symantec" será evidente dentro de este documento por un período de tiempo hasta que sea operacionalmente práctico completar el cambio de marca de las Autoridades los servicios de Certificación. Cualquier referencia a VeriSign como una entidad corporativa deberá ser estrictamente considerada como lenguaje legado que únicamente refleja la historia de la propiedad.

Avisos de marca

Symantec, el logo Symantec y el sello de verificación son marcas registradas de Symantec Corporation o de sus afiliados en los Estados Unidos de América y en otros países. El logo VeriSign, VeriSign Trust, y otras marcas relacionadas, son marcas registradas de VeriSign, Inc o de sus afiliados o subsidiarios en los Estados Unidos de América o en otros países, y licenciadas por Symantec Corporation. Otras marcas y marcas de servicio en este documento son propiedad de sus respectivos dueños.

Sin limitar los anteriores derechos reservados, y excepto lo licenciado más abajo, ninguna parte de esta publicación puede ser reproducida, almacenada o introducida en un sistema de recuperación, o transmitida en forma alguna o por medio alguno (electrónico, mecánico, fotocopia, grabación u otros), sin previo permiso escrito de Symantec Corporation.

Sin perjuicio de lo anterior, se entrega un permiso gratuito y no exclusivo para reproducir y distribuir esta Declaración de Prácticas de Certificación de E-Sign S.A., siempre y cuando (i) este aviso de derechos de autor y los primeros párrafos sean exhibidos al principio de cada copia y (ii) este documento sea correcta y completamente reproducido, incluyendo la atribución del documento a Symantec Corporation.

Las solicitudes de cualquier otro permiso para reproducir esta Declaración de Prácticas de Certificación de E-Sign S.A. (al igual que solicitudes de copias a Symantec) se deben dirigir a:

E-Sign S.A.
Av. Andrés Bello 2777 Of. 1503
Las Condes
Santiago - Chile
Attn: Desarrollo de Prácticas
Tel: +56 2 4331501
Fax: +56 2 2033726
E-mail: practicas@e-sign.cl

TABLA DE CONTENIDOS

1	INTRODUCCIÓN	1
1.1	Resumen	2
1.2	Nombre del Documento e Identificación	3
1.3	Participantes de la PKI	3
1.3.1	Autoridades Certificadoras	3
1.3.2	Autoridades de Registro	4
1.3.3	Suscriptores	4
1.3.4	Partes que Confían	5
1.3.5	Otros Participantes	5
1.4	Uso del Certificado	5
1.4.1	Usos Apropriados del Certificado	5
1.4.2	Usos Prohibidos del Certificado	7
1.5	Administración de Política	7
1.5.1	Organización Administradora del Documento	7
1.5.2	Persona de Contacto	8
1.5.3	Persona que Determina la Idoneidad de la CPS	8
1.5.4	Procedimiento de Aprobación de la CPS	8
1.6	Definiciones y Acrónimos	8
2	Responsabilidades de Publicación y Repositorio	8
2.1	Repositorios	8
2.2	Publicación de la Información de Certificados	9
2.3	Tiempo o Frecuencia de la Publicación	10
2.4	Controles de Acceso a los Repositorios	10
3	Identificación y Autenticación	10
3.1	Nombres	10
3.1.1	Tipos de Nombres	10
3.1.2	Necesidad de que los Nombres sean Significativos	14
3.1.3	Anonimato o Seudónimos de los Suscriptores	14
3.1.4	Reglas de Interpretación de Diversas Formas de Nombre	14
3.1.5	Unicidad de los Nombres	14
3.1.6	Reconocimiento, Autenticación, y el Rol de las Marcas Comerciales	15
3.2	Validación de Identidad Inicial	15
3.2.1	Método para probar la posesión de la Llave Privada	15
3.2.2	Autenticación de la Identidad de una Organización	15
3.2.3	Autenticación de la Identidad de un Individuo	20
3.2.4	Información no Verificada del Suscriptor	21
3.2.5	Validación de Autoridad	21
3.2.6	Criterios para la Interoperación	21
3.3	Identificación y Autenticación para las Solicitudes de Reasignación de Llaves	21
3.3.1	Identificación y Autenticación Para Re Asignación de Llave Rutinaria	22
3.3.2	Identificación y Autenticación Para Reasignación de Llave Después de la Revocación	23
3.4	Identificación y Autenticación Para la Solicitud de Revocación	23
4	Requerimientos Operacionales del Ciclo de Vida de los Certificados	24
4.1	Solicitud de Certificados	24
4.1.1	¿Quién puede Presentar una Solicitud de Certificado?	24
4.1.2	Proceso de Enrolamiento y Responsabilidades	24

4.2	<i>Procesamiento de Solicitud de Certificado</i>	26
4.2.1	Realización de Funciones de Identificación y Autenticación	26
4.2.2	Aprobación o Rechazo de las Solicitudes de Certificado	26
4.2.3	Plazo para Procesar las Solicitudes de Certificados	26
4.3	<i>Emisión de Certificado</i>	27
4.3.1	Acciones de la CA durante la Emisión del Certificado	27
4.3.2	Notificaciones al Suscriptor de la Emisión del Certificado por parte de la CA	27
4.4	<i>Aceptación de Certificado</i>	27
4.4.1	Conducta que Constituye Aceptación del Certificado	27
4.4.2	Publicación del Certificado por la CA	28
4.4.3	Notificación de la Emisión del Certificado a Otras Entidades por parte de la CA	28
4.5	<i>Uso del Par de Llaves y del Certificado</i>	28
4.5.1	Uso de la Llave Privada y del Certificado por el Suscriptor	28
4.5.2	Uso de la Llave Pública y del Certificado por la Parte que Confía	28
4.6	<i>Renovación de Certificado</i>	29
4.6.1	Circunstancias para la Renovación de Certificado	29
4.6.2	Quién puede Solicitar la Renovación	29
4.6.3	Procesamiento de Solicitudes de Renovación de Certificado	29
4.6.4	Notificación al Suscriptor de la Emisión de un Nuevo Certificado	30
4.6.5	Conducta que Constituye Aceptación del Certificado de Renovación	30
4.6.6	Publicación del Certificado de Renovación por la CA	30
4.6.7	Notificación de Emisión del Certificado a Otras Entidades por parte de la CA	30
4.7	<i>Reasignación de Llaves del Certificado</i>	30
4.7.1	Circunstancias para la Reasignación de Llaves del Certificado	31
4.7.2	Quién puede solicitar la certificación de una nueva Llave Pública	31
4.7.3	Procesamiento de solicitudes de reasignación de Llaves del Certificado	31
4.7.4	Notificación al Suscriptor de la Emisión de un Nuevo Certificado	31
4.7.5	Conducta que constituye aceptación del certificado para Llaves Reasignadas	31
4.7.6	Publicación del certificado de Llave Reasignada por la CA	32
4.7.7	Notificación de la Emisión del Certificado a Otras Entidades por parte de la CA	32
4.8	<i>Modificación del Certificado</i>	32
4.8.1	Circunstancias para la Modificación del Certificado	32
4.8.2	Quién Puede Solicitar Modificación del Certificado	32
4.8.3	Procesamiento de Solicitudes de Modificación del Certificado	32
4.8.4	Notificación al Suscriptor de la Emisión de Nuevo Certificado	32
4.8.5	Conducta que Constituye Aceptación del Certificado Modificado	32
4.8.6	Publicación del Certificado Modificado por la CA	32
4.8.7	Notificación de Emisión del Certificado a Otras Entidades por parte de la CA	32
4.9	<i>Revocación y Suspensión de Certificado</i>	32
4.9.1	Circunstancias para la revocación	33
4.9.2	Quién Puede Solicitar la Revocación	34
4.9.3	Procedimiento para la Solicitud de Revocación	35
4.9.4	Período de gracia de solicitud de revocación	36
4.9.5	Tiempo dentro del cual la CA debe procesar la solicitud de revocación	36
4.9.6	Requisitos de comprobación de revocación para las Partes que Confían	36
4.9.7	Frecuencia de emisión de CRL	37
4.9.8	Latencia máxima de CRL	37
4.9.9	Disponibilidad de comprobación en línea de revocación/estado	37
4.9.10	Requisitos de comprobación de revocación en-línea	38
4.9.11	Otras formas de publicidad de revocación disponibles	38
4.9.12	Requisitos especiales en relación con compromiso de llaves	38
4.9.13	Circunstancias para la suspensión	38
4.9.14	Quién puede solicitar la suspensión	38
4.9.15	Procedimiento para la solicitud de suspensión	38
4.9.16	Límites del periodo de suspensión	39

4.10	<i>Servicios de estado de certificados</i>	39
4.10.1	Características Operacionales	39
4.10.2	Disponibilidad del Servicio	39
4.10.3	Características Opcionales	39
4.11	<i>Fin de la Suscripción</i>	39
4.12	<i>Custodia y Recuperación de Llaves</i>	39
4.12.1	Políticas y prácticas de custodia y recuperación llaves	39
4.12.2	Políticas y prácticas de encapsulamiento y recuperación de Llave de Sesión	40
5	<i>Instalación, Gestión y Controles Operacionales</i>	41
5.1	<i>Controles Físicos</i>	41
5.1.1	Localización del Sitio y Construcción	41
5.1.2	Acceso Físico	41
5.1.3	Energía y Aire Acondicionado	42
5.1.4	Exposición del Agua	42
5.1.5	Prevención y Protección contra Incendios	42
5.1.6	Almacenamiento de Medios	42
5.1.7	Eliminación de Residuos	42
5.1.8	Respaldo Fuera de las Instalaciones	43
5.2	<i>Controles de Procedimiento</i>	43
5.2.1	Funciones de Confianza	43
5.2.2	Número de personas requeridas por tarea	43
5.2.3	Identificación y Autenticación para Cada Rol	44
5.2.4	Roles que Requieren Separación de Funciones	44
5.3	<i>Controles de Personal</i>	44
5.3.1	Requisitos de Calificaciones, Experiencia, y Autorización	45
5.3.2	Procedimientos de Revisión de Antecedentes	45
5.3.3	Requisitos de Capacitación	45
5.3.4	Frecuencia y Requisitos de Reforzamiento	46
5.3.5	Frecuencia y Secuencia de Rotación Laboral	46
5.3.6	Sanciones por Acciones no Autorizadas	46
5.3.7	Requerimientos para Contratista Independiente	47
5.3.8	Documentación Proporcionada al Personal	47
5.4	<i>Procedimientos de Registro de Auditoría</i>	47
5.4.1	Tipos de Eventos Registrados	47
5.4.2	Frecuencia de Procesamiento del Registro	48
5.4.3	Periodo de Retención para el Registro de Auditoría	48
5.4.4	Protección de Registro de Auditoría	48
5.4.5	Procedimientos de Respaldo de los Registros de Auditoría	48
5.4.6	Sistema de Recolección de Auditoría (Interna vs. Externa)	48
5.4.7	Notificación al Sujeto Causante del Evento	48
5.4.8	Evaluación de Vulnerabilidades	49
5.5	<i>Archivo de Registros</i>	49
5.5.1	Tipos de Registros Archivados	49
5.5.2	Periodo de Retención Para el Archivo	49
5.5.3	Protección del Archivo	49
5.5.4	Procedimientos de Respaldo del Archivo	49
5.5.5	Requisitos de Sellado de Tiempo de los Registros	49
5.5.6	Sistema de Recopilación de Archivo (Interna o Externa)	49
5.5.7	Procedimientos para Obtener y Verificar la Información del Archivo	50
5.6	<i>Cambio de Llave</i>	50
5.7	<i>Compromiso y Recuperación de Desastres</i>	50
5.7.1	Procedimientos de Manejo de Incidentes y Compromisos	50
5.7.2	Corrupción de Recursos de Computación, Software y/o Datos	51
5.7.3	Procedimientos de Compromiso de Llave Privada de Entidad	51

5.7.4	Capacidades de Continuidad del Negocio después de un Desastre	51
5.8	Terminación de la CA o de la RA	53
6	Controles de Seguridad Técnicos	55
6.1	Generación e Instalación del Par de Llaves	55
6.1.1	Generación de Par de Llaves	55
6.1.2	Entrega de la Llave Privada al Suscriptor	56
6.1.3	Entrega de Llave Pública al Emisor del Certificado	56
6.1.4	Entrega de la Llave Pública de la CA a las Partes que Confían	57
6.1.5	Tamaños de Llaves	57
6.1.6	Generación y Control de Calidad de Parámetros de Llave Pública	59
6.1.7	Propósitos de Uso de la Llave (por campo Key Usage de X.509 v3)	59
6.2	Protección de la Llave Privada y Controles de Ingeniería del Módulo Criptográfico	59
6.2.1	Normas y Controles para el Módulo Criptográfico	59
6.2.2	Control Multi-Personal (m de un total de n) de la Llave Privada	59
6.2.3	Custodia de la Llave Privada	60
6.2.4	Respaldo de la Llave Privada	60
6.2.5	Archivo de Llave Privada	60
6.2.6	Transferencia de la Llave Privada Hacia o Desde un Módulo Criptográfico	60
6.2.7	Almacenamiento de la Llave Privada en el Módulo Criptográfico	60
6.2.8	Método de Activación de la Clave Privada	60
6.2.9	Método de Desactivación de la Llave Privada	62
6.2.10	Método de Destrucción de la Llave Privada	63
6.2.11	Clasificación de Módulo Criptográfico	63
6.3	Otros Aspectos de la Gestión de Par de Llaves	63
6.3.1	Archivo de Llaves Públicas	63
6.3.2	Períodos Operacionales del Certificado y Períodos de Uso del Par de Llaves	63
6.4	Datos de Activación	65
6.4.1	Generación e Instalación de los Datos de Activación	65
6.4.2	Protección de Datos de Activación	66
6.4.3	Otros Aspectos de los Datos de Activación	66
6.5	Controles de Seguridad Computacional	66
6.5.1	Requerimientos Técnicos Específicos de Seguridad Computacional	66
6.5.2	Calificación de Seguridad Computacional	67
6.6	Controles Técnicos de Ciclo de Vida	67
6.6.1	Controles de Desarrollo de Sistemas	67
6.6.2	Controles de Gestión de Seguridad	68
6.6.3	Controles de Seguridad del Ciclo de Vida	68
6.7	Controles de Seguridad de la Red	68
6.8	Sellado de Tiempo	68
7	Perfiles de Certificado, CRL y OCSP	68
7.1	Perfil de Certificado	68
7.1.1	Número(s) de Versión	69
7.1.2	Extensiones de Certificado	69
7.1.3	Identificadores de Objeto de Algoritmos	71
7.1.4	Formas de Nombres	71
7.1.5	Restricciones de Nombres	71
7.1.6	Identificador de Objeto de Política de Certificación	71
7.1.7	Uso de la Extensión Policy Constraints	72
7.1.8	Sintaxis y Semántica de Calificadores de Política	72
7.1.9	Semántica de Procesamiento para la Extensión Crítica Certificate Policies	72
7.2	Perfil de CRL	72

7.2.1	Número(s) de Versión	73
7.2.2	Extensiones CRL y CRL Entry	73
7.3	Perfil OCSP	73
7.3.1	Número(s) de Versión	73
7.3.2	Extensiones OCSP	73
8	Auditorías de Cumplimiento y Otras Evaluaciones	74
8.1	Frecuencia y Circunstancias Evaluaciones	74
8.2	Identidad/Calificaciones del Evaluador	75
8.3	Relación del Evaluador con la Entidad Evaluada	75
8.4	Tópicos Cubiertos por la Evaluación	75
8.5	Acciones a Tomar como Resultado de la Deficiencia	75
8.6	Comunicación de los Resultados	75
9	Otros Aspectos Comerciales y Legales	77
9.1	Tarifas	77
9.1.1	Tarifas de Emisión o Renovación de Certificados	77
9.1.2	Tarifas de Acceso a los Certificados	77
9.1.3	Tarifa para Revocación o Acceso a Información de Estado	77
9.1.4	Tarifas por Otros Servicios	77
9.1.5	Política de Reembolsos	77
9.2	Responsabilidad Financiera	78
9.2.1	Cobertura de Seguros	78
9.2.2	Otros Activos	78
9.2.3	Cobertura de Garantía Extendida	78
9.3	Confidencialidad de la Información de Negocios	78
9.3.1	Alcance de la Información Confidencial	78
9.3.2	Información Fuera del Alcance de Información Confidencial	78
9.3.3	Responsabilidad de Proteger la Información Confidencial	79
9.4	Confidencialidad de Información Personal	79
9.4.1	Plan de Privacidad	79
9.4.2	Información Tratada como Privada	79
9.4.3	Información que no se Considera Privada	79
9.4.4	Responsabilidad de Proteger Información Privada	79
9.4.5	Notificación y Consentimiento para el Uso de Información Privada	79
9.4.6	Divulgación de Conformidad con Proceso Judicial o Administrativo	79
9.4.7	Otras Circunstancias de Divulgación de Información	79
9.5	Derechos de Propiedad Intelectual	80
9.5.1	Derechos de Propiedad en Certificados e Información de Revocación	80
9.5.2	Derechos de Propiedad en la CPS	80
9.5.3	Derechos de Propiedad en Nombres	80
9.5.4	Derechos de Propiedad en Llaves y Material de Llaves	80
9.6	Declaraciones y Garantías	81
9.6.1	Declaraciones y Garantías de la CA	81
9.6.2	Declaraciones y Garantías de la RA	82
9.6.3	Declaraciones y Garantías del Suscriptor	82
9.6.4	Declaraciones y Garantías de la Parte que Confía	83
9.6.5	Declaraciones y Garantías de los Demás Participantes	83
9.7	Renuncia de Garantías	83
9.8	Limitaciones de Responsabilidad	83
9.9	Indemnizaciones	84

9.9.1	Indemnización por los Suscriptores	84
9.9.2	Indemnización por las Partes que Confían	84
9.10	<i>Vigencia y Término</i>	84
9.10.1	Vigencia	84
9.10.2	Término	84
9.10.3	Efecto del Término y Supervivencia	85
9.11	<i>Avisos Individuales y Comunicaciones con los Participantes</i>	85
9.12	<i>Modificaciones</i>	85
9.12.1	Procedimiento de Enmiendas	85
9.12.2	Mecanismo y Período de Notificación	85
9.12.3	Circunstancias en las que el OID Debe ser Cambiado	86
9.13	<i>Disposiciones de Resolución de Disputas</i>	86
9.13.1	Disputas entre Symantec, E-Sign y Clientes	86
9.13.2	Disputas con Suscriptores Usuarios Finales o Partes que Confían	86
9.14	<i>Ley Aplicable</i>	86
9.15	<i>Conformidad con la Ley aplicable</i>	87
9.16	<i>Disposiciones Varias</i>	87
9.16.1	Acuerdo Completo	87
9.16.2	Asignación	87
9.16.3	Divisibilidad	87
9.16.4	Cumplimiento (Honorarios de Abogado y Renuncia de Derechos)	87
9.16.5	Fuerza Mayor	87
9.17	<i>Otras Disposiciones</i>	87
<i>Apéndice A. Tabla de Acrónimos y Definiciones</i>		88
Tabla de Acrónimos		88
Definiciones		88

1 INTRODUCCIÓN

Este documento es la Declaración de Prácticas de Certificación (“CPS”) de E-Sign S.A. (“E-Sign”) Esta CPS establece las prácticas que las autoridades certificadoras (“CAs”) de E-Sign, incluida la de Firma Electrónica Avanzada, utilizan para proporcionar los servicios de certificación que incluyen, pero no están limitados a: emisión, administración, revocación y renovación de certificados, conforme a los requerimientos específicos de la Política de Certificación de la Symantec Trust Network (“CP”).

La CP es la principal declaración de política que regula la STN. Establece los requerimientos de negocios, legales y técnicos, para la aprobación, emisión, administración, uso, revocación y renovación de certificados digitales dentro de la STN y la prestación de servicios de confianza asociados. Estos requerimientos, llamados los “Estándares STN”, protegen la seguridad e integridad de la STN, se aplican a todos sus participantes y, por lo tanto, permiten asegurar un nivel de confianza uniforme a través de toda la STN. Mayor información relacionada con la STN y los estándares STN puede ser encontrada en la CP.

E-Sign tiene autoridad sobre una parte de la STN denominada su “Subdominio” de la STN. El Subdominio E-Sign incluye las entidades subordinadas a ella, como por ejemplo sus Clientes, Suscriptores y Partes que Confían.

Mientras la CP establece los requerimientos que todos los participantes de la STN deben cumplir, esta CPS describe como E-Sign cumple estos requerimientos dentro del Subdominio E-Sign de la STN. Más específicamente, esta CPS establece los procedimientos que E-Sign emplea para:

- Administrar de manera segura la infraestructura que soporta el Subdominio E-Sign de la STN y
- Emitir, administrar, revocar y renovar Certificados bajo la STN.

dentro del Subdominio E-Sign de la STN, y en concordancia con los requerimientos de la CP y los Estándares STN.

Esta CPS se encuentra ajustada al Internet Engineering Task Force (IETF) RFC 3647 para la construcción de Políticas de Certificado y de Declaraciones de Prácticas de Certificación.

Las CA dentro de la jerarquía de la Symantec Trust Network se ajustan a la versión actual de los requisitos de CA/ Browser Forum (línea de base CABF) para la emisión y gestión de los certificados públicos de confianza publicados en www.cabforum.org. En el caso de cualquier incompatibilidad entre este documento y esos requisitos, dichos requisitos tendrán prioridad sobre este documento.

En este momento, los certificados SSL de validación de dominio y de validación de organización emitidos por las CA de E-Sign en el marco de las presentes CPS se rigen por los requisitos CABF. Estos certificados son emitidos conteniendo el identificador de la política correspondiente (s) especificado en la sección 1.2 de la CP que señala la adhesión y cumplimiento de estos requisitos. Las CA de E-Sign afirman que todos los Certificados emitidos que contienen dichos identificador(es) de la política son emitidos y administrados de conformidad con los requisitos CABF.

El sub-dominio de E-Sign en la STN, se encuentra certificado por la CA de Symantec Trust Network y opera en cumplimiento de los requisitos de la Declaración de Prácticas de Certificación de E-Sign.

1.1 Resumen

E-Sign es un Centro de Servicio como se describe en CP § 1.1.2.1.2 lo que significa E-Sign puede aprobar o rechazar Solicitudes de Certificados en el caso de los Certificados a Nivel Minorista o, en el caso de los Certificados Empresariales, acuerda con un Centro de Procesamiento para proporcionar a los Clientes Empresariales servicios de back-end para el ciclo de vida de certificados. Los Afiliados Centros de Servicio que proporcionan Certificados de cliente ("Centros de Servicio Cliente") se convierten en CAs dentro de la STN, pero externalizan las funciones de back-end a Symantec o a otro Centro de Procesamiento. Al proporcionar Certificados de servidor, sin embargo, los Centros de Servicio se convierten en RAs dentro de la STN de una CA de Symantec que emite Certificados de servidor. Estos Centros de Servicio ("Centros de Servicio") desempeñarán funciones de validación para aprobar o rechazar solicitudes de Certificados para Secure Server ID o Global Server ID. Los Centros de Servicio también pueden proveer Managed PKI a sus Clientes Empresariales. Estos Clientes de Managed PKI entran en un acuerdo de Managed PKI con el Centro de Servicio, que en virtud de su contrato con Symantec u otro Centro de Procesamiento, acuerda que el Centro de Procesamiento ofrezca servicios de back-end para el ciclo de vida de certificados a estos Clientes Managed PKI.

Esta CPS es específicamente aplicable a:

- Autoridades Certificadoras Primarias Públicas de Symantec (PCAs)
- CAs de Infraestructura de E-Sign, y CAs Administrativas de E-Sign que soportan la Symantec Trust Network.
- CAs Públicas de E-Sign y CAs de Clientes empresariales que emiten certificados bajo el subdominio E-Sign de la STN.

De modo más general, la CPS también regula el uso de los servicios de la STN, dentro del Subdominio E-Sign de la STN por todos los individuos y entidades dentro del Subdominio E-Sign (colectivamente denominados, "Participantes de Subdominio E-Sign"). Las CAs Privadas y las jerarquías administradas por E-Sign fuera de la STN están fuera del alcance de esta CPS.

La STN incluye cuatro Clases diferentes de certificados, Clases 1 a 4. La Política de Certificación es un único documento que define las políticas de esos certificados, una para cada una de las Clases, y fija los estándares STN para cada clase.

E-Sign ofrece actualmente tres clases de certificados dentro de su subdominio de la STN. Esta CPS describe de qué forma E-Sign cumple con los requisitos de la CP para cada clase dentro de su subdominio. Por esto, la CPS cubre, en un único documento, las prácticas y procedimientos referentes a la emisión y administración de las tres clases de certificado.

E-Sign puede publicar Declaraciones de Prácticas de Certificación complementarias a esta CPS, para cumplir con requerimientos específicos de política del Gobierno, u otros requerimientos y estándares de la industria.

Estas políticas de certificado complementarias deben ser puestas a disposición de los suscriptores de los certificados emitidos bajo las políticas complementarias, y de sus Partes que Confían.

La CPS es sólo uno de un conjunto de documentos relevantes para el Subdominio de E-Sign de la STN. Los otros documentos incluyen:

- Documentos auxiliares confidenciales relacionados con seguridad y operaciones¹ que complementan las CP y CPS, suministrando mayor grado de detalle en los requisitos, tales como:
 - Política de seguridad física de Symantec, que entrega los principios de seguridad que regulan la infraestructura de la STN
 - Guía Symantec de Requerimientos de Seguridad y Auditoría (SAR), que describe detalladamente los requerimientos para Symantec y Afiliados referentes a seguridad del personal, física, de telecomunicaciones, lógica y de la administración de llaves criptográficas, y
 - Guía de Referencia de Ceremonia de Llaves, que describe detalladamente los requerimientos operacionales en materia de administración de llaves.
- Acuerdos complementarios establecidos por E-Sign. Estos acuerdos vinculan legalmente a Clientes, Suscriptores y Partes que Confían de E-Sign. Entre otras cosas, los acuerdos transmiten los Estándares STN para dichos Participantes de la STN y, en algunos casos, especifican prácticas respecto de cómo se deben cumplir los Estándares STN.

En muchas instancias, la CPS se refiere a estos documentos para prácticas específicas y detalladas que implementan estándares STN, dado que incluir dichas especificaciones dentro de la CPS podría comprometer la seguridad del Sub.-dominio de E-Sign de la STN.

1.2 Nombre del Documento e Identificación

Este documento es la Declaración de Prácticas de Certificación de E-Sign. Los certificados STN contienen los valores identificadores de objeto correspondientes a la clase de certificado aplicable bajo la STN. Por lo tanto, E-Sign no ha asignado a esta CPS un valor identificador de objeto. Los Identificadores de Objeto de Política de Certificados son utilizados conforme a lo señalado en la Sección 7.1.6.

Los certificados SSL de validación de dominio y de organización contienen el valor 2.16.840.1.113733.1.7.54, que indica la adhesión y el cumplimiento de los requisitos básicos de CA / Browser Forum.

1.3 Participantes de la PKI

1.3.1 Autoridades Certificadoras

El término de Autoridad Certificadora (CA) es un término genérico que se refiere a todas aquellas entidades autorizadas para emitir certificados de llave pública dentro de la STN. El término CA engloba una subcategoría de emisores denominados Autoridades Primarias de Certificación ("PCA"). Las PCA actúan como raíces de cuatro dominios², uno por cada clase de certificado. Cada PCA es una entidad de Symantec. Las Autoridades Certificadoras de E-Sign que emiten certificados a suscriptores usuarios finales y otras CAs están subordinadas a las PCAs.

Symantec también opera las CAs "Symantec® Universal Root Certification Authority" y "Symantec ECC Universal Root Certification Authority". Las CAs Universal Root

¹ A pesar de que estos documentos no están públicamente disponibles, sus especificaciones están incluidas en la auditoría Annual Web Trust for Certification Authorities de Symantec y puede ser puesta a disposición de clientes bajo un Acuerdo especial.

² Los certificados de Class 4 no son actualmente emitidos por la STN

emiten CAs subordinadas Clase 3 y en casos especiales, Clase 2.

Los clientes empresariales de E-Sign pueden operar sus propias CAs como una CA subordinada a una PCA de E-Sign. Dichos clientes entablan una relación contractual con E-Sign, en virtud de la cual deben atenerse a todos los requerimientos de las CP STN y de la CPS de E-Sign. Estas CAs subordinadas pueden, sin embargo, implementar prácticas más estrictas de acuerdo a sus requerimientos internos.

Una CA STN que técnicamente está fuera de las tres jerarquías bajo cada una de las PCAs es Secure Server Certification Authority. Esta CA no tiene una CA superior, como una raíz o PCA. Más bien, la CA Secure Server actúa como su propia raíz, y se ha emitido a sí misma un Certificado raíz autofirmado. Emite también certificados para Suscriptores usuarios finales. Por lo tanto, la Jerarquía Secure Server consiste solamente en la CA Secure Server. La CA Secure Server emite certificados Secure Server, los que son considerados Certificados Organizacionales Class 3.

La CA Secure Server Certification Authority emplea prácticas de ciclo de vida que son substancialmente similares con aquellas de otras CAs de Class 3 dentro de la STN. Así, Symantec ha aprobado y designado la CA Secure Server CA como una CA Class 3 dentro de la STN. Se considera que los certificados que ella emita otorgan garantía de confianza comparable con otros Certificados Organizacionales de Class 3.

1.3.2 Autoridades de Registro

Una Autoridad de Registro (RA) es una entidad que ejecuta labores de identificación y autenticación de solicitantes de Certificados de usuario final, inicia o transmite solicitudes de revocación de certificados de usuario final, y aprueba solicitudes de renovación o regeneración de llaves de certificados, en nombre de una CA de la STN. E-Sign puede actuar como RA para los certificados que emite.

Terceras personas que entablan una relación contractual con E-Sign, pueden operar sus propias RA y autorizar la emisión de certificados por una CA de E-Sign. Las RAs de terceras partes deben cumplir con todos los requisitos de la CP de la STN, la CPS de E-Sign y los términos del acuerdo contractual de servicios empresariales con E-Sign. Sin embargo, las RAs pueden implementar prácticas más restrictivas, de acuerdo a sus requerimientos internos³.

1.3.3 Suscriptores

Los suscriptores, dentro del Subdominio E-Sign de la STN, incluyen todos los usuarios finales (incluidos entidades) de certificados emitidos por una CA de E-Sign. Un suscriptor es la entidad señalada como Suscriptor usuario final de un certificado. Los Suscriptores usuarios finales de un certificado pueden ser individuos, organizaciones o componentes de infraestructura, como firewalls, routers, servidores confiables u otros dispositivos utilizados para comunicaciones seguras dentro de una Organización.

En ciertos casos los certificados son emitidos directamente a entidades o individuos para su propio uso. Sin embargo, pueden existir otras situaciones en las cuales la parte requirente de un certificado es distinta del sujeto al cual corresponde la credencial. Por ejemplo, una organización puede requerir certificados para permitir que sus empleados representen a la organización en transacciones o negocios electrónicos. En tales situaciones, la entidad que solicita la emisión de los certificados (es decir paga por él, ya sea a través de la suscripción a un servicio específico, o como

³ Un ejemplo de una RA de terceros es un cliente de servicios Managed PKI.

el emisor mismo) es diferente de la entidad que es el sujeto del certificado (generalmente el titular de la credencial). En esta CPS son utilizados dos términos distintos para distinguir estos dos roles: “Suscriptor” es la entidad que contrata con E-Sign la emisión de credenciales y; “Sujeto” es la persona a la cual se encuentra asociada la credencial. El Suscriptor carga con la responsabilidad última por el uso de la credencial pero el Sujeto es el individuo que es autenticado cuando la credencial es presentada.

Cuando se utiliza “Sujeto”, es para distinguirlo del suscriptor. Cuando se utiliza “Suscriptor”, puede significar el Suscriptor como una entidad distinta, o puede estar siendo usado para abarcar a ambas. El contexto en el cual sea usado en esta CPS permitirá distinguir su significado correcto.

Técnicamente las CAs también son suscriptores de certificados dentro de la STN, ya sea como una PCA emitiendo un certificado autofirmado para ella misma, o como una CA a la que se le emite un certificado por parte de una CA superior. Las referencias a “entidades finales” y “suscriptores” en esta CPS, sin embargo, aplican solamente a Suscriptores usuarios finales.

1.3.4 Partes que Confían

Una Parte que Confía es un individuo o una entidad que actúa confiando en un certificado y/o en una firma digital emitida bajo el subdominio E-Sign. Una Parte que Confía puede o no ser también un Suscriptor bajo el subdominio E-Sign.

1.3.5 Beneficiarios de los certificados

Los beneficiarios de los certificados son identificados de acuerdo con las directrices de CA / Browser Forum. Los beneficiarios de los Certificados de las CA de E-Sign incluyen, pero no están limitados a:

1. El suscriptor que es parte en el Acuerdo de Suscriptor de Certificado;
2. Todos los proveedores de aplicaciones de software con los que la entidad emisora raíz se ha celebrado un contrato para la inclusión de su certificado raíz en el software distribuido por dicho proveedor de aplicación de software, y
3. Todas las Partes que Confían que razonablemente confían en un Certificado Válido

1.3.6 Otros Participantes

No aplicable.

1.4 Uso del Certificado

1.4.1 Usos Apropriados del Certificado

1.4.1.1 Certificados Emitidos a Individuos

Los Certificados Individuales son usados normalmente por individuos para firmar o encriptar correos electrónicos (e-mail) y para autenticarse en aplicaciones (autenticación de cliente). Aun cuando los usos más comunes para un certificado individual están incluidos en la Tabla 1 de más abajo, un certificado individual puede ser utilizado para propósitos distintos, a condición de que la Tercera Parte que Confía pueda confiar razonablemente en que el certificado y su uso no está en modo alguno prohibido por la ley, la CP STN, la CPS bajo las cuales ha sido emitido dicho certificado o cualquiera de los acuerdos con Suscriptores.

Clase de certificado	Nivel de Seguridad			Uso		
	Nivel de seguridad bajo	Nivel de seguridad medio	Nivel de seguridad alto	Firmar	Encriptar	Autenticación de Cliente
Certificados Class 1	✓			✓	✓	✓
Certificados Class 2		✓		✓	✓	✓
Certificados Class 3			✓	✓	✓	✓

Tabla 1. Uso de certificados individuales.

1.4.1.2 Certificados Emitidos a Organizaciones

Los Certificados organizacionales son emitidos a organizaciones luego de haber sido verificado que la Organización existe legalmente, y que los otros atributos de la Organización incluidos en el certificado (excluyendo la información no verificada del suscriptor) hayan sido autenticados, como por ej. la propiedad de un dominio de Internet o de correo electrónico. No es el objetivo de esta CPS el limitar los usos que pueden darse a los Certificados organizacionales. Mientras que los usos más comunes se encuentran señalados en la Tabla 2 de más abajo, un Certificado organizacional puede ser utilizado para otros propósitos, siempre y cuando una tercera Parte que Confía puede razonablemente confiar en que el certificado y su uso no se encuentra prohibido en modo alguno por la ley, por la CP de STN, por cualquier CPS bajo la cual haya sido emitido el certificado, o cualquier acuerdo con Suscriptores.

Clase de certificado	Nivel de Seguridad		Uso			
	Nivel de seguridad alto	Nivel de seguridad medio	Firma de Código o Contenido	Sesiones seguras SSL/TLS	Autenticación	Firma y encriptación
Certificados Class 3	✓	✓	✓	✓	✓	✓

Tabla 2. Uso de Certificados Organizacionales⁴.

1.4.1.3 Niveles de seguridad

Los **Certificados de bajo nivel de seguridad** son certificados que no deben ser usados para autenticar o asegurar no repudio. La firma digital provee un nivel modesto de seguridad de que el e-mail proviene de un remitente con una dirección e-mail cierta. El Certificado, no obstante, no entrega garantía de la identidad del Suscriptor. La aplicación de cifrado permite a una Parte que Confía el uso del Certificado de un Suscriptor para cifrar los mensajes al Suscriptor, si bien la Parte que Confía remitente

⁴ "En ciertas circunstancias, los Certificados Class 2 pueden ser emitidos por un cliente de Managed PKI a una organización afiliada (y no a un individuo no perteneciente a una organización). Dicho certificado puede ser utilizado solamente para una autenticación organizacional y para firma de aplicación. A menos que haya sido expresamente autorizado por E-Sign a través de un Acuerdo de Servicio para Empresas que imponga prácticas de autenticación y exigencias de prácticas consistentes con estas CPS, los Suscriptores tendrán prohibido utilizar dichos certificados para firma de código y contenido, encriptación SSL y firma S/MIME, y el uso de esa llave debe ser inhabilitada para dichos usos."

no puede estar segura de que el destinatario es de hecho la persona nombrada en el certificado.

Los **certificados de nivel medio de seguridad** son certificados adecuados para garantizar algunas comunicaciones vía e-mail inter e intra organizacional, comercial y personal que requieren un nivel medio de seguridad respecto de la identidad del Suscriptor, en relación a los certificados Class 1 y 3.

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

1.4.2 Usos Prohibidos del Certificado

Los certificados deben ser usados solamente en la medida que su uso sea consistente con la normativa legal aplicable, y en particular, los certificados deben ser utilizados sólo de manera permitida por la normativa sobre importaciones y exportaciones.

Ni los certificados de Symantec ni los de E-Sign han sido diseñados, concebidos ni autorizados para uso o reventa como equipamiento de control en circunstancias peligrosas o para usos que requieren un rendimiento a prueba de fallas, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicación aérea, sistemas de control de tráfico aéreo, o sistemas de control de armas, en los que una falla podría acarrear directamente la muerte, lesiones personales o daños medioambientales graves. Además, los Certificados Class 1 no deberán utilizarse como prueba de identidad o como soporte de no repudio de identidad o autoridad. Los Certificados de Cliente están destinados a aplicaciones de cliente y no deberán utilizarse como Certificados de servidor o Certificados Organizacionales.

Los certificados de CA no deben ser utilizados para una función distinta de las funciones de CA. Asimismo, los certificados para Suscriptores usuarios finales no deben ser usados como certificados de CA.

Symantec y E-Sign regeneran periódicamente las llaves de CAs Intermedias. Las aplicaciones de terceros o plataformas que tienen una CA Intermedia incorporada como un certificado raíz, pueden no funcionar como fueron diseñadas después de que la llave de la CA Intermedia haya sido regenerada. Por lo tanto, E-Sign no garantiza el uso de las CA Intermedias como certificados raíz y recomienda que las CA Intermedias no sean embebidas en aplicaciones y/o plataformas como certificados raíz. E-Sign recomienda el uso de raíces PCA como certificados raíz.

1.5 Administración de Política

1.5.1 Organización Administradora del Documento

E-Sign S.A.
Avenida Andrés Bello 2.777, oficina 1503
Las Condes
Santiago
Chile
At: Desarrollo de Prácticas - CPS
Fonos: (56) (2) 433.1500, (56) (2) 433.1501
Fax: (56) (2) 203 3726
practicas@e-sign.cl

1.5.2 Persona de Contacto

The Certificate Policy Manager
Symantec Trust Network Policy Management Authority
a cargo de E-Sign S.A.
Avenida Andrés Bello 2.777, oficina 1503
Las Condes
Santiago
Chile
Attn: Practices Development – CPS
Fonos: (56) (2) 433.1500, (56) (2) 433.1501
Fax: (56) (2) 203 3726
practicass@e-sign.cl

1.5.3 Persona que Determina la Idoneidad de la CPS

La organización identificada en la Sección 1.5.2 es responsable de determinar si esta CPS y otros documentos en la naturaleza de declaración de prácticas de certificación que suplementan o están subordinadas a esta CPS son idóneas bajo la CP y esta CPS.

1.5.4 Procedimiento de Aprobación de la CPS

La aprobación de esta CPS y sus posteriores modificaciones se harán por el PMA. Las modificaciones deberán también constar en un documento que contenga una forma modificada de la CPS o un aviso de actualización. Las versiones modificadas o actualizaciones estarán vinculadas a la sección Actualizaciones y Avisos de las Prácticas del Repositorio E-Sign, la que se encuentra en la sección de Actualización de Prácticas: <https://www.e-sign.cl/repositorios>. Las actualizaciones sustituyen a las disposiciones señaladas o que estén en conflicto de la versión de referencia de la CPS.

1.6 Definiciones y Acrónimos

Ver Apéndice A para las definiciones y acrónimos.

2 Responsabilidades de Publicación y Repositorio

2.1 Repositorios

E-Sign es responsable por las funciones de repositorio para sus propias CA y para las CA de sus Clientes Empresariales (ya sea de Managed PKI o clientes ASB). E-Sign publica los certificados que emite para Suscriptores usuarios finales en el repositorio de acuerdo con CPS 2.2.

Después de la revocación de un Certificado de Suscriptor usuario final, E-Sign publica un aviso de tal revocación en el repositorio. E-Sign emite CRLs para sus propias CAs y para las CAs de los clientes empresariales dentro de su Subdominio, de conformidad con las disposiciones de esta CPS. Además, respecto de los clientes empresariales que han contratado el servicio de Online Certificate Status Protocol ("OCSP"), E-Sign ofrece servicios OCSP de conformidad con las disposiciones de esta CPS.

2.2 Publicación de la Información de Certificados

E-Sign mantiene un repositorio basado en web que permite a las Partes que Confían hacer consultas en línea sobre la revocación y otra información del estado del Certificado. E-Sign entrega a las Partes que Confían información sobre cómo encontrar el repositorio adecuado para comprobar el estado del Certificado y si el servicio de OCSP (Online Certificate Status Protocol) está disponible, sobre cómo encontrar el respondedor OCSP correcto.

E-Sign publica los Certificados que emite en nombre de sus propias CAs. Después de la revocación de un certificado de suscriptor usuario final, E-Sign publicará el aviso de dicha revocación en el repositorio. Además, E-Sign emite Listas de Certificados Revocados (CRL) y, si están disponibles, proporciona servicios de OCSP (Online Certificate Status Protocol) para sus propias CAs.

E-Sign publicará siempre una versión actualizada de los siguientes documentos:

- La CP STN
- La CPS de E-Sign,
- Acuerdos de Suscriptor de Certificado Digital
- Acuerdos de Parte que Confía

E-Sign es responsable de la función de repositorio para las CAs de E-Sign y CAs de Clientes Empresariales que emiten certificados en el Sub.-dominio de E-Sign de la STN

E-Sign publica cierta información de la CA en la sección de repositorio del sitio web de E-Sign en <https://www.e-sign.cl>, como se describe a continuación.

E-Sign publica las CP STN, esta CPS, Acuerdos de Suscriptor y Acuerdos de Parte que Confía en la sección de repositorio del sitio web de E-Sign.

E-Sign publica Certificados de acuerdo con la Tabla 3

Tipo de certificado	Requerimientos de publicación
PCA STN y CAs Raíz Emisoras de la STN	Disponible para la Parte que Confía mediante inclusión en el software actual de navegación y como parte de la Cadena de Certificación que puede ser obtenida con el Certificado de Suscriptor usuario final, a través de las funciones de búsqueda descritas más adelante.
Certificados de CA emisoras de E-Sign	Disponible para la Parte que Confía como parte de la cadena de certificados que puede ser obtenida con el Certificado de Suscriptor usuario final, a través de las funciones de búsqueda descritas más adelante.
Certificado de la CA de E-Sign que soporta los Certificados de Managed PKI Lite y Certificados de CA de los Clientes Managed PKI	Disponible a través de la consulta en el servidor de directorio LDAP en directory.verisign.com .
Certificados de Respondedores OCSP Symantec	Disponible a través de la búsqueda en el servidor de directorio LDAP en directory.verisign.com .
Certificados de Suscriptores usuarios finales excepto por ciertos Certificados Class 3 dependiendo de su uso	Publicados opcionalmente y disponibles para Partes de Confianza mediante funciones de búsqueda en el repositorio E-Sign en https://digitalid.e-sign.cl/c2/client/search.htm , https://digitalid.e-sign.cl/fea/client/search.htm , https://arech.e-sign.cl/eu/client/search.htm , https://arech.e-sign.cl/ro/client/search.htm y consulta en el servidor de directorio LDAP de Symantec en directory.verisign.com , excepto por los certificados SSL Class 3 y Certificados Code Signing los cuales están disponibles mediante funciones de búsqueda en el Repositorio E-Sign en https://digitalid.e-sign.cl/global/services/globalserver/search.htm y

	https://digitalid.e-sign.cl/secure/services/server/search.htm .
Certificados de Suscriptores usuarios finales, emitidos a través de Clientes de Managed PKI	Disponible a través de las funciones de búsqueda descritas anteriormente, aunque a discreción del Cliente de Managed PKI, el Certificado puede ser accesible sólo mediante búsqueda usando el número de serie del Certificado.

Tabla 3 – Requerimientos de Publicación de Certificados

2.3 Tiempo o Frecuencia de la Publicación

Las actualizaciones de esta CPS se publican de conformidad con la Sección 9.12. Las actualizaciones a los Acuerdos de Suscriptor y Acuerdos de Parte que Confía son publicadas cuando son emitidas. Los certificados son publicados cuando son emitidos. La información sobre el estado de los certificados se publica de conformidad con las disposiciones de esta CPS.

2.4 Controles de Acceso a los Repositorios

La información publicada en la sección de repositorio de la página web de E-Sign es información de acceso público. El acceso de sólo lectura a dicha información no está restringido. E-Sign requiere que las personas acepten el Acuerdo de Parte que Confía o el Acuerdo de Uso de la CRL como condición para acceder a los Certificados, a información sobre el estado de los certificados o a la CRL. E-Sign ha implementado medidas de seguridad lógicas y físicas para evitar que personas no autorizadas puedan añadir, borrar o modificar las entradas del repositorio.

3 Identificación y Autenticación

3.1 Nombres

A menos que se indique lo contrario en la CP de la STN, la presente CPS o el contenido del certificado digital, los nombres que figuran en los certificados emitidos bajo la STN, están autenticados.

3.1.1 Tipos de Nombres

Si bien la red STN es ahora propiedad de Symantec Corporation han sido emitidos certificados antiguos en nombre del propietario anterior. Cualquier certificado antiguo que indique la Organización (O) como "VeriSign Inc." y la Unidad Organizacional (OU) como "VeriSign Trust Network" deberá ser entendido como referencia a Symantec Corporation y la Symantec Trust Network, respectivamente.

Los certificados de CA de E-Sign contienen Nombres Distinguidos X.501 en los campos Emisor y Sujeto. Los Nombres Distinguidos de las CA de E-Sign constan de los componentes especificados en la Tabla 4.

Atributo	Valor
País (C) =	"CL", "US" o el código ISO del país donde opera la CA.
Organización (O) =	"Symantec Corporation." ⁵ o "E-Sign S.A." o nombre de la organización ⁶ .

⁵ Una excepción a esto es la AC Secure Server CA, que indica "RSA Data Security, Inc.," pero es ahora una Autoridad Certificadora de Symantec.

⁶ Para una AC dedicada a una organización cliente, el componente (o =) será el nombre legal de la organización

Unidad Organizacional(OU) =	Los certificados CA de E-Sign pueden contener varios atributos OU. Tales atributos pueden contener uno o más de los siguientes: <ul style="list-style-type: none"> • Nombre del CA • Symantec Trust Network • Una declaración haciendo referencia a los términos del Acuerdo de la Parte que Confía aplicable que rigen el uso del certificado • Un aviso de copyright. • Texto para describir el tipo de certificado.
Estado o provincia (S)=	No se utiliza.
Localidad (L) =	No se usa, excepto para la CA Symantec Commercial Software Publishers CA que utiliza "Internet".
Nombre común (CN) =	Este atributo incluye el nombre de CA (si el nombre de CA no está especificado en un atributo OU) o no es utilizado.

Tabla 4 - Atributos de Nombre Distinguido en los certificados de CA

Los Certificados de Suscriptor usuario final contienen un nombre distinguido X.501 en el campo nombre del sujeto que consiste en los componentes especificados en la tabla 5 a continuación.

Atributo	Valor
País (C) =	"CL", el código ISO del país donde opera la CA o no se utiliza.
Organización (O) =	El atributo Organización se utiliza de la siguiente manera: <ul style="list-style-type: none"> • "E-Sign S.A.." para respondedores OCSP y, opcionalmente, para los Certificados individuales que no tienen afiliación a una organización. • Nombre de la organización suscriptora para los Certificados de servidor Web y Certificados individuales que tienen afiliación a una organización.
Unidad Organizacional(OU) =	Los Certificados de Suscriptor de usuario final E-Sign pueden contener múltiples atributos OU. Tales atributos pueden contener uno o más de los siguientes: <ul style="list-style-type: none"> • Unidad Organizacional suscriptora (para los Certificados organizacionales y Certificados individuales que tienen afiliación a una organización) • Symantec Trust Network • Una declaración con referencia al Acuerdo de Parte que Confía aplicable que rige los términos de uso del Certificado • Un aviso de derechos de copia • "Authenticated by E-Sign S.A. " y "Member, Symantec Trust Network" en Certificados cuyas solicitudes hayan sido autenticadas por E-Sign • "Persona Not Validated" para Certificados Individuales Class 1 • Texto para describir el tipo de Certificado. • "No organization affiliation" (para certificados de firma de código emitido a personas)
Estado o provincia (S)=	Indica el Estado o Provincia del Suscriptor (Estado no es un campo obligatorio en certificados emitidos a personas).
Localidad (L) =	Indica la Localidad o Ciudad del Suscriptor (Localidad no es un campo obligatorio en certificados emitidos a personas).
Nombre común (CN) =	Este atributo incluye: <ul style="list-style-type: none"> • El Nombre de Respondedor OCSP (para Certificados de Respondedor OCSP) • Nombres de dominio (para Certificados de servidor Web) • Nombre de la organización (para Certificados de firma de código/objeto) • Nombre (para Certificados individuales).
E-Mail (E) =	Dirección de correo electrónico para Certificados Class 1 individuales y en general para Certificados de Suscriptor MPKI

Tabla 5 - Atributos del Nombre Distinguido en Certificados de Suscriptor de usuario final

El componente Nombre Común (CN=), del nombre distinguido del Sujeto de los Certificados Suscriptor de usuario final es autenticado en el caso de Certificados Class 2- Class 3.

- El valor autenticado del Nombre Común incluido en el DN del Sujeto de Certificados Organizacionales es un nombre de dominio (en el caso de Secure

Server ID y Global Server ID) o el nombre legal de la organización o unidad dentro de la organización.

- El valor autenticado del Nombre Común incluido en el DN del Sujeto de un Certificado ASB Class 3 Organizacional, sin embargo, es el nombre personal generalmente aceptado del representante de la organización autorizado a utilizar la llave privada de la organización, y el componente de organización (O=) es el nombre legal de la organización.
- El valor de Nombre Común incluido en el DN del Sujeto de Certificados individuales representa el nombre personal generalmente aceptado del individuo.

3.1.1.1 Requisitos CABF para Nombres

Los certificados SSL con Dominio validado y Organización validada se ajustan a las especificaciones de CA/Browser Forum Baseline Requirements.

Los siguientes atributos de nombre deberán ser usados para completar el Emisor en Certificados emitidos bajo esta CP:

CountryName Emisor (requerido)

El componente *countryName* (C =), es requerido y contiene el código de país de dos letras ISO 3166-1 para el país en el que se encuentra la sede de negocios del emisor.

OrganizationName Emisor (requerido)

El campo *organizationName* (O=) es requerido y contiene el nombre de la organización del Emisor (o su abreviatura), marca comercial u otra identificación significativa de la CA, que identifica con precisión a la CA. El campo no debe contener una denominación genérica, como "Raíz" o "CA1".

CommonName Emisor (opcional)

Si el campo *commonName* (CN =) del Emisor está presente, debe contener un nombre que identifica con precisión la CA emisora.

Los siguientes atributos de nombre deberán ser utilizados para completar el Sujeto en los Certificados emitidos bajo esta CP:

subjectAlternativeName (requerido)

La extensión *subjectAlternativeName* es requerida y contiene al menos una entrada. Cada entrada es o bien un *dNSName* que contiene el Nombre de Dominio Completamente Calificado o una *iPAddress* contiene la dirección IP de un servidor. La CA de E-Sign confirma que el Solicitante controla el Nombre de Dominio Completamente Calificado (FQDN) o la dirección IP o se le ha concedido el derecho de uso por parte del Titular del Nombre de Dominio o del cesionario de la dirección IP, según corresponda. Los FQDN comodines están permitidos.

Antes de la emisión de un Certificado que contenga una dirección IP reservada o un Nombre Interno de Servidor en la extensión *subjectAlternativeName* o en el campo *commonName* del Sujeto, la CA de E-Sign notifica al Solicitante que el uso de tales Certificados ha sido discontinuado por CA/Browser Forum y que la práctica será eliminada antes de Octubre de 2016. Además, al 1 de Julio de 2012, la CA de E-Sign no deberá emitir certificados con Fecha de Expiración posterior al 1 de Noviembre 2015 con una dirección IP reservada o un Nombre Interno de Servidor en la extensión *subjectAlternativeName* o en el campo *commonName* del Sujeto. A partir del 1 de Octubre de 2016, la CA de E-Sign deberá revocar todos los certificados no expirados

cuya extensión *subjectAlternativeName* o campo *commonName* del Sujeto contenga una dirección IP reservada o un Nombre Interno de Servidor.

CountryName (opcional)

Si está presente, el componente *countryName* (C =), será el código de país de dos letras ISO 3166-1. Si está presente, la CA de E-Sign verificará el país asociado con el Sujeto, de conformidad con la sección 3.2.2.

OrganizationName (opcional)

Si el campo *organizationName* (O =) está presente, el campo contiene el nombre o DBA del Sujeto y los campos de dirección requeridos contienen una ubicación del Sujeto, según sean verificadas de conformidad con la sección 3.2.2.

Si el Sujeto es una persona física, debido a que los atributos de nombres del Sujeto para los individuos (por ejemplo, *givenName* y apellidos), no están ampliamente soportados por el software de aplicación, la CA puede utilizar el campo *organizationName* para comunicar el nombre o DBA del sujeto (ver 3.2.2.1 Verificación de Solicitante Individual).

Si los campos incluyen discrepancias que la CA considera de menor importancia, tales como las variaciones comunes y abreviaturas, la CA deberá documentar la discrepancia y deberá utilizar abreviaturas aceptadas a nivel local al abreviar el nombre de organización (por ejemplo, si el registro oficial muestra "Nombre de la Empresa Sociedad Anónima", la CA puede incluir "Nombre de la Empresa, S.A."). El campo *organizationName* puede incluir un DBA verificada o nombre comercial del Sujeto.

Si el campo *organizationName* está presente, entonces *localityName*, *stateOrProvinceName* (si procede), y *CountryName* también deberán ser requeridos y *streetAddress* y *postalCode* son opcionales. Si *organizationName* está ausente, entonces el Certificado no deberá contener los atributos *streetAddress*, *localityName*, *stateOrProvinceName*, o *postalCode*. La CA puede incluir el campo *CountryName* del Sujeto sin incluir otra Información de Identidad del Sujeto de conformidad con los requisitos anteriores para *CountryName*.

OrganizationalUnitName (opcional)

El componente *organizationalUnitName* (OU=), cuando está presente, puede contener información que no ha sido verificada por la CA. Metadatos como los caracteres '.', '-', y ' ' (es decir, el espacio), y/o cualquier otra indicación de que el valor está ausente, incompleto o no es aplicable, no deben ser utilizadas.

E-Sign implementa un proceso que impide que un atributo OU incluya un nombre, DBA, nombre comercial, marca registrada, dirección, localización, o texto de otra índole que se refiera a una persona natural o jurídica específica, a menos que E-Sign haya verificado esta información de acuerdo con la sección 3.2.2 y el Certificado también contenga los atributos *subject:organizationName*, *subject:localityName* y *subject:CountryName*, también verificados de acuerdo con la sección 3.2.2.

Cuando un valor OU es enviado de una Solicitud, el valor está sujeto a una búsqueda de varias listas de alto riesgo según la sección 3.2.2.1, *Solicitudes de Alto Riesgo*. Si se encuentra una coincidencia, el valor es revisado por la RA para asegurarse de que es preciso y no engañoso. Si el valor OU identifica el nombre de una persona jurídica, el valor es verificado de acuerdo con la sección 3.2.2.1, *Verificación de la Identidad del Sujeto compuesta por Nombre de País y otra Información de Identidad*.

***commonName* (opcional)**

El componente *commonName* (CN=) está discontinuado (desaconsejado, pero no prohibido). Si está presente, *commonName* contiene una única dirección IP o el un Nombre de Dominio Completamente Calificado que es también uno de los valores contenidos en la extensión *subjectAlternativeName* del Certificado.

***domainComponent* (opcional)**

El componente *domainComponent* (dc=) es opcional. Si está presente, *domainComponent* contiene todos los componentes del Nombre de Dominio Registrado del sujeto en secuencia ordenada, con el componente más importante, el más cercano a la raíz del espacio de nombres, escrito al final.

Otros atributos del Sujeto

Los atributos opcionales, cuando están presentes en el campo del sujeto, deben contener información que haya sido verificada por la CA. Metadatos como los caracteres ' ', '-', y ' ' (es decir, el espacio), y/o cualquier otra indicación que el valor está ausente, incompleto o no es aplicable, no deberán ser utilizados.

E-Sign no incluirá Nombres de Dominio Totalmente Calificados en los atributos del Sujeto, excepto como se especifica para *subjectAlternativeName* y *CommonName* arriba.

3.1.2 Necesidad de que los Nombres sean Significativos

Los certificados de suscriptor de usuario final Class 2 y Class 3 contienen nombres con semántica comúnmente entendida que permite la determinación de la identidad de la persona u organización que es el Sujeto del Certificado.

Los certificados de CA de E-Sign contienen nombres con semántica comúnmente entendida que permiten la determinación de la identidad de la CA que es el Sujeto del Certificado.

3.1.3 Anonimato o Seudónimos de los Suscriptores

La identidad de Suscriptores individuales de certificados Class 1 no es autenticada. Los suscriptores de certificados Class 1 pueden usar seudónimos. A menos que sea requerido por ley o solicitado por una autoridad del Estado o de Gobierno para proteger la identidad de algunos suscriptores usuarios finales (p. ej., menores, o información sensible de empleados de gobierno), no es permitido que suscriptores de Certificados Class 2 y Class 3 puedan utilizar seudónimos (nombres que no sean el verdadero nombre personal de un Suscriptor o de organización). Cada solicitud de anonimato en un Certificado será evaluada en sus méritos por el PMA y, si es permitido el certificado indicará que la identidad ha sido autenticada, pero está protegida.

3.1.4 Reglas de Interpretación de Diversas Formas de Nombre

Ninguna estipulación

3.1.5 Unicidad de los Nombres

E-Sign se asegura de que los Nombres Distinguidos del Sujeto de los Suscriptores son únicos en el dominio de una CA específica a través de componentes automatizados del proceso de enrolamiento de Suscriptor. Es posible que un

suscriptor pueda tener dos o más certificados con el mismo Nombre Distinguido del Sujeto.

3.1.6 Reconocimiento, Autenticación, y el Rol de las Marcas Comerciales

Los Solicitantes de Certificados tienen prohibido el uso en sus Solicitudes de Certificados de nombres que infrinjan los Derechos de Propiedad Intelectual de otros. E-Sign, sin embargo, no verifica si un Solicitante de Certificados tiene Derechos de Propiedad Intelectual en el nombre que aparece en la Solicitud de Certificado ni arbitra, media o resuelve disputa alguna respecto de propiedad de un nombre de dominio, marca registrada o marca de servicio. E-Sign tiene la facultad, sin responsabilidad alguna hacia cualquier Solicitante de Certificado, para rechazar o suspender cualquier Solicitud de Certificado debido a tal disputa.

3.2 Validación de Identidad Inicial

3.2.1 Método para probar la posesión de la Llave Privada

El Solicitante del Certificado debe demostrar que legítimamente posee la llave privada que corresponde a la llave pública que será listada en el Certificado. El método para probar la posesión de una llave privada será PKCS # 10, otra demostración criptográficamente equivalente, u otro método aprobado por E-Sign y Symantec. Este requisito no es aplicado cuando un par de llaves es generado por una CA, en nombre de un Suscriptor, por ejemplo, cuando las llaves pre-generadas son colocadas en tarjetas inteligentes.

3.2.2 Autenticación de la Identidad de una Organización

Toda vez que un certificado contenga un nombre de organización, la identidad de la organización y otra información de enrolamiento proporcionada por Solicitantes de Certificado (a excepción de la Información No Verificada del Suscriptor) es confirmada, de conformidad con los procedimientos establecidos en los Procedimientos de Validación documentados por E-Sign.

Como mínimo E-Sign debe:

- Determinar que la organización existe mediante el uso de al menos un servicio o base de datos de prueba de identidad de tercera parte, o alternativamente, la documentación organizacional emitida por o archivada ante la agencia gubernamental o autoridad competente respectiva que confirma la existencia de la organización,
- Confirmar al Solicitante del Certificado por teléfono, correo postal de confirmación, o un procedimiento comparable, cierta información sobre la organización, que la organización ha autorizado la Solicitud de Certificado, y que la persona que envía la Solicitud de Certificado en nombre del Solicitante de Certificado está autorizado para hacerlo. Cuando un certificado incluye el nombre de una persona como representante autorizado de la Organización, la filiación laboral de ese individuo y su autoridad para actuar en nombre de la Organización también deben ser confirmadas.

Cuando un nombre de dominio o dirección de correo electrónico está incluido en el certificado, E-Sign autentifica el derecho de la Organización para utilizar ese nombre de dominio, ya sea como un nombre de dominio completamente calificado o un dominio de correo electrónico.

Los controles adicionales necesarios para satisfacer las regulaciones de exportación de los Estados Unidos y las licencias expedidas por el Department of Commerce Bureau of Industry and Science de los Estados Unidos ("BIS") son realizados por E-Sign cuando sea necesario.

Otros procedimientos se llevan a cabo para tipos específicos de Certificados como se describe en la Tabla 6 a continuación.

Tipo de Certificado	Procedimientos adicionales
Certificado SSL Protegido por Hardware	Symantec verifica que el par de llaves se generen en hardware certificado FIPS 140
Certificado Managed PKI para SSL Intranet	Symantec verifica que el nombre de host o la dirección IP asignada a un dispositivo no es accesible desde Internet (público), y es propiedad del suscriptor del certificado.
Certificado de firma de Contenido autenticados	Antes de firmar digitalmente cualquier contenido con ACS, Symantec autentifica que el contenido es el contenido original firmado por la Organización mediante su Certificado de Firma de Código

Tabla 6 - Procedimientos Específicos de Autenticación

3.2.2.1 Requisitos CABF para Verificación de Solicitantes Organizacionales

Los certificados SSL con Dominio validado y Organización validada adhieren a los requisitos de CA / Browser Forum Baseline.

Autorización del Registrador de Dominio

Las CAs de E-Sign deberán confirmar que, a la fecha en que el Certificado fue emitido, el Solicitante tenía derecho a usar, o tenía el control del Nombre de Dominio Totalmente Calificado y las direcciones IP que figuran en el Certificado, o fue autorizado por una persona que tenía tal derecho o control (por ejemplo, bajo una relación Titular-Representante o Licenciante Licenciataria) para obtener un Certificado que contiene el (los) Nombre(s) de Dominio Totalmente Calificado (s) y la (s) dirección(es) IP.

Si la CA confía en la confirmación por parte de un Registrador de Dominios del derecho a usar o controlar el (los) nombre(s) de dominio registrado(s), y el dominio de nivel superior es un código de país de dos letras (ccTLD), la CA deberá obtener la confirmación directamente desde el Registrador de Dominios para el nivel de Nombres de Dominio al cual aplican las reglas del ccTLD. Por ejemplo, si el FQDN solicitado es www.mysite.users.example.co.uk, la CA deberá obtener la confirmación del Titular del Dominio del Nombre de Dominio example.co.uk de, porque las solicitudes de Nombres de Dominio inmediatamente subordinados a .co.uk se rigen por las reglas del registro de .uk.

Si la CA utiliza el sistema de correo de Internet para confirmar que el Solicitante cuenta con autorización del Titular del Nombre de Dominio para obtener un Certificado para el Nombre de Dominio Totalmente Calificado solicitado, la CA deberá utilizar una dirección de sistema de correo formado de una de las siguientes maneras:

1. Suministrado por el Registrador de Dominios;
2. Tomado del campo "registrant", "technical contact" o "administrative contact" de la información de contacto de Titular del Nombre de Dominio como aparece en el registro WHOIS del Dominio, o;

3. Anteponiendo una parte local a un Nombre de Dominio de la siguiente manera:
- Parte local - Uno de los siguientes: 'admin', 'administrator', 'webmaster', 'hostmaster', o "postmaster", y
 - Nombre de Dominio - Formado quitando cero o más componentes del Nombre de Dominio Registrado o del Nombre de Dominio Totalmente Calificado solicitado.

Si el Titular del Nombre de Dominio ha utilizado un servicio de registro privado, anónimo, o delegado, y la CA se basa en una Autorización de Dominio como una alternativa a lo anterior, la Autorización de Dominio debe ser recibida directamente desde el servicio de registro privado, anónimo, o delegado identificado en el registro WHOIS del Nombre de Dominio Registrado. El documento debe contener el membrete del servicio de registro privado, anónimo, o delegado, la firma del Gerente General, o su equivalente, o un representante autorizado de dicho funcionario, fechada en o después de la fecha de solicitud de certificado, y el (los) Nombre(s) de Dominio Totalmente Calificado(s) que se incluirán en el Certificado.

Si el registro WHOIS identifica el servicio de registro privado, anónimo o delegado, como el Titular del Nombre de Dominio, entonces la autorización de dominio deberá contener una declaración que concede al Solicitante el derecho a utilizar el Nombre de Dominio Totalmente Calificado en un Certificado. La CA se pondrá en contacto directamente con el servicio de registro privado, anónimo o delegado, usando la información de contacto obtenida de una fuente de tercera parte confiable e independiente y obtendrá la confirmación del Titular del Nombre de Dominio de que la Autorización de Dominio es auténtica.

Verificación de la Identidad del Sujeto compuesto sólo por Nombre de País

Si el Solicitante solicita un Certificado que contiene Información la Identidad del Sujeto compuesto solamente por el campo countryName, la CA verificará el país asociado con el Sujeto utilizando uno de los siguientes métodos:

- la asignación rango de Direcciones IP por país, ya sea para
 - la dirección IP del sitio web, según lo indicado por el registro DNS para el sitio web o
 - la dirección IP del Solicitante;
- el código de dos letras del país (ccTLD) del Nombre de Dominio solicitado;
- información proporcionada por el Registrador de Dominios, o
- un método identificado en la sección "*Verificación de la Identidad del Sujeto compuesta por Nombre de País y otra Información de Identidad*".

La CA debe implementar un proceso para examinar los servidores proxy con el fin de evitar la confianza en direcciones IP asignadas en países que no sean aquel en el que el Solicitante está localizado realmente.

Verificación de la Identidad del Sujeto compuesta por Nombre de País y otra Información de Identidad

Si el Solicitante solicita un Certificado que contendrá el campo CountryName y otra Información de Identidad del Sujeto, entonces la CA deberá verificar la identidad del Solicitante y la autenticidad de la solicitud el certificado del Representante del Solicitante mediante un proceso de verificación que cumpla los siguientes conjuntos de requisitos. La CA deberá inspeccionar cualquier documento invocado en esta Sección para detectar una eventual alteración o falsificación.

- A. Opción de Verificación de Identidad de Nombre o Dirección

Si la Información de Identidad del Sujeto incluye el nombre o la dirección de una organización, la CA deberá verificar la identidad y la dirección de la organización y que la dirección es la dirección de existencia u operación del Solicitante. La CA deberá verificar la identidad y dirección del Solicitante usando la documentación proporcionada por, o mediante la comunicación con, al menos uno de los siguientes:

- 1) Una agencia gubernamental (por ejemplo, la Secretaria de Estado) en la jurisdicción de creación, existencia, o reconocimiento legal del Solicitante;
- 2). Una base de datos externa de terceros (por ejemplo, la base de datos de Dun and Bradstreet) que sea actualizada periódicamente, la que E-Sign ha evaluado de acuerdo con Precisión de Fuentes de Datos (más adelante);
- 3). Una visita al sitio por la CA de E-Sign o de un tercero que actúe como agente de la CA, o
- 4) Una Carta de Certificación.

La CA puede utilizar la misma documentación o comunicación descrita en 1 a 4 anteriores para verificar tanto la identidad del Solicitante como su dirección.

Alternativamente, la CA puede verificar la dirección del solicitante (pero no su identidad) con una factura de servicios públicos, estado de cuenta bancaria, estado de tarjeta de crédito, documento de impuestos emitido por el gobierno, u otra forma de identificación que cumpla con los requisitos de Precisión de Fuentes de Datos (mas adelante).

B. Opción de Verificación de Identidad de DBA / Nombre Comercial

Si la Información de Identidad del Sujeto incluye un DBA o nombre comercial, la CA deberá verificar el derecho del solicitante de utilizar el DBA/nombre comercial utilizando al menos uno de los siguientes métodos:

1. Documentación proporcionada por, o la comunicación con una agencia del gobierno en la jurisdicción de creación, existencia, o reconocimiento legal del solicitante;
2. Documentación o comunicación proporcionada por una fuente de terceros que cumplan con los requisitos de Precisión de Fuentes de Datos (más adelante);
3. La comunicación con una agencia del gobierno responsable de la gestión de tales DBAs o nombres comerciales;
4. Una Carta de Certificación acompañada de un apoyo documental que cumpla con los requisitos de Precisión de Fuentes de Datos (más adelante), o
5. Una factura de servicios públicos, estado de cuenta bancaria, estado de tarjeta de crédito, documento de impuestos emitido por el gobierno, u otra forma de identificación que cumpla con los requisitos de Precisión de Fuentes de Datos (más adelante)

Método Confiable de Comunicación

Si el solicitante de un Certificado que contiene Información Identidad del Sujeto es una organización, E-Sign utiliza un Método Confiable de Comunicación para verificar la autenticidad de la solicitud el certificado del Representante del Solicitante, incluyendo: correo electrónico, servicios de postal y teléfono.

La CA puede utilizar las fuentes citadas por Verificación de Identidad de Nombre o Dirección (arriba) para verificar el Método Confiable de Comunicación. En tanto la CA utilice un Método Confiable de Comunicación, la CA puede establecer la autenticidad de la solicitud de certificado directamente con el Representante del Solicitante o con una fuente con autoridad dentro de la organización del Solicitante, tales como oficinas comerciales principales, oficinas corporativas, oficinas de recursos humanos, las oficinas de tecnología de la información, o de otros departamentos del Solicitante que la CA estime conveniente.

Además, la CA cuenta con un proceso que permite a un Solicitante especificar las personas que pueden solicitar Certificados. Si un Solicitante especifica, por escrito, las personas que pueden solicitar un Certificado, entonces la CA no aceptará solicitudes de certificado que se encuentren fuera de esta especificación. La CA deberá facilitar al Solicitante una lista de sus solicitantes de certificados autorizados ante solicitud por escrito verificada del solicitante.

Verificación de Solicitante Individual

Si un Solicitante es una persona natural, entonces la CA de E-Sign deberá verificar el nombre del Solicitante, la dirección del Solicitante y la autenticidad de la solicitud de certificado (véase también 3.1.1.1 OrganizationName).

La CA deberá verificar el nombre del Solicitante con una copia legible, que visiblemente muestre la cara del Solicitante, de al menos una identificación con foto válida y vigente emitida por el Gobierno (pasaporte, licencia de conducir, identificación militar, documento nacional de identidad, o tipo de documento equivalente). La CA deberá inspeccionar la copia para detectar cualquier indicio de una eventual alteración o falsificación.

La CA verificará la dirección del Solicitante mediante una forma de identificación que cumpla con los requisitos de "Precisión de Fuentes de Datos" tales como una identificación del Gobierno, factura de servicios públicos, o estado de cuenta bancaria o de tarjeta de crédito. La CA puede confiar en la misma identificación emitida por el Gobierno que fue utilizada para verificar el nombre del Solicitante.

La CA verificará la solicitud de certificado con el Solicitante con un Método Confiable de Comunicación.

Edad de los Datos del Certificado

La CA no deberá utilizar datos o documentos para validar una solicitud de certificado si estos datos o documentos fueron obtenidos más de treinta y nueve (39) meses antes de la emisión de los certificados.

Lista de Denegados

La CA deberá mantener una base de datos interna de todos los Certificados revocados con anterioridad y todas las solicitudes de certificados rechazadas con anterioridad por motivo de sospechas de suplantación de identidad o de otro uso o motivación fraudulentos, por lo menos siete (7) años de conformidad con los requisitos de retención de documentación (sección 5.5.2 de esta CPS).

La CA deberá utilizar esta información para identificar posteriores solicitudes de certificados sospechosas.

Solicitudes de Alto Riesgo

E-Sign deberá identificar las solicitudes de certificados de riesgo alto, y llevar a cabo las actividades de verificación adicional, y tomar las precauciones adicionales, que sean razonablemente necesarias para garantizar que estas solicitudes están debidamente verificadas en virtud de estos Requisitos.

La CA puede identificar las solicitudes de alto riesgo mediante la verificación de las listas de nombres de organización adecuadas que son más comúnmente atacadas a través phishing y otros esquemas fraudulentos, y mediante la señalización automática de solicitudes de certificados que coincidan con estas listas para un examen más detallado antes de la emisión. Ejemplos de estas listas son: bases de datos internas mantenidas por la CA de Certificados revocados con anterioridad y solicitudes de

certificados rechazados con anterioridad debido a sospechas de phishing u otro uso fraudulento.

La CA deberá utilizar la información identificada por los criterios de alto riesgo de la CA para marcar las solicitudes de certificados sospechosas. La CA deberá seguir un procedimiento documentado para realizar la verificación adicional de cualquier solicitud de certificado marcado como sospechosa o de alto riesgo.

Precisión de Fuentes de Datos

Antes de confiar en una fuente de datos para verificar la Información de Identidad del Sujeto, la CA deberá evaluar la precisión y confiabilidad de la fuente de datos. La CA no deberá utilizar una fuente de datos para verificar la Información de Identidad del Sujeto, si la evaluación de la CA determina que tal fuente de datos no es razonablemente precisa y confiable.

3.2.3 Autenticación de la Identidad de un Individuo

La autenticación de la identidad individual es diferente según la clase de certificado. El mínimo de autenticación estándar para cada clase de certificado STN es explicado en la Tabla 7 a continuación.

Clase de Certificado	Autenticación de la Identidad
Class 1	Sin autenticación de identidad. Hay una confirmación limitada de dirección de correo electrónico del suscriptor, al requerir que el suscriptor sea capaz de responder a un correo electrónico a esa dirección.
Class 2	Autenticar la identidad, comparando la identidad del suscriptor con: <ul style="list-style-type: none"> • información residente en la base de datos de un servicio de prueba de identidad aprobado por E-Sign, como una agencia de crédito importante u otra fuente de información confiable, o • información contenida en los registros de negocios o bases de datos de información de empresas (directorios de empleados o de clientes) de una RA que aprueba certificados a sus propias personas afiliadas
Class 3	<p>La autenticación de los Certificados individuales Class 3 se basa en la presencia personal (física) del Solicitante de Certificado ante un agente de la CA o RA, o ante un notario público, u otro agente con autoridad comparable dentro de la jurisdicción del Solicitante del Certificado. El agente, notario u otro oficial deberá comprobar la identidad del Solicitante de Certificado contra una forma reconocida de identificación fotográfica emitida por el gobierno, como un pasaporte o una licencia de conducir y otra credencial de identificación.</p> <p>La autenticación de certificados de Class 3 de Administrador se basa en la autenticación de la organización y la confirmación por parte de la organización de la identidad y la autorización de la persona para actuar como Administrador.</p> <p>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 sus Solicitudes de Certificado se basará en la confirmación de su identidad en relación con su filiación laboral o retención como contratista independiente y procedimientos de comprobación de antecedentes ⁷</p>

⁷ E-Sign puede aprobar Certificados de Administrador para que sean asociados con destinatarios no humanos, tales como un dispositivo, o un servidor. La autenticación de una solicitud de Administrador Certificado Class 3 para un destinatario no humano deberá incluir:

- Autenticación de la existencia y la identidad del servicio nombrado como Administrador en la Solicitud de Certificado
- Autenticación de que el servicio ha sido implementado de una manera segura consistente con la realización de una función administrativa

Tabla 7. Autenticación de la identidad individual

3.2.4 Información no Verificada del Suscriptor

La información no verificada del suscriptor incluye:

- Unidad Organizacional (OU) con ciertas excepciones⁸
- Nombre del suscriptor en certificados Class 1
- Cualquier otra información designada como no verificada en el certificado.

3.2.5 Validación de Autoridad

Siempre que el nombre de un individuo está asociado con un nombre de organización en un certificado de tal forma que indique la afiliación de la persona o la autorización para actuar en nombre de la organización, E-Sign o la RA:

- determina que la organización existe mediante el uso de al menos un servicio o base de datos de prueba de identidad de tercera parte, o alternativamente, la documentación aplicable emitida o archivada por el gobierno que confirma la existencia de la organización, y
- Usa la información contenida en los registros de negocios o de bases de datos de información empresarial (Directorios de empleados o clientes) de la RA que aprueba certificados a sus propios individuos afiliados o confirma por teléfono, correo postal de confirmación, o procedimiento similar para la organización, la filiación laboral con la organización de la persona que presenta la Solicitud de Certificado y, en su caso, su autoridad para actuar en nombre de la organización.

3.2.6 Criterios para la Interoperación

E-Sign puede proporcionar servicios de interoperabilidad que permiten a una entidad emisora ajena a la red STN poder interoperar con la STN certificando unilateralmente a esa CA. Las CA habilitadas para poder interoperar de esta manera, cumplirán con la Política de Certificación de la STN complementado por políticas adicionales cuando sea requerido.

E-Sign sólo permitirá la interoperabilidad con la red STN de una CA ajena a la STN en circunstancias en que la CA, como mínimo:

- Entra en un acuerdo contractual con E-Sign
- Opera bajo una CPS que cumple con los requisitos STN para las clases de certificados que emitirá
- Pasa una evaluación de cumplimiento antes de ser autorizada a interoperar
- Pasa una evaluación anual del cumplimiento de elegibilidad para interoperar.

3.3 Identificación y Autenticación para las Solicitudes de Reasignación de Llaves

Antes del vencimiento de un Certificado de Suscriptor existente, es necesario que el Suscriptor obtenga un nuevo certificado para mantener la continuidad de uso del certificado. E-Sign generalmente requiere que el suscriptor genere un nuevo par de llaves para reemplazar el par de llaves existente (técnicamente definido como "reasignación de llaves"). Sin embargo, en ciertos casos (es decir, para los certificados de servidor Web) los suscriptores pueden solicitar un nuevo certificado para un par de llaves existentes (técnicamente definido como "renovación").

• La confirmación de la identidad y la autorización de la persona que enrole el certificado de Administrador para el servicio nombrado como Administrador en la Solicitud de Certificado.

⁸ Los certificados con Dominio validado y Organización Validada pueden contener valores de Unidad Organizacional que estén validados

En términos generales, tanto la "Reasignación de llaves" como la "Renovación" son descritas habitualmente como "Renovación de Certificado", enfocándose en el hecho de que el antiguo certificado está siendo sustituido por un nuevo certificado y no enfatizando si se genera o no un nuevo par de llaves. Para todas las clases y tipos de Certificados E-Sign, a excepción de los certificados de servidor Class 3, esta distinción no es importante ya que siempre es generado un nuevo par de llaves como parte del proceso de reemplazo de Certificados de Suscriptor usuario final de E-Sign. Sin embargo, para los certificados de servidor Class 3, dado que el par de llaves de Suscriptor es generado en el servidor Web y la mayoría de las herramientas para generación de llaves de servidor Web permiten la creación de una nueva Solicitud de Certificado para un par de llaves existentes, hay una distinción entre "Reasignación de llave" y "renovación".

3.3.1 Identificación y Autenticación Para Re Asignación de Llave Rutinaria

Los procedimientos de re asignación de llave aseguran que la persona u organización que solicita a la re asignación de llave de un Certificado de Suscriptor de usuario final es de hecho, el Suscriptor del Certificado.

Un procedimiento aceptable es mediante el uso de una Frase Secreta (o su equivalente), o la prueba de la posesión de la llave privada. Los Suscriptores eligen y envían junto con su información de enrolamiento una Frase Secreta (o su equivalente). Durante la renovación de un Certificado, si un Suscriptor envía correctamente la Frase Secreta del Suscriptor (o su equivalente) con la información de reenrolamiento del Suscriptor, y la información de enrolamiento (incluyendo la información del contacto Corporativo y Técnico) no ha cambiado, la renovación de certificado es emitida automáticamente. Como alternativa al uso de una frase secreta (o equivalente) Symantec puede enviar un mensaje de correo electrónico a la dirección asociada con el contacto corporativo verificado para el certificado que se renueva, solicitando la confirmación del pedido de renovación del Certificado y la autorización para emitir el certificado. Una vez recibida la confirmación autorizando la emisión del Certificado, Symantec emitirá el Certificado si la información de enrolamiento (incluyendo la información del contacto Corporativo y Técnico⁹) no ha cambiado.

Después de la reasignación de llave o la renovación de esta manera, y al menos en instancias alternas de posteriores reasignaciones de llave o renovaciones a partir de entonces, E-Sign o la RA reconfirmarán la identidad del Suscriptor en conformidad con los requisitos de identificación y autenticación de una Solicitud de Certificado original.¹⁰

En particular, para Certificados SSL Organizacionales Class 3 a través de www.e-sign.cl, E-Sign re autentifica el nombre de la Organización y el nombre de dominio incluido en el certificado a intervalos descritos en la sección 6.3.2. En los casos en que:

- La frase secreta es utilizada correctamente para renovación posterior del certificado, o se obtiene una respuesta de confirmación a un correo electrónico al contacto corporativo y:
- El Nombre Distinguido del certificado no ha sido modificado, y

⁹ Si la información de contacto ha cambiado a través de un procedimiento formal aprobado de cambio de contacto, el certificado todavía calificará para renovación automática.

¹⁰ La autenticación de una solicitud de reasignación de llaves/renovación de un Certificado Class 3 Organizational ASB, sin embargo, requiere el uso de una Frase Secreta, así como la misma identificación y autenticación que la Solicitud de Certificado original.

- La información de los contactos Corporativo y Técnico no ha cambiado respecto de la que fue verificada previamente,

E-Sign no tendrá que reconfirmar por teléfono, correo de confirmación, o un procedimiento comparable con el Solicitante del Certificado, cierta información del acerca de la organización, que la organización ha autorizado la Solicitud de Certificado, y que la persona que envía la Solicitud de Certificado en nombre del Solicitante de Certificado está autorizada a hacerlo. "

La reasignación de llaves después de 30 días a partir de la expiración del Certificado es re-autenticada como una Solicitud de Certificado original y no es emitida automáticamente.

3.3.2 Identificación y Autenticación Para Reasignación de Llave Después de la Revocación

La reasignación de llaves/renovación después de la revocación no está permitida si la revocación se produjo debido a que:

- el Certificado (distinto de un Certificado Class 1) fue emitido a una persona distinta de aquella nombrada como el Sujeto del Certificado, o
- el Certificado (distinto de un Certificado Class 1) fue emitido sin la autorización de la persona o entidad nombrada como el Sujeto de dicho Certificado, o
- la entidad que aprueba la Solicitud de Certificado de Suscriptor descubre o tiene razones para creer que un hecho sustancial en la Solicitud de Certificado es falso, o
- Por cualquier otra razón considerada necesaria por Symantec o E-Sign para proteger la red STN

Sujeto al párrafo anterior, la renovación de un Certificado Organizacional o de CA posterior a la revocación del Certificado es permisible siempre y cuando los procedimientos de renovación aseguren que la organización o la CA que busca la renovación es de hecho el Suscriptor del Certificado. Los Certificados Organizacionales renovados deberán contener el mismo DN del Sujeto que aquél del Certificado Organizacional que está siendo renovado.

La renovación de un Certificado individual después de la revocación debe asegurar que la persona que busca la renovación es, de hecho, el Suscriptor. Un procedimiento aceptable es el uso de una Frase Secreta (o su equivalente). En ausencia de este procedimiento o de otro procedimiento aprobado por E-Sign, los requisitos para la identificación y autenticación de una Solicitud de Certificado original deben ser utilizados para la renovación de un Certificado después de una revocación.

3.4 Identificación y Autenticación Para la Solicitud de Revocación

Antes de la revocación de un Certificado, E-Sign 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 autenticar las solicitudes de revocación por parte del Suscriptor incluyen:

- Hacer que el Suscriptor para ciertos tipos de certificados envíe en línea la Frase Secreta del Suscriptor (o su equivalente), y revocar el Certificado de forma automática si ésta coincide con la Frase Secreta (o su equivalente) registrada, (Note que esta opción puede no estar disponible para todos los clientes.)

- Recibir de un mensaje del Suscriptor que solicita la revocación y contiene una firma digital verificable con referencia al Certificado que pretende ser revocado,
- Comunicación con el Suscriptor, proveyendo razonable seguridad, en función de la Clase del Certificado, que la persona u organización que solicita la revocación es, de hecho el Suscriptor. Dependiendo de las circunstancias, tal comunicación puede efectuarse a través de uno o más de los siguientes medios: teléfono, facsímile, e-mail, correo o servicio courier.

E-Sign podrá restringir estos procedimientos, dependiendo del tipo de certificado.

Los Administradores de E-Sign pueden solicitar la revocación de certificados de Suscriptores usuarios finales dentro del Subdominio de E-Sign. E-Sign autentifica la identidad de los Administradores vía control de acceso usando autenticación SSL y de cliente antes de permitir que ejecuten funciones de revocación, u otro procedimiento aprobado por la STN.

Las RA que utilizan el módulo Automated Administration Software Module podrán presentar a E-Sign solicitudes de revocación en grupos. Tales solicitudes deberán ser autenticadas mediante una solicitud firmada digitalmente con la llave privada residente en el token de hardware de Automated Administration de la RA.

Las solicitudes para revocar un Certificado de CA serán autenticadas por E-Sign para asegurarse de que la revocación ha sido solicitada de hecho por la CA.

4 Requerimientos Operacionales del Ciclo de Vida de los Certificados

4.1 Solicitud de Certificados

4.1.1 ¿Quién puede Presentar una Solicitud de Certificado?

A continuación se muestra una lista de personas que pueden enviar solicitudes de certificados:

- Cualquier persona que sea el sujeto del certificado,
- Cualquier representante autorizado de una Organización o entidad,
- Cualquier representante autorizado de una CA,
- Cualquier representante autorizado de una RA.

4.1.2 Proceso de Enrolamiento y Responsabilidades

4.1.2.1 Suscriptores de Certificado de Usuario Final

Todos los Suscriptores de Certificado de usuario final deberán manifestar consentimiento con el Acuerdo de Suscriptor que contiene las declaraciones y garantías descritas en la Sección 9.6.3 y someterse a un proceso de enrolamiento consistente en:

- completar una Solicitud de Certificado y aportar información veraz y correcta,
- generar, o hacer que se genere, un par de llaves,
- entregar su llave publica a E-Sign directamente o a través de una RA,
- demostrar la posesión y/o el control exclusivo de la llave privada que corresponde a la llave pública entregada a E-Sign.

4.1.2.2 Requisitos CABF para Solicitudes de Certificados

Los certificados SSL con Dominio validado y Organización validada adhieren a los requisitos de CA / Browser Forum Baseline.

Antes de la emisión de un Certificado, la CA deberá obtener la siguiente documentación del Solicitante:

1. Una solicitud de certificado, que podrá ser electrónica, y
2. Un Acuerdo de Suscriptor aceptado, que podrá ser electrónico.

La CA debe obtener cualquier documentación adicional que la CA determine como necesaria para cumplir con estos Requisitos.

Antes de la emisión de un Certificado, la CA deberá obtener del Solicitante una solicitud de certificado en la forma prescrita por la CA y que cumpla con estos Requisitos. Una solicitud de certificado puede ser suficiente para que sean emitidos varios certificados para el mismo Solicitante, sujeto a los requisitos de edad y actualización de la Sección 3.2.2.1, Edad de los Datos del Certificado, siempre y cuando cada certificado es respaldado por una solicitud de certificado válida y vigente, firmada en nombre del Solicitante por el Representante del Solicitante apropiado. La solicitud de certificado puede ser efectuada, presentada y/o firmada electrónicamente.

Solicitud y Certificación

La solicitud de certificado debe contener una solicitud de, o en nombre de, el Solicitante de la emisión de un Certificado, y una certificación de que toda la información allí contenida es correcta de, o en nombre de, el Solicitante.

Requisitos de Información

La solicitud de certificado puede incluir toda la información objetiva sobre el Solicitante que será incluida en el certificado, y la información adicional que sea necesaria que la CA obtenga del Solicitante para cumplir con estos Requisitos, y con la Política de Certificados y/o Declaración de Prácticas de Certificación de la CA. En los casos en que la solicitud de certificado no contiene toda la información necesaria sobre el Solicitante, la CA de E-Sign deberá obtener la información restante del Solicitante o, habiéndola obtenido de una fuente de datos de terceros confiable e independiente, confirmarla con el Solicitante.

La Información del Solicitante debe incluir, pero no se limita a, por lo menos un Nombre de Dominio Completamente Calificado o dirección IP a ser incluida en la extensión SubjectAltName del Certificado.

Suscriptor de la clave privada

Terceros que no sean el Suscriptor no deberán archivar la Llave Privada del Suscriptor.

Si la CA o cualquiera de sus RA designadas generasen la Llave Privada en nombre del Suscriptor, la CA deberá cifrar la Llave Privada para su transporte al Suscriptor.

Si la CA o cualquiera de sus RA designadas tienen información de que la Llave Privada de un Suscriptor ha sido comunicada a una persona no autorizada o a una organización no afiliada con el Suscriptor, la CA deberá revocar todos los certificados que incluyen la Llave Pública correspondiente a la Llave Privada comunicada.

Suscriptor y Acuerdo

Antes de la emisión de un Certificado, la CA deberá obtener, para el beneficio expreso de la CA y los Beneficiarios de los Certificados, el acuerdo del Solicitante con el Acuerdo de Suscriptor con la CA.

La CA deberá implementar un proceso para asegurar que cada Acuerdo de Suscripción vincula legalmente al Solicitante. En cualquier caso, el Acuerdo debe ser aplicado a la obtención del Certificado a ser emitido de conformidad con la solicitud de certificado.

La CA utiliza un Acuerdo electrónico o de "click para continuar"; tales acuerdos son legalmente vinculantes. Un acuerdo por separado puede ser utilizado para cada solicitud de certificado, o un único Acuerdo puede ser utilizado para cubrir múltiples solicitudes de certificados en el futuro y los Certificados resultantes, siempre y cuando cada Certificado que la CA emita al Solicitante esté claramente cubierto por ese Acuerdo de Suscriptor.

4.1.2.3 Certificados de CA y RA

Los Suscriptores de Certificados de CA y RA celebran un contrato con E-Sign. Las CA y RA Solicitantes deberán 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 el par de llaves de CA o RA, el solicitante deberá cooperar con E-Sign para determinar el nombre distinguido apropiado y el contenido de los Certificados que el solicitante emitirá.

4.2 Procesamiento de Solicitud de Certificado

4.2.1 Realización de Funciones de Identificación y Autenticación

E-Sign o la RA llevarán a cabo una identificación y autenticación de toda la información de Suscriptor requerida, en los términos de la Sección 3.2

4.2.2 Aprobación o Rechazo de las Solicitudes de Certificado

E-Sign o la RA aprobarán una solicitud de certificado si se cumplen las siguientes condiciones:

- Identificación y autenticación exitosa de toda la información de Suscriptor requerida en términos de la Sección 3.2
- El pago ha sido recibido

E-Sign o la RA rechazarán una solicitud de certificado si:

- La identificación y autenticación de toda la información de Suscriptor requerida en términos de la Sección 3.2 no se puede completar o
- El Suscriptor no presenta la documentación de apoyo que sea solicitada o
- El suscriptor no responde a las notificaciones en un plazo determinado, o
- El pago no ha sido recibido, o
- La RA cree que la emisión de un certificado para el Suscriptor podrá acarrear descrédito para la STN.

4.2.3 Plazo para Procesar las Solicitudes de Certificados

E-Sign comienza a procesar las solicitudes de certificados dentro de un plazo razonable tras la recepción. No hay especificación de plazo para completar la tramitación de una solicitud a menos que se indique lo contrario en el Acuerdo de Suscriptor pertinente, CPS u otros Acuerdos entre los participantes de la STN. Una solicitud de certificado permanece activa hasta que es rechazada.

4.3 Emisión de Certificado

4.3.1 Acciones de la CA durante la Emisión del Certificado

Un Certificado es creado y emitido tras la aprobación de una Solicitud de Certificado por E-Sign o tras la recepción de la solicitud de la RA para emitir el Certificado. E-Sign crea y emite un Certificado para un Solicitante de Certificado sobre la base de la información de una Solicitud de Certificado luego de la aprobación de tal Solicitud de Certificado.

4.3.2 Notificaciones al Suscriptor de la Emisión del Certificado por parte de la CA

E-Sign, ya sea directamente o a través de una RA, notificará a los suscriptores que se han creado tales Certificados, y proporcionará a los Suscriptores el acceso a los Certificados notificándolos de que sus Certificados están disponibles. Los Certificados serán puestos a disposición de los Suscriptores usuarios finales, ya sea permitiéndoles descargarlos de un sitio Web, o a través de un mensaje enviado al Suscriptor el cual contiene el Certificado.

4.3.3 Requisitos CABF para la Emisión de Certificados por una CA Raíz

Los certificados SSL con Dominio validado y Organización validada adhieren a los requisitos de CA / Browser Forum Baseline.

Las Llaves Privadas de la CA Raíz de E-Sign no deberán ser utilizadas para firmar Certificados de Suscriptor. Las Llaves Privadas de la CA Raíz de E-Sign deberán ser utilizadas para firmar Certificados sólo en los casos siguientes:

1. Certificados auto-firmados para representar a la misma CA Raíz;
2. Certificados de CAs subordinadas y Certificados Cruzados;
3. Certificados para fines de infraestructura (por ejemplo, certificados de función administrativa, certificados de CA internos para dispositivos operacionales, y certificados de verificación de respuesta OCSP).

La emisión de certificados por la CA Raíz deberá requerir que una persona autorizada por la CA (es decir, el operador del sistema de la CA, el oficial de sistema, o el administrador de PKI) emita deliberadamente una orden directa para que la CA Raíz lleve a cabo una operación de firma de certificado. Los controles adicionales para la emisión de certificados por la CA Raíz son descritos en la Sección 5.6, Cambio de Llaves y la Sección 6.1, Generación del Par de Llaves.

4.4 Aceptación de Certificado

4.4.1 Conducta que Constituye Aceptación del Certificado

Las siguientes conductas constituyen la aceptación del certificado:

- La descarga de un Certificado o la instalación de un Certificado desde un mensaje que lo adjunta constituyen la aceptación del Certificado por parte del Suscriptor.

- La falta de objeciones del Suscriptor al certificado o a su contenido constituyen la aceptación del Certificado.

4.4.2 Publicación del Certificado por la CA

E-Sign publica los Certificados que emite en un repositorio de acceso público.

4.4.3 Notificación de la Emisión del Certificado a Otras Entidades por parte de la CA

Las RAs pueden recibir la notificación de la emisión de los Certificados que aprueban.

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 se permitirá una vez que el Suscriptor ha aceptado el Acuerdo de Suscriptor y ha aceptado el certificado. El certificado deberá ser utilizado legalmente en conformidad con el Acuerdo de Suscriptor de E-Sign, los términos de la CP de la STN y esta CPS. El uso del certificado debe ser consistente con las extensiones del campo KeyUsage incluidas en el certificado (por ejemplo, si la opción Digital Signature no está habilitada, el certificado no debe ser utilizado para firmar).

Los Suscriptores protegerán sus llaves privadas de uso no autorizado y dejarán de utilizar la llave privada tras la expiración o revocación del certificado.

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

Las partes que confían aceptarán los términos del Acuerdo de la Parte que Confía aplicables, como una condición para confiar en el certificado.

La confianza en un certificado debe ser razonable bajo las circunstancias. Si las circunstancias indican una necesidad de garantías adicionales, la Parte que Confía debe obtener tales garantías para que tal confianza sea considerada razonable.

Antes de realizar cualquier acto de la confianza, las Partes que Confían evaluarán independientemente:

- la conveniencia de la utilización de un certificado para cualquier propósito dado y determinar que el certificado, de hecho, será utilizado para un propósito adecuado que no esté prohibido y tampoco restringido por esta CPS. E-Sign no es responsable de evaluar si la utilización de un Certificado es apropiada.
- Que el certificado está siendo utilizado de acuerdo con las extensiones del campo KeyUsage incluidas en el certificado (por ejemplo, si la opción Digital Signature no está habilitada, no se puede confiar en el certificado para validar la firma de un Suscriptor).
- El estado del certificado y todas las CA en la cadena que emitió el certificado. Si alguno de los certificados en la cadena de certificados ha sido revocado, la Parte que Confía es la única responsable de investigar si la confianza en una firma digital creada por un Certificado de Suscriptor usuario final antes de la revocación de un certificado en la cadena de certificados, es razonable. Cualquier manifestación de tal confianza es realizada únicamente bajo riesgo de la Parte que Confía.

Asumiendo que el uso del certificado es apropiado, las Partes que Confían deberán utilizar el software y/o hardware apropiado para realizar la verificación de la firma

digital u otras operaciones criptográficas que deseen realizar, como condición para confiar en los certificados en relación con cada una de esas operaciones. Tales operaciones incluyen la identificación de una cadena de certificados y la verificación de las firmas digitales en todos los certificados en la cadena de certificados.

4.6 Renovación de Certificado

La renovación del certificado es la emisión de un nuevo certificado para el suscriptor sin cambiar la llave pública o cualquier otra información en el certificado. La renovación del certificado es soportada para certificados Class 3 donde el par de llaves es generado en un servidor Web dado que las herramientas de generación de llaves de la mayoría de los servidores Web permiten la creación de una nueva Solicitud de Certificado para un par de llaves existentes.

4.6.1 Circunstancias para la Renovación de Certificado

Antes de la expiración de un Certificado de Suscriptor existente, es necesario que el suscriptor renueve un nuevo certificado para mantener la continuidad del uso del certificado. un certificado también puede ser renovado después de la expiración.

Antes de la expiración de un certificado de Suscriptor existente, E-Sign notificará la suscriptor de la proximidad de la fecha de expiración de tal certificado.

4.6.2 Quién puede Solicitar la Renovación

Sólo el suscriptor de un certificado individual o un representante autorizado para un certificado Organizacional pueden solicitar la renovación del certificado.

4.6.3 Procesamiento de Solicitudes de Renovación de Certificado

Los procedimientos de renovación aseguran que la persona u organización que solicita la renovación de un Certificado de Suscriptor usuario final es de hecho el suscriptor (o está autorizado por el Suscriptor) del certificado.

Un procedimiento aceptable es mediante el uso de una Frase Secreta (o su equivalente), o la prueba de la posesión de la llave privada. Los suscriptores eligen y envían junto con la información de su enrolamiento, una Frase Secreta (o su equivalente). Durante la renovación de un certificado, si un suscriptor envía correctamente la Frase Secreta del Suscriptor (o su equivalente) con la información de reenrolamiento del Suscriptor, y la información de enrolamiento (incluyendo información de contactos Corporativo y Técnico ¹¹) no ha cambiado, la renovación del certificado es emitida de forma automática. Como alternativa al uso de una Frase Secreta (o equivalente) E-Sign puede enviar un mensaje de correo electrónico a la dirección de correo electrónico asociada con el contacto corporativo verificado para el certificado que está siendo renovado, solicitando la confirmación de la solicitud de renovación de certificados y la autorización para emitir el certificado. Una vez recibida la confirmación autorizando la emisión del certificado, E-Sign emitirá el certificado si la

¹¹ Si la información de contacto ha cambiado a través de un procedimiento cambio de contacto formal aprobado el certificado aún estará calificado para renovación automática.

información de enrolamiento (incluyendo información de contactos Corporativo y Técnico¹²) no ha cambiado.

Tras la renovación de esta forma, y al menos en instancias alternativas de posteriores renovaciones a partir de entonces, E-Sign o una RA deberán reconfirmar la identidad del suscriptor, de conformidad con los requisitos especificados en esta CPS para la identificación y autenticación de una Solicitud de Certificado original.

En particular, para las solicitudes de renovación posteriores para Certificados SSL Organizacionales Class 3 a través de www.e-sign.cl, E-Sign reautenticará el nombre de la Organización y el nombre de dominio incluido en el certificado en los intervalos descritos en la sección 6.3.2. En los casos en que:

- La Frase Secreta es utilizada correctamente para la renovación posterior del certificado, o se obtiene un respuesta de confirmación a un correo electrónico al enviado al contacto Corporativo, y;
- El Nombre Distinguido del certificado no ha sido modificado, y
- La información de los contactos Corporativo y Técnico no ha cambiado desde que fue verificada previamente,

E-Sign no necesitará reconfirmar por teléfono, correo de confirmación, o procedimiento comparable con el solicitante del certificado cierta información acerca de la organización, que la organización ha autorizado la solicitud de certificado, y que la persona que envía la solicitud de certificado en nombre del solicitante de certificado está autorizada a hacerlo."

Aparte de este procedimiento u otro procedimiento aprobado por E-Sign, los requisitos dispuestos para la autenticación de una solicitud de certificado original serán utilizados para la renovación de un certificado de suscriptor de usuario final.

4.6.4 Notificación al Suscriptor de la Emisión de un Nuevo Certificado

La notificación al Suscriptor de la emisión de la renovación del certificado está de acuerdo con la Sección 4.3.2

4.6.5 Conducta que Constituye Aceptación del Certificado de Renovación

La conducta que constituye Aceptación de un certificado renovado está de acuerdo con la Sección 4.4.1

4.6.6 Publicación del Certificado de Renovación por la CA

El certificado renovado es publicado en un repositorio de acceso público de E-Sign.

4.6.7 Notificación de Emisión del Certificado a Otras Entidades por parte de la CA

Las RAs pueden recibir notificación de la emisión de los certificados que aprueban.

4.7 Reasignación de Llaves del Certificado

La reasignación de llaves del certificado es la solicitud para la emisión de un nuevo certificado que certifique la nueva llave pública. La reasignación de llaves del

¹² Si la información de contacto ha cambiado a través de un procedimiento cambio de contacto formal aprobado el certificado aún estará calificado para renovación automática.

certificado es compatible con todas las clases de certificados. Para certificados individuales que incluyen la extensión Subject Alternative Name, E-Sign considera la reasignación de llaves como una Solicitud de Certificado en términos de la Sección 4.1.

4.7.1 Circunstancias para la Reasignación de Llaves del Certificado

Antes de la expiración de un Certificado de Suscriptor existente, es necesario que el suscriptor reasigne la llave del certificado para mantener la continuidad del uso del certificado. La reasignación de llaves del certificado también puede ser realizada después de la expiración.

E-Sign notificará al Suscriptor cuyo certificado vaya a expirar acerca de este hecho.

4.7.2 Quién puede solicitar la certificación de una nueva Llave Pública

Sólo el suscriptor para un certificado individual o un representante autorizado para un certificado Organizacional pueden solicitar renovación de certificado.

4.7.3 Procesamiento de solicitudes de reasignación de Llaves del Certificado

Los procedimientos de reasignación de llave aseguran que la persona u organización que solicita la renovación de un Certificado de Suscriptor usuario final, de hecho, el suscriptor (o está autorizado por el suscriptor) del certificado.

Un procedimiento aceptable es mediante el uso de una Frase Secreta (o su equivalente), o la prueba de la posesión de la llave privada. Los suscriptores eligen y envían junto con información de su enrolamiento, una Frase Secreta (o su equivalente). Durante la renovación de un certificado, si un Suscriptor envía correctamente la Frase Secreta (o su equivalente) con la información del reenrolamiento del suscriptor, y la información de enrolamiento (incluyendo información de contactos ¹³) no ha cambiado, la renovación del Certificado es emitida de forma automática. De acuerdo a las disposiciones de la Sección 3.3.1 tras la renovación de esta manera, y al menos en las instancias alternativas de posteriores reasignaciones de llaves a partir de entonces, E-Sign o un RA reconfirmarán la identidad del suscriptor, de conformidad con los requisitos especificados en esta CPS para la identificación y autenticación de una Solicitud de Certificado original.

Aparte de este procedimiento u otro procedimiento aprobado por Symantec, para la reasignaciones de llaves de un Certificado de Suscriptor de usuario final serán utilizados los requisitos dispuestos para la autenticación de una Solicitud de Certificado original.

4.7.4 Notificación al Suscriptor de la Emisión de un Nuevo Certificado

La notificación al Suscriptor de la emisión del certificado para llaves reasignadas está de acuerdo con la Sección 4.3.2

4.7.5 Conducta que constituye aceptación del certificado para Llaves Reasignadas

¹³ Si la información de contacto ha cambiado a través de un procedimiento formal aprobado para el cambio en contacto, el certificado aún calificará para renovación automática.

La conducta que constituye la aceptación de un certificado para llaves reasignadas está en conformidad con la Sección 4.4.1

4.7.6 Publicación del certificado de Llave Reasignada por la CA

El certificado para llaves reasignadas es publicado en el repositorio de acceso público de E-Sign.

4.7.7 Notificación de la Emisión del Certificado a Otras Entidades por parte de la CA

Las RAs pueden recibir notificación de la emisión de los certificados que aprueban.

4.8 Modificación del Certificado

4.8.1 Circunstancias para la Modificación del Certificado

La modificación del Certificado de se refiere a la solicitud de la emisión de un nuevo certificado por cambios en la información de un certificado existente (que no sea la llave pública del suscriptor).

La modificación del Certificado es considerada como una Solicitud de Certificado en términos de la Sección 4.1.

4.8.2 Quién Puede Solicitar Modificación del Certificado

Consulte la Sección 4.1.1.

4.8.3 Procesamiento de Solicitudes de Modificación del Certificado

E-Sign o la RA llevará a cabo una identificación y autenticación de toda la información necesaria del Suscriptor en términos de la Sección 3.2.

4.8.4 Notificación al Suscriptor de la Emisión de Nuevo Certificado

Consulte la Sección 4.3.2.

4.8.5 Conducta que Constituye Aceptación del Certificado Modificado

Consulte la Sección 4.4.1.

4.8.6 Publicación del Certificado Modificado por la CA

Consulte la Sección 4.4.2.

4.8.7 Notificación de Emisión del Certificado a Otras Entidades por parte de la CA

Consulte la Sección 4.4.3.

4.9 Revocación y Suspensión de Certificado

4.9.1 Circunstancias para la revocación

Sólo en las circunstancias enumeradas a continuación un certificado de Suscriptor usuario final será revocado por Symantec (o por el Suscriptor) y publicado en una CRL. Symantec marcará el certificado como inactivo en su base de datos a petición de un suscriptor que ya no puede usar (o ya no desea usar) un certificado por una razón que no sea una de las que son mencionadas a continuación; sin embargo, no publicará el certificado en una CRL.

Un certificado de suscriptor usuario final es revocado si:

- E-Sign, un cliente o un suscriptor tiene motivo para creer o sospechar que ha existido un compromiso de la llave privada del suscriptor.
- E-Sign o un cliente tiene motivo para creer que el suscriptor ha quebrantado una obligación, declaración o garantía establecidas en el Acuerdo del Suscriptor aplicable,
- El Acuerdo del Suscriptor con el suscriptor ha sido terminado,
- La vinculación entre un Cliente Empresarial con un Suscriptor ha terminado o ha finalizado de alguna otra manera
- La vinculación entre una organización que es Suscriptor de Certificado de ASB Organizacional Class 3 y el representante de la organización que controla la llave privada del Suscriptor es terminada o se ha finalizado de terminado de alguna otra manera,
- E-Sign o un Cliente tiene motivo para creer que el certificado fue emitido de una forma que no cumple con los procedimientos requeridos por la CPS aplicable, el certificado fue emitido a una persona distinta de aquella nombrada como el Sujeto del certificado, o el certificado fue emitido sin la autorización de la persona nombrada como Sujeto de tal certificado,
- E-Sign o un cliente tiene motivo para creer que un dato en la Solicitud de Certificado es falso,
- E-Sign o un cliente determina que prerequisite sustancial para la Emisión de Certificados no fue ni satisfecho ni dispensado
- En el caso de los Certificados Organizacionales Class 3, el nombre de la organización del Suscriptor cambia.
- La información descrita en el certificado, aparte de la Información de Suscriptor No Verificada, es incorrecta o ha cambiado, o
- El uso continuado de este certificado es perjudicial para la red STN.

Al considerar si el uso del certificado es perjudicial para la red STN, E-Sign considera, entre otras cosas, lo siguiente:

- La naturaleza y el número de quejas recibidas
- La identidad del (de los) denunciante(s)
- La legislación pertinente en vigor
- Las respuestas a la supuesta utilización perjudicial, de parte del Suscriptor

Al considerar si el uso de un Certificado de Firma de Código es perjudicial para la STN, E-Sign además, considera, entre otras cosas, lo siguiente:

- El nombre del código que se firma
- El comportamiento del código
- Métodos de distribución del código
- Divulgación de información efectuada a los destinatarios del código
- Cualquier alegato adicional sobre el código

E-Sign también puede revocar un Certificado de Administrador si la autoridad del administrador para actuar como Administrador ha sido terminada o de alguna otra manera ha finalizado

Los Acuerdos de Suscriptor de E-Sign requieren que los Suscriptores usuarios finales notifiquen inmediatamente a E-Sign de un compromiso conocido o sospechado de su llave privada.

4.9.1.1 Requerimientos CABF para Razones para Revocación

Los certificados SSL con Dominio validado y Organización validada adhieren a los requisitos de CA / Browser Forum Baseline.

E-Sign deberá revocar un certificado dentro de 24 horas si ocurre una o más de las siguientes situaciones:

1. El Suscriptor solicita por escrito que la CA revoque su Certificado;
2. El Suscriptor notifica a la CA que la solicitud de certificado original no fue autorizada y no concede la autorización con efecto retroactivo;
3. La CA obtiene pruebas de que la Llave Privada del Suscriptor (correspondiente a la Llave Pública del Certificado) ha sufrido un Compromiso de Llave, o que el certificado ha sido mal utilizado de otro modo (por ejemplo, la Llave, Privada ha sido archivada);
4. La CA se tiene conocimiento de que un Suscriptor ha violado una o más de sus obligaciones materiales bajo el Acuerdo de Suscriptor;
5. La CA tiene conocimiento de cualquier circunstancia que indica que el uso de un Nombre de Dominio Totalmente Calificado o la dirección IP en el certificado ya no está permitido legalmente (por ejemplo, un tribunal o árbitro ha revocado el derecho de un Titular del Nombre de Dominio para utilizar el Nombre de Dominio, un acuerdo relevante de licencia o servicios entre el Titular del Nombre de Dominio y el Solicitante ha terminado, o el Titular del Nombre de Dominio no ha logrado renovar el Nombre de Dominio);
6. La CA tiene conocimiento de que un Certificado Wildcard ha sido utilizado para autenticar un Nombre de Dominio Totalmente Calificado subordinado fraudulentamente engañoso;
7. La CA tiene conocimiento de un cambio sustancial en la información contenida en el Certificado;
8. La CA tiene conocimiento de que el Certificado no fue emitido de conformidad con la CPS de E-Sign;
9. La CA determina que cualquiera de la información que aparece en el Certificado es incorrecta o engañosa;
10. La CA cesa sus operaciones por cualquier razón y no ha hecho arreglos para que otra entidad que preste apoyo a la revocación del Certificado;
11. El derecho de la CA para emitir certificados en virtud de esta CP expira o es revocado o terminado, a menos que la CA haya hecho los arreglos necesarios para seguir manteniendo el Repositorio de CRL/OCSP;
12. La CA tiene conocimiento de un posible compromiso de la Llave Privada de la CA Subordinada utilizada para la emisión del Certificado;
13. La CA o cualquiera de sus RA designadas tiene conocimiento de que la Llave Privada de un Suscriptor ha sido comunicada a una persona no autorizada o a una organización no afiliada con el Suscriptor,
14. La revocación es requerida de alguna otra manera por la CPS de E-Sign, o
15. El contenido técnico o el formato del Certificado presenta un riesgo inaceptable para los Proveedores de Software de Aplicación o las Partes que Confían (por ejemplo, según lo determinado por CA/Browser Forum).

4.9.2 Quién Puede Solicitar la Revocación

Los Suscriptores Individuales pueden solicitar la revocación de sus propios Certificados individuales a través de un representante autorizado de E-Sign o de una RA. En el caso de los certificados Organizacionales, un representante debidamente autorizado de la organización tendrá derecho para solicitar la revocación de los certificados emitidos para la organización. Un representante de E-Sign debidamente autorizado o una RA tendrá derecho a solicitar la revocación de un Certificado de Administrador de la RA. La entidad que aprobó una solicitud de Certificado de Suscriptor 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 emitidos a sus propias CA. Las RA tienen derecho, a través de sus representantes debidamente autorizados, para solicitar la revocación de sus propios certificados, y sus Entidades Superiores tendrán derecho a solicitar o iniciar la revocación de los Certificados de aquéllas.

4.9.3 Procedimiento para la Solicitud de Revocación

4.9.3.1 Procedimiento para solicitar la revocación de un certificado de suscriptor usuario final

Un Suscriptor usuario final que solicita revocación debe comunicar la solicitud a E-Sign o al cliente que aprueba la solicitud de certificado del suscriptor, quienes a su vez iniciarán la revocación del certificado en forma inmediata. Para los clientes Empresariales, el suscriptor debe comunicar la solicitud al Administrador Empresarial que comunicará la solicitud de revocación a E-Sign para su procesamiento. La comunicación de la solicitud de revocación será efectuada en acuerdo con CPS § 3.4.

Cuando un Cliente Empresarial inicia la revocación de un certificado de suscriptor de usuario final por iniciativa propia, el Cliente de Managed PKI o el Cliente ASB instruyen a E-Sign para revocar el certificado.

Una vez que el certificado de suscriptor es revocado, es registrado en la CRL que será publicada como actualización de la CRL que se encuentra publicada en el momento de tal revocación.

El proceso de revocación es llevado a cabo individualmente, es decir, la revocación de un grupo de certificados no está soportada.

4.9.3.2 Requisitos CABF para el Proceso de Revocación de Certificados

Los certificados SSL con Dominio validado y Organización validada adhieren a los requisitos de CA / Browser Forum Baseline.

Solicitud de Revocación

Las CAs de E-Sign deberán proporcionar un proceso para que los Suscriptores soliciten la revocación de sus propios Certificados descrito en la sección 4.9 de la presente CPS.

E-Sign mantendrá una capacidad continua 24x7 para aceptar y responder a las solicitudes de revocación y requerimientos relacionados.

Informes de Problemas de Certificado

Las CAs de E-Sign darán a conocer públicamente a los Suscriptores, Partes que Confían, Proveedores de Aplicaciones de Software, y otras terceras partes, las instrucciones para informar sospecha de Compromiso de la Llave Privada, el uso

indebido de Certificados, u otros tipos de fraude, compromiso, uso indebido, conducta inapropiada, o cualquier otro asunto relacionado con los Certificados.

Investigación

Las CAs de E-Sign deberán iniciar la investigación de un Informe de Problemas de Certificado dentro de las veinticuatro (24) horas siguientes a la recepción y decidir si la acción de revocación o de otra índole apropiadas se justifica basándose en al menos los siguientes criterios:

1. La naturaleza del presunto problema;
2. El número de Informes de Problemas de Certificado recibidos acerca de un determinado Certificado o Suscriptor;
3. La entidad que presenta la queja (por ejemplo, una denuncia de un oficial de la ley que un sitio Web se dedica a actividades ilegales debería tener más peso que una queja de un consumidor que argumenta que no recibió los bienes que ordenados), y
4. La legislación pertinente

Respuesta

E-Sign mantendrá una capacidad continua 24x7 para aceptar y responder internamente a una revocación por Informe de Problemas Certificado de alta prioridad y en su caso, derivar tal queja a las autoridades policiales y/o revocar un certificado que es objeto de dicha queja.

4.9.3.3 Procedimiento para solicitar la revocación de un certificado de CA o RA

Una CA o RA que solicite la revocación de su certificado de CA o de RA debe comunicar la solicitud a E-Sign. E-Sign entonces revocará el certificado. E-Sign también puede iniciar la revocación del certificado de CA o de RA.

4.9.4 Período de gracia de solicitud de revocación

Las solicitudes de revocación serán enviadas tan pronto como sea posible, dentro de un tiempo comercialmente razonable.

4.9.5 Tiempo dentro del cual la CA debe procesar la solicitud de revocación

E-Sign da pasos comercialmente razonables para procesar las solicitudes de revocación sin demora. E-Sign notificará al suscriptor que se ha revocado el Certificado, así como a la RA externa respectiva, cuando ésta haya solicitado la revocación.

4.9.6 Requisitos de comprobación de revocación para las Partes que Confían

Las Partes que Confían deberán comprobar el estado de los Certificados en los cuales desean confiar. Un método a través del cual las Partes que Confían pueden comprobar el estado del Certificado es consultando la CRL más reciente de la CA que emitió el Certificado en el cual la Parte que Confía desea confiar. Alternativamente, las Partes que Confían podrán cumplir con este requisito, ya sea comprobando el estado del Certificado usando el repositorio basado en Web aplicable o mediante el uso de OCSP (si está disponible). Las CAs deberán proporcionar a las Partes que Confían, información sobre cómo encontrar la CRL, el repositorio basado en Web, o el respondedor OCSP (donde esté disponible) apropiados para comprobar el estado de revocación.

4.9.7 Frecuencia de emisión de CRL

Las CRL para los Certificados de Suscriptor usuario final son emitidas al menos una vez al día. Las CRL para certificados de CA deberán ser emitidas por lo menos una vez al año, pero también cada vez que un certificado de CA sea revocado.

Las CRL para CA raíces para firma de contenido autenticado (Authenticated Content Signing, ACS) son publicadas anualmente y también cada vez que un certificado de CA es revocado.

Si un certificado listado en una CRL expira, puede ser removido de las CRL emitidas después del vencimiento del Certificado.

4.9.7.1 Requisitos CABF para Emisión de CRL

Los certificados SSL con Dominio validado y Organización validada adhieren a los requisitos de CA / Browser Forum Baseline.

Requisitos de Estado de Certificados de Suscriptor

Si la CA publica una CRL, la CA deberá actualizar y volver a emitir la CRL al menos una vez cada siete (7) días, y el valor del campo nextUpdate no debe ser mayor de diez (10) días respecto del valor del campo thisUpdate.

Requisitos de Estado de Certificados de CA Subordinada

La CA deberá actualizar y volver a emitir las CRL, por lo menos (i) una vez cada doce (12) meses y (ii) dentro de las 24 horas posteriores a la revocación de un certificado de CA subordinada, y el valor del campo nextUpdate no debe ser mayor de doce (12) meses respecto del valor del campo thisUpdate.

4.9.8 Latencia máxima de CRL

Las CRL son publicadas en el repositorio dentro de un plazo comercialmente razonable tras su generación. Esto generalmente se realiza automáticamente pocos minutos después de la generación.

4.9.9 Disponibilidad de comprobación en línea de revocación/estado

La información en línea de revocación y de otros estados de certificado está disponible a través de un repositorio basado en Web y, en donde sea ofrecido, OCSP. Además de la publicación de las CRL, E-Sign ofrece información de estado de certificado a través de funciones de consulta en el repositorio de E-Sign.

La información de estado del certificado está disponible, a través de funciones de consulta basada en Web accesible a través del repositorio de E-Sign en

- <https://digitalid.e-sign.cl/c2/client/search.htm> (para Certificados Individuales de Firma Tributaria)
- <https://digitalid.e-sign.cl/fea/client/search.htm> (para Certificados Individuales de Firma Electrónica Avanzada)
- <https://arech.e-sign.cl/eu/client/search.htm> (para Certificados Individuales de Firma Electrónica Avanzada para el Estado de Chile)
- <https://arech.e-sign.cl/ro/client/search.htm> (para Certificados de Administradores de RA para el Estado de Chile)
- <https://digitalid.e-sign.cl/global/services/globalserver/search.htm> (para Certificados de Sitio Seguro Global)

- <https://digitalid.e-sign.cl/secure/services/server/search.htm> (para Certificados de Sitio Seguro)

E-Sign también ofrece información de estado de certificados OCSP. Los Clientes Empresariales que contratan servicios OCSP pueden comprobar el estado de certificado mediante el uso de OCSP. La dirección del respondedor OCSP relevante es comunicada al Cliente Empresarial.

4.9.9.1 Requisitos CABF para la Disponibilidad de OCSP

Los certificados SSL con Dominio validado y Organización validada adhieren a los requisitos de CA / Browser Forum Baseline.

A partir del 1 enero de 2013, la CA deberá admitir una capacidad de OCSP mediante el método GET para los certificados emitidos de conformidad con estos Requisitos.

Estado del Certificado para Certificados de Suscriptor

La CA deberá actualizar la información proporcionada a través de OCSP por lo menos cada cuatro (4) días. Las respuestas OCSP de este servicio debe tener una fecha máxima de expiración de diez (10) días.

Estado de Certificados para Certificados de CA Subordinadas

La CA deberá actualizar la información proporcionada a través de OCSP por lo menos (i) cada doce (12) meses y (ii) dentro de las 24 horas después de la revocación de un Certificado de CA Subordinada.

4.9.10 Requisitos de comprobación de revocación en-línea

Una Parte que Confía debe comprobar el estado de un certificado en el cual quiere confiar. Si una Parte que Confía no comprueba el estado de un certificado en el cual la Parte que Confía desea confiar consultando la CRL pertinente más reciente, la Parte que Confía deberá comprobar el estado de certificado consultando el repositorio aplicable o solicitando el estado del certificado utilizando el respondedor OCSP (si los servicios OCSP son ofrecidos).

4.9.11 Otras formas de publicidad de revocación disponibles

No es aplicable

4.9.12 Requisitos especiales en relación con compromiso de llaves

E-Sign realiza esfuerzos comercialmente razonables para notificar a las Partes que Confían si descubre, o tiene motivos para creer, que ha habido un compromiso de la llave privada de uno de sus propias CA o una de las CA dentro de sus subdominios.

4.9.13 Circunstancias para la suspensión

E-Sign no soporta la suspensión de certificados digitales.

4.9.14 Quién puede solicitar la suspensión

E-Sign no soporta la suspensión de certificados digitales.

4.9.15 Procedimiento para la solicitud de suspensión

E-Sign no soporta la suspensión de certificados digitales.

4.9.16 Límites del periodo de suspensión

E-Sign no soporta la suspensión de certificados digitales.

4.10 Servicios de estado de certificados

Las operaciones de CA de E-Sign son llevadas a cabo en la infraestructura segura de Symantec, por lo cual el servicio de información de estado de certificados es mantenido por Symantec de acuerdo a los procedimientos establecidos en esta CPS.

4.10.1 Características Operacionales

El Estado de los certificados públicos está disponible a través de CRL en el sitio web de Symantec, directorio LDAP y a través de un respondedor OCSP (donde esté disponible).

4.10.2 Disponibilidad del Servicio

Los servicios de estado de certificados están disponibles las 24 horas al día 7 días a la semana sin interrupción programada.

Para certificados SSL con Organización validada y Dominio validado, las capacidades CRL y OCSP deberán proporcionar un tiempo de respuesta de diez (10) segundos o menos bajo condiciones de operación normal.

4.10.3 Características Opcionales

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

4.11 Fin de la Suscripción

Un suscriptor puede terminar una suscripción de un certificado E-Sign al:

- Permitir que su certificado expire sin renovarlo o reasignar la llave de dicho certificado
- Revocar su certificado antes de la expiración del certificado, sin reemplazar los certificados.

4.12 Custodia y Recuperación de Llaves

Con la excepción de las empresas que implementan servicios Managed PKI Key Management Services, ningún participante del subdominio E-Sign, incluyendo a E-Sign, puede custodiar llaves privadas de CA, RA o de Suscriptores usuarios finales.

Los clientes empresariales que utilizan la opción Key Escrow dentro de Managed PKI Service de Symantec pueden custodiar copias de las llaves privadas de Suscriptores cuyas Solicitudes de Certificado aprueban. La empresa cliente puede custodiar llaves ya sea en las instalaciones de la empresa o en el centro de datos seguro de Symantec. Si es operado con las instalaciones de la empresa, Symantec no almacena copias de las llaves privadas del Suscriptor, pero de todas maneras juega un papel importante en el proceso de recuperación de las llaves del Suscriptor.

4.12.1 Políticas y Prácticas de Custodia y Recuperación de Llaves

Los clientes Empresariales que utilizan la opción Key Escrow dentro del servicio Managed PKI de Symantec (o un servicio equivalente aprobado por Symantec) están autorizados para custodiar llaves privadas de los Suscriptores usuarios finales. Las llaves privadas en custodia serán almacenadas en forma cifrada utilizando la aplicación Managed PKI Key Manager. Excepto para los clientes empresariales que usan Managed PKI Key Manager Service (o un servicio equivalente aprobado por Symantec), las llaves privadas de CA o de Suscriptores usuarios finales no serán custodiadas.

Las llaves privadas de suscriptores usuarios finales serán recuperadas sólo en las circunstancias permitidas dentro de la Guía Managed PKI Key Management Service Administrator's Guide, según la cual:

- Los clientes Empresariales que usan Managed PKI Key Manager deberán confirmar la identidad de cualquier persona que se presente como el Suscriptor para asegurar que una supuesta petición del Suscriptor para acceder a la llave privada del Suscriptor proviene, de hecho, del Suscriptor y no de un impostor,
- Los clientes empresariales recuperarán la llave privada de un suscriptor sin la autorización del suscriptor sólo para sus fines legítimos y legales, tales como el cumplimiento de procesos judiciales o administrativos o de órdenes de registro, y no para propósitos ilegales, fraudulentos, o ilícitos de otro tipo, y
- Tales Clientes Empresariales deberán tener controles de personal para prevenir que administradores de Key Management Service y otras personas obtengan acceso no autorizado a llaves privadas.

Se recomienda que los Clientes Empresariales que usen la opción Key Escrow dentro de Managed PKI Service de Symantec:

- Notifiquen a los suscriptores que sus llaves privadas son custodiadas
- Protejan las llaves de suscriptores en custodia de divulgaciones no autorizadas,
- Protejan toda la información, incluida las propias llaves del administrador que podrían utilizarse para recuperar las llaves de los suscriptores en custodia.
- Liberen las llaves de suscriptores en custodia sólo frente a solicitudes de recuperación, debidamente autenticadas y autorizadas.
- Revoquen el par de llaves del suscriptor antes de recuperar la llave de cifrado bajo ciertas circunstancias tales como la discontinuación del uso de un certificado perdido..
- No comuniquen información alguna relativa a una llave de recuperación al suscriptor, salvo cuando el propio suscriptor ha solicitado la recuperación.
- No revelen ni permitan que se revelen llaves en custodia o información relacionada con llaves en custodia a ninguna tercera parte menos que sea requerido por la ley, dictamen o regulación de gobierno; por la política organizacional de la empresa, o por orden de un tribunal de jurisdicción competente.

4.12.2 Políticas y prácticas de encapsulamiento y recuperación de Llave de Sesión

Las llaves privadas son almacenadas en la base de datos del Key Manager de forma encriptada. La llave privada de cada suscriptor es encriptada de forma individual con su propia llave simétrica triple-DES. Un registro del custodia de la Llave (KER) es generado y luego la llave triple DES es combinada con una llave de sesión aleatoria para formar una máscara de llave de sesión (MSK). La MSK resultante, junto con la información de solicitud de certificado, es enviada de forma segura y almacenada en la base de datos de Managed PKI en Symantec. El KER (que contiene la llave privada del usuario final) y la llave de sesión individuales son almacenados en la base de datos de Key Manager y todo el material residual de la llave es destruido.

La base de datos de Managed PKI es operada con el centro de datos seguro de Symantec. El Cliente Empresarial puede optar por operar la base de datos de Key Manager ya sea en las instalaciones de la empresa o con el centro de datos seguro de Symantec.

La recuperación de una llave privada y un certificado digital requiere que el administrador de Managed PKI inicie sesión en el Centro de Control de Managed PKI, seleccione el par de llaves apropiado a recuperar y haga clic en el hipervínculo "recover". El MSK para ese par de llaves es retornado de la base de datos de Managed PKI sólo después de que un administrador aprobado hace clic en el enlace "recover". El Key Manager recupera la llave de sesión de KMD y lo combina con el MSK para regenerar la llave triple DES que fue utilizada originalmente para cifrar la llave privada, permitiendo la recuperación de la llave privada del usuario final. Como paso final, un archivo PKCS # 12 cifrado es devuelto al administrador y es distribuido en última instancia al usuario final.

5 Instalación, Gestión y Controles Operacionales

Las operaciones de CA de E-Sign son llevadas a cabo en la infraestructura segura de Symantec, por lo cual la gestión y el control de la operación de la CA de E-Sign son implementados por Symantec de acuerdo a los procedimientos establecidos en esta CPS.

5.1 Controles Físicos

E-Sign ha puesto en marcha la Política de Seguridad Física de E-Sign, que soporta los requisitos de seguridad de esta CPS. El cumplimiento de estas políticas está incluido en los requisitos de auditoría independiente de E-Sign descritos en la Sección 8. La Política de Seguridad Física de E-Sign contiene información de seguridad sensible y sólo está disponible previo acuerdo con E-Sign. Como parte de la STN, los sistemas físicos de CA de E-Sign, son operados en las instalaciones seguras de Symantec. Una visión general de los requisitos es descrita en los siguientes apartados.

5.1.1 Localización del Sitio y Construcción

Las operaciones de las CA y RA de E-Sign, son llevadas a cabo dentro de un entorno protegido físicamente que disuade, previene y detecta el uso no autorizado de, el acceso a, o la divulgación de información y sistemas sensibles sean estos encubiertos o abiertos.

E-Sign también cuenta con instalaciones de recuperación de desastres para sus operaciones de CA. Las instalaciones de recuperación de desastres de E-Sign están protegidas por múltiples anillos de seguridad física comparable a los de la instalación principal de E-Sign.

5.1.2 Acceso Físico

Los sistemas de CA de E-Sign, están protegidos por un mínimo de cuatro anillos de seguridad física, con acceso al anillo inferior requerido antes de poder acceder al anillo superior.

Privilegios de acceso físico progresivamente restrictivos controlan el acceso a cada anillo. La actividad operativa sensible de la CA, cualquier actividad relacionada con el ciclo de vida del proceso de certificación como autenticación, verificación y emisión,

se producen dentro de anillos físicos muy restrictivos. El acceso a cada anillo requiere el uso de una tarjeta credencial de empleados de proximidad. El acceso físico es automáticamente registrado en una bitácora y grabado en vídeo. Los anillos adicionales refuerzan el cumplimiento del control de acceso individual a través del uso de autenticación de dos factores, incluyendo biometría. En tales áreas de seguridad no se permite personal sin escolta, incluyendo empleados que no sean de confianza o visitantes.

El sistema de seguridad física incluye anillos adicionales para la seguridad de gestión de llaves que sirve para proteger tanto el almacenamiento en línea y fuera de línea de CSU y material de llaves. Las áreas utilizadas para crear y almacenar material criptográfico imponen control dual, cada uno a través del uso de autenticación dos factores incluyendo biometría. Las CSU en línea están protegidas mediante el uso de gabinetes con llave. Las CSU fuera de línea son protegidas mediante el uso de cajas fuertes, gabinetes y contenedores. El acceso a las CSU y al material de llaves está restringido de acuerdo con los requisitos de segregación de funciones de E-Sign. La apertura y cierre de gabinetes o contenedores en estos anillos se registra en bitácora para fines de auditoría.

5.1.3 Energía y Aire Acondicionado

Las instalaciones seguras de E-Sign cuentan con equipamiento primario y de respaldo en cuanto a:

- Sistemas de energía para asegurar el acceso continuo e ininterrumpido a energía eléctrica, y
- Sistemas de calefacción/ventilación/aire acondicionado con control de temperatura y humedad relativa.

5.1.4 Exposición del Agua

E-Sign ha tomado precauciones razonables para minimizar el impacto de la exposición al agua de los sistemas de E-Sign.

5.1.5 Prevención y Protección contra Incendios

E-Sign ha tomado precauciones razonables para prevenir y extinguir incendios u otros daños por exposición a las llamas o al humo de sus respectivas instalaciones. Las medidas de prevención y de protección contra el fuego de E-Sign han sido diseñadas para cumplir con las regulaciones locales de seguridad contra incendios.

5.1.6 Almacenamiento de Medios

Todos los medios que contienen software y datos de producción, información de auditoría, archivo o de copias de seguridad es almacenada dentro de las instalaciones de E-Sign o en una instalación de almacenamiento seguro fuera del sitio con apropiados controles de acceso físico y lógico diseñados para limitar el acceso a personal autorizado y proteger tales medios frente a daños accidentales (por ejemplo, agua, fuego, y electromagnéticos).

5.1.7 Eliminación de Residuos

Los documentos y materiales sensibles son triturados antes de su eliminación. Los medios utilizados para capturar o transmitir información sensible son dejados ilegibles antes de su eliminación. Los dispositivos criptográficos son destruidos físicamente o su

contenido es dejado en cero de acuerdo a la guía del fabricante antes de su eliminación.

Otros desechos son eliminados de acuerdo a los requerimientos de eliminación de desechos normales definidos por E-Sign.

5.1.8 Respaldo Fuera de las Instalaciones

E-Sign ejecuta respaldos de rutina de datos críticos del sistema, datos de registro de auditoría y otra información delicada. Los medios de respaldo realizado fuera de las instalaciones son almacenados en forma físicamente segura usando las instalaciones de almacenamiento de un tercero y las instalaciones de recuperación de desastres de E-Sign.

5.2 Controles de Procedimiento

5.2.1 Funciones de Confianza

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 Certificados,
- La aprobación, rechazo u otro procesamiento de Solicitudes de Certificado, solicitudes de revocación, o solicitudes de renovación o información de solicitudes,
- La emisión o revocación de Certificados, incluyendo al personal que tiene acceso a porciones restringidas de su repositorio,
- El manejo de información de Suscriptor o solicitudes.

Personas de Confianza incluyen, pero no están limitados a:

- Personal de servicio al cliente,
- Personal de operaciones criptográficas,
- Personal de seguridad,
- Personal de administración de sistemas,
- Personal designado de ingeniería, y
- Ejecutivos que han sido designados para administrar la confiabilidad de la infraestructura.

E-Sign considera las categorías de personal identificado en esta sección como Personas de Confianza que tienen un Puesto de Confianza. Las personas que deseen convertirse en Personas de Confianza mediante la obtención de un Puesto de Confianza deben completar con éxito los requisitos de selección establecidos en esta CPS.

5.2.2 Número de personas requeridas por tarea

E-Sign ha establecido, mantiene e impone rigurosos procedimientos de control para asegurar la segregación de funciones sobre la base de la responsabilidad del trabajo y para asegurar que son necesarias varias Personas de Confianza para realizar tareas delicadas.

Hay políticas y procedimientos de control establecidas para garantizar la segregación de funciones sobre la base de las responsabilidades del trabajo. Las tareas más delicadas, como el acceso a y la gestión de hardware criptográfico de la CA (unidad de firma criptográfica o CSU) y de material de llave asociado, requieren varias Personas de Confianza.

Estos procedimientos de control interno están diseñados para asegurar que, como mínimo, dos Personas de Confianza son requeridas para tener acceso ya sea físico o lógico al dispositivo. El acceso al hardware criptográfico de la CA es estrictamente reforzado por varias Personas de Confianza, a lo largo de su ciclo de vida, desde la recepción e inspección de entrada hasta la destrucción lógica y/o física final. Una vez que el módulo es activado con llaves operacionales, son invocados controles de acceso adicionales para mantener el control disgregado sobre el acceso tanto físico como lógico al dispositivo. Las personas con acceso físico a los módulos no tienen asignadas "Partes Secretas" y viceversa.

Otras operaciones manuales, tales como la validación y emisión de Certificados Class 3, no emitidos mediante un sistema de validación y emisión automatizadas, requieren la participación de al menos dos (2) Personas de Confianza, o una combinación de al menos una persona de confianza y un proceso de validación y emisión automatizadas. Las operaciones manuales para Recuperación de Llaves, pueden requerir opcionalmente la validación de dos (2) Administradores autorizados.

5.2.3 Identificación y Autenticación para Cada Rol

Para todo el personal que aspira a convertirse en Persona de Confianza, la verificación de identidad es realizada a través de la presencia personal (física) de tal personal ante Personas de Confianza que cumplen funciones de recursos humanos o de seguridad en E-Sign y una revisión de formas de identificación comúnmente reconocidas (p. ej., pasaportes y licencias de conducir). La identidad es confirmada adicionalmente a través de los procedimientos de comprobación de antecedentes en CPS § 5.3.1.

E-Sign se asegura de que el personal ha alcanzado el Estado de Confianza y ha recibido aprobación departamental antes de que a ese personal:

- Le sean emitidos dispositivos de acceso y le sea concedido acceso a las instalaciones requeridas;
- Le sean emitidas credenciales electrónicas para acceder y realizar funciones específicas en CA, RA u otros sistemas de IT de la STN.

5.2.4 Roles que Requieren Separación de Funciones

Los roles que requieren la separación de funciones incluyen (pero no están limitados a)

- la validación de información en las Solicitudes de Certificado;
- la aceptación, rechazo, u otro tipo de procesamiento de Solicitudes de Certificado, solicitudes de revocación, solicitudes de recuperación de llaves o solicitudes de renovación, o información de enrolamiento;
- la emisión o revocación de los certificados, incluido el personal que tiene acceso a partes restringidas del repositorio;
- el manejo de información o de solicitudes del suscriptor
- la generación, emisión o destrucción de un certificado de CA
- la carga de una CA para un entorno de Producción

5.3 Controles de Personal

El personal que aspira a convertirse en Personas de Confianza debe presentar pruebas de los requisitos de antecedentes, calificaciones y experiencia necesarios para desempeñar sus responsabilidades de trabajo prospectivo en forma competente y satisfactoria, así como la prueba de cualquier autorización del gobierno, en su caso, necesaria para realizar servicios de certificación en virtud de contratos con el gobierno.

La verificación de antecedentes es repetida por lo menos cada 5 años para el personal que ocupa Puestos de Confianza.

5.3.1 Requisitos de Calificaciones, Experiencia, y Autorización

E-Sign requiere que el personal que aspira a convertirse en Persona de Confianza presente pruebas de los requisitos de antecedentes, calificaciones y experiencia necesarios para desempeñar sus responsabilidades de trabajo prospectivo en forma competente y satisfactoria, así como la prueba de cualquier autorización del gobierno, en su caso, necesaria para realizar servicios de certificación en virtud de contratos con el gobierno.

5.3.2 Procedimientos de Revisión de Antecedentes

Antes del comienzo del empleo en un Rol de Confianza, E-Sign lleva a cabo revisiones de antecedentes que incluyen lo siguiente:

- confirmación del empleo anterior,
- verificación de referencia profesional,
- confirmación del más alto o más relevante grado académico obtenido,
- búsqueda de antecedentes penales (local, regional, y nacional),
- verificación de registros de crédito o financieros,
- búsqueda de registros de licencia de conducir, y
- búsqueda de registros del Servicio de Registro Civil e Identificación.

En la medida en que alguno de los requisitos impuestos por la presente sección no pueda ser satisfecho a causa de una prohibición o limitación en la legislación local o de otras circunstancias, E-Sign utilizará una técnica de investigación sustituta permitida por la ley que proporcione información muy similar, que incluye pero no está limitada a la obtención de una verificación de antecedentes realizado por la agencia gubernamental aplicable.

Los factores revelados en una verificación de antecedentes que pueden ser considerados para rechazar candidatos a Cargos de Confianza o para tomar medidas contra una Persona de Confianza existente en general incluyen (pero no están limitados a) lo siguiente:

- Falsedades formuladas por el candidato o Persona de Confianza,
- Referencias profesionales altamente desfavorables o poco fiables,
- Ciertas condenas penales, y
- Indicaciones de una falta de responsabilidad financiera.

Los informes que contienen esa información son evaluados por recursos humanos y personal de seguridad, quienes determinan el curso de acción apropiado en función de la naturaleza, magnitud y frecuencia del comportamiento descubierto por la verificación de antecedentes. Tales acciones que pueden incluir medidas que incluyen hasta la cancelación de las ofertas de empleo formuladas a los candidatos a Puestos de Confianza o el despido de Personas de Confianza existentes.

El uso de la información revelada en una investigación de antecedentes para tomar las acciones está sujeto a las leyes locales aplicables.

5.3.3 Requisitos de Capacitación

E-Sign proporciona a su personal capacitación con la contratación, así como la capacitación necesaria para el desempeño de sus responsabilidades de trabajo de manera competente y satisfactoria. E-Sign mantiene los registros de dicha formación.

E-Sign revisa y mejora periódicamente sus programas de capacitación según sea necesario.

Los programas de capacitación de E-Sign se adaptan a las responsabilidades de la persona e incluyen lo siguiente, según proceda:

- Conceptos básicos de PKI,
- Responsabilidades del empleo,
- Políticas y procedimientos de seguridad y operativa de E-Sign
- Uso y funcionamiento del hardware y el software desplegado,
- Reportes y gestión de incidentes y compromisos, y
- Recuperación de desastres y procedimientos de continuidad de negocio.

5.3.3.1 Requisitos CABF para Capacitación y Nivel de Habilidades

Los certificados SSL con Dominio validado y Organización validada adhieren a los requisitos de CA / Browser Forum Baseline.

E-Sign proporciona a todo el personal que realiza tareas de verificación de información capacitación de habilidades que cubre el conocimiento básico de Infraestructura de Llave Pública, políticas y procedimientos de autenticación y verificación de antecedentes (incluyendo esta CPS), amenazas comunes en el proceso de verificación de información (incluyendo phishing y otras tácticas de ingeniería social) , y los Requisitos CABF pertinentes.

E-Sign mantiene registros de dicha capacitación y se asegura de que los funcionarios a quienes se confían las tareas de Especialistas de Validación mantengan un nivel de habilidad que les permita ejercer estas funciones de manera satisfactoria. Los Especialistas de Validación que participan en la emisión de Certificados deberán mantener niveles de habilidad consistentes con los programas de formación y de desempeño de la CA.

E-Sign documenta que cada Especialista de Validación posee las habilidades requeridas por la tarea antes de permitir que el Especialista de Validación realice esa tarea. E-Sign requiere que todos los Especialistas de Validación pasen por un examen proporcionado por la CA en los requisitos de verificación de información señalados en los Requisitos CABF.

5.3.4 Frecuencia y Requisitos de Reforzamiento

E-Sign ofrece cursos de reforzamiento y actualizaciones a su personal en la medida y la frecuencia necesarias para garantizar que tal personal mantiene el nivel necesario de habilidad para llevar a cabo sus responsabilidades laborales de manera competente y satisfactoria.

5.3.5 Frecuencia y Secuencia de Rotación Laboral

No es aplicable

5.3.6 Sanciones por Acciones no Autorizadas

Ante acciones no autorizadas u otras violaciones a las políticas y procedimientos de E-Sign son aplicadas acciones disciplinarias apropiadas. Las acciones disciplinarias pueden incluir medidas que llegan hasta e incluyen el despido y son proporcionales a la frecuencia y la gravedad de las acciones no autorizadas.

5.3.7 Requerimientos para Contratista Independiente

En circunstancias limitadas, pueden ser utilizados contratistas o consultores independientes para llenar de Posiciones de Confianza. Cualquiera de estos contratistas o consultores debe cumplir con los mismos criterios funcionales y de seguridad que son aplicados a los empleados de E-Sign en una posición comparable. A los contratistas y consultores independientes que no han completado o no aprueban los procedimientos de verificación de antecedentes especificados en CPS § 5.3.2 se les permite el acceso a las instalaciones de seguridad de E-Sign sólo en la medida en que son acompañados y supervisados directamente por Personas de Confianza en todo momento.

5.3.8 Documentación Proporcionada al Personal

E-Sign ofrece a sus empleados la capacitación necesaria y demás documentación necesaria para llevar a cabo sus responsabilidades laborales de manera competente y satisfactoria.

5.4 Procedimientos de Registro de Auditoría

Los procedimientos de registro de auditoría de la CA de E-Sign son realizados por Symantec de acuerdo a los procedimientos establecidos en esta CPS.

5.4.1 Tipos de Eventos Registrados

E-Sign registra manual o automáticamente los siguientes eventos significativos:

- Eventos de gestión del ciclo de vida de llaves de CA, incluyendo:
 - Generación copia de seguridad, almacenamiento, recuperación, archivo y destrucción de llave
 - Eventos de gestión del ciclo de vida del dispositivo criptográfico.
- Eventos de la gestión del ciclo de vida del certificado de la CA y del suscriptor, incluyendo:
 - Renovación, regeneración de llaves, y revocación solicitudes de certificado
 - Procesamiento exitoso o no de solicitudes
 - Generación y emisión de certificados y CRL.
- Eventos relacionados con Seguridad incluyendo:
 - Intentos de acceso al sistema de PKI exitosos y fallidos
 - Acciones realizadas por personal de E-Sign en PKI y en el sistema de seguridad
 - Archivos o registros de seguridad sensibles leídos, escritos o borrados
 - Cambios de perfil de seguridad
 - Caídas del sistema, fallos de hardware y otras anomalías
 - Actividad de firewalls y routers
 - Entrada/salida de visitantes a las instalaciones de CA.

Las entradas del registro incluyen los siguientes elementos:

- Fecha y hora de la entrada
- Número de serie o secuencia de entrada, para entradas en bitácora diaria automática
- Identidad de la entidad que ingresa el registro en la bitácora
- Descripción/tipo de entrada.

Las RA de E-Sign y los Administradores Empresariales registran la información de Solicitudes de Certificado incluyendo:

- Tipo de documento(s) de identificación presentada por el Solicitante del Certificado
- Registro de datos o números de identificación únicos, o una combinación de ellos (por ejemplo, el número de licencia de conducir del Solicitante de Certificado) correspondientes a documentos de identificación, si es aplicable
- Ubicación del almacenamiento de copias de solicitudes y documentos de identificación
- Identidad de la entidad que acepta la solicitud
- Método utilizado para validar los documentos de identificación, si es aplicable
- Nombre de la CA receptora de o la RA emisora, si es aplicable.

5.4.2 Frecuencia de Procesamiento del Registro

El sistema y los logs de auditoría de la CA son monitoreados continuamente para proporcionar alertas en tiempo real de sucesos de seguridad y operativos significativos. Además, E-Sign revisa los registros de auditoría para detectar actividades sospechosas o inusuales en respuesta a las alertas generadas en base a irregularidades e incidentes en los sistemas de la CA y RA de E-Sign.

El proceso del registro de auditoría consiste en una revisión de los registros y la documentación de auditoría para todos los eventos importantes en un resumen del registro de auditoría. Las revisiones del registro de auditoría incluyen la verificación de que el registro no ha sido manipulado, una 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 también están documentadas.

5.4.3 Periodo de Retención para el Registro de Auditoría

Los registros de auditoría se retienen en el lugar en el que se generan por lo menos durante 2 meses a contar desde su procesamiento y luego se archivan de acuerdo a la Sección 5.5.2.

5.4.4 Protección de Registro de Auditoría

Los registros de auditoría están protegidos con un sistema de auditoría de registro electrónico que incluye mecanismos para proteger los archivos de registro contra accesos no autorizados, modificación, borrado u otras manipulaciones.

5.4.5 Procedimientos de Respaldo de los Registros de Auditoría

Respaldos incrementales de registros de auditoría son creados a diario y los respaldos completos se hacen de forma semanal.

5.4.6 Sistema de Recolección de Auditoría (Interna vs. Externa)

Los datos de auditoría automatizados son generados y grabados a nivel de aplicación, red y sistema operativo. Los datos de auditoría manuales son registrados por el personal de E-Sign.

5.4.7 Notificación al Sujeto Causante del Evento

Cuando un evento es registrado por el sistema de recolección de auditoría, no se requiere la entrega de una notificación al individuo, organización, dispositivo o aplicación que causó el evento.

5.4.8 Evaluación de Vulnerabilidades

Los eventos en el proceso de auditoría son registrados, en parte, para monitorear vulnerabilidades del sistema. Las EVSL (evaluaciones de vulnerabilidad de seguridad lógica) son ejecutadas, revisadas y analizadas después de examinar estos eventos monitoreados. Las EVSL están basadas en datos registrados automáticamente en tiempo real y son realizadas diaria, mensual y anualmente. Una EVSL anual será una entrada para una auditoría de cumplimiento anual.

5.5 Archivo de Registros

Los procedimientos de archivo de registros de la CA de E-Sign son realizados por Symantec de acuerdo a los procedimientos establecidos en esta CPS.

5.5.1 Tipos de Registros Archivados

E-Sign archiva:

- Todos los datos de auditoría recopilados en términos de la Sección 5.4
- Información de la solicitud Certificado
- Documentación de respaldo a las solicitudes de certificados
- Información de ciclo de vida del certificado p. ej., información de solicitudes de revocación, regeneración de llaves y renovación

5.5.2 Periodo de Retención Para el Archivo

Los registros serán conservados durante al menos los plazos establecidos a continuación después de la fecha en que el Certificado expira o es revocado.

- Cinco (5) años para los Certificados Class 1,
- Diez (10) años y seis (6) meses para Certificados Class 2 y Class 3

5.5.3 Protección del Archivo

E-Sign protege el archivo para que sólo las Personas de Confianza autorizadas puedan obtener acceso al archivo. El archivo está protegido contra accesos, modificación, borrado u otras manipulaciones no autorizadas por el sistema de almacenamiento dentro de un Sistema de Confianza. Los medios que contienen los datos de archivo y las aplicaciones necesarias para procesar los datos de archivo serán mantenidos para asegurar que los datos de archivo pueden ser accedidos por el período de tiempo establecido en esta CPS.

5.5.4 Procedimientos de Respaldo del Archivo

E-Sign respalda incrementalmente los archivos electrónicos de su información de certificados emitidos a diario y ejecuta respaldos completos semanalmente. Las copias de los registros en papel serán mantenidos en una instalación segura fuera del sitio.

5.5.5 Requisitos de Sellado de Tiempo de los Registros

Los certificados, CRLs, y otras entradas de bases de datos de revocación deberán contener información de fecha y hora. Tal información de tiempo no necesita estar basada criptográficamente.

5.5.6 Sistema de Recopilación de Archivo (Interna o Externa)

Los sistemas de recopilación de archivo de E-Sign son internos, a excepción de los clientes de RA empresariales. E-Sign asiste a las RA empresariales en la preservación de un registro de auditoría. Tal sistema de recopilación de archivo por lo tanto es externo a esa RA empresarial.

5.5.7 Procedimientos para Obtener y Verificar la Información del Archivo

Sólo el Personal de Confianza autorizado puede obtener acceso al archivo. La integridad de la información es verificada cuando ésta es restaurada.

5.6 Cambio de Llave

Los pares de llaves de CA de E-Sign son retiradas de servicio al final de sus respectivos tiempos de vida máximos como está definido en esta CPS. Los certificados de CA de E-Sign pueden ser renovados en tanto el tiempo de vida certificado acumulado del par de llaves de la CA no exceda el tiempo de vida máximo para un par de llaves de la CA. Los nuevos pares de llaves serán generados en la medida que sea necesario, por ejemplo para reemplazar un par de llaves de la CA que son retiradas, para complementar las existentes y para apoyar nuevos servicios.

Antes de la expiración del certificado de CA para una CA Superior, los procedimientos de cambio de llaves son puestos en práctica para facilitar una transición sin problemas para las entidades dentro de la jerarquía de la CA Superior del antiguo par de llaves de la CA Superior al nuevo par de llaves de la CA. El proceso de cambio de llaves de CA de E-Sign, requiere que:

- Una CA Superior deje de emitir nuevos Certificados de CA Subordinada a más tardar 60 días antes del punto en el tiempo ("Fecha de Detención de la Emisión"), donde la vida útil restante del par de llaves de la CA Superior es igual al Periodo de Validez del Certificado aprobada para el (los) tipo(s) específico(s) de Certificados emitidos por CAs Subordinadas en la jerarquía de la CA Superior.
- Después de la validación exitosa de solicitudes de Certificado de CA Subordinada (o de Suscriptor usuario final) recibidas después de la " Fecha de Detención de la Emisión ", los certificados serán firmados con un nuevo par de llaves de la CA.

La CA Superior continúa emitiendo CRL firmado con la llave privada original de la CA Superior hasta la fecha de vencimiento del último Certificado emitido usando el par de llaves original

5.7 Compromiso y Recuperación de Desastres

La infraestructura de CA de E-Sign es operada en la infraestructura segura de Symantec, por lo cual la gestión de Compromisos y de Recuperación de Desastres es implementada de manera conjunta por Symantec y E-Sign de acuerdo a los procedimientos establecidos en esta CPS.

5.7.1 Procedimientos de Manejo de Incidentes y Compromisos

Los respaldos de la siguiente información de la CA se mantendrán en el almacenamiento fuera de sitio y serán puestos a disposición en el evento de un Compromiso o desastre: datos de Solicitud de Certificado, datos de auditoría, y registros de base de datos para todos los Certificados emitidos. Deberán ser generados respaldos de las llaves privadas de la CA y deberán ser mantenidos en conformidad con el CP § 6.2.4. Symantec mantiene respaldos de la información de CA

mencionada previamente para sus propias CAs, así como para las CAs de los clientes empresariales dentro de su Sub-dominio.

5.7.2 Corrupción de Recursos de Computación, Software y/o Datos

En el caso de producirse algún daño de los recursos de computación, software y/o datos, tal ocurrencia es informada inmediatamente a E-Sign Security y son puestos en marcha los procedimientos de gestión de incidentes de E-Sign. Tales procedimientos requieren un escalamiento, investigación de incidentes y respuesta de incidentes apropiado. Si es necesario, también se pondrán en marcha los procedimientos de compromiso de llave o recuperación de desastres de E-Sign.

5.7.3 Procedimientos de Compromiso de Llave Privada de Entidad

Ante el Compromiso sospechado o conocido de una llave privada de CA de E-Sign, o de la infraestructura de la STN o de una CA de un Cliente, son puestos en marcha los procedimientos de Respuesta al Compromiso de Llaves de E-Sign por parte del Equipo de Respuesta a Incidentes de Seguridad (ESIRT,). Este equipo, que incluye personal de Seguridad, de Operaciones Comerciales Criptográficas, de Servicios de Producción, y otros representantes de la administración de Symantec, evalúa la situación, desarrolla un plan de acción, y pone en práctica el plan de acción con la aprobación de la administración ejecutiva de E-Sign.

Si es requerida la revocación de Certificados de CA, son realizados los siguientes procedimientos:

- El estado de revocación del Certificado es comunicado a las Partes que Confían a través del Repositorio de E-Sign, de acuerdo con CPS § 4.9.7,
- Se efectuarán esfuerzos comercialmente razonables para dar aviso adicional de la revocación a todos los Participantes afectados de la STN, y
- La CA generará un nuevo par de llaves, de acuerdo con CPS § 5.6, excepto cuando la CA está siendo terminada de acuerdo con CPS § 5.8.

5.7.4 Capacidades de Continuidad del Negocio después de un Desastre

Symantec ha creado y mantiene planes de continuidad de negocios de manera que en el evento de una interrupción del negocio, las funciones críticas del negocio puedan ser recuperadas. Symantec mantiene una Instalación de Recuperación de Desastres (DRF) localizada en una instalación propiedad de Symantec separada geográficamente de la Instalación de Producción primaria. El DRF es una instalación de seguridad diseñada bajo especificaciones del gobierno federal estadounidense y militares y también equipada específicamente para cumplir con los estándares de seguridad de Symantec.

En el caso de un desastre natural o provocado por el hombre que requiera el cese permanente de operaciones de la instalación primaria de Symantec, los equipos Corporate Symantec Business Continuity Team y Symantec Authentication Operations Incident Management Team se coordinarán con equipos de gestión funcional cruzada para tomar la decisión de declarar formalmente una situación de desastre y gestionar el incidente. Una vez que es declarada una situación de desastre será iniciada la restauración de la funcionalidad de los servicios de Producción de Symantec en el DRF.

Symantec ha desarrollado un Plan de Recuperación de Desastres (DRP) para sus servicios de PKI administrada. El DRP identifica condiciones para la activación del plan y lo que constituye un tiempo aceptable para la interrupción y recuperación del

sistema. El DRP define los procedimientos para que los equipos reconstituyan las operaciones de STN de Symantec usando datos de respaldo y las copias de respaldo de las llaves de la STN. Adicionalmente el DRP de Symantec incluye:

- La frecuencia para la toma de copias de seguridad de la información y el software esencial del negocio,
- Requisitos para almacenar los materiales criptográficos críticos (por ejemplo, materiales de dispositivo criptográfico seguro y de activación) en una ubicación alternativa,
- La distancia de separación entre el sitio de recuperación de desastres y el sitio principal de la CA,
- Procedimientos para asegurar la instalación de recuperación de Desastres durante el período de tiempo después de un desastre y previo a la restauración de un entorno seguro, ya sea en el sitio original o uno remoto,

El DRP de Symantec identifica requisitos administrativos que incluyen:

- Programa de mantenimiento para el plan;
- Requisitos de sensibilización y educación;
- Las responsabilidades de los individuos, y
- La prueba periódica de planes de contingencia.

El tiempo objetivo para recuperar la funcionalidad del servicio de Producción crítico es no mayor que 24 horas.

Symantec lleva a cabo a lo menos una prueba de recuperación de desastres por año calendario para asegurar los servicios en el DRF. También se llevan a cabo anualmente Ejercicios de Continuidad de Negocios formales en coordinación con el equipo Corporate Symantec Business Continuity Team donde son probados y evaluados procedimientos para tipos adicionales de escenarios (p.ej. pandemias, terremotos, inundaciones, apagones).

Symantec adopta pasos significativos para desarrollar, mantener y probar planes de recuperación de negocios confiables y los planes de Symantec para un desastre o interrupción significativa del negocio es consistente con muchas de los mejores prácticas establecidas en la industria.

Symantec mantiene hardware redundante y respaldos de software de sistema de su CA e infraestructura en su recinto de recuperación de desastres. Además, las llaves privadas de CA son respaldadas y mantenidas para fines de recuperación de desastre de acuerdo a CPS §6.2.4.

Symantec mantiene fuera del sitio respaldos de información de CA importante para las CAs de Symantec, así como las CAs de los Service Centers, incluyendo las CAs de E-Sign, y de Clientes Empresariales, en el Subdominio de E-Sign. Dicha información incluye, pero no está limitada a: datos de solicitud de Certificados, datos de auditoría (por la Sección 4.5), y registros de base de datos para todos los certificados emitidos.

Para servicios donde la entidad que emite Certificados es E-Sign (ver CPS §1.1.2.1.2), E-Sign ha implementado un sitio de recuperación de desastres a más de 2,5 kilómetros de las instalaciones seguras principales. E-Sign ha desarrollado e implementado un plan de recuperación de desastres para mitigar los efectos de cualquier tipo de desastre natural o provocado por el hombre. Este plan debe ser probado, verificado y actualizado regularmente para encontrarse operacional en el evento de un desastre.

El plan de recuperación de desastres detalla los equipos y acciones a realizar para abordar la restauración de los servicios de sistemas de información y funciones claves del negocio. El sitio de recuperación ante desastres de E-Sign tiene implementados las protecciones de seguridad física y controles operacionales requeridos por la guía Symantec Security and Audit Requirements Guide (SAR) para proporcionar una instalación operacional de respaldo segura y en buenas condiciones.

En el caso de un desastre natural o provocado por el hombre que requiere el cese temporal o definitivo de las operaciones de la instalación principal de E-Sign, el Equipo de Respuesta de Emergencia de E-Sign (EREE) inicia el proceso de recuperación de desastres.

E-Sign tiene la capacidad de restaurar o recuperar las operaciones esenciales dentro de los siete (7) días siguientes al desastre con, al menos, soporte para las siguientes funciones:

- emisión de Certificados,
- revocación de Certificados,
- publicación de información de revocación, y
- suministro de información de recuperación de llaves para los Clientes Empresariales que usen Managed PKI Key Manager.

El equipamiento de recuperación de desastres de E-Sign es protegido por protecciones de seguridad física comparable a los anillos de seguridad física especificados en CPS § 5.1.1.

El plan de recuperación de desastres de E-Sign ha sido diseñado para que las operaciones sean reanudadas en el sitio principal de E-Sign tan pronto como sea posible después de un desastre mayor.

E-Sign mantiene hardware redundante y respaldos de software de su sistema de Service Center e infraestructura en su recinto de recuperación de desastres.

El DRP identifica las condiciones para activar el plan y lo que constituye tiempos de interrupción y de recuperación del sistema aceptables. Además, el DRP de E-Sign incluye:

- La frecuencia para la toma de copias de seguridad de la información y el software esencial del negocio,
- Requisitos para almacenar los materiales criptográficos críticos (por ejemplo, materiales de dispositivo criptográfico seguro y de activación) en una ubicación alternativa,
- La distancia de separación entre el sitio de recuperación de desastres y el sitio principal de la CA,
- Procedimientos para asegurar la instalación de recuperación de Desastres durante el período de tiempo después de un desastre y previo a la restauración de un entorno seguro, ya sea en el sitio original o uno remoto,

El DRP de E-Sign identifica requisitos administrativos que incluyen:

- Programa de mantenimiento para el plan;
- requisitos de sensibilización y educación;
- Las responsabilidades de los individuos, y
- La prueba periódica de planes de contingencia.

5.8 Terminación de la CA o de la RA

En el caso de que sea necesario que una CA de E-Sign o la CA de un Cliente Empresarial deje de operar, E-Sign hace un esfuerzo comercialmente razonable para notificar a los Suscriptores, Partes que Confían, y otras entidades afectadas de dicha terminación antes de la terminación de CA. En caso de que la terminación de la CA sea requerida, E-Sign y, en el caso de una CA de cliente, el cliente aplicable, desarrollarán un plan de terminación para minimizar las interrupciones a los Clientes, Suscriptores, y Partes que Confían. Tales planes de terminación podrán abordar lo siguiente, según corresponda:

- Provisión de notificación a las partes afectadas por la terminación, con una anticipación mínima de 30 días, como suscriptores, Partes que Confían, y Clientes, informándoles de la situación de la CA,
- Manejo del costo de tal notificación,
- La revocación de los certificados emitidos a la CA por E-Sign,
- La conservación de los archivos de la CA y los registros por los períodos de tiempo que se requiere en esta CPS,
- La continuación de servicios a Suscriptores y de atención al cliente,
- La continuación de los servicios de revocación, tales como la emisión de CRL o el mantenimiento de los servicios de verificación en línea del estado,
- La revocación de certificados no vencidos sin revocar de suscriptores de usuario final y CA subordinadas, si es necesario,
- Reembolso (si es necesario) a los Suscriptores cuyos Certificados no vencidos y sin revocar certificados son revocados en el marco del plan de terminación o la provisión, o, alternativamente, la emisión de Certificados de reemplazo por un sucesor de la CA,
- Disposición de la llave privada de la CA y de los tokens de hardware que contienen tal llave privada, y
- Las provisiones necesarias para la transición de los servicios de la CA a una CA sucesora.
- La entidad habilitada para aprobar el cierre término de la CA será el Directorio de E-SIGN.

5.9 Seguridad de Datos

5.9.1 Objetivos

E-Sign desarrolla, implementa y mantiene un programa de seguridad integral diseñado para:

1. Proteger la confidencialidad, integridad y disponibilidad (CIA) de los Datos de Certificados y Procesos de Gestión de Certificados;
2. Proteger contra las amenazas o peligro anticipado a la confidencialidad, integridad y disponibilidad de los Datos de Certificados y Procesos de Gestión de Certificados;
3. Proteger contra el acceso, uso, divulgación, alteración o destrucción no autorizado o ilegal de los Datos de Certificados o Procesos de Gestión de Certificados;
4. Proteger contra la pérdida o la destrucción accidental o deterioro de cualquier Dato de Certificado o Proceso de Gestión de Certificados, y
5. Cumplir con todos los demás requisitos de seguridad aplicables a la CA por ley.

5.9.2 Evaluación de Riesgos

E-Sign realiza una evaluación anual de riesgos que:

1. Identifica amenazas previsible internas y externas que podrían resultar en acceso no autorizado, revelación, mal uso, alteración o destrucción de cualquier Dato de Certificado o Procesos de Gestión de Certificados;
2. Evalúa la probabilidad y el daño potencial de estas amenazas, teniendo en cuenta la sensibilidad de los Datos de Certificado y Procesos de Gestión de Certificados, y
3. Evalúa la suficiencia de las políticas, procedimientos, sistemas de información, tecnología, y otros arreglos que la CA tiene en marcha para hacer frente a tales amenazas.

5.9.3 Plan de Seguridad

Basándose en los resultados de la Evaluación de Riesgos anual, E-Sign desarrolla, implementa y mantiene un Plan de Seguridad que consiste en procedimientos de seguridad, medidas y productos diseñados para alcanzar los objetivos antes mencionados, y para administrar y controlar los riesgos identificados durante la Evaluación de Riesgos , en proporción a la sensibilidad de los Datos de Certificado y Procesos de Gestión de Certificados.

El Plan de Seguridad incluye salvaguardas administrativas, organizacionales, técnicas y físicas adecuadas a la sensibilidad de los Datos de Certificado y Procesos de Gestión de Certificados. El Plan de Seguridad toma en cuenta la tecnología disponible y el costo de la implementación de las medidas específicas, e implementa un nivel razonable de seguridad adecuado para el daño que pudiera resultar de una brecha de seguridad y la naturaleza de los datos que deben ser protegidos.

6 Controles de Seguridad Técnicos

6.1 Generación e Instalación del Par de Llaves

La infraestructura de CA de E-Sign es operada en la infraestructura segura de Symantec, por lo cual la gestión de las llaves de CA de E-Sign es llevada a cabo por Symantec de acuerdo a los procedimientos establecidos en esta CPS.

6.1.1 Generación de Par de Llaves

La generación de par de llaves de una CA es desarrollada por varios individuos preseleccionados, capacitados, y confiables que utilizan Sistemas de Confianza y procesos que entregan la seguridad y fuerza criptográfica requerida para las llaves generadas. Para la CA Primarias y las CA de Raíz Emisoras, los módulos criptográficos usados para la generación de las llaves cumplen los requerimientos del FIPS 140-1 nivel 3. Para otras CA (incluyendo las CA de E-Sign y las CA de Clientes de Managed PKI), los módulos criptográficos usados cumplen requerimientos de FIPS 140-1 nivel 2.

Todos los pares de llaves de la CA son generados en Ceremonias de Generación de Llave planificadas con antelación de acuerdo a los requerimientos de la Guía de Referencia de Ceremonia de Llaves, la Guía CA Key Management Tool User's Guide, y la Guía de SAR de Symantec. Las actividades ejecutadas en cada ceremonia de generación de llave son registradas, fechadas y firmadas por todos los individuos involucrados. Estos registros se guardan para fines de auditoría y seguimiento durante un plazo estimado apropiado por la administración de E-Sign.

La generación del par de llaves de una RA es realizada generalmente por la RA utilizando un módulo criptográfico certificado según estándares FIPS 140-1 nivel 1 provisto por su software de navegación Web.

Los Clientes Empresariales generan el par de llaves utilizado por sus servidores de Automated Administration. E-Sign recomienda que la generación del par de llaves del servidor de Automated Administration sea realizada utilizando un módulo criptográfico certificado FIPS 140-1 nivel 2.

La generación de pares de llaves de un Suscriptor Usuario Final es llevada a cabo generalmente por el Suscriptor. Para certificados Class 1, certificados Class 2 y certificados Class 3 de firma de código/objeto, el Suscriptor usa típicamente un módulo criptográfico certificado FIPS 140-1 nivel 1 provisto con el software navegación Web para la generación de la llave. Para Certificados de servidor, el suscriptor típicamente usa la utilidad de generación de llave entregada con el software de servidor Web. Para Certificados de Firma Electrónica Avanzada, el Suscriptor debe usar un módulo de hardware certificado FIPS 140-1 nivel 2 o Common Criteria EAL 3.

Para Certificados ACS Application ID, E-Sign genera un par de claves en nombre del suscriptor con una semilla de números aleatorios generados en un módulo criptográfico que, como mínimo, cumpla con los requisitos de FIPS 140-1 nivel 3.

6.1.2 Entrega de la Llave Privada al Suscriptor

Cuando los pares de llaves de un Suscriptor usuario final son generados por el Suscriptor usuario final, la entrega de la llave privada a un Suscriptor no es aplicable. Para los Certificados ACS Application ID, la entrega la llave privada a un Suscriptor tampoco es aplicable.

En caso de que los pares de llaves de la RA o del Suscriptor usuario final sean pre-generados por E-Sign en tokens de hardware o tarjetas inteligentes, tales dispositivos son distribuidos a la RA o al Suscriptor usuario final utilizando un servicio de despacho comercial y un embalaje que evidencie la intrusión. Los datos necesarios para activar el dispositivo son comunicados a la RA o al Suscriptor usuario final mediante un proceso fuera de banda. La distribución de los tales dispositivos es registrada por E-Sign.

Cuando los pares de llaves del Suscriptor usuario final son pre-generados por Clientes Empresariales en tokens de hardware o tarjetas inteligentes, tales dispositivos son distribuidos a los Suscriptores del usuarios finales utilizando un servicio de despacho comercial y un embalaje que evidencie la intrusión. Los datos necesarios para activar el dispositivo son comunicados a la RA o al Suscriptor usuario final mediante un proceso fuera de banda. La distribución de los tales dispositivos es registrada por el Cliente Empresarial.

Para los Clientes Empresariales que usan Managed PKI Key Manager para los servicios de recuperación de claves, el Cliente puede generar los pares de llaves de cifrado (en nombre de los Suscriptores cuyas Solicitudes de Certificados aprueba) y transmitir tales pares de llaves a los Suscriptores a través de un archivo PKCS #12 protegido por contraseña.

6.1.3 Entrega de Llave Pública al Emisor del Certificado

Los Suscriptores usuarios finales y las RA envían electrónicamente su llave pública a E-Sign para la certificación mediante el uso de una Solicitud de Firma de Certificado PKCS#10 (CSR) u otro paquete firmado digitalmente en una sesión protegida por

Secure Sockets Layer (SSL). En caso de que los pares de llaves de la CA, de la RA o del Suscriptor usuario final sean generados por Symantec, este requisito no es aplicable.

6.1.4 Entrega de la Llave Pública de la CA a las Partes que Confían

E-Sign forma parte de la STN de Symantec por lo que las CA de E-Sign dependen jerárquicamente de la CA Primaria de Symantec, lo que implica que, en la práctica, la llave pública de la raíz de la jerarquía de E-Sign corresponde a la llave pública de la CA Primaria de Symantec.

E-Sign pone los Certificados de CA para su CAs Primarias y CAs raíces a disposición de los Suscriptores y Partes que Confían a través de su inclusión en el software de navegación Web. En la medida en que son generados nuevos Certificados de CA Primaria y de CA raíz, Symantec entrega estos nuevos certificados a los fabricantes de navegadores Web para su inclusión en las versiones nuevas y en actualizaciones del navegador Web.

E-Sign generalmente entrega la cadena total de certificado (incluyendo su CA emisora y todas las CA en la cadena) al Suscriptor usuario final en el acto de la emisión del Certificado. Los Certificados de las CA de E-Sign también puede ser descargados del Directorio LDAP en: directory.verisign.com.

6.1.5 Tamaños de Llaves

Los pares de llaves deberán tener una longitud suficiente para evitar que otros calculen la llave privada del par de llaves utilizando criptoanálisis durante el período de utilización esperado de dichos pares de llaves. La norma E-Sign para el tamaño mínimo de las llaves es el uso de pares de llaves equivalentes en fuerza a 2048 bits RSA para CA Primarias y CAs¹⁴.

La tercera y quinta generación de CA Primarias de Symantec (G3 y G5) tienen pares de llaves RSA de 2048 bits.

Symantec emite certificados para RA y entidades finales con pares de llaves de un tamaño mínimo equivalente en fuerza a RSA de 2048 bits.

La cuarta generación (G4) de Class 3 PCA de Symantec (CA de Raíz Universal ECC) incluye una llave ECC de 384 bits.

Todas las Clases de certificados de CA Primarias, de CAs, de RAs y de entidad final de E-Sign y de la STN utilizan ya sea SHA-1 o SHA-2 para el algoritmo de hash de la firma digital y algunas versiones de Processing Center de Symantec soportan el uso de algoritmos de hash SHA-256 y SHA-384 en Certificados de Suscriptor entidad final.

6.1.5.1 Requisitos CABF para los Tamaños de Llave

¹⁴ La confianza de la CA está extendida para las Raíces de Confianza desfasadas de primera y segunda generación (G1 y G2) de Symantec con pares de llaves RSA de 1024 bits para soporte de plataformas desfasadas de cliente y pueden ser emitidos certificados de usuario final de 1024 bits RSA con expiración en o antes del 31 de Diciembre de 2011. Para preservar la continuidad de negocios de aplicaciones desfasadas más allá del 2011, serán permitidas excepciones individuales adicionales con aprobación previa para afiliados de Symantec Corporation que operen las capacidades de software de Processing.Center de acuerdo con la sección 6.3.2.

Los certificados SSL con Dominio validado y Organización validada adhieren a los requisitos de CA / Browser Forum Baseline.

Los Certificados de CA Raíz debe cumplir con el siguientes requisitos para el tipo de algoritmo y el tamaño de la llave:

	Periodo de validez que comiencen al 31 de diciembre 2010 o antes	Periodo de validez comenzados después del 31 de diciembre 2010
Algoritmo de Digest	MD5 no Recomendado SHA-1, SHA-256, SHA-384 o SHA-512	SHA-1 *, SHA-256, SHA-384 o SHA-512
Mínimo tamaño del módulo RSA (bits)	2048 **	2048
Curva ECC	NIST P-256, P-384 o P-521	NIST P-256, P-384 o P-521

Tabla 4A - Algoritmos y tamaños de llave CA/Browser Forum para Certificados de CA Raíz

Los Certificados de CAs subordinadas deben cumplir con los siguientes requisitos para el tipo de algoritmo y el tamaño de la llave:

	Periodo de validez que comiencen al 31 de diciembre 2010 o antes y que terminen al 31 de diciembre 2013 o antes	Periodo de validez que comiencen después del 31 de diciembre 2010 o que terminen después de 31 de diciembre 2013
Algoritmo de Digest	SHA-1, SHA-256, SHA-384 o SHA-512	SHA-1 *, SHA-256, SHA-384 o SHA-512
Mínimo tamaño del módulo RSA (bits)	1024	2048
Curva ECC	NIST P-256, P-384 o P-521	NIST P-256, P-384 o P-521

Tabla 4B – Algoritmos y tamaños de llave CA/Browser Forum para Certificados de CA Subordinada

La CA sólo deberá emitir certificados de Suscriptor con llaves que contengan los siguientes tipos de algoritmo y tamaños de clave.

	Periodo de validez termina al 31 de diciembre 2013 o antes	Periodo de validez que termina después del 31 de diciembre 2013
Algoritmo de Digest	SHA-1 *, SHA-256, SHA-384 o SHA-512	SHA-1 *, SHA-256, SHA-384 o SHA-512
Mínimo tamaño del módulo RSA (bits)	1024	2048
Curva ECC	NIST P-256, P-384 o P-521	NIST P-256, P-384 o P-521

Tabla 4C - Algoritmos y tamaños de llave CA/Browser Forum para Certificados de Suscriptor

* SHA-1 podrá ser utilizado hasta que SHA-256 sea ampliamente soportado por los navegadores utilizados por un parte sustancial de partes que confían en todo el mundo.

** Un Certificado de CA Raíz emitido antes del 31 Diciembre 2010 con un tamaño de llave RSA menor a 2048 bits aún puede servir como un ancla de confianza para Certificados de Suscriptor emitidos en acuerdo con estos Requisitos.

La CA de E-Sign deberá rechazar una solicitud de certificado, si la Llave Pública solicitada no cumple con los tamaños de llave de algoritmos mínimos establecidos en esta sección.

6.1.6 Generación y Control de Calidad de Parámetros de Llave Pública

No es aplicable

6.1.7 Propósitos de Uso de la Llave (por campo Key Usage de X.509 v3)

Consulte la Sección 7.1.2.1.

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

La infraestructura de CA de E-Sign es operada en la infraestructura segura de Symantec, por lo cual la gestión de las llaves de CA de E-Sign es llevada a cabo por Symantec de acuerdo a los procedimientos establecidos en esta CPS.

Symantec ha implementado una combinación de controles físicos, lógicos y de procedimiento para garantizar la seguridad de las llaves privadas de las CA de E-Sign y de Clientes Empresariales. Se requiere por contrato que los Suscriptores tomen las precauciones necesarias para evitar la pérdida, divulgación, modificación o el uso no autorizado de las llaves privadas.

6.2.1 Normas y Controles para el Módulo Criptográfico

Para la generación de par de llaves de CA Primaria y CA de Raíz Emisora y el almacenamiento de llaves privadas de CA, Symantec utiliza módulos de hardware criptográfico que están certificados o cumplen los requisitos de FIPS 140-1 Nivel 3.

6.2.2 Control Multi-Personal (m de un total de n) de la Llave Privada

Symantec ha implementado mecanismos técnicos y de procedimiento que requieren la participación de varios individuos de confianza para realizar operaciones criptográficas sensibles en la CA. Symantec utiliza Partición de Secreto para disgregar los datos de activación necesarios para hacer uso de una llave privada de la CA en distintas partes llamadas "Partes Secretas" que están en manos de personas capacitadas y de confianza llamadas "Tenedores de Partes". Un número mínimo de Partes Secretas (m) de un total de Partes Secretas, creado y distribuido para un módulo criptográfico de hardware especial (n) es necesario para activar una llave privada de la CA almacenada en el módulo.

El número mínimo de partes necesarias para firmar un certificado de la CA es de tres (3). Debe tenerse en cuenta que el número de partes distribuidas para tokens de recuperación de desastres puede ser menor que el número distribuidos para tokens operativos, mientras que el número mínimo de partes necesarias sigue siendo el mismo. Las Partes Secretas están protegidas de conformidad con esta CPS.

6.2.3 Custodia de la Llave Privada

Las llaves privadas de CA no son puestas en custodia. La custodia de las llaves privadas para Suscriptores usuarios finales se explica en más detalle en la Sección 4.12.

6.2.4 Respaldo de la Llave Privada

Symantec crea copias de respaldo de las llaves privadas de la CA para propósitos de recuperación de rutina y de recuperación de desastres. Tales llaves son almacenadas en forma encriptada dentro de módulos de hardware criptográfico y dispositivos de almacenamiento de llaves asociados. Los módulos criptográficos utilizados para almacenamiento de claves privadas de la CA cumplen con los requisitos de la esta CPS. Las llaves privadas de la CA son copiadas a los módulos de hardware criptográfico de respaldo de conformidad con la esta CPS.

Los módulos que contienen copias de respaldo en las instalaciones de las llaves privadas de la CA están sujetos a los requisitos de CPS. Los módulos que contienen copias de recuperación de desastres de las llaves privadas de la CA están sujetos a los requisitos de la esta CPS.

Symantec no almacena copias de las llaves privadas de RA. Para el respaldo de llaves privadas del Suscriptor usuario final, véase la Sección 6.2.3 y la Sección 4.12. Para certificados ACS Application, E-Sign no almacena copias de las llaves privadas de suscriptores.

6.2.5 Archivo de Llave Privada

Cuando un Certificado de CA de E-Sign expira, el par de llaves asociado con el certificado será conservado en forma segura durante un período de al menos 5 años, utilizando módulos de hardware criptográfico que cumpla con los requisitos de esta CPS. Estos pares de llaves de CA no serán utilizados para evento de firma alguno después de la fecha de vencimiento del correspondiente certificado de CA, a menos que el certificado de CA haya sido renovado en términos de esta CPS.

E-Sign no archiva copias de las llaves privadas de la RA y de Suscriptores.

6.2.6 Transferencia de la Llave Privada Hacia o Desde un Módulo Criptográfico

Symantec genera pares de llaves de CA en los módulos de hardware criptográfico en los que serán utilizadas las llaves. Además, Symantec hace copias de dichos pares de llaves de CA para propósitos de recuperación de rutina y de recuperación ante desastres. En el caso de que los pares de llaves de CA sean respaldados a otro módulo de hardware criptográfico, tales pares de llaves son transportados entre los módulos en forma cifrada.

6.2.7 Almacenamiento de la Llave Privada en el Módulo Criptográfico

Las llaves privadas de la CA o RA mantenidas en módulos de hardware criptográfico son almacenadas en forma encriptada.

6.2.8 Método de Activación de la Clave Privada

Todos los Participantes del subdominio de E-Sign deben proteger los datos de activación de sus llaves privadas contra pérdida, robo, cambios, entrega o uso no autorizado.

6.2.8.1 Certificados Class 1

El estándar para la protección de la llave privada de certificados Class 1 es que los Suscriptores adopten las medidas comerciales razonables para la protección física de la estación de trabajo del suscriptor, para prevenir el uso de la estación de trabajo y su llave privada asociada sin la autorización del suscriptor. Además, E-Sign recomienda que los suscriptores usen una contraseña de conformidad con la Sección 6.4.1 o seguridad de fuerza equivalente para autenticar al suscriptor antes de la activación de la llave privada, lo que incluye, por ejemplo, una contraseña para operar la llave privada, una contraseña de inicio de sesión de Windows o de protector de pantalla o una contraseña de inicio de sesión en red.

6.2.8.2 Certificados Class 2

El estándar para la protección de la llave privada de certificados Class 2 es que los Suscriptores:

- Utilicen una contraseña de conformidad con la Sección 6.4.1 o seguridad de fuerza equivalente para autenticar al suscriptor antes de la activación de la llave privada, lo que incluye, por ejemplo, una contraseña para operar la llave privada, o una contraseña de inicio de sesión de Windows o de protector de pantalla y
- Adoptar las medidas comercialmente razonables para la protección física de la estación de trabajo del Suscriptor para prevenir el uso de la estación de trabajo y su llave privada asociada sin la autorización del Suscriptor.

Cuando están desactivadas, las llaves privadas serán mantenidas en forma encriptada solamente.

6.2.8.3 Certificados Class 3 distintos de Certificados de Administrador

El estándar para la protección de la llave privada de certificados Class 3 (que no sean de Administradores) es que los Suscriptores:

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

Se recomienda el uso de una contraseña junto con una tarjeta inteligente o un dispositivo de acceso biométrico, de conformidad con la Sección 6.4.1. Cuando estén desactivadas, las llaves privadas serán mantenidas en forma encriptada solamente.

6.2.8.4 Llaves Privadas de Administradores (Class 3)

El Estándar de protección de llave privada de Administradores requiere que éstos:

- Utilicen una tarjeta inteligente, un dispositivo de acceso biométrico, una contraseña de conformidad con la Sección 6.4.1, o seguridad de fuerza equivalente para autenticar al Administrador antes de la activación de la llave privada, lo que incluye, por ejemplo, una contraseña para operar la llave privada, una contraseña de inicio de sesión de Windows o una contraseña de protector de pantalla, y

- Adopten las medidas comercialmente razonables para la protección física de la estación de trabajo del Administrador para prevenir el uso de la estación de trabajo y su clave privada asociada sin la autorización del Administrador.

E-Sign recomienda que los Administradores utilicen una tarjeta inteligente, un dispositivo de acceso biométrico, o seguridad de fuerza equivalente, junto con el uso de una contraseña de conformidad con la Sección 6.4.1 para autenticar al Administrador antes de la activación de la llave privada.

Cuando están desactivadas, las llaves privadas serán mantenidas en forma encriptada solamente.

6.2.8.5 RA Empresariales que utilizan un Módulo Criptográfico (con Automated Administration o con Managed PKI Key Manager Service)

El Estándar de protección de clave privada para los Administradores mediante tal módulo criptográfico requiere que éstos:

- Utilicen el módulo criptográfico, junto con una contraseña de conformidad con la Sección 6.4.1 para autenticar al administrador antes de la activación de la clave privada, y
- Adopten las medidas comercialmente razonables para la protección física de la estación de trabajo que hospeda al lector del módulo criptográfico para evitar el uso de la estación de trabajo y de la clave privada asociada con el módulo criptográfico sin la autorización del Administrador.

6.2.8.6 Llaves Privadas Mantenidoas por los Centros de Procesamiento (Class 1-3)

La llave privada de una CA en línea deberá ser activada por un número mínimo de Tenedores de Partes, tal como se define en la Sección 6.2.2, quienes entregan sus datos de activación (almacenados en los medios seguros). Una vez que la llave privada sea activada, la llave privada puede estar activa por un período indefinido hasta que sea desactivada cuando la CA queda fuera de línea. Del mismo modo, un número mínimo de Tenedores de Partes serán requeridos para entregar sus datos de activación para activar la llave privada una CA fuera de línea. Una vez que la llave privada es activada, estará activa sólo por una vez.

6.2.9 Método de Desactivación de la Llave Privada

Las llaves privadas de las CA de E-Sign son desactivadas después de retirarlas del lector de tokens. Las llaves privadas de la RA de E-Sign (utilizadas para la autenticación de la aplicación de la RA) son desactivadas al terminarse la sesión en el sistema. Las RA de E-Sign están obligadas a cerrar la sesión en sus estaciones de trabajo al salir de su área de trabajo.

Las llaves privadas de Administradores de Cliente, RA, y de Suscriptor usuario final pueden ser desactivadas después de cada operación, al cerrar su sesión en el sistema, o al retirar la tarjeta inteligente del lector de tarjetas inteligentes dependiendo del mecanismo de autenticación utilizado por el usuario. En todos los casos, los suscriptores usuarios finales tienen una obligación de proteger adecuadamente sus llaves privadas de acuerdo con esta CPS. La llave privada asociada con un certificado ACS Application es eliminada inmediatamente después de que ha sido utilizada para la firma de código.

6.2.10 Método de Destrucción de la Llave Privada

Cuando sea necesario, Symantec destruye claves privadas de la CA de una manera que asegura razonablemente que no permanecen restos residuales de la llave que podrían conducir a la reconstrucción de la llave. Symantec utiliza la función de sus módulos de hardware criptográfico para dejar en cero y otros medios apropiados para garantizar la completa destrucción de las llaves privadas de la CA. Si se realiza, las actividades de destrucción de la llave de CA son registradas en el sistema. La llave privada asociada con un certificado de ACS Application es eliminada inmediatamente después de que ha sido utilizado para la firma de código.

6.2.11 Clasificación de Módulo Criptográfico

Consulte la Sección 6.2.1

6.3 Otros Aspectos de la Gestión de Par de Llaves

6.3.1 Archivo de Llaves Públicas

Los Certificados de las CA y de las RA de E-Sign y de Suscriptor usuario final son respaldados y archivados como parte de los procedimientos de respaldo de rutina de Symantec.

6.3.2 Períodos Operacionales del Certificado y Períodos de Uso del Par de Llaves

El Periodo Operacional de un certificado finaliza en el momento de su expiración o revocación. El Periodo Operacional para las llaves privadas es el mismo que el Periodo Operacional para los Certificados asociados, excepto que ellos pueden continuar siendo usados para descifrado y verificación de firma. Los máximos Periodos Operacionales para Certificados de E-Sign para Certificados emitidos en o después de la fecha efectiva de esta CPS son establecidos en la Tabla 8 a continuación. Los Certificados de Suscriptores usuarios finales que son renovaciones de certificados de suscriptor existentes pueden tener un periodo de validez más prolongado (hasta 3 meses).

Adicionalmente, las CAs de E-Sign dejan de emitir nuevos Certificados en una fecha apropiada previa a la expiración del Certificado de la CA de tal manera que ningún certificado emitido por una CA Subordinada expire después de la expiración de cualquier Certificado de CA Superior.

Certificado Emitido Por:	Periodo de Validez
CA Primaria auto-firmada (1024 bits RSA)	Hasta 30 años
CA Primaria auto-firmada (2048 bits RSA)	Hasta 50 años
CA Primaria auto-firmada (256 bit ECC)	Hasta 30 años
CA Primaria auto-firmada (384 bits ECC)	Hasta 30 años
CA Primaria para CA intermedia fuera de línea	Generalmente 10 años, pero hasta 15 años después de renovación
CA Primaria para CA en línea	Generalmente 5 años, pero hasta 10 años después de renovación ¹⁵
CA intermedia fuera de línea para CA en línea	Generalmente 5 años, pero hasta 10 años después de renovación ¹⁶

¹⁵ Los certificados OnSite Administrator de CA-Class 3, Class 3 Secure Server Operational Administrator CA y Class 3 OnSite Enterprise Administrator CA – G2 de VeriSign® tienen una validez de más de 10 años para soportar los sistemas desfasados y serán revocados en su caso.

CA en Línea para Suscriptor usuario final individual	Normalmente hasta 3 años, pero en las condiciones descritas abajo, hasta 6 años ¹⁷ sin opción de renovar o reasignar la llave. Después de 6 años se requiere un nuevo enrolamiento
CA en Línea para Suscriptor Entidad-Final Organizacional	Normalmente hasta 6 años ¹⁸¹⁹ en las condiciones descritas abajo sin opción de renovar o reasignar la llave. Después de 6 años se requiere un nuevo enrolamiento

Tabla 8 - Períodos Operacionales de Certificado

En términos de la Sección 6.3.2 de la CP STN, el PMA de Symantec ha aprobado una excepción para extender un número limitado de CAs más allá de los límites especificados, para asegurar servicios PKI ininterrumpidos durante una migración de los pares de llaves de la CA. Esta excepción puede ser aplicada a E-Sign cuando opera las capacidades de software de Processing Center solamente para infraestructura y CAs de Administradores que no estén asociadas a CAs que emitan certificados SSL. Esta excepción no puede ser utilizada para extender la validez de una CA más allá de una validez total de 14 años hasta un máximo en el 31 de Agosto de 2014, y no puede estar disponible después del 31 de Diciembre de 2011.

Excepto por lo que se menciona en esta sección, los participantes del subdominio E-Sign cesarán todo uso de sus pares de llaves después de que sus periodos de uso han expirado.

Los certificados emitidos por las CAs a Suscriptores usuarios finales pueden tener periodos operacionales de más de tres años, hasta seis años, si los siguientes requerimientos son satisfechos:

- Protección de los pares de llaves de Suscriptor en relación con su ambiente operacional para Certificados Organizacionales, operación dentro de la protección mejorada de un centro de datos y para Certificados Individuales, los pares de llaves de los suscriptores residen en un dispositivo de hardware, como tarjeta inteligente
- Se les exige a los suscriptores que deben cumplir con los procesos de re-autenticación por lo menos cada 3 años meses bajo la Sección 3.2.3,
- Si un suscriptor no puede completar exitosamente los procesos de re-autenticación o no puede probar la posesión de tal llave privada al ser requerida por lo anterior, la CA revocará el Certificado del Suscriptor.

E-Sign también opera una CA Servidor Seguro como una CA raíz emisora auto firmada desfasada que es parte de la red Symantec Trust Network y tiene un periodo operacional de 15 años. Los certificados de Suscriptor usuario final emitidos por esta CA cumplen los requerimientos para CA de certificados de Suscriptor usuario final especificados en la Tabla 8 anterior.

La CA “Symantec® Class 3 International Server CA”, “Thawte SGC CA” es una CA en línea firmadas por una PCA. La validez de esa CA puede exceder los períodos de

¹⁶ Si son emitidos certificados de Suscriptor usuario final de 6 años, el período operacional del certificado de CA en línea será de 10 años sin opción de renovar. La reasignación de llave será requerida después de 5 años.

¹⁷ Si son emitidos certificados de Suscriptor usuario final de 6 años, el período operacional del certificado de CA en línea será de 10 años sin opción de renovar. La reasignación de llave será requerida después de 5 años.

¹⁸

¹⁹ Como mínimo, el Nombre Distinguido de los certificados emitidos con una validez de más de 3 años es re-verificado después de tres años a partir de fecha de emisión. Con la excepción del certificado de Administración Automatizada de VeriSign®, los certificados Organizacionales de entidad final utilizados únicamente para apoyar el funcionamiento de una parte de la red STN podrán ser emitidos con un período de validez de 5 años y hasta un máximo de 10 años después de la renovación.

validez descritos en la Tabla 8 anterior para cumplir con ciertas obligaciones contractuales con los fabricantes de navegadores que consideran el uso de la tecnología SGC/step up, y asegurar interoperabilidad continua de certificados que ofrecen estas capacidades.

6.3.2.1 Requisitos CABF del Período de Validez

Los certificados SSL con Dominio validado y Organización validada adhieren a los requisitos de CA / Browser Forum Baseline. Dichos Certificados emitidos después de la Fecha Efectiva deben tener un Período de Validez no superior a 48 meses (4 años).

Excepto por lo dispuesto a continuación, los Certificados emitidos después del 1 de Abril 2015 deben tener un Período de Validez no superior a 36 meses (3 años). Después del 1 de Abril de 2015, las CAs podrán seguir emitiendo certificados con un Período de Validez superior a 36 meses pero no superior a 48 meses, siempre que la CA documente que el certificado es para un sistema o software que:

- a) estaba en uso antes de la Fecha Efectiva;
- b) se encuentra actualmente en uso ya sea por el Solicitante o un número sustancial de Partes que Confían;
- c) deja de operar si el periodo de validez es menor a 48 meses;
- d) no contiene riesgos de seguridad conocidos para las Partes que Confían, y
- e) es difícil de arreglar o reemplazar sin un desembolso económico importante.

6.4 Datos de Activación

La infraestructura de CA de E-Sign es operada en la infraestructura segura de Symantec, por lo cual la gestión de los Datos de Activación de las llaves de CA de E-Sign es llevada a cabo por Symantec de acuerdo a los procedimientos establecidos en esta CPS.

6.4.1 Generación e Instalación de los Datos de Activación

Los datos de activación (Partes Secretas) usadas para proteger tokens que contengan las llaves privadas de las CA de Symantec y de E-Sign son generados de acuerdo a los requerimientos de CPS § 6.2.2 y la Guía de Referencia de Ceremonia de Generación de Llave. La creación y distribución de Partes Secretas queda registrada.

Las RA de Symantec y de E-Sign deben elegir contraseñas fuertes para proteger sus llaves privadas. Las guías de selección de contraseñas de Symantec requieren que las contraseñas:

- Sean generadas por el usuario;
- Tengan al menos 8 caracteres;
- Tengan al menos un carácter alfabético y uno numérico
- Tengan al menos una letra minúscula,
- No contengan demasiadas ocurrencias del mismo carácter,
- No sean igual al nombre del perfil del operador, y
- No contengan una porción larga del nombre de perfil del usuario

E-Sign recomienda encarecidamente que los Administradores Empresariales, las RA, y los Suscriptores usuarios finales elijan contraseñas que cumplan los mismos requerimientos. E-Sign también recomienda el uso de mecanismos de autenticación de dos factores (ej., token y frase clave, biométrico y token, o biométrico y frase clave) para la activación de llave privada.

6.4.2 Protección de Datos de Activación

Los tenedores de partes de Symantec deben salvaguardar sus Partes Secretas y firmar un acuerdo reconociendo sus responsabilidades como Tenedor de Partes.

Las RA de E-Sign deben guardar sus llaves privadas de Administrador y de RA en forma encriptada usando protección de contraseña y la opción de “alta seguridad” de su navegador.

E-Sign recomienda encarecidamente que los Administradores de Cliente, las RA y Suscriptores usuarios finales almacenen sus llaves privadas en forma encriptada y protejan sus llaves privadas mediante el uso de un dispositivo de hardware y/o frase clave fuerte. Se recomienda el uso de mecanismos de autenticación de dos factores (p.ej., token y frase clave, biométrico y token, o biométrico y frase clave).

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 para las llaves privadas son transmitidos, los Participantes del subdominio E-Sign deberán proteger la transmisión utilizando métodos que protejan contra pérdida, robo, modificación, divulgación no autorizada o uso no autorizado de tales llaves privadas. En la medida en que es utilizada la combinación nombre de usuario y contraseña de Windows o de inicio de sesión de red como datos de activación para un Suscriptor usuario final, las contraseñas transferidas a través de una red deberán estar protegidas contra el acceso de usuarios no autorizados.

6.4.3.2 Destrucción de Datos de Activación

Los datos de activación para las llaves privadas de la CA serán retirados de 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. Después de que el período de retención de registros en la Sección 5.5.2 expira, Symantec retirará de servicio los datos de activación mediante la sobreescritura y/o la destrucción física.

6.5 Controles de Seguridad Computacional

E-Sign realiza todas las funciones de CA y RA usando Sistemas de Confianza que cumplen con los requisitos de la Guía SAR de Symantec. Los Clientes Empresariales deben utilizar Sistemas de Confianza.

6.5.1 Requerimientos Técnicos Específicos de Seguridad Computacional

E-Sign asegura que los sistemas que mantienen software de la CA y los archivos de datos son Sistemas de Confianza seguros ante el acceso no autorizado. Además, E-Sign limita el acceso a los servidores de producción a aquellos individuos con un motivo de negocio válido para tal acceso. Los usuarios de aplicación general no tienen cuentas en los servidores de producción.

La red de producción de E-Sign está separada lógicamente de otros componentes. Esta separación previene el acceso a la red excepto a través de procesos de aplicaciones definidas. E-Sign utiliza cortafuegos para proteger la red de producción

contra intromisiones internas y externas y limita la naturaleza y fuente de actividades de red que pueden acceder a sistemas de producción.

E-Sign requiere el uso de contraseñas que tienen una longitud de caracteres mínimo y una combinación de caracteres alfanuméricos y especiales. E-Sign requiere que las contraseñas sean cambiadas de manera periódica.

El acceso directo a las bases de datos de E-Sign que soportan las Operaciones de CA de E-Sign está limitado a Personas de Confianza en el grupo de Operaciones de Producción de E-Sign que tienen una razón comercial válida para tal acceso.

La red de producción de E-Sign está separada lógicamente de otros componentes. Esta separación previene el acceso a la red excepto a través de procesos de aplicaciones definidas. E-Sign utiliza cortafuegos para proteger la red de producción contra intromisiones internas y externas y limita la naturaleza y fuente de actividades de red que pueden acceder a sistemas de producción.

E-Sign requiere el uso de contraseñas que tienen una longitud de caracteres mínimo y una combinación de caracteres alfanuméricos y especiales. E-Sign requiere que las contraseñas sean cambiadas de manera periódica.

El acceso directo a las bases de datos de E-Sign utilizadas por Operaciones del Service Center de E-Sign está limitado a Personas de Confianza en el grupo de Operaciones de Producción de Service Center de E-Sign, que tienen una razón comercial válida para tal acceso.

6.5.1.1 Requisitos CABF para Seguridad del Sistema

Los certificados SSL con Dominio validado y Organización validada adhieren a los requisitos de CA/Browser Forum Baseline. Para tales Certificados, el Proceso de Gestión del Certificado debe incluir:

- seguridad física y los controles ambientales;
- controles de integridad del sistema, incluida la gestión de configuración, mantenimiento de integridad del código de confianza, y la detección/prevenición de malware;
- seguridad de red y gestión de cortafuegos, incluyendo las restricciones de puertos y filtrado de direcciones IP;
- gestión de usuarios, asignaciones de roles de confianza separados, educación, sensibilización y capacitación, y
- controles de acceso lógico, registro de actividades y tiempos límite por inactividad para determinar responsabilidad individual.

La CA deberá obligar al uso de autenticación de múltiple factor para todas las cuentas, capaces de causar directamente la emisión de un certificado.

6.5.2 Calificación de Seguridad Computacional

Ninguna estipulación.

6.6 Controles Técnicos de Ciclo de Vida

6.6.1 Controles de Desarrollo de Sistemas

Las aplicaciones son desarrolladas e implementadas por E-Sign de acuerdo con los estándares de desarrollo de sistemas y gestión de cambios de E-Sign. E-Sign también ofrece software para sus Clientes Empresariales para realizar ciertas funciones de RA y CA. Tal software es desarrollado de conformidad con los estándares de desarrollo de sistemas de E-Sign.

Cuando es cargado por primera vez, el software desarrollado por Symantec proporciona un método para verificar que el software en el sistema fue originado desde Symantec, no ha sido modificado antes de la instalación, y es la versión que debería ser utilizada.

6.6.2 Controles de Gestión de Seguridad

E-Sign tiene mecanismos y/o políticas disponibles para controlar y supervisar la configuración de sus sistemas de CA. E-Sign crea un hash de todos los paquetes de software y actualizaciones de software de E-Sign. Este hash es utilizado para verificar la integridad de tal software manualmente. En el momento de la instalación y en lo sucesivo en forma periódica, E-Sign valida la integridad de sus sistemas de CA.

6.6.3 Controles de Seguridad del Ciclo de Vida

Ninguna estipulación

6.7 Controles de Seguridad de la Red

E-Sign ejecuta todas sus funciones de CA y las de RA usando redes aseguradas de acuerdo a la Guía Security and Audit Requirements (SAR) para evitar el acceso no autorizado y otras actividades maliciosas. E-Sign protege la comunicación de información delicada mediante el uso de encriptación y firmas digitales.

6.8 Sellado de Tiempo

Los Certificados, las CRLs, y otras entradas de bases de datos de revocación deberán contener información de fecha y hora. Tal información de tiempo no necesita estar basada criptográficamente.

7 Perfiles de Certificado, CRL y OCSP

7.1 Perfil de Certificado

Los Certificados de E-Sign se ajustan en general a (a) Recomendación ITU-T X.509 de (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, Junio 1997 y (b) RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, Abril 2002 ("RFC 5280")²⁰. En tanto sea aplicable al tipo de Certificado, los Certificados STN adhieren a la versión vigente de CA/Browser Forum Baseline Requirements para la Emisión y Gestión de Certificados de Confianza Pública.

Como mínimo, los certificados X.509 deberán contener los campos básicos y los valores prescritos indicados o las restricciones de valores en la Tabla 9 a continuación:

Campo	Valor o restricción de Valor
--------------	-------------------------------------

²⁰ Aun cuando los certificados STN generalmente adhieren a RFC 5280, ciertas provisiones limitadas pueden no estar soportadas.

Número de serie	Valor único por DN de Emisor que muestra al menos 20 bits de entropía
Algoritmo de Firma	Identificador de objeto del algoritmo utilizado para firmar el certificado (ver CP § 7.1.3)
DN Emisor	Véase la sección 7.1.4
Válido desde	Base de Tiempo Coordinado Universal. Sincronizado con el reloj maestro de U.S. Naval Observatory. Codificados de acuerdo a RFC 5280
Válido hasta	Base de Tiempo Coordinado Universal. Sincronizado con el reloj maestro de U.S. Naval Observatory. Codificados de acuerdo a RFC 5280
DN Sujeto	Ver CP § 7.1.4
Llave Pública del Sujeto	Codificados de acuerdo a RFC 5280
Firma	Generada y codificada de acuerdo a RFC 5280

Tabla 9 - Campos del perfil de certificado básico

7.1.1 Número(s) de Versión

Los Certificados de E-Sign son Certificados X.509 Versión 3, aunque está permitido que algunos Certificados Raíz sean Certificados X.509 Versión 1 para dar soporte a sistemas desfasados. Los Certificados de CA deberán ser Certificados de CA X.509 Versión 1 o Versión 3. Los Certificados de Suscriptor usuario final deberán ser X.509 Versión 3.

7.1.2 Extensiones de Certificado

E-Sign completa los Certificados de la STN X.509 Versión 3 con las extensiones requeridas por la Sección 7.1.2.1-7.1.2.8. Las extensiones Privadas son permitidas, pero el uso de extensiones privadas no está garantizado bajo la CP de la red STN y esta CPS salvo que se incluyan como referencia.

7.1.2.1 Uso de la Llave

Los certificados X.509 Versión 3 son completados generalmente de acuerdo con la RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, Abril de 2002. El campo de criticidad de la extensión KeyUsage generalmente se establece en TRUE para los certificados de CA y se puede ser establecido en TRUE o FALSE para certificados de Suscriptores entidades finales.

Nota: El bit no-Repudio ²¹ no necesita ser habilitado en estos certificados ya que la industria PKI no ha alcanzado aún un consenso en cuanto al significado del bit de no-Repudio. Hasta que tal consenso surja, el bit de no-Repudio podría no ser significativo para las potenciales Partes que Confían. Por otra parte, la mayoría de las aplicaciones de uso general no siempre respetan el bit de no-Repudio. Por lo tanto, la habilitación del bit podría no ayudar a las Partes que Confían a tomar una decisión en cuanto a la confianza. Consecuentemente, esta CPS no requiere que el bit de no-Repudio sea habilitado. Podrá ser habilitado en el caso de certificados de par de llaves duales de firma emitidos a través de Managed PKI Key Manager, o, en su defecto, cuando sea solicitado. Cualquier controversia relativa al no-Repudio derivados de la utilización de un certificado digital es un asunto exclusivo entre el suscriptor y la(s) Parte(s) que Confía(n). Ni Symantec, ni E-Sign incurrirán en responsabilidad en relación con ello.

7.1.2.2 Extensión de Políticas de Certificado

La extensión CertificatePolicies de Certificados X.509 Versión 3 es completada con el identificador de objeto de la CP de la STN de acuerdo con la Sección 7.1.6 de la CP y

²¹ El bit de no repudio también puede ser denominado como ContentCommitment en Certificados Digitales, de acuerdo con el estándar X.509.

con los calificadores de política establecidos en la sección 7.1.8 de la CP. El campo de criticidad de esta extensión será establecido en FALSO.

7.1.2.2.1 Requisitos CABF para la Extensión Políticas de Certificado.

Los certificados SSL con Dominio validado y Organización validada adhieren a los requisitos de CA/Browser Forum Baseline. Los Certificados de CA Raíz no deberían contener la extensión CertificatePolicies.

7.1.2.3 Nombres alternativos del Sujeto

La extensión subjectAltName de Certificados X.509 Versión 3 está poblada de conformidad con RFC 5280 con la excepción de aquellos emitidos bajo cuentas Public Lite, las cuales pueden opcionalmente excluir la dirección de correo electrónico en *SubjAltName*. El campo de criticidad de esta extensión será establecido en FALSO.

7.1.2.4 Restricciones Básicas

La extensión BasicConstraints de los Certificados de CA X.509 versión 3 de E-Sign tendrán el campo CA establecido en VERDADERO. La extensión BasicConstraints de los Certificados de Suscriptor usuario-final tendrán el campo CA establecido en FALSO. El campo de criticidad de esta extensión será establecido en VERDADERO para Certificados de CA, pero puede ser establecido en VERDADERO o FALSO para Certificados de Suscriptor usuario-final.

Los Certificados de CA X.509 Versión 3 de E-Sign tendrán un campo "pathLenConstraint" de la Extensión BasicConstraints establecido como el número máximo de certificados de CA que pueden seguir a este Certificado en una ruta de certificación. Los Certificados de CA emitidos a un Cliente Empresarial en línea que emite Certificados de Suscriptor Usuario-final tendrán un campo "pathLenConstraint" fijo en el valor "0" indicando que sólo un Certificado de usuario final puede seguir en la ruta de certificación.

7.1.2.5 Uso Extendido de Llave

Por defecto, la extensión ExtendedKeyUsage es establecida como una extensión no crítica. Los Certificados de CA STN no incluyen la extensión ExtendedKeyUsage.

7.1.2.6 Puntos de Distribución de CRL

La mayoría de los Certificados X.509 versión 3 de Suscriptor usuario final y de CA intermedia de E-Sign incluyen la extensión cRLDistributionPoints que contiene la URL de la ubicación en la que una Parte que Confía puede obtener una CRL para comprobar el estado del certificado de CA. El campo de criticidad de esta extensión se establece en FALSE.

7.1.2.7 Identificador de Llave de Autoridad

E-Sign generalmente completa la extensión Authority Key Identifier de los Certificados X.509 versión 3 de Suscriptor usuario final y de CA Intermedia. Cuando el emisor del certificado contiene la extensión Subject Key Identifier, el identificador de clave de la Autoridad está compuesto del hash SHA-1 de 160 bits de la llave pública de la CA que emite el certificado. De lo contrario, la extensión Authority Key Identifier incluye el nombre distinguido del sujeto y el número de serie de la CA emisora. El campo criticidad de esta extensión se establece en FALSE.

7.1.2.8 Identificador de Llave del Sujeto

En caso de que E-Sign incluya en los Certificados X.509 Versión 3 de la STN una extensión `subjectKeyIdentifier`, el `keyIdentifier` basado en la llave pública del sujeto del certificado es generado de acuerdo con uno de los métodos descritos en el RFC 5280. En caso de que esta extensión sea utilizada, el campo de criticidad de esta extensión es establecido en FALSE.

7.1.3 Identificadores de Objeto de Algoritmos

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

- identificador de objeto **sha256withRSAEncryption**:: = {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
- identificador de objeto **ecdsa-with-Sha256**:: = {iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2}
- identificador de objeto **ecdsa-with-Sha384**:: = {iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 3}
- identificador de objeto **sha-1WithRSAEncryption**::= {iso(1) member-body(2) us(840)rsadsi(113549) pkcs(1) pkcs-1(1) 5}
- identificador de objeto **md5WithRSAEncryption**::= {iso(1) member-body(2) us(840)rsadsi(113549) pkcs(1) pkcs-1(1) 4}

Las firmas de Certificado producidas utilizando estos algoritmos cumplirán con RFC 3279. `sha-1WithRSAEncryption` o `sha256WithRSAEncryption` serán utilizadas por sobre `md5WithRSAEncryption` ²².

7.1.4 Formas de Nombres

E-Sign completa los Certificados de la STN con un Nombre del Emisor y un Nombre Distinguido del Sujeto de acuerdo a la Sección 3.1.1. El Nombre del Emisor deberá ser completado en cada Certificado emitido conteniendo el País, Nombre de Organización y el Nombre Común de la CA Emisora.

Además, E-Sign puede incluir dentro de los certificados de Suscriptor usuario final campos `Organizational Unit` adicionales que contienen un aviso indicando que las condiciones de uso del certificado son establecidas en una URL que es un puntero al correspondiente Acuerdo de la Parte que Confía aplicable. Este campo OU debe aparecer si en la extensión de política del certificado no está incluido un puntero al Acuerdo de la Parte que Confía aplicable.

7.1.5 Restricciones de Nombres

Ninguna estipulación

7.1.6 Identificador de Objeto de Política de Certificación

Si la extensión `Certificate Policies` es utilizada, los certificados contienen el identificador de objeto para la Política de Certificados correspondiente a la Clase apropiada de Certificado según lo establecido en la CP de la STN, Sección 1.2. Para los Certificados desfasados emitidos con anterioridad a la publicación de la CP de la

²² `md5WithRSAEncryption` sólo se utiliza con autorización previa para preservar la continuidad del negocio de las aplicaciones heredadas.

STN que incluyen la extensión Políticas de Certificados, los certificados se refieren a la CPS de la STN.

7.1.6.1 Requisitos CABF para el Identificador de Objeto Certificate Policy

Los certificados SSL con Dominio validado y Organización validada adhieren a los requisitos de CA/Browser Forum Baseline. Tales Certificados emitidos contienen el identificador de política correspondiente especificado en la sección 1.2 de la CP STN que indica que el Certificado es emitido y administrado en cumplimiento de estos Requisitos.

Después del 1 de Julio de 2012, un Certificado emitido a una CA Subordinado que no sea Afiliado de la CA Emisora:

- Debe incluir el identificador de la política correspondiente identificado en la sección 1.2 que indica la adhesión y el cumplimiento de estos Requisitos CABF por parte de la CA subordinada, y
- No debe contener el identificador "anyPolicy" (2.5.29.32.0).

Después del 1 de julio de 2012, un certificado emitido a una CA subordinada que sea Afiliado de la CA Emisora:

- puede incluir el identificador de la política correspondiente identificado en la sección 1.2 que indica la adhesión y el cumplimiento de estos Requisitos CABF por parte de la CA subordinada, y
- puede contener el identificador "anyPolicy" (2.5.29.32.0) en lugar del identificador de política explícita.

7.1.7 Uso de la Extensión Policy Constraints

Ninguna estipulación

7.1.8 Sintaxis y Semántica de Calificadores de Política

E-Sign generalmente completa los Certificados X.509 Versión 3 con un calificador de política dentro de la extensión Políticas de Certificados. Por lo general, dichos Certificados contienen un calificador de puntero de CPS que apunta al Acuerdo de la Parte que Confía aplicable o a la CPS de E-Sign. Además, algunos certificados contienen un Calificador Aviso para el Usuario que apunta al Acuerdo de la Parte que Confía correspondiente.

7.1.9 Semántica de Procesamiento para la Extensión Crítica Certificate Policies

Ninguna estipulación

7.2 Perfil de CRL

En tanto sea aplicable al tipo de certificado, las CRL correspondientes se ajustan a los requisitos de la versión actual de CA/Browser Forum Baseline Requirements para la Emisión y Gestión de Certificados de Confianza Pública.

Las CRL Versión 2 se ajustan a las especificaciones de RFC 5280 y contienen los campos y contenidos básicos especificados en la Tabla 13 a continuación:

Campo	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 CPS § 7.1.3)
Emisor	Entidad que ha firmado y emitido la CRL. La CRL es firmada usando la llave privada que la CA utiliza para firmar los certificados que emite.
Fecha de vigencia	Fecha de emisión de la CRL. Las CRL son efectivas desde la emisión.
Próxima Actualización	Fecha en la que será publicada la próxima CRL. La 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 13 - Campos Básicos de Perfil de CRL

7.2.1 Número(s) de Versión

E-Sign soporta CRLs X.509 tanto en Versión 1 como en Versión 2 . Las CRL versión 2 cumplen con los requerimientos de la RFC 5280.

7.2.2 Extensiones CRL y CRL Entry

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 Class 2 Enterprise utilizando el OCSP Empresarial que cumple con RFC 2560, y
- Certificados Class 2 Empresarial y Class 3 organizacional con el protocolo Symantec Trusted Global Validation (TGV), que cumple con RFC 5019.

Requisitos CABF para Firma de OCSP

Los certificados SSL con Dominio validado y Organización validada adhieren a los requisitos de CA/Browser Forum Baseline.

Las respuestas OCSP se ajustarán a las especificaciones de RFC5019 y son:

- Firmadas por la CA que emitió los Certificados cuyo estado de revocación está siendo comprobado, o
- Firmadas por un Respondedor OCSP cuyo Certificado está firmado por la CA que emitió el Certificado, cuyo estado de revocación está siendo comprobado. Tal Certificado de firma de Respondedor OCSP deberá contener la extensión id-pkix-ocsp-nocheck como se define en RFC2560.

7.3.1 Número(s) de Versión

Son soportadas la versión 1 de la especificación OCSP según se define en RFC2560 y la versión 1 de la especificación OCSP según se define en RFC 5019.

7.3.2 Extensiones OCSP

El servicio TGV utiliza sellado de tiempo seguro y período de validez para establecer cuán reciente es cada respuesta OCSP. E-Sign no utiliza un código aleatorio para establecer cuán reciente es actual de cada respuesta OCSP y los clientes no deben esperar un código aleatorio en la respuesta a una solicitud que contiene un código aleatorio. En su lugar, los clientes deben utilizar el reloj local para revisar cuán reciente es la respuesta.

8 Auditorías de Cumplimiento y Otras Evaluaciones

La infraestructura de CA de E-Sign es operada en la infraestructura segura de Symantec por lo cual las operaciones PKI de E-Sign son realizadas por Symantec de acuerdo a los procedimientos establecidos en esta CPS.

Un examen anual de WebTrust para Autoridades de Certificación versión 2.0 o superior (o equivalente) se lleva a cabo para las operaciones de los centros de datos de E-Sign y las operaciones de gestión de llaves que soportan los servicios público y de CA de Managed PKI de E-Sign, incluyendo las CA raíz de STN, las CA Class 3 Organizational CA, las CAs Class 2 Organizational e Individual, y las CAs Class 1 Individual CA especificadas en la Sección 1.3.1. Las CAs específicas del cliente no son auditadas específicamente como parte de la auditoría de las operaciones de E-Sign, a menos que sea requerido por el Cliente. E-Sign tendrán derecho a requerir que los Clientes Empresariales se sometan a una auditoría de cumplimiento bajo esta CPS y los programas de auditoría para este tipo de Clientes.

Además de las auditorías de cumplimiento, E-Sign tendrá derecho a realizar otros exámenes e investigaciones para garantizar la confiabilidad del Subdominio de E-Sign de la red STN, que incluyen, pero no están limitados a:

- E-Sign tendrá el derecho, a su discreción única y exclusiva, para realizar en cualquier momento una "Auditoría/Investigación Exigente" en un Cliente en el caso de que E-Sign tenga razones para creer que la entidad auditada no ha cumplido con las Normas de la STN, ha sufrido un incidente o compromiso, o ha actuado o dejado de actuar, de un modo que, el incidente o compromiso, o el acto u omisión de la entidad auditada constituye una amenaza real o potencial a la seguridad o integridad de la red STN.
- E-Sign tendrá derecho a realizar "Revisiones a la Gestión de Riesgo Suplementarias" en un Cliente después de resultados incompletos o excepcionales en una Auditoría de Cumplimiento o como parte del proceso de gestión de riesgo global en el curso ordinario del negocio.

E-Sign podrá delegar la realización de estas auditorías, revisiones e investigaciones en una firma de auditoría de terceros. Las entidades que están sujetas a una auditoría, revisión o investigación deberán entregar una cooperación razonable con E-Sign y con el personal que realiza la auditoría, revisión o investigación.

Los certificados SSL con Dominio validado y Organización validada adhieren a los requisitos de CA/Browser Forum Baseline

E-Sign deberá llevar a cabo auto auditorías para supervisar la adherencia a su Política de Certificados y requisitos CPS y controlar estrictamente la calidad de su servicio al menos trimestralmente contra una muestra seleccionada aleatoriamente del mayor entre un Certificado y al menos el 3% de los Certificados emitidos durante el período que comienza inmediatamente después de que la muestra de la auto auditoría previa haya sido tomada.

8.1 Frecuencia y Circunstancias de las Evaluaciones

Las Auditorías de Cumplimiento son llevadas a cabo al menos una vez al año con cargo exclusivo a la entidad auditada. Las auditorías son llevadas a cabo sobre secuencias ininterrumpidas de períodos de auditoría con cada período con una duración no mayor a un año.

8.2 Identidad/Calificaciones del Evaluador

Las auditorías de cumplimiento de la CA de E-Sign son realizadas por una firma de contadores públicos que:

- Demuestra dominio en la realización de WebTrust para Certificatio Authorities v2.0 o
- Demuestra dominio de la tecnología de infraestructura de llave pública, herramientas y técnicas de seguridad de la información, auditoría de seguridad, y la función de certificación de terceros, y
- Está acreditada por el Instituto Americano de Contadores Públicos Certificados (AICPA), que requiere la posesión de ciertas habilidades, las medidas de aseguramiento de la calidad, tales como revisión por pares, pruebas de competencia, normas con respecto a la asignación adecuada de personal para compromisos y requerimientos de educación profesional continua.
- Se halla bajo regulación legal, gubernamental, o un código de ética profesional, y
- Mantiene una póliza de seguro por Responsabilidad Profesional / Errores u Omisiones, con una cobertura mínima de un millón de dólares de los Estados Unidos de América.

8.3 Relación del Evaluador con la Entidad Evaluada

Las auditorías de cumplimiento de las operaciones de E-Sign son realizadas por una firma de contadores públicos que es independiente de E-Sign.

8.4 Tópicos Cubiertos por la Evaluación

El alcance de la auditoría WebTrust para Autoridades de Certificación (o equivalente) anual de las CA de E-Sign incluye los controles ambientales, las operaciones de gestión de claves de la CA y controles de Infraestructura/Administrativos de la CA, gestión del ciclo de vida certificado y de divulgación de las prácticas negocio de la CA.

8.5 Acciones a Tomar como Resultado de la Deficiencia

Con respecto a las auditorías de cumplimiento de las operaciones de E-Sign, las excepciones o deficiencias importantes identificadas durante la Auditoría de Cumplimiento darán lugar a una determinación de las acciones a ser adoptadas. Esta determinación será realizada por la administración de E-Sign con la información aportada por los auditores. La administración de E-Sign es responsable de desarrollar e implementar un plan de acción correctiva, que será desarrollado dentro de 30 días e implementado en un período de tiempo comercialmente razonable. Si E-Sign determina que tales excepciones o deficiencias suponen una amenaza inmediata a la seguridad o integridad del subdominio E-Sign, se evaluará la suspensión de las operaciones de las CA de E-Sign. Para las excepciones o deficiencias de menor gravedad, la administración de E-Sign evaluará la importancia de tales materias y determinará el curso de acción apropiado.

8.6 Comunicación de los Resultados

E-Sign pone a disposición del público su Informe de Auditoría anual a más tardar tres (3) meses después del final del período de la auditoría. En el caso de un retraso superior a tres meses, E-Sign deberá presentar una carta explicativa firmada por el Auditor Calificado. Una copia del informe de auditoría WebTrust para CAs de E-Sign

puede ser encontrado en el repositorio de E-Sign en <https://www.e-sign.cl/default/repositorio>.

9 Otros Aspectos Comerciales y Legales

9.1 Tarifas

9.1.1 Tarifas de Emisión o Renovación de Certificados

E-Sign tendrá derecho a cobrar a los Suscriptores usuarios finales por la emisión, gestión y renovación de Certificados. Las tarifas se encuentran publicadas en <https://www.e-sign.cl>.

9.1.2 Tarifas de Acceso a los Certificados

E-Sign no cobra una tarifa como condición para poner un certificado disponible en un repositorio, o para hacer accesible de otra forma los Certificados a Partes que Confían.

9.1.3 Tarifa para Revocación o Acceso a Información de Estado

E-Sign no cobra una tarifa como condición para dejar la CRL requerida por la CP disponible en un repositorio o disponible de otra manera para las Partes que Confían. E-Sign, sin embargo, tiene derecho a cobrar una tarifa por proporcionar una CRL personalizada, servicios de OCSP, u otros servicios de valor agregado sobre información de estado y revocación.

E-Sign no permite el acceso a la información de revocación, a información de estado de Certificados o de sellado de tiempo en sus repositorios a terceros que ofrecen productos o servicios que utilizan esa información de estado de certificados, sin el consentimiento previo y expreso de E-Sign por escrito.

9.1.4 Tarifas por Otros Servicios

E-Sign no cobra una tarifa por acceder a esta CPS. Cualquier uso que se hace para otros fines distintos de la simple visualización del documento, como la reproducción, distribución, modificación o creación de trabajos derivados, estarán sujetos a un contrato de licencia con la entidad titular de los derechos en el documento.

9.1.5 Política de Reembolsos

En el Subdominio de E-Sign existe la siguiente política de reembolso (que se reproduce en <https://www.e-sign.cl/default/legal>):

E-Sign adhiere y respalda rigurosas prácticas y políticas en la realización de operaciones de certificación y emisión de certificados. No obstante, si por alguna razón un suscriptor no está completamente satisfecho con el certificado que le ha sido emitido, el suscriptor puede solicitar que E-Sign revoque el certificado dentro de los treinta (30) días de la emisión y que proporcione un reembolso al suscriptor. Después del período inicial de treinta (30) días, un suscriptor puede solicitar que E-Sign revoque el certificado y proporcione un reembolso si E-Sign ha violado una garantía u obligación material contenida en la presente CPS o en el Plan de Protección NetSure (sm) en relación con el suscriptor o el certificado del suscriptor. Después de que E-Sign haya revocado el certificado del suscriptor, E-Sign prontamente abonará en la cuenta del abonado con tarjeta de crédito (si el certificado fue pagado con tarjeta de crédito) o de lo contrario reembolsará al suscriptor a través de cheque, por el importe total de las tarifas aplicables pagadas por el certificado. Para solicitar un reembolso, por favor llame al servicio al cliente al (+562) 433.1500. Esta política de reembolso no

es un remedio exclusivo y no limita otros remedios que pueden estar disponibles para los suscriptores.

9.2 Responsabilidad Financiera

9.2.1 Cobertura de Seguros

A los Clientes Empresariales se les anima a mantener un nivel comercialmente razonable de cobertura de seguro por errores y omisiones, ya sea a través de un programa de seguro contra errores y omisiones con una compañía de seguros o de una retención auto-asegurada. E-Sign mantiene seguros con cobertura contra dicho tipo de errores y omisiones.

9.2.2 Otros Activos

Los Clientes Empresariales deben disponer de suficientes recursos financieros para mantener sus operaciones y cumplir con sus obligaciones, y deben ser razonablemente capaces de soportar el riesgo de la responsabilidad frente a los suscriptores y las Partes que Confían. Los recursos financieros de E-Sign se señalan en la información publicada en: www.e-sign.com.

9.2.3 Cobertura de Garantía Extendida

Ninguna estipulación

9.3 Confidencialidad de la Información de Negocios

9.3.1 Alcance de la Información Confidencial

Los siguientes registros de suscriptores, de acuerdo a la Sección 9.3.2, se mantendrán confidenciales y privados ("Información Confidencial/Privada"):

- Registros de solicitudes de la CA, ya sean aprobadas o rechazadas
- Registros de Solicitud de Certificado
- Llaves privadas en manos de los clientes empresariales que utilizan Managed PKI Key Manager y la información necesaria para recuperar estas llaves privadas.
- Registros transaccionales (tanto registros completos como la bitácora de auditoría de las transacciones)
- Bitácora de registros de auditoría creados o retenidos por Symantec o un cliente.
- Informes de auditoría efectuados por E-Sign o un cliente (en la medida en que dichos informes son conservados), o de sus respectivos auditores (ya sea internos o públicos)
- Planes de contingencia y los planes de recuperación de desastres,
- Las medidas de seguridad que controlan las operaciones de hardware y software de E-Sign y la administración de los servicios de Certificados y los servicios de enrolamiento designados.

9.3.2 Información Fuera del Alcance de Información Confidencial

Los Certificados, la revocación de certificados y otra información de estado, los repositorios de E-Sign y la información contenida en ellos, no se consideran Información Confidencial/Privada. La información que no esté expresamente

considerada Información Confidencial/Privada en la Sección 9.3.1 no se considerará confidencial ni privada. Esta sección está sujeta a las leyes de privacidad aplicables.

9.3.3 Responsabilidad de Proteger la Información Confidencial

E-Sign protege la información privada de compromiso y de divulgación a terceros.

9.4 Confidencialidad de Información Personal

9.4.1 Plan de Privacidad

E-Sign ha implementado una política de privacidad, que se encuentra en: <https://www.e-sign.cl/default/privacidad>, de acuerdo con CP 9.4.1.

9.4.2 Información Tratada como Privada

Cualquier información sobre los Suscriptores que no está a disposición del público a través del contenido del certificado emitido, el directorio de certificados y CRLs en línea es tratada como privada

9.4.3 Información que no se Considera Privada

Sujeto a las leyes locales, toda la información hecha pública en un certificado se considera no privada.

9.4.4 Responsabilidad de Proteger Información Privada

Los participantes del Subdominio E-Sign de la red STN que reciben información privada la protegerán de compromiso y divulgación a terceros y deberán cumplir con todas las leyes locales de privacidad de su jurisdicción.

9.4.5 Notificación y Consentimiento para el Uso de Información Privada

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

9.4.6 Divulgación de Conformidad con Proceso Judicial o Administrativo

E-Sign tendrá derecho a revelar Información Confidencial/Privada si, de buena fe, E-Sign cree que:

- La divulgación es necesaria en respuesta a citaciones y órdenes de registro.
- La divulgación es necesaria en respuesta a un proceso judicial, administrativo u otro proceso legal durante el proceso de exhibición en una acción civil o administrativa, tales como citaciones, interrogatorios, 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

Ninguna estipulación

9.5 Derechos de Propiedad Intelectual

La asignación de Derechos de Propiedad Intelectual entre los participantes del Subdominio E-Sign que no sean Suscriptores y Partes que Confían, está regida por los acuerdos aplicables entre tales participantes del Subdominio E-Sign. Las siguientes subsecciones de la sección 9.5 se aplican a los Derechos de Propiedad Intelectual en relación a los Suscriptores y Partes que Confían.

9.5.1 Derechos de Propiedad en Certificados e Información de Revocación

Las CAs retienen todos los Derechos de Propiedad Intelectual en y hacia los Certificados y la información de revocación que emiten. E-Sign y sus Clientes conceden el permiso para reproducir y distribuir Certificados en un régimen no exclusivo y libre de regalías, siempre que éstos sean reproducidos en su totalidad y que el uso de los Certificados sea sujeto al Acuerdo de la Parte que Confía referenciado en el Certificado. E-Sign y sus Clientes concederán permiso para usar la información de revocación para llevar a cabo funciones de la Parte que Confía sujeto al Acuerdo de Uso de CRL, Acuerdo de la Parte que Confía, o cualquier otro acuerdo aplicable.

9.5.2 Derechos de Propiedad en la CPS

Los participantes de la STN reconocen que Symantec se reserva todos los derechos de propiedad intelectual en y hacia esta CPS.

9.5.3 Derechos de Propiedad en Nombres

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

9.5.4 Derechos de Propiedad en Llaves y Material de Llaves

Los pares de llaves correspondientes a certificados de CA y Suscriptores usuarios finales son propiedad de la CA y los Suscriptores usuarios finales que son los respectivos Sujetos de estos Certificados, sujeto a los derechos de los Clientes empresariales que utilizan Managed PKI Key Manager, sin importar el medio físico en el que están almacenados y protegidos, y tales personas conservan todos los Derechos de Propiedad Intelectual en y hacia esos pares de llaves. Sin limitar la generalidad de lo anterior, las llaves públicas de la Raíz de Symantec, de la cual depende la jerarquía de certificación de la CA de E-Sign, y los Certificados Raíz que los contienen, incluyendo todas las llaves públicas y certificados autofirmados de PCA, son propiedad de Symantec. Symantec entrega licencias a los fabricantes de software y hardware para reproducir dichos Certificados raíz para poner copias en dispositivos de hardware o software de confianza. Por último, las Partes Secretas de la llave privada de una CA son propiedad de la CA, y la CA conserva todos los Derechos de Propiedad Intelectual en y hacia tales Partes Secretas aún cuando no se pueda obtener la posesión física de esas partes o de la CA de Symantec.

9.6 Declaraciones y Garantías

9.6.1 Declaraciones y Garantías de la CA

E-Sign garantiza que:

- No hay declaraciones falsas sustanciales en el Certificado conocidas por o procedentes de las entidades que aprobaron la Solicitud de Certificado o que emitieron el Certificado,
- No hay errores en la información en el Certificado introducidos por las entidades que aprobaron la Solicitud de Certificado o que emitieron el Certificado, como resultado de no ejercer un cuidado razonable en la gestión de la Solicitud de Certificado o en la creación del Certificado,
- Sus certificados cumplen todos los requisitos materiales de esta CPS, y
- Los servicios de revocación y el uso de un repositorio se ajustan a la CPS aplicable en todos los aspectos materiales.

Los Acuerdos de Suscriptor pueden incluir declaraciones y garantías adicionales.

9.6.1.1 Garantías y obligaciones CABF

Los certificados SSL de validación de dominio y organización validados conforme a la CA / Browser Forum. Mediante la emisión de tal certificado, la entidad emisora de certificados hace aplicables las garantías que figuran en esta sección para los beneficiarios de certificados que figuran en la sección 1.3.5.

La CA representa y garantiza a los beneficiarios de certificados que, durante el período en que el certificado es válido, la CA ha cumplido con estos requisitos y con su Política de Certificados y / o Declaración de Prácticas de Certificación en la emisión y la gestión del Certificado. Las garantías de certificados incluyen específicamente, pero no se limitan a, los siguientes:

1. Derecho de Uso de los nombres de dominio o dirección IP: Que, en el momento de la emisión, la entidad emisora (i) implementó un procedimiento para verificar que el solicitante tenía derecho a usar, o tenía el control del nombre de dominio(s) y direcciones IP que figuran en el asunto del certificado y en la extensión `subjectAltName` (o se delegó a tal derecho o control por parte de alguien que tenía tal derecho a utilizar o controlar, sólo en el caso de nombres de dominio), (ii) ha seguido el procedimiento en la emisión del certificado, y (iii) describió acuciosamente el procedimiento en la Política de Certificado de la CA y / o Declaración de Prácticas de Certificación;
2. Autorización de Certificados: Que, en el momento de la emisión, la entidad emisora (i) implementó un procedimiento para verificar que el Sujeto autorizó la emisión del certificado y que el representante de la requirente está autorizado para solicitar el certificado en nombre del sujeto, (ii), seguido el procedimiento al emitir el Certificado, y (iii) el procedimiento descrito con precisión en la Política de Certificación de la CA y / o Declaración de Prácticas de Certificación;
3. Precisión de la Información: Que, en el momento de la emisión, la entidad emisora (i) implementó un procedimiento para verificar la exactitud de toda la información contenida en el certificado (con la excepción de la materia: el atributo `organizationalUnitName`), (ii) ha seguido el procedimiento en la emisión del certificado, y (iii) describió acuciosamente el procedimiento en la Política de Certificado de la CA y / o Declaración de Prácticas de Certificación;
4. Certeza de la información: Que, en el momento de la emisión, la entidad emisora (i) implementó un procedimiento para reducir la probabilidad de que la información contenida en el Certificado del sujeto (salvo el atributo `organizationalUnitName`) fuese

engañoso, (ii) ha seguido el procedimiento en la emisión del certificado, y (iii) describió acuciosamente el procedimiento en la Política de Certificado de la CA y / o Declaración de Prácticas de Certificación;

5. Identidad del solicitante: Que, si el certificado contiene información sobre la identidad del sujeto, la CA (i) implementó un procedimiento para verificar la identidad del solicitante, de conformidad con los puntos 3.1.1.1 y 3.2.2.1, (ii) ha seguido el procedimiento en la emisión del certificado, y (iii) describió acuciosamente el procedimiento en la Política de Certificado de la CA y / o Declaración de Prácticas de Certificación;

6. Acuerdo de Suscriptor: Que, si la entidad emisora y el suscriptor no son Afiliados, el suscriptor y CA son partes de un Acuerdo de Suscriptor legalmente válido y exigible que cumpla estos requisitos, o, si la entidad emisora y el suscriptor están afiliados, el Representante del solicitante haya reconocido y aceptado las Condiciones de Uso;

7. Estado: Que la CA mantiene 24 x 7 un repositorio de acceso público con información actualizada sobre el estado (válido o revocado) de todos los certificados no vencidos, y

8. Revocación: Que el CA revocará el certificado por cualquiera de las razones especificadas en las presentes prescripciones.

Obligaciones de la CA Raíz

La CA raíz será responsable por la ejecución y garantías de la CA subordinada, por el cumplimiento de dichos requisitos por la CA subordinada, y por todas las obligaciones de cumplimiento e indemnización de la CA subordinada, bajo estos requerimientos, como si la entidad emisora raíz hubiese sido la CA Subordinada emitiendo los certificados.

9.6.2 Declaraciones y Garantías de la RA

Las RAs garantizan que:

- No hay declaraciones falsas sustanciales en el Certificado, conocidas por o procedentes de las entidades que aprobaron la Solicitud de Certificado o que emitieron el Certificado,
- No hay errores en la información del Certificado introducidos por las entidades que aprobaron la Solicitud de Certificado, como resultado de no ejercer un cuidado razonable en la gestión de la Solicitud de Certificado,
- Sus certificados cumplen todos los requisitos materiales de esta CPS, y
- Los servicios de revocación (cuando corresponda) y el uso de un repositorio se ajustan a la CPS aplicable en todos los aspectos materiales.

Los Acuerdos de Suscriptor pueden incluir declaraciones y garantías adicionales.

9.6.3 Declaraciones y Garantías del Suscriptor

Los suscriptores garantizan que:

- Cada firma digital creada utilizando la clave privada correspondiente a la clave pública listada en el Certificado es la firma digital del Suscriptor y el Certificado ha sido aceptado y está operativo (no expirado o revocado) en el momento de crear la firma digital,
- Sus llaves privadas están protegidas y que nunca alguna persona no autorizada ha tenido acceso a la llave privada del Suscriptor,
- Todas las declaraciones hechas por el Suscriptor en la Solicitud de Certificado enviada por el Suscriptor, son verdaderas,
- Toda la información proporcionada por el Suscriptor y contenida en el Certificado es verdadera,

- El Certificado está siendo utilizado exclusivamente para fines autorizados y legales, de conformidad con esta CPS, y
- El Suscriptor es un suscriptor usuario final y no una CA, y no está utilizando la llave privada que corresponde a alguna de las llaves públicas incluidas en el certificado para los efectos de firmar digitalmente cualquier Certificado (o cualquier otro formato de llave pública certificada) o CRL, como CA o de cualquier otra manera.

Los Acuerdos de Suscriptor pueden incluir declaraciones y garantías adicionales.

9.6.4 Declaraciones y Garantías de la Parte que Confía

Los Acuerdos de la Parte que Confía requieren que las Partes que Confían reconozcan que tienen información suficiente para tomar una decisión informada hasta un punto tal que optan por confiar en la información contenida en un Certificado, que ellos son los únicos responsables de decidir si deben o no confiar en tal información, y que ellos asumirán las consecuencias legales de su incumplimiento en el ejercicio de las obligaciones de la Parte que Confía en términos de esta CPS.

Los Acuerdos de la Parte que Confía podrán incluir declaraciones y garantías adicionales.

9.6.5 Declaraciones y Garantías de los Demás Participantes

Ninguna estipulación

9.7 Renuncia de Garantías

Dentro de los límites permitidos por la legislación aplicable, los Acuerdos de Suscriptor y los Acuerdos de la Parte que Confía renunciarán a las posibles garantías de E-Sign, incluyendo cualquier garantía de comerciabilidad o idoneidad para un propósito particular.

9.8 Limitaciones de Responsabilidad

Dentro de los límites permitidos por la legislación aplicable, los Acuerdos de Suscriptor y los Acuerdos de la Parte que Confía limitarán la responsabilidad de E-Sign. Las limitaciones de responsabilidad deberán incluir una exclusión de daños indirectos, especiales, incidentales y derivados. También deberán incluir las siguientes topes de responsabilidad que limitan los daños de E-Sign en relación a un Certificado específico:

Clase	Topes de responsabilidad
Class 1	Cien Dólares EE.UU. (\$ 100.00 EE.UU.)
Class 2	Cinco Mil Dólares EE.UU. (\$ 5,000.00 EE.UU.)
Class 3	Cien Mil Dólares EE.UU. (\$ 100,000.00 EE.UU.)

Tabla 14 - Topes de Responsabilidad

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

La responsabilidad (y/o la limitación de la misma) de las RAs empresariales y de la CA aplicable deberán ser establecidas en el(los) acuerdo(s) entre ellas.

La responsabilidad (y/o la limitación de la misma) de las Partes que Confían deberán ser las establecidas en los Acuerdos de Partes que Confían aplicables.

9.9 Indemnizaciones

9.9.1 Indemnización por los Suscriptores

Dentro de los límites permitidos por la legislación aplicable, los Suscriptores tienen la obligación de indemnizar a E-Sign por:

- Falsedad o tergiversación de hecho por el Suscriptor en la Solicitud de Certificado del Suscriptor,
- La no revelación de un hecho sustancial en la Solicitud de Certificado, si la falsedad u omisión es consecuencia de negligencia o con la intención de engañar a cualquiera de las partes,
- Faltas del Suscriptor para la protección de la llave privada del Suscriptor, para utilizar un Sistema de Confianza o para tomar, en cualquier otro caso las precauciones necesarias para evitar el compromiso, la pérdida, la divulgación, la modificación o el uso no autorizado de la llave privada del Suscriptor, o
- El uso por parte del Suscriptor de un nombre (incluyendo, sin limitaciones dentro de un nombre común, un nombre de dominio o una dirección de correo electrónico) que infrinja los Derechos de Propiedad Intelectual de un tercero.

El Acuerdo de Suscriptor aplicable puede incluir obligaciones de indemnización adicionales.

9.9.2 Indemnización por las Partes que Confían

Dentro de los límites permitidos por la legislación aplicable, los Acuerdos de la Parte que Confía exigirá a las Partes que Confían indemnizar a E-Sign por:

- La falta de la Parte que Confía para llevar a cabo las obligaciones de una Parte que Confía,
- La confianza de la Parte que Confiada en un Certificado que no es razonable bajo las circunstancias, o
- La falta de la Parte que Confía en la comprobación del estado de tal Certificado para determinar si el Certificado está expirado o revocado.

El Acuerdo de la Parte que Confía aplicable puede incluir obligaciones de indemnización adicionales.

9.10 Vigencia y Término

9.10.1 Vigencia

La CPS entra en vigencia a partir de su publicación en el repositorio de E-Sign. Las enmiendas a esta CPS entran en vigencia a partir de su publicación en el repositorio de E-Sign.

9.10.2 Término

Este CPS en su forma enmendada, de tiempo en tiempo, se mantendrá vigente hasta que sea reemplazada por una nueva versión.

9.10.3 Efecto del Término y Sobrevivencia

Tras el término de esta CPS, los participantes del Subdominio E-Sign son obligados por sus términos, para todos los certificados emitidos por el resto de los períodos de validez de tales certificados.

9.11 Avisos Individuales y Comunicaciones con los Participantes

A menos que se especifique lo contrario por acuerdo entre las partes, los participantes del Subdominio E-Sign deberán usar métodos comercialmente razonables para comunicarse entre sí, teniendo en cuenta la criticidad y la materia sujeto de la comunicación.

9.12 Modificaciones

9.12.1 Procedimiento de Enmiendas

Las enmiendas a esta CPS pueden ser realizadas por la Autoridad de Administración de Políticas (PMA) de E-Sign. Las modificaciones pueden ser en la forma ya sea de un documento que contenga una forma enmendada de la CPS o de una actualización. Las versiones modificadas o actualizaciones estarán vinculadas a la sección de Actualización de Prácticas de E-Sign localizado en: <https://www.e-sign.cl/repositorios>. Las Actualizaciones sustituyen a las disposiciones designadas o conflictivas de la versión de referencia de la CPS. El PMA deberá determinar si los cambios en la CPS requieren un cambio en los identificadores de objeto de política de Certificado de las políticas de Certificados correspondientes a cada Clase de Certificado.

9.12.2 Mecanismo y Período de Notificación

E-Sign y el PMA se reservan el derecho de modificar la CPS sin notificación por enmiendas que no son sustanciales, incluyendo, sin limitación, correcciones de errores tipográficos, cambios de URLs, y los cambios en la información de contactos. La decisión del PMA de clasificar las enmiendas como sustanciales o no, quedará a la única discreción del PMA.

Las enmiendas propuestas a la CPS deberán aparecer en la sección Actualización de Prácticas de E-Sign, que se encuentra en: <https://www.e-sign.cl/repositorios>.

El PMA solicita propuestas de enmienda a la CPS de otros participantes del Subdominio E-Sign. Si el PMA considera que tal enmienda es deseable y propone la aplicación de la enmienda, el PMA deberá dar aviso de tal modificación de conformidad con esta sección.

Sin perjuicio de cualquier indicación en la CPS en el sentido contrario, si el PMA considera que las enmiendas sustanciales a la CPS son necesarias inmediatamente para detener o para prevenir una violación de la seguridad de la STN o cualquier parte de ella, E-Sign y el PMA tendrán derecho a efectuar tales modificaciones mediante la publicación en el repositorio E-Sign. Tales cambios se harán efectivos inmediatamente después de su publicación. Dentro de un período razonable después de la publicación, E-Sign notificará de tales cambios a los participantes del Subdominio E-Sign.

9.12.2.1 Período de Comentarios

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

9.12.2.2 Mecanismo para Tramitar los Comentarios

El PMA deberá tomar en cuenta todos 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 enmiendas propuestas y volver a publicarlas como una nueva enmienda cuando sea requerido, o (c) retirar las enmiendas propuestas. El PMA tiene derecho a retirar las enmiendas propuestas mediante notificación a los participantes del Subdominio E-Sign y aviso en la sección Actualización de Prácticas de E-Sign. A menos que las enmiendas propuestas sean modificadas o retiradas, entrarán en vigor a partir de 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 correspondiente a una política de Certificados, la enmienda deberá contener los nuevos identificadores de objeto para las políticas de Certificados correspondientes a cada Clase de Certificado. De lo contrario, las enmiendas no requerirán un cambio en el identificador de objeto de política de Certificado.

9.13 Disposiciones de Resolución de Disputas

9.13.1 Disputas entre Symantec, E-Sign y Clientes

Las disputas entre los participantes del subdominio E-Sign serán resueltas de conformidad con lo dispuesto en los acuerdos pertinentes entre las partes.

9.13.2 Disputas con Suscriptores Usuarios Finales o Partes que Confían

Dentro de los límites permitidos por la legislación aplicable, los Acuerdos de Suscriptor y los Acuerdos de la Parte que Confía deberán contener una cláusula de resolución de disputas. Las disputas que involucren a E-Sign requieren un período de negociación inicial de sesenta (60) días, seguido de un litigio en el tribunal competente, en el caso de los reclamantes que son residentes de Chile, o, en el caso de todos los demás reclamantes, arbitraje administrado por la Cámara de Comercio Internacional (“ICC”), de conformidad con el Reglamento de Conciliación y Arbitraje de ICC, a menos que sea aprobado de otra manera por E-Sign.

9.14 Ley Aplicable

Sujeto a los límites que aparecen en la legislación aplicable, las leyes de la República de Chile, serán aplicadas a la ejecución, elaboración, interpretación y validez de esta CPS, independientemente del contrato u otra opción de aplicación de la ley y sin el requisito de establecer un nexo comercial en la República de Chile. Esta elección de la ley se hace para asegurar que los procedimientos e interpretación sean uniformes para todos los participantes del Subdominio E-Sign, sin importar dónde se encuentren.

Esta disposición respecto de la ley aplicable sólo se aplica a esta CPS. Los acuerdos que incorporen la CPS como referencia, pueden tener sus propias normas sobre aplicación de la ley, dado que esta Sección 9.14 regula la obligatoriedad, elaboración, interpretación y validez de los términos de la CPS por separado, y aparte de las restantes disposiciones de cualquiera de esos acuerdos, con sujeción a las limitaciones de la legislación aplicable.

9.15 Conformidad con la Ley aplicable

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

9.16 Disposiciones Varias

9.16.1 Acuerdo Completo

No es aplicable

9.16.2 Asignación

No es aplicable

9.16.3 Divisibilidad

En caso de que una cláusula o disposición de esta CPS se considere inaplicable por un tribunal de justicia u otro tribunal competente, el resto de la CPS seguirá siendo válida.

9.16.4 Cumplimiento (Honorarios de Abogado y Renuncia de Derechos)

No es aplicable

9.16.5 Fuerza Mayor

En la medida permitida por la legislación aplicable, Acuerdos de Suscriptor y Acuerdos Parte que Confía deberá incluir una cláusula de fuerza mayor que proteja a Symantec.

9.17 Otras Disposiciones

No es aplicable

Apéndice A. Tabla de Acrónimos y Definiciones

Tabla de Acrónimos

Término	Definición
<i>AICPA</i>	Instituto Americano de Auditores Públicos Certificados
<i>ACS</i>	Authenticated Content Signing (Firma de Contenido Autenticado)
<i>ANSI</i>	American National Standards Institute (Instituto de Estándares Nacionales Americano)
<i>AR</i>	Autoridad de Registro
<i>ASB</i>	Authentication Service Bureau (Oficina de Servicios de Autenticación)
<i>BIS</i>	Bureau of Industry and Science (Oficina de Industria y Ciencia del Departamento de Comercio de Estados Unidos)
<i>CA</i>	Certification Authority (Autoridad de Certificación)
<i>ccTLD</i>	Código País, dominio de nivel superior
<i>CP</i>	Certificate Policy (Política de Certificados)
<i>CPS</i>	Certification Practice Statement (Declaración de Prácticas de Certificación)
<i>CRL</i>	Certificate Revocation List (Lista de revocación de certificados)
<i>DBA</i>	Haciendo negocios como
<i>DNS</i>	Sistema de Nombres de Dominio
<i>DN</i>	Distinguished Name (Nombre Distinguido)
<i>EAL</i>	Evaluation Assurance Level (Nivel de seguridad de evaluación, de acuerdo a Common Criteria).
<i>FIPS</i>	Federal Information Processing Standards
<i>FQDN</i>	Nombre de dominio completamente calificado
<i>ICC</i>	International Chamber of Commerce (Cámara Internacional de Comercio)
<i>IM</i>	Mensaje instantáneo
<i>IANA</i>	Autoridad de Asignación de Números de Internet
<i>ICANN</i>	Corporación de Internet para la Asignación de Nombres y Números
<i>ISO</i>	Organización Internacional de Normalización
<i>KRB</i>	Key Recovery Block (Bloque de recuperación de llave)
<i>LSVA</i>	Logical security vulnerability Assessment (Evaluación de vulnerabilidades de seguridad lógica)
<i>NIST</i>	Instituto Nacional de Estándares y Tecnología (USA)
<i>OCSP</i>	Online Certificate Status Protocol (Protocolo de Estado de Certificado en Línea)
<i>OID</i>	Identificador de objetos
<i>PCA</i>	Primary Certification Authority (Autoridad Primaria de Certificación)
<i>PIN</i>	Personal Identification Number (Número de identificación personal).
<i>PKCS</i>	Public-Key Cryptography Standard (Norma de Criptografía de Llave Pública)
<i>PKI</i>	Public Key Infrastructure (Infraestructura de Llave Pública).
<i>PMA</i>	Policy Management Authority (Autoridad de Administración de Políticas).
<i>RA</i>	Registration Authority (Autoridad de Registro).
<i>RFC</i>	Request For Comment
<i>SAS</i>	Statement on Auditing Standards (Declaración de Normas de Auditoría, promulgada por el Instituto Americano de Contadores Públicos Certificados, AICPA)
<i>S/MIME</i>	Secure Multipurpose Internet Mail Extensions (Extensiones de correo multipropósito).
<i>SSL</i>	Secure Sockets Layer (Capa de sockets segura)
<i>STN</i>	Symantec Trust Network
<i>TLD</i>	Dominio de nivel superior
<i>TLS</i>	Seguridad en la capa de transporte
<i>VOID</i>	Protocolo de voz por internet

Definiciones

Término	Definición
Acuerdo de Parte que Confía	Un acuerdo usado por una CA que fija los términos y condiciones bajo los cuales un individuo u organización actúa como una Parte que Confía.

Acuerdo de Suscriptor	Un acuerdo usado por una CA o RA para fijar los términos y condiciones bajo los cuales un individuo o una organización actúan como Suscriptor.
Acuerdo de Uso de CRL	Un acuerdo que fija los términos y condiciones bajo los cuales se puede usar una CRL o la información que contiene.
Administración Automática	Un procedimiento por el que las Solicitudes de Certificado son aprobadas automáticamente si la información de inscripción concuerda con la información de la base de datos.
Administrador	Una persona de confianza dentro de la organización de un Centro de Procesamiento, Service Center, Cliente de Certificados Administrables o que ejecute la validación y otras funciones CA o RA.
Administrador de Key Manager	Un Administrador que lleva a cabo funciones de generación y recuperación de llaves para un Cliente Managed PKI usando Key Manager de Managed PKI.
Administrador de Managed PKI (MPKI)	Un Administrador que realiza validación u otras funciones de RA para un Cliente de Managed PKI (MPKI).
Afiliado	Un tercero de confianza líder, por ejemplo en la industria tecnológica, financiera o de telecomunicaciones, que ha entrado en un acuerdo con Symantec para ser un canal de distribución y servicios de la STN dentro de un territorio específico.
Auditoria de Cumplimiento	Una auditoria periódica de un Centro de Procesamiento, Service Centers, Cliente de Certificados Administrables, o para determinar la conformidad con los estándares de la Symantec Trust Network que sean aplicables.
Autenticación Manual	Un procedimiento mediante el cual las Solicitudes de Certificado son revisadas y aprobadas manualmente una a una por un Administrador usando una interfaz basada en Web.
Autoridad de Certificación (CA)	Una entidad autorizada a emitir, gestionar, revocar y renovar los Certificados dentro de la STN.
Autoridad de Certificación Intermedia (CA Intermedia)	Una Autoridad de Certificación cuyo Certificado se encuentra en una Cadena de Certificado entre el Certificado de la CA raíz y el Certificado de la Autoridad de Certificación que emitió el Certificado Suscriptor usuario final.
Autoridad de Certificación Primaria (PCA)	Una CA que actúa como CA raíz para una Clase de Certificados específica y emite Certificados a las CAs subordinadas a ella.
Bloque de Recuperación de Llave (KRB)	Una estructura de datos que contiene una llave privada de Suscriptor que está encriptada usando una llave de encriptación. Los KRBs se generan usando el software Key Manager de Managed PKI (MPKI).
CA en Línea	Las CAs que firman Certificados de Suscriptores usuarios finales que son mantenidas en línea de manera de proporcionar servicios de firma continuos.
CA Fuera de Línea	PCAs de la STN, CAs Raíz emisoras y otras CAs intermedias designadas que son mantenidas fuera de línea por motivos de seguridad para protegerlas de posibles ataques por parte de intrusos mediante la red. Estas CAs no firman directamente Certificados de Suscriptores usuarios finales.
CA RSA Secure Server	La Autoridad de Certificación que emite IDs Secure Server.
Cadena de Certificación	Una lista ordenada de Certificados que contiene un Certificado Suscriptor usuario final y Certificados de CA, que termina en un Certificado raíz.

Centro de Control de Managed PKI (MPKI)	Una interfase basada en Web que permite a Administradores de Managed PKI (MPKI) ejecutar Autenticación Manual de Solicitudes de Certificados.
Centro de Procesamiento	Una organización (Symantec) que crea un recinto seguro que alberga, entre otras cosas, los módulos criptográficos usados para emitir Certificados. En las líneas de negocios de Consumidor y Sitio Web, los Centros de Procesamiento actúan como CAs dentro de la red STN y ejecutan todos los servicios del ciclo de vida del Certificado de emisión, administración, revocación y renovación de Certificados. En la línea de negocios Empresarial, los Centros de Procesamiento entregan servicios de ciclo de vida en nombre de sus Clientes Managed PKI (MPKI) o de los Clientes Managed PKI (MPKI) de los Centros de Servicios subordinados a ellos.
Centro de Servicio	Un modelo de operación que no mantiene unidades de firma de Certificados para la emisión de Certificados para el propósito de emitir Certificados de una clase o tipo específica, sino que depende de un Centro de Procesamiento para ejecutar la emisión, administración, revocación y renovación de tales Certificados.
Ceremonia de Generación de Llave	Un procedimiento mediante el cual es generado un par de llaves de CA o RA, su llave privada es transferida a un modulo criptográfico, su llave privada es respaldada y/o su llave pública es certificada.
Certificado	Un mensaje que, al menos, dice el nombre o identifica la CA, identifica el Suscriptor, contiene la llave pública del Suscriptor, identifica el Periodo Operacional del Certificado, contiene un número de serie de Certificado y está firmado digitalmente por la CA.E-SignE-Sign
Certificado Secure Server	Un Certificado organizacional Class 3 usado para soportar sesiones SSL entre navegadores web y servidores web.
Certificado a Nivel Minorista	Un Certificado emitido por E-Sign, que actúa como CA, a individuos u organizaciones que envían solicitudes una a una a E-Sign en su sitio Web.
Certificado de Administrador	Un Certificado emitido a un Administrador que solo puede ser usado para ejecutar funciones CA o RA.
Class	Un nivel específico de seguridad como se define dentro de la CP. Ver CP § 1.1.1.
Cliente	Una organización que es Cliente Managed PKI, Cliente Gateway o Cliente ASB.
Compromiso	Una violación (o sospecha de violación) de una política de seguridad, en que puede haber ocurrido la divulgación de o pérdida de control sobre información delicada. En relación con las llaves privadas, un Compromiso es la pérdida, robo, divulgación, modificación, uso no autorizado u otro compromiso de la seguridad de tal llave privada.
Declaración de Prácticas de Certificación (CPS)	Una declaración de las prácticas que E-Sign emplea al aprobar o rechazar las Solicitudes de Certificado y al emitir, gestionar y revocar Certificados, y requiere que sus Clientes de Managed PKI y sus Clientes Gateway usen.
Derechos de Propiedad Intelectual	Derechos bajo uno o más de los siguientes: cualquier derecho de copia, patente, secreto comercial, marca registrada y otros derechos de propiedad intelectual.
DN	Nombre distintivo (Distinguished name)
Empresa, según se usa en Cliente Empresarial	Una línea de negocios que usa un Afiliado para dar servicios de Managed PKI (MPKI) para Clientes Managed PKI (MPKI).
Entidad Superior	Una entidad sobre cierta entidad dentro de una jerarquía STN (la jerarquía Class 1, 2 o 3)

Estándares STN	Los requisitos de negocios, legales y técnicos para emitir, administrar, revocar, renovar y usar Certificados en la red STN.
Frase Secreta	Una frase secreta elegida por un Postulante de Certificado durante la inscripción de un Certificado. Cuando se emite un Certificado el Solicitante de Certificado se convierte en Suscriptor y una CA o una RA pueden usar la Frase Secreta para autenticar al Suscriptor cuando el Suscriptor busca revocar o renovar el Certificado del Suscriptor.
Guía de Administrador de Servicio de Gestión de Llaves Managed PKI	Un documento que establece los requerimientos y prácticas operacionales para Clientes Managed PKI que usan Key Manager de Managed PKI.
Guía de Requerimientos de Prácticas Legales del Afiliado	Un documento Symantec que contiene requisitos para las CPS, acuerdos, procedimientos de validación y políticas de privacidad del Afiliado, así como otros requerimientos que el Afiliado debe cumplir.
Guía de Requisitos de Auditoria y Seguridad (SAR)	Un documento Symantec que fija los requisitos de seguridad y auditoria y las practicas para Centros de Procesamiento y Centros de Servicios.
Individuo Afiliado	Una personal natural que esté relacionada con un Cliente Managed PKI, un Cliente Managed PKI Lite o una entidad de Cliente Gateway (i) como gerente, director, empleado, socio, contratista, practicante u otra persona en la entidad, (ii) como miembro de una comunidad de interés registrada en Symantec o (iii) como una persona que tenga una relación con la entidad donde la entidad tenga negocios u otros registros que den seguridad adecuadas de la identidad de tal persona.
Información Confidencial /Privada	Información que debe ser mantenida en calidad de confidencial y privada de acuerdo: CP §2.8.1.
Información No Verificada de Suscriptor	Información enviada por un Solicitante de Certificado a una CA o RA, e incluida dentro de un Certificado, que no haya sido confirmada por la CA o RA y por la que la CA o RA aplicable no entrega otra seguridad aparte de que la información fue proporcionada por el Solicitante del Certificado.
Infraestructura de Llave Pública (PKI)	La arquitectura, organización, técnicas, prácticas y procedimientos que apoyan colectivamente la implementación y operación de un sistema criptográfico de Llave pública basado en Certificados. El PKI Symantec Trust Network consiste de sistemas que colaboran para entregar e implementar la Symantec Trust Network.
Investigación/Auditoria Exigente	Una auditoria o investigación de Symantec en que Symantec tiene motivos para creer que ha ocurrido una falta de una entidad para cumplir los estándares Symantec Trust Network , un incidente o Compromiso en relación con la entidad, o una amenaza real o potencial a la seguridad de la STN.
Jerarquía RSA Secure Server	La jerarquía PKI compuesta por la Autoridad de Certificación de RSA Secure Server.
Key Manager de Managed PKI	Una solución de recuperación de llaves para aquellos Clientes de Managed PKI que optan por implementar recuperación de llaves bajo un Acuerdo especial de Managed PKI.

Lista de Revocación de certificados (CRL)	Una lista emitida periódicamente, firmada digitalmente por una CA, de Certificados identificados que han sido revocados antes de su fecha de expiración de acuerdo con CP 3.4. El listado generalmente indica el nombre del emisor del CRL, la fecha de emisión, la fecha de la siguiente emisión, los números de serie revocados y los momentos y motivos específicos de los rechazos.
Managed PKI (MPKI)	Un servicio de PKI administrable totalmente integrado ofrecido por E-Sign que permite a Clientes empresariales de E-Sign la distribución de Certificados a individuos, como empleados, socios, proveedores, y clientes, al igual que a dispositivos, como servidores, enrutadores y firewalls. Managed PKI permite a las empresas asegurar aplicaciones de mensajería, intranet, extranet, red privada virtual y comercio electrónico.
Modulo de Software de Administración Automatizada	Software proporcionado por E-Sign que ejecuta Administración Automatizada.
No Repudio	Un atributo que una comunicación que entrega protección contra una parte de una comunicación que niegue falsamente su origen, negando que fue enviada o negando su entrega. La negación de origen incluye la negación de que la Comunicación se origino de la misma fuente que una secuencia de uno o más mensajes anteriores, aun si la identidad asociada al remitente es desconocida. Nota: solo una adjudicación de una corte, panel de arbitraje u otro tribunal puede evitar el repudio. Por ejemplo, una firma digital verificada con referencia a un Certificado STN puede entregar prueba en apoyo de una determinación de No-Repudio por parte de un tribunal, pero por si misma no constituye No-Repudio.
Objetivos de Control de Administración de Certificados	Criterios que una entidad debe cumplir para satisfacer una Auditoria de Cumplimiento.
Parte que Confía	Un individuo u organización que actúa confiando en un certificado y/o firma digital.
Parte Secreta	Una parte de una Llave privada de CA o una parte de los datos de activación necesarios para operar una Llave privada de CA bajo el Acuerdo de Partición de Secreto.
Partición de Secreto	La práctica de dividir una llave privada de CA o los datos de activación para operar una llave privada de CA para imponer el control multi personal en las operaciones de llave privada de CA bajo CP 6.2.2.
Participante STN	Un individuo u organización que es uno o más de los siguientes dentro de la red STN: Symantec, E-Sign, un Cliente, un Centro de Servicio Universal, un Revendedor, un Suscriptor o una Parte que Confía.
Periodo Operacional	El periodo que comienza en la fecha y hora de emisión de un Certificado (o en una fecha posterior y hora fijada en el Certificado) y que termina con la fecha y hora en que el Certificado vence o es revocado.
Persona de Confianza	Un empleado, contratista o consultor de una entidad dentro de la red STN responsable por la administración de confianza infraestructural de la entidad, sus productos, sus servicios, sus instalaciones y/o sus practicas como se definen en CP § 5.2.1.
PKCS #10	Estándar de Criptografía de Llave Pública #10, desarrollado por RSA Security Inc., que define una estructura para una Solicitud de Firma de Certificado.
PKCS #12	Estándar de Criptografía de Llave Pública #12, desarrollado o RSA Security Inc que define una forma segura para la transferencia de llaves privadas.

Plan de Protección NetSure	Un programa de garantía extendida que se describe en CP 9.2.3.
PMA	La organización en E-Sign responsable por promulgar políticas en la red STN.
Políticas de Certificado	El documento llamado "Políticas de Certificado de la Symantec Trust Network" y es la principal declaración de política de gobierno la Symantec Trust Network
Posición de Confianza	Los cargos en una entidad STN que deben ser ocupados por una Persona de Confianza.
Protocolo de Estado de Certificado En Línea (OCSP)	Un protocolo para entregar a las Partes que Confían información de estado de Certificados en tiempo real.
Proveedor de Aplicación	Un desarrollador de software de navegación Internet u otro software que muestra o utiliza certificados y distribuye certificados raíz como KDE, Microsoft Corporation, Mozilla Corporation, Opera Software ASA, y Red Hat, Inc.
RA	Una entidad aprobada por una CA para apoyar a los Solicitantes de Certificados para solicitar Certificados, y para aprobar o rechazar solicitudes de Certificados, revocar Certificados o renovar Certificados.
Repositorio Symantec	La base de datos Symantec de Certificados y otra información relevante de la red STN accesible en línea.
Revendedor	Una entidad que presta servicios de comercialización en nombre de E-Sign a mercados específicos.
Revisión complementaria de administración de riesgos	Una revisión de una entidad por Symantec que sigue a los hallazgos incompletos o excepcionales en una Auditoria de Cumplimiento de la entidad, o como parte del proceso de administración del riesgo global en el curso regular del negocio.
Revisión de Practicas y Seguridad	La revisión a E-Sign ejecutada por Symantec antes que E-Sign iniciara sus operaciones.
RSA	Un sistema criptográfico de Llave pública inventado por Rivest, Shamir y Adleman.
Secure Sockets Layer (SSL)	El método estándar de la industria desarrollado por Netscape Communications Corporation para proteger comunicaciones en la Web. El protocolo de seguridad SSL proporciona encriptación de datos, autenticación de servidor, integridad de mensajes, y opcionalmente autenticación de cliente para una conexión TCP/IP.
Service Center de Cliente	Un Service Center que es un Afiliado que entrega Certificados de cliente tanto en la línea de negocios de Consumidor o Empresarial.
Servicio de Notaria Digital Symantec	Un servicio ofrecido a Clientes Managed PKI (MPKI) que entrega un comprobante firmado digitalmente (un Recibo Digital) de que un documento o un conjunto de datos puntuales existieron en un momento dado.
Servicio de Recuperación de Llaves	Un servicio E-Sign que entrega llaves de encriptación necesarias para recuperar un Bloque de Recuperación de Llave como parte del uso de Key Manager de Managed PKI por un Cliente Managed PKI (MPKI) para recuperar la Llave privada de un Suscriptor.
Sistema de Confianza	Hardware, software y procedimientos de computación que estén razonablemente asegurados contra intromisión y mal uso; entregan un nivel razonable de disponibilidad, confiabilidad y operación correcta; están equipados razonablemente para ejecutar sus funciones originales; e imponen la política de seguridad aplicable. Un Sistema de Confianza no necesariamente es un "sistema confiable" como se reconoce en la nomenclatura clasificada de gobierno.

Solicitante de Certificado	Un individuo u organización que solicita la emisión de un certificado por una CA
Solicitud de Certificado	Una solicitud de un Postulante de Certificado (o agente autorizado del Postulante de Certificado) a un CA para la emisión de un Certificado.
Solicitud de Firma de Certificado (CSR)	Un mensaje que contiene una solicitud para emitir un Certificado.
Subdominio	La parte de la red STN bajo el control de una entidad y todas las entidades subordinadas a ella dentro de la jerarquía STN.
Sujeto	El tenedor de una llave privada que corresponde a una llave pública. El término "Sujeto" puede, en el caso de un Certificado organizacional, se refiere al equipo o dispositivo que contiene una llave privada. Al Sujeto se le asigna un nombre no ambiguo, que está ligado a la llave pública contenida en el Certificado del Sujeto.
Suscriptor	En el caso de un Certificado Individual. La persona que es el Sujeto de, y a la cual le ha sido emitido, un Certificado. En el caso de un Certificado organizacional, una organización que es dueña del equipo o dispositivo que es el Sujeto de, y al cual le ha sido emitido, un Certificado. Un Suscriptor es capaz de usar, y está autorizado a usar, la llave provada que corresponde a la llave pública listada en el Certificado.
Symantec	Significa, con respecto a cada porción pertinente de esta CPS, Symantec Corporation y/o cualquier subsidiaria propiedad completa de Symantec responsable de las operaciones específicas en la emisión.
Symantec Trust Network (STN)	La Infraestructura de Llave Pública basada en Certificado regida por las Políticas de Certificados de la Symantec Trust Network, que permite el despliegue y uso de Certificados a nivel mundial por Symantec, E-Sign y sus Clientes, Suscriptores y Partes que Confían.

Apéndice B. Historial de Cambios

Historial de Cambios: versión 3.8.8

Descripción	Sección y Cambios realizados
<p>Se incorporan cambios para cumplimiento de Requisitos CABF</p>	<p>1 <u>Las CA dentro de la jerarquía de la Symantec Trust Network se ajustan a la versión actual de los requisitos de CA/ Browser Forum (línea de base CABF) para la emisión y gestión de los certificados públicos de confianza publicados en www.cabforum.org. En el caso de cualquier incompatibilidad entre este documento y esos requisitos, dichos requisitos tendrán prioridad sobre este documento.</u></p> <p><u>En este momento, los certificados SSL de validación de dominio y de validación de organización emitidos por las CA de E-Sign en el marco de las presentes CPS se rigen por los requisitos CABF. Estos certificados son emitidos conteniendo el identificador de la política correspondiente (s) especificado en la sección 1.2 de la CP que señala la adhesión y cumplimiento de estos requisitos. Las CA de E-Sign afirman que todos los Certificados emitidos que contienen dichos identificador(es) de la política son emitidos y administrados de conformidad con los requisitos CABF.</u></p> <p><u>El sub-dominio de E-Sign en la STN, se encuentra certificado por la CA de Symantec Trust Network y opera en cumplimiento de los requisitos de la Declaración de Prácticas de Certificación de E-Sign.</u></p> <p>1.2 <u>Los certificados SSL de validación de dominio y de organización contienen el valor 2.16.840.1.113733.1.7.54 que indica la adhesión y el cumplimiento de los requisitos básicos de CA / Browser Forum.</u></p> <p>1.3.1 <u>Las CAs Universal Root emiten CAs subordinadas Clase 3 y en casos especiales, Clase 2.</u></p> <p>1.3.5 <u>1.3.5 Beneficiarios de los certificados</u> <u>Los beneficiarios de los certificados son identificados de acuerdo con las directrices de CA / Browser Forum. Los beneficiarios de los Certificados de las CA de E-Sign incluyen, pero no están limitados a:</u></p> <ol style="list-style-type: none"> <u>1. El suscriptor que es parte en el Acuerdo de Suscriptor de Certificado;</u> <u>2. Todos los proveedores de aplicaciones de software con los que la entidad emisora raíz se ha celebrado un contrato para la inclusión de su certificado raíz en el software distribuido por dicho proveedor de aplicación de software, y</u> <u>3. Todas las Partes que Confían que razonablemente confían en un Certificado Válido</u> <p>3.1.1.1 Se incorporan Requisitos CABF para Nombres</p> <p>3.2.2.1 Se incorporan Requisitos CABF para Verificación de Solicitantes Organizacionales</p> <p>4.1.2.2 Se incorporan Requisitos CABF para Solicitudes de Certificados</p> <p>4.3.3 Se incorporan Requisitos CABF para la Emisión de Certificados por una</p>

	<p>CA Raíz</p> <p>4.9.1.1 Se incorporan Requisitos CABF para Razones para Revocación</p> <p>4.9.3.2 Se incorporan Requisitos CABF para el Proceso de Revocación de Certificados</p> <p>4.9.7.1 Se incorporan Requisitos CABF para Emisión de CRL</p> <p>4.9.9.1 Se incorporan Requisitos CABF para la Disponibilidad de OCSP</p> <p>4.10.2 <u>Para certificados SSL con Organización validada y Dominio validado, las capacidades CRL y OCSP deberán proporcionar un tiempo de respuesta de diez (10) segundos o menos bajo condiciones de operación normal.</u></p> <p>5.3.3.1 Se incorporan Requisitos CABF para Capacitación y Nivel de Habilidades</p> <p>5.7.4 Se incorporan Requisitos CABF para Plan de Recuperación de Desastres</p> <p>6.1.5.1 Se incorporan Requisitos CABF para los Tamaños de Llave</p> <p>7.1.2.2.1 Se incorporan Requisitos CABF para la Extensión Políticas de Certificado</p> <p>7.1.6.1 Se incorporan Requisitos CABF para el Identificador de Objeto Certificate Policy</p> <p>7.3 <u>Requisitos CABF para Firma de OCSP</u></p> <p><u>Los certificados SSL con Dominio validado y Organización validada adhieren a los requisitos de CA/Browser Forum Baseline. Las respuestas OCSP se ajustarán a las especificaciones de RFC5019 y son:</u></p> <ul style="list-style-type: none"> <u>• Firmadas por la CA que emitió los Certificados cuyo estado de revocación está siendo comprobado, o</u> <u>• Firmadas por un Respondedor OCSP cuyo Certificado está firmado por la CA que emitió el Certificado, cuyo estado de revocación está siendo comprobado. Tal Certificado de firma de Respondedor OCSP deberá contener la extensión id-pkix-ocsp-nocheck como se define en RFC2560.</u> <p>8 <u>Los certificados SSL con Dominio validado y Organización validada adhieren a los requisitos de CA/Browser Forum Baseline E-Sign deberá llevar a cabo auto auditorías para supervisar la adherencia a su Política de Certificados y requisitos CPS y controlar estrictamente la calidad de su servicio al menos trimestralmente contra una muestra seleccionada aleatoriamente del mayor entre un Certificado y al menos el 3% de los Certificados emitidos durante el período que comienza inmediatamente después de que la muestra de la auto auditoría previa</u></p>
--	--

	<p><u>haya sido tomada.</u></p> <p>9.6.1.1</p> <p>Se incorporan Requisitos CABF para Garantías y Obligaciones CABF</p>
Se clarifica la verificación de OU	<p>3.2.4</p> <ul style="list-style-type: none"> • Unidad Organizacional (OU) con ciertas excepciones⁸ <p>⁸ Los certificados con Dominio validado y Organización Validada pueden contener valores de Unidad Organizacional que estén validados</p>
Se actualiza descripción del mecanismo disponible para custodia y recuperación de llaves	<p>4.12</p> <p>Los clientes empresariales que utilizan <u>la opción Key Escrow dentro de Managed PKI Key Management Service (KMS) de Symantec</u> pueden custodiar copias de las llaves privadas de Suscriptores cuyas Solicitudes de Certificado aprueban. La empresa cliente puede <u>utilizar KMS custodiar llaves ya sea enoperado con</u> las instalaciones de la empresa o <u>enen</u> el centro de datos seguro de Symantec.</p> <p>4.12.1</p> <p>Los clientes Empresariales que utilizan <u>la opción Key Escrow dentro del servicio Managed PKI de Symantec Key Management Service</u> (o un servicio equivalente aprobado por Symantec) están autorizados para custodiar llaves privadas de los Suscriptores usuarios finales.</p> <p>4.12.1</p> <p>Se recomienda que los Clientes Empresariales que usen <u>KMS la opción Key Escrow dentro de Managed PKI Service de Symantec</u>:</p> <ul style="list-style-type: none"> • Notifiquen a los suscriptores que sus llaves privadas son custodiadas
Actualización del contenido de logs de eventos	<p>5.4.1</p> <p>Las entradas del registro incluyen los siguientes elementos:</p> <ul style="list-style-type: none"> • Fecha y hora de la entrada • Número de serie o secuencia de entrada, para entradas en bitácora diaria automática • Identidad de la entidad que ingresa el registro en la bitácora • <u>Descripción</u>/tipo de entrada.

Se agrega mejoramiento de proceso de Log	<p>5.4.2 Los registros de auditoría son examinados por lo menos una vez por semana El sistema y los logs de auditoría de la CA son monitoreados continuamente para proporcionar alertas en tiempo real de para sucesos de seguridad y operativos funcionamiento significativos.</p>
BCP actualizado con migración a Symantec	<p>5.7.4 Se reemplaza la descripción del Plan de Continuidad de Negocios de Verisign por el PCN de Verisign</p>
Declaración de Seguridad de Datos	<p>5.9 Se incorpora declaración de Seguridad de Datos</p> <p>5.9.1 Se incorpora declaración de objetivos de Seguridad de Datos</p> <p>5.9.2 Se incorpora declaración de evaluación de riesgos</p> <p>5.9.3 Se incorpora declaración de plan de seguridad</p>
La excepción para extender la validez de llaves de CA desfasadas de 1024-bits más allá de 14 años y limitadas a una validez máxima hasta el 31 de Agosto de 2012 y disponible sólo hasta el 31 de Diciembre de 2011	<p>6.1.5 La norma E-Sign para el tamaño mínimo de las llaves es el uso de pares de llaves equivalentes en fuerza a 2048 bits RSA para CA Primarias y CAs¹³.</p> <p>¹³ La confianza de la CA está extendida para las Raíces de Confianza desfasadas de primera y segunda generación (G1 y G2) de Symantec con pares de llaves RSA de 1024 bits para soporte de plataformas desfasadas de cliente y pueden ser emitidos certificados de usuario final de 1024 bits RSA con expiración en o antes del 31 de Diciembre de 2011. Para preservar la continuidad de negocios de aplicaciones desfasadas más allá del 2011, serán permitidas excepciones individuales adicionales con aprobación previa <u>para afiliados de Symantec Corporation que operen las capacidades de software de Processing.Center de acuerdo con la sección 6.3.2.</u></p> <p>6.3.2 <u>En términos de la Sección 6.3.2 de la CP STN, el PMA de Symantec ha aprobado una excepción para extender un número limitado de CAs más allá de los límites especificados, para asegurar servicios PKI ininterrumpidos durante una migración de los pares de llaves de la CA. Esta excepción puede ser aplicada a E-Sign cuando opera las capacidades de software de Processing Center solamente para infraestructura y CAs de Administradores que no estén asociadas a CAs que emitan certificados SSL. Esta excepción no puede ser utilizada para extender la validez de una CA más allá de una validez total de 14 años hasta un máximo en el 31 de Agosto de 2014, y no puede estar disponible después del 31 de Diciembre de 2011.</u></p>

<p>Extiende del periodo de validez de certificados de 2 a 3 años antes de requerir renovación o regeneración de llaves.</p>	<p>6.3.2</p> <table border="1" data-bbox="603 219 1481 387"> <thead> <tr> <th data-bbox="603 219 979 248">Certificado Emitido Por:</th> <th data-bbox="984 219 1481 248">Periodo de Validez</th> </tr> </thead> <tbody> <tr> <td data-bbox="603 255 979 387">CA en Línea para Suscriptor usuario final individual</td> <td data-bbox="984 255 1481 387">Normalmente hasta 2 3 años, pero en las condiciones descritas abajo, hasta 6 años sin opción de renovar o reasignar la llave. Después de 6 años se requiere un nuevo enrolamiento</td> </tr> </tbody> </table> <p>Los certificados emitidos por las CAs a Suscriptores usuarios finales pueden tener periodos operacionales de más de des tres años, hasta seis años, si los siguientes requerimientos son satisfechos:</p> <ul style="list-style-type: none"> Protección de los pares de llaves de Suscriptor en relación con su ambiente operacional para Certificados Organizacionales, operación dentro de la protección mejorada de un centro de datos y para Certificados Individuales, los pares de llaves de los suscriptores residen en un dispositivo de hardware, como tarjeta inteligente 	Certificado Emitido Por:	Periodo de Validez	CA en Línea para Suscriptor usuario final individual	Normalmente hasta 2 3 años, pero en las condiciones descritas abajo, hasta 6 años sin opción de renovar o reasignar la llave. Después de 6 años se requiere un nuevo enrolamiento
Certificado Emitido Por:	Periodo de Validez				
CA en Línea para Suscriptor usuario final individual	Normalmente hasta 2 3 años, pero en las condiciones descritas abajo, hasta 6 años sin opción de renovar o reasignar la llave. Después de 6 años se requiere un nuevo enrolamiento				
<p>Clarificación respecto del soporte de RFC 5280</p>	<p>7.1</p> <p>Los Certificados de E-Sign se ajustan en general a (a) Recomendación ITU-T X.509 de (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, Junio 1997 y (b) RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, Abril 2002 ("RFC 5280")²⁰.</p> <p><u>²⁰ Aun cuando los certificados STN generalmente adhieren a RFC 5280, ciertas provisiones limitadas pueden no estar soportadas.</u></p>				
<p>Clarificación respecto del soporte de los requerimientos CABF</p>	<p>7.1</p> <p><u>En tanto sea aplicable al tipo de Certificado, los Certificados STN adhieren a la versión vigente de CA/Browser Forum Baseline Requirements para la Emisión y Gestión de Certificados de Confianza Pública.</u></p>				
<p>Actualización de requerimientos para el número de serie del certificado</p>	<p>7.1</p> <table border="1" data-bbox="603 1095 1481 1180"> <thead> <tr> <th data-bbox="603 1095 826 1124">Campo</th> <th data-bbox="831 1095 1481 1124">Valor o restricción de Valor</th> </tr> </thead> <tbody> <tr> <td data-bbox="603 1131 826 1180">Número de serie</td> <td data-bbox="831 1131 1481 1180">Valor único por DN de Emisor que muestra al menos 20 bits de entropía</td> </tr> </tbody> </table>	Campo	Valor o restricción de Valor	Número de serie	Valor único por DN de Emisor que muestra al menos 20 bits de entropía
Campo	Valor o restricción de Valor				
Número de serie	Valor único por DN de Emisor que muestra al menos 20 bits de entropía				
<p>Actualización de requerimientos para las formas de nombres en el certificado</p>	<p>7.1.4</p> <p>E-Sign completa los Certificados de la STN con un Nombre Distinguido del Emisor y un Nombre Distinguido del Sujeto de acuerdo a la Sección 3.1.1. <u>El Nombre del Emisor deberá ser completado en cada Certificado emitido conteniendo el País, Nombre de Organización y el Nombre Común de la CA Emisora.</u></p>				
<p>Actualización respecto de las normas aplicables al perfil de CRLs</p>	<p>7.2</p> <p><u>En tanto sea aplicable al tipo de certificado, las CRL correspondientes se ajustan a los requisitos de la versión actual de CA/Browser Forum Baseline Requirements para la Emisión y Gestión de Certificados de Confianza Pública.</u></p> <p>Las CRL <u>Versión 2 se ajustan a las especificaciones de RFC 5280 y</u> contienen los campos y contenidos básicos especificados en la Tabla 13 a continuación:</p>				
<p>Clarificación de la versión del examen WebTrust para Autoridades de Certificación</p>	<p>8</p> <p>Un examen anual de WebTrust para Autoridades de Certificación versión 2.0 o superior (o equivalente) se lleva a cabo para las operaciones de los centros de datos de E-Sign</p>				
<p>Clarificación de condiciones de evaluaciones</p>	<p>8.1</p> <p><u>Las auditorías son llevadas a cabo sobre secuencias ininterrumpidas de períodos de auditoría con cada período con una duración no mayor a un año.</u></p>				

<p>Agrega condiciones para la calificación de Evaluador</p>	<p>8.2 Las auditorías de cumplimiento de la CA de E-Sign son realizadas por una firma de contadores públicos que:</p> <ul style="list-style-type: none"> • <u>Demuestra dominio en la realización de WebTrust para Certification Authorities v2.0 o</u> • Demuestra dominio de la tecnología de infraestructura de llave pública, herramientas y técnicas de seguridad de la información, auditoría de seguridad, y la función de certificación de terceros, y • Está acreditada por el Instituto Americano de Contadores Públicos Certificados (AICPA), que requiere la posesión de ciertas habilidades, las medidas de aseguramiento de la calidad, tales como revisión por pares, pruebas de competencia, normas con respecto a la asignación adecuada de personal para compromisos y requerimientos de educación profesional continua. • <u>Está regida por ley, regulación gubernamental, o código profesional de ética y</u> • <u>mantiene un seguro de responsabilidad profesional contra errores y omisiones con una póliza con límites de cobertura de al menos un millón de dólares.</u>
<p>Actualización respecto de condiciones para la comunicación de resultados de evaluación</p>	<p>8.6 Los resultados de las auditorías de cumplimiento y otras evaluaciones serán comunicadas a la Administración de E-Sign, a la Autoridad de Administración de Políticas (PMA) de E-Sign, así como también a otras entidades que considere la Administración de E-Sign. E-Sign pone a disposición del público su Informe de Auditoría anual a más tardar tres (3) meses después del final del período de la auditoría. En el caso de un retraso superior a tres meses, E-Sign deberá presentar una carta explicativa firmada por el Auditor Calificado. Una copia del informe de auditoría WebTrust para CAs de E-Sign puede ser encontrado en el repositorio de E-Sign en https://www.e-sign.cl/default/repositorio.</p>

<p>Actualización de las garantías vinculadas con certificados SSL de validación de dominio y organización, de conformidad con la CA / Browser Forum</p>	<p>9.17.1.1 Garantías y obligaciones CABF</p> <p>Los certificados SSL de validación de dominio y organización validados conforme a la CA / Browser Forum requisitos iniciales. Mediante la emisión de tal certificado, la entidad emisora de certificados hace aplicables las garantías que figuran en esta sección para los beneficiarios de certificados que figuran en la sección 1.3.5.</p> <p>La CA representa y garantiza a los beneficiarios de certificados que, durante el período en que el certificado es válido, la CA ha cumplido con estos requisitos y con su Política de Certificados y / o Declaración de Prácticas de Certificación en la emisión y la gestión del Certificado. Las garantías de certificados incluyen específicamente, pero no se limitan a, los siguientes:</p> <ol style="list-style-type: none"> 1. Derecho de Uso de los nombres de dominio o dirección IP: Que, en el momento de la emisión, la entidad emisora (i) implementó un procedimiento para verificar que el solicitante tenía derecho a usar, o tenía el control del nombre de dominio(s) y direcciones IP que figuran en el asunto del certificado y en la extensión subjectAltName (o se delegó a tal derecho o control por parte de alguien que tenía tal derecho a utilizar o controlar, sólo en el caso de nombres de dominio), (ii) ha seguido el procedimiento en la emisión del certificado, y (iii) describió acuciosamente el procedimiento en la Política de Certificado de la CA y / o Declaración de Prácticas de Certificación; 2. Autorización de Certificados: Que, en el momento de la emisión, la entidad emisora (i) implementó un procedimiento para verificar que el Sujeto autorizó la emisión del certificado y que el representante de la requirente está autorizado para solicitar el certificado en nombre del sujeto, (ii), seguido el procedimiento al emitir el Certificado, y (iii) el procedimiento descrito con precisión en la Política de Certificación de la CA y / o Declaración de Prácticas de Certificación; 3. Precisión de la Información: Que, en el momento de la emisión, la entidad emisora (i) implementó un procedimiento para verificar la exactitud de toda la información contenida en el certificado (con la excepción de la materia: el atributo organizationalUnitName), (ii) ha seguido el procedimiento en la emisión del certificado, y (iii) describió acuciosamente el procedimiento en la Política de Certificado de la CA y / o Declaración de Prácticas de Certificación; 4. Certeza de la información: Que, en el momento de la emisión, la entidad emisora (i) implementó un procedimiento para reducir la probabilidad de que la información contenida en el Certificado del sujeto (salvo el atributo organizationalUnitName) fuese engañoso, (ii) ha seguido el procedimiento en la emisión del certificado, y (iii) describió acuciosamente el procedimiento en la Política de Certificado de la CA y / o Declaración de Prácticas de Certificación; 5. Identidad del solicitante: Que, si el certificado contiene información sobre la identidad del sujeto, la CA (i) implementó un procedimiento para verificar la identidad del solicitante, de conformidad con los puntos 3.1.1.1 y 3.2.2.1, (ii) ha seguido el procedimiento en la emisión del certificado, y (iii) describió acuciosamente el procedimiento en la Política de Certificado de la CA y / o Declaración de Prácticas de Certificación; 6. Acuerdo de Suscriptor: Que, si la entidad emisora y el suscriptor no son Afiliados, el suscriptor y CA son partes de un Acuerdo de Suscriptor legalmente válido y exigible que cumpla estos requisitos, o, si la entidad emisora y el suscriptor están afiliados, el Representante del solicitante haya reconocido y aceptado las Condiciones de Uso; 7. Estado: Que la CA mantiene 24 x 7 un repositorio de acceso público con información actualizada sobre el estado (válido o revocado) de todos los certificados no vencidos, y 8. Revocación: Que el CA revocará el certificado por cualquiera de las razones especificadas en las presentes prescripciones. <p>Obligaciones de la CA Raíz</p> <p>La CA raíz será responsable por la ejecución y garantías de la CA subordinada, por el cumplimiento de dichos requisitos por la CA subordinada, y por todas las obligaciones de cumplimiento e indemnización de la CA subordinada, bajo estos requerimientos, como si la entidad emisora raíz hubiese sido la CA Subordinada emitiendo los certificados.</p>
---	---