CertiSur S.A.

Normas para el Proceso de Certificación

Para los Servicios de Certificación DigiCert bajo la Symantec Trust Network

Versión 3.3

Fecha de vigencia: 15 de Febrero de 2019

CertiSur S.A.
Av. Santa Fe 788, 2° Piso (C1059ABO) Buenos Aires, República Argentina
Teléfono (54 11) 4311 2457 www.certisur.com

Normas para el Proceso de Certificación de CertiSur S.A.

© 2019 CertiSur S.A. Todos los derechos reservados.

Fecha de Revisión: Enero de 2019

Importante – Información sobre Adquisición

El 31 de Octubre de 2017, DigiCert, Inc. perfeccionó la adquisición de la Unidad de Negocios Website Security de Symantec Corporation. Como resultado de dicha operación, DigiCert es ahora el propietario registrado de estas Normas para el Proceso de Certificación y los Servicios de Infraestructura de Clave Pública (PKI, por sus siglas en inglés) descriptos en este documento.

No obstante lo señalado, las referencias alternadas a "VeriSign", "Symantec" y "DigiCert" resultarán evidentes a lo largo del documento durante un cierto período de tiempo, hasta que resulte práctico desde el punto de vista operacional completar el cambio de nombre de las Autoridades Certificantes y sus servicios. Cualquier referencia a VeriSign o a Symantec como una corporación debe ser estrictamente considerada como un lenguaje anterior que solamente refleja históricamente la propiedad de los servicios.

Notificación de Derechos de Propiedad Intelectual. Marcas Registradas

Symantec, el logotipo de Symantec y marcas relacionadas son marcas registradas de Symantec Corporation o sus empresas vinculadas en Estados Unidos de Norte América y otros países. El logotipo de VeriSign, VeriSign Trust y otras marcas relacionadas son marcas registradas de VeriSign, Inc. o sus empresas vinculadas en Estados Unidos de Norte América y otros países. CertiSur y el logotipo de CertiSur son marcas registradas de propiedad de CertiSur S.A. Las demás marcas registradas y/o marcas de servicio mencionadas en este documento son propiedad de sus respectivos dueños.

Sin limitar los derechos mencionados más arriba y con excepción de los permisos citados en el próximo párrafo, ninguna parte de este documento puede ser reproducida, almacenada o introducida en cualquier sistema desde donde la información pueda ser recuperada o transmitida, de cualquier manera (electrónica, mecánica, fotocopiado, grabación, etc.), sin permiso escrito previo de parte de DigiCert, Inc. y/o CertiSur S.A.

Sin perjuicio de lo mencionado, se otorga el permiso de reproducir y distribuir estas Normas para el Proceso de Certificación de CertiSur S.A. en forma no exclusiva y sin pago de regalías, siempre que: (i) la notificación de los derechos de Propiedad Intelectual y de marcas registradas y los primeros párrafos de esta página aparezcan de manera destacada al principio de cada copia, y (ii) este documento sea reproducido en forma precisa, por completo, sin modificaciones, atribuyendo su autoría a DigiCert, Inc.

Las solicitudes para reproducir estas Normas para el Proceso de Certificación de CertiSur S.A., como así también la solicitud de copias, deben dirigirse a CertiSur S.A., Av. Santa Fe 788, 2° Piso, (C1059ABO) Buenos Aires, Argentina, Teléfono (54 11) 4311 2457, Fax (54 11) 4311 1450, Correo Electrónico: legal@certisur.com.

ÍNDICE

1. Introducción

Este documento constituye las Normas para el Proceso de Certificación de CertiSur S.A. ("CPS"). Establece los procedimientos que las Autoridades de Certificación de CertiSur S.A. ("AC") emplean para suministrar los servicios de certificación que incluyen, pero no se limitan, a la emisión, administración, revocación y renovación de certificados, en un todo de acuerdo con los requerimientos específicos de la Política de Certificación de DigiCert para la Symantec Trust Network ("Política de Certificación").

La Política de Certificación ("CP") constituye la disposición principal que regula la Symantec Trust Network ("STN"). Establece los requerimientos legales, técnicos y de negocio para la aprobación, emisión, administración, uso, revocación y renovación de Certificados digitales dentro de la Symantec Trust Network y la prestación de servicios de confianza asociados. Estos requerimientos, denominados "Requerimientos Estándar dentro de la STN" protegen la seguridad e integridad de la Symantec Trust Network, aplicables a todos sus participantes y, por ende, permiten asegurar un nivel de confianza uniforme a través de toda la Symantec Trust Network. Puede obtenerse mayor información acerca de la Symantec Trust Network y de los Requerimientos Estándar dentro de la STN en la Política de Certificación.

CertiSur S.A. ("CertiSur") tiene autoridad sobre una porción de la Symantec Trust Network, denominada "Subdominio CertiSur" dentro de la STN. El Subdominio CertiSur incluye las entidades subordinadas al mismo, como por ejemplo sus Clientes, Suscriptores y Partes Confiadas.

Mientras que la Política de Certificación establece los requerimientos que todos los Participantes de la STN deben cumplimentar, estas Normas para el Proceso de Certificación describen la forma en que CertiSur cumple con dichos requerimientos dentro del Subdominio CertiSur de la STN. Específicamente, estas Normas para el Proceso de Certificación establecen los procedimientos que CertiSur emplea para:

- administrar de manera segura la infraestructura que soporta la STN, y
- emitir, administrar, revocar y renovar los Certificados bajo la STN.

Todo ello dentro del Subdominio CertiSur dentro de la STN y de acuerdo con las exigencias de la Política de Certificación (CP) y los Requerimientos Estándar dentro de la STN.

Estas Normas cumplimentan, en lo referido a su elaboración, con lo previsto en el RFC 3647 de la Internet Engeneering Task Force (IETF) con relación a la Política de Certificación y a las Normas para el Proceso de Certificación. Las Autoridades Certificantes dentro de la jerarquía de la Symantec Trust Network cumplen la versión actual de los requerimientos del CA/Browser Forum, incluyendo:

- Requerimientos para la Emisión y Administración de Certificados de Validación Extendida (EV).
- Requerimientos para la Emisión y Administración de Certificados de Firma de Código de Validación Extendida (Code-Signing EV).

- Requerimientos Básicos para la Emisión y Administración de Certificados de Confianza Públicos.

Todos estos Requerimientos con arreglo a su publicación en el sitio Web www.cabforum.org. En caso de existir alguna inconsistencia entre el presente documento y los mencionados Requerimientos, dichos Requerimientos tendrán preeminencia sobre el presente.

En la actualidad, los Certificados SSL EV (Validación Extendida), de Firma de Código EV (Validación Extendida) y los Certificados SSL de Dominio Validado (DV) y de Organización (OV) Validada emitidos por las Autoridades Certificantes de DigiCert bajo las presentes Normas cumplen con los requerimientos del CA/Browser Forum. Estos Certificados de Dominio Validado (DV) y de Organización Validada (OV)[1] son emitidos incorporando el correspondiente identificador de política especificado en la Sección 1.2 de estas Normas, indicando la sujeción y el cumplimiento de dichos Requerimientos. Las Autoridades Certificantes de DigiCert afirman que todos los Certificados emitidos conteniendo estos identificadores de política son emitidos y administrados de acuerdo con los Requerimientos del CA/Browser Forum.

La Dirección de CertiSur y/o de DigiCert puede efectuar excepciones a esta política en casos individuales para mitigar impactos significativos a clientes, socios de negocio, partes confiadas y/o terceros dentro del ecosistema de certificados, en la medida en que no existan soluciones alternativas prácticas. Cada una de estas excepciones dispuestas por la Dirección son documentadas, analizadas e informadas como parte de los procesos de auditoría.

DigiCert no emite Certificados de Autoridades Certificantes Intermedias para inspección de SSL debajo de Autoridades Certificantes Raíz con Confianza Pública. Solamente Autoridades Certificantes Raíz que no posean o que no hayan tenido confianza dentro de productos de Proveedores de Aplicaciones de Software (con raíces privadas) pueden ser utilizadas para generar Autoridades Certificantes Intermedias empleadas para inspección de SSL.

A partir del 1º de Febrero de 2017, la Symantec Trust Network adopta la versión vigente de los Requerimientos Mínimos para la Emisión y Administración de Certificados de Firma de Código de Confianza Pública, tal como están publicados en https://aka.ms/csbr. En caso de existir alguna inconsistencia entre el presente documento y estos Requerimientos, estos últimos tendrán precedencia.

Los Certificados de Firma de Código emitidos a partir del 1º de Febrero de 2017 y aquellos emitidos para ser empleados en Microsoft Authenticode y tecnologías subsiguientes incluirán al identificador de la política de certificación aplicable, 2.23.140.1.4.1, para indicar el cumplimiento de los Requerimientos Mínimos para la Emisión y Administración de Certificados de Firma de Código de Confianza Pública.

[1] Adicionalmente, Symantec y CertiSur emiten certificados organizacionales (no para Servidor SSL) que no están sujetos a los Requerimientos Básicos del CA/Browser Forum. Adicionalmente a las normas que corresponden exclusivamente al CA/Browser Forum (por ejemplo, para los Certificados SSL de Organización Validada), estas Normas incluyen disposiciones que corresponden a cualquier certificado de Clase 2 o de Clase 3 que es emitido para una organización y que contiene información de la organización. Estos certificados son denominados a lo largo de estas Normas como Certificados Organizacionales.

1.1 Resumen

CertiSur es un Service Center, tal como está descripto en la Sección 1.1, lo cual significa que CertiSur puede aprobar o rechazar Solicitudes de Certificado en el caso de Certificados a nivel minorista o, en el caso de Certificados para Empresas, acordar con un Processing Center el suministro a los Usuarios de las Empresas los servicios de procesamiento necesarios que soportan el ciclo de vida de los Certificados. Los Afiliados que son Service Center suministran Certificados en modo cliente ("Client Service Centers") en su carácter de Autoridades Certificantes dentro de la Symantec Trust Network, pero delegan las funciones de procesamiento necesarias en DigiCert o en otro Processing Center. Sin embargo, cuando suministran Certificados para Servidor, los Service Center se convierten en Autoridades de Registro dentro de la Symantec Trust Network para una Autoridad Certificante DigiCert que emite dichos Certificados para Servidor. Estos centros de servicio ("Service Centers") desarrollan las funciones de validación para aprobar o rechazar las Solicitudes de Certificado para Servidor. Estos Afiliados también pueden suministrar servicios de Managed PKI a sus Clientes Corporativos. Estos Clientes de Managed PKI suscriben un Acuerdo de Managed PKI con el Service Center, que bajo su contrato con DigiCert u otro Processing Center, acuerdan suministrar las funciones de procesamiento necesarias que soportan el ciclo de vida de los Certificados para dichos Clientes de Managed PKI.

Estas Normas para el Proceso de Certificación son específicamente aplicables a:

- Autoridades Primarias de Certificación DigiCert (PCAs)
- Autoridades Certificantes de Infraestructura de CertiSur y Autoridades Certificantes de Administración de CertiSur[2], en el marco de la Symantec Trust Network
- Autoridades Certificantes de CertiSur bajo la Symantec Trust Network y Autoridades Certificantes de Empresas que emiten Certificados dentro del Subdominio CertiSur de la Symantec Trust Network.

Más genéricamente, las Normas para el Proceso de Certificación regulan el uso de los servicios de la Symantec Trust Network dentro del Subdominio CertiSur de la STN para todos los individuos y entidades dentro del Subdominio CertiSur (colectivamente denominados "Participantes del Subdominio CertiSur"). Las Autoridades Certificantes Privadas y jerarquías administradas por CertiSur fuera de la Symantec Trust Network no están alcanzadas por estas Normas[3].

---

[2] Symantec opera jerarquías de Clase 3 tanto públicas como privadas e internas. La Jerarquía de Autoridad Certificante Interna de Clase 3 está diferenciada por contar con una Autoridad Primaria de Certificación privada y el valor de Identificador de Objeto para la Política de Certificación (Certificate Policy Object Identifier u OID) específico está indicado en la Sección 1.2. El Certificado de la Autoridad Primara de Certificación Interna está configurado explícitamente para excluir Autenticación de Servidor y Firma de Código de los certificados emitidos con propósitos internos.

[3] Los Certificados de Firma de Contenido Autenticado (Authenticated Content Signing Certificates o ACS) son emitidos por una Autoridad Certificante que no pertenece a la Symantec Trust Network. No obstante, en ciertas secciones de estas Normas se efectúan algunas referencias a dichos certificados, a los efectos de que los clientes puedan entender ciertos procedimientos diferenciados que son utilizados para estos certificados.

Nota: En la fecha que se indica en cada caso, las Autoridades Certificantes Raíz están excluidas del alcance de las presentes Normas:

- Con efecto a partir del 1º de Diciembre de 2015:
  Autoridad Primaria de Certificación VeriSign Clase 3 Pública
  Country = US
  Organization = VeriSign, Inc.
  Organizational Unit = Class 3 Public Primary Certification Authority

- Con efecto a partir del 27 de Marzo de 2015:
  Autoridad Primaria de Certificación VeriSign Clase 3 Pública – G2
  Country = US
  Organization = VeriSign, Inc.
  Organizational Unit = Class 3 Public Primary Certification Authority – G2
  Organizational Unit = © 1998 VeriSign, Inc – For authorized used only
  Organizational Unit = VeriSign Trust Network

Cualquier referencia a Autoridades Primarias de Certificación o Autoridades Primarias de Certificación de Clase 3 en las Presentes Normas no tienen aplicación a estas Autoridades Certificantes Raíz. Estos Certificados Raíz serán utilizados para propósitos privados y serán deshabilitados de las listas de raíces confiables en los navegadores. La Política de Certificación de la Symantec Trust Network y las Presentes Normas no regirán más la utilización de estos certificados raíz ni ninguno de sus servicios subordinados.

La Symantec Trust Network incluye cuatro clases diferentes de Certificados, Clases 1 a 4. La Política de Certificación es un único documento que define cuatro políticas de certificación, una para cada una de las Clases y define los Requerimientos Estándar de la Symantec Trust Network para cada Clase.

CertiSur ofrece tres Clases de Certificados dentro de su Subdominio de la STN. Estas Normas describen de qué forma CertiSur cumple con los requerimientos de la Política de Certificación para cada Clase, dentro de su Subdominio. Por lo tanto, las Normas para el Proceso de Certificación cubren, en un único documento, las normas y procedimientos concernientes a la emisión y administración de las tres Clases de Certificados.

CertiSur puede publicar políticas de certificación suplementarias a las contenidas en estas Normas para el Proceso de Certificación, a efectos de cumplimentar requerimientos específicos dictados por alguna autoridad Gubernamental o como consecuencia de exigencias de estándares de la industria.

Estas políticas de certificación suplementarias estarán disponibles para los Suscriptores de los Certificados emitidos bajo dichas políticas suplementarias y las respectivas Partes Confiadas.

Estas Normas, sin embargo, constituyen solamente uno de los documentos relevantes del Subdominio CertiSur de la STN. Los demás documentos incluyen:

- Documentos auxiliares confidenciales relacionados con seguridad y operaciones[4], que complementan la Política de Certificación y las Normas para el Proceso de Certificación, suministrando mayor grado de detalle en los requerimientos.

- Acuerdos complementarios establecidos por CertiSur. Estos acuerdos vinculan legalmente a Clientes, Suscriptores y Partes Confiadas de CertiSur. Entre otras cosas, los acuerdos transmiten los Requerimientos Estándar dentro de la STN para dichos Participantes de la STN y, en algunos casos, establecen normas específicas respecto de cómo deben cumplir con dichos Requerimientos.

En muchos casos, estas Normas se refieren a estos documentos auxiliares para detalles específicos de implementación de los estándares de la STN, ya que la inclusión de dichos detalles en las Normas podría comprometer la seguridad del Subdominio CertiSur dentro de la STN.

1.2 Nombre del Documento e Identificación

Este documento constituye las Normas para el Proceso de Certificación de CertiSur S.A. Los Certificados de la Symantec Trust Network contienen valores de identificación del objeto (object identifier values) que se corresponden con la Clase de la Symantec Trust Network aplicable. Por lo tanto, CertiSur no le ha asignado a estas Normas ningún valor de identificación de objeto. Los Identificadores de Objeto de la Política de Certificación (Certificate Policy Object Identifiers) son utilizados de acuerdo con lo previsto en La Sección 7.1.6.

Los Certificados SSL de Dominio Validado (DV) y de Organización Validada (OV) contienen el correspondiente valor de Identificador de Objeto de la Política de Certificación (Certificate Policy Object Identifiers u OID) establecido en la Política de Certificación de la Symantec Trust Network que indica que los mismos son emitidos y administrados de acuerdo con los Requerimientos Básicos del CA/Browser Forum.

1.3 Participantes de la Infraestructura de Clave Pública (PKI)

1.3.1 Autoridades Certificantes

El término Autoridad Certificante es un término genérico que se refiere a todas aquellas entidades autorizadas a emitir Certificados dentro de la Symantec Trust Network. El término Autoridad Certificante incluye una subcategoría de emisores denominados Autoridades Primarias de Certificación. Las Autoridades Primarias de Certificación actúan como raíces de cuatro dominios[5], uno por cada Clase de Certificado. Cada Autoridad Primaria de Certificación es una entidad DigiCert. De forma subordinada a las Autoridades Primarias de Certificación existen Autoridades de Certificación que emiten Certificados para Suscriptores usuarios finales o para otras Autoridades Certificantes.

[4] Sin perjuicio de que estos documentos confidenciales no están disponibles públicamente, sus especificaciones están incluidas en las Auditorías Anuales WebTrust para Autoridades Certificantes de DigiCert y pueden estar disponibles para un cliente en particular, mediando un Acuerdo específico.

[5] Los Certificados Clase 4 no están actualmente emitidos bajo la Symantec Trust Network

DigiCert opera la jerarquía de Autoridad Certificante Administrativa Interna de Clase 3 que está limitada a usos administrativos internos de DigiCert.

DigiCert también opera la Autoridad de Certificación Raíz Universal de Symantec ("Symantec Universal Root Certification Authority") y la Autoridad de Certificación Raíz Universal de Criptografía de Curvas Elípticas de Symantec ("Symantec ECC Universal Root Certification Authority"). La Autoridad de Certificación Raíz Universal emite Certificados de Autoridades Certificantes de Clase 3 y de selectas Autoridades Certificantes Subordinadas de Clase 2.

Los Clientes Corporativos de CertiSur pueden operar sus propias Autoridades Certificantes como Autoridades Certificantes Subordinadas a la Autoridad Certificante de CertiSur. Estas organizaciones establecen una relación contractual con CertiSur que los vincula y obliga con respecto a todos los requerimientos de la Política de Certificación de la Symantec Trust Network y de las Normas para el Proceso de Certificación de CertiSur bajo la STN. Estas Autoridades Certificantes Subordinadas pueden implementar, sin embargo, prácticas más restrictivas basadas en sus requerimientos internos.

1.3.2 Autoridades de Registro

Una Autoridad de Registro es una entidad que desarrolla tareas de identificación y autenticación de solicitantes de certificados para certificados de usuarios finales, inicia o comunica requerimientos de revocación de certificados de usuarios finales y aprueba solicitudes para renovar o re-emitir la clave de los certificados, en nombre de una Autoridad Certificante de la Symantec Trust Network. CertiSur puede actuar como una Autoridad de Registro para los certificados que emite. DigiCert no delega la validación de dominios o de direcciones IP a Autoridades de Registro externas o terceros.

Terceras partes, que se relacionen contractualmente con CertiSur, pueden operar sus propias Autoridades de Registro y autorizar la emisión de Certificados bajo una Autoridad Certificante de la Symantec Trust Network, sobre la base de una validación inicial y luego periódicamente renovada, por parte de DigiCert, en cumplimiento de las resoluciones del CA/Browser Forum relacionadas con la reutilización de datos para esa tarea. Estas Autoridades de Registro están vinculadas y obligadas con referencia a todos los requerimientos de la Política de Certificación de la Symantec Trust Network, de las Normas para el Proceso de Certificación de CertiSur S.A. bajo la STN y los términos de los acuerdos de servicio establecidos con CertiSur. Estas Autoridades de Registro pueden implementar, sin embargo, prácticas más restrictivas basadas en sus requerimientos internos.[6]

[6] Un ejemplo de una tercera parte actuando como Autoridad de Registro es un cliente de los Servicios de Managed PKI

1.3.3 Suscriptores

Se consideran Suscriptores bajo la Symantec Trust Network a todos los usuarios finales (incluyendo entidades u organizaciones) de certificados emitidos por una Autoridad Certificante de la Symantec Trust Network. Un Suscriptor es la entidad nominada como Suscriptor usuario final de un Certificado. Los suscriptores usuarios finales pueden ser individuos, organizaciones o componentes de infraestructura, como por ejemplo un cortafuego (firewall), ruteador (router), servidores confiables u otros dispositivos utilizados para asegurar las comunicaciones dentro de una Organización.

En algunos casos, los certificados son emitidos directamente para individuos o entidades para su propio uso. Sin embargo, pueden existir habitualmente otras situaciones en donde la entidad que solicita un certificado es diferente del sujeto para el cual el certificado será emitido. Por ejemplo, una organización puede solicitar certificados para sus empleados a los efectos de representarla en transacciones o negocios electrónicos. En estas circunstancias, la entidad que está solicitando la emisión del certificado (por ejemplo, pagando por el certificado ya sea suscribiéndose a determinado servicio o como ella misma en carácter de emisora) es diferente de la entidad que será el sujeto del certificado (generalmente, el poseedor de la credencial). Por ello, hay dos términos diferentes que se utilizan en estas Normas para distinguir estos dos diferentes roles. "Suscriptor" es la entidad que contrata con CertiSur la emisión de la credencial y "Sujeto" es la persona para la cual la credencial será emitida. El Suscriptor es el responsable por la utilización de la credencial pero el Sujeto es el individuo que es autenticado cuando la credencial es presentada.

Cuando se emplea el término "Sujeto", es para indicar una distinción respecto de "Suscriptor". Cuando se emplea el término "Suscriptor", puede significar que es una entidad diferente pero también puede ser empleado para abarcar ambos conceptos. El contexto en el cual se emplean los términos dentro de estas Normas brindará el significado adecuado.

Las Autoridades Certificantes son, en sí mismas, desde el punto de vista técnico, Suscriptores de Certificados, ya sea como una Autoridad Primaria de Certificación emitiendo un Certificado para sí misma, autofirmado, o como una Autoridad Certificante a la cual le emite un Certificado una Autoridad Certificante superior. Sin embargo, las referencias a Suscriptores o Entidades usuarios finales en estas Normas se aplican solamente a Suscriptores usuarios finales.

1.3.4 Partes Confiadas

Una Parte Confiada es un individuo o una entidad que actúa confiando en un certificado y/o en una firma digital emitidos bajo la Symantec Trust Network. Una parte confiada puede ser o no un Suscriptor dentro de la Symantec Trust Network.

1.3.5 Otros Participantes

No aplicable.

1.4 Uso del Certificado

1.4.1 Usos Apropiados del Certificado

1.4.1.1 Certificados Emitidos a Individuos

Los Certificados para Individuos son normalmente utilizados por personas para firmar y encriptar correos electrónicos o para autenticarse ante aplicaciones (autenticación de cliente). Si bien los usos más comunes para los certificados de individuos están detallados en la Tabla 1 que se encuentra a continuación, un certificado para individuo puede ser empleado para otros fines, en la medida en que la Parte Confiable esté en condiciones razonables de confiar en ese certificado y que el uso no esté prohibido por ley, por la Política de Certificación de la Symantec Trust Network, por las Normas para el Proceso de Certificación bajo las cuales el certificado fue emitido o por cualquier acuerdo con los Suscriptores.

Clase de Certificado	Nivel de Confianza			Uso		
	Bajo	Medio	Alto	Firma	Encriptación	Autenticación de Cliente
Certificados Clase 1	✓			✓	✓	✓
Certificados Clase 2		✓		✓	✓	✓
Certificados Clase 3			✓	✓	✓	✓

Tabla 1. Usos de Certificados para Individuos

1.4.1.2 Certificados Emitidos a Organizaciones

Los Certificados para Organizaciones son emitidos después de autenticar que la Organización existe legalmente y que otros atributos de la misma incluidos en el Certificado (excluyendo la información no verificada del suscriptor) estén también autenticados, como por ejemplo la titularidad de un dominio de Internet o del correo electrónico. No es intención de estas Normas establecer un límite a los tipos de utilización de los Certificados para Organizaciones. Si bien los usos más comunes están descriptos en la Tabla 2 a continuación, los certificados para organizaciones pueden ser empleados para otros usos, en la medida en que la Parte Confiable esté en condiciones razonables de confiar en ese certificado y que el uso no esté prohibido por ley, por la Política de Certificación de la Symantec Trust Network, por las Normas para el Proceso de Certificación bajo las cuales el certificado fue emitido o por cualquier acuerdo con los Suscriptores

	Nivel de Confianza				Uso			
Clase de Certificado	**Medio**	**Alto con Validación Extendida (EV)**	**Alto con Organización Validada (OV) según el CA/Browser Forum**	**Alto**	**Firma de Código o Contenido**	**Asegurar Sesiones SSL/TLS**	**Autenti-cación**	**Firma y Encripta-ción**
Certificados Clase 3				✓	✓	✓	✓	✓
Certificados SSL de Validación Extendida (EV) Clase 3		✓		✓		✓	✓	✓
Certificados de Firma de Código de Validación Extendida (EV) Clase 3		✓		✓	✓		✓	✓
Certificados de Organización Validada (OV) Clase 3			✓	✓		✓	✓	✓
Certificados de Dominio Validado (DV) de Clase 3	✓					✓	✓ **Dominio solamen-te**	✓

Tabla 2. Usos de Certificados para Organizaciones[7]

1.4.1.3 Niveles de Confianza

Los **certificados de bajo nivel de confianza** son certificados que no pueden ser utilizados con propósitos de autenticación o para soportar el No Repudio. La firma digital provee un nivel bajo de confianza con relación a que el mail fue remitido por su autor desde una cierta casilla de correo electrónico. El Certificado, sin embargo, no suministra prueba de la identidad del Suscriptor. La encriptación le permite a una Parte Confiada utilizar el Certificado del Suscriptor para enviar correos electrónicos encriptados al Suscriptor, sin perjuicio de que la Parte Confiada remitente no puede confiar en que el receptor sea efectivamente la persona nominada en el Certificado.

Los **certificados de nivel de confianza medio** son certificados que permiten asegurar correos electrónicos entre diferentes organizaciones o dentro de ellas, comerciales o personales, que requieren un nivel medio de confianza respecto de la identidad del Suscriptor, en relación con las Clases 1 y 3.

[7] Bajo circunstancias limitadas, un cliente del servicio de Managed PKI puede emitir un Certificado de Clase 2 para una organización vinculada (y no a un individuo dentro de la organización). Este certificado puede ser utilizado solamente para la autenticación de la organización y aplicaciones de firma. Excepto que expresamente esté autorizado por DigiCert a través de un Acuerdo de Servicio Empresarial imponiendo requerimientos de autenticación y prácticas consistentes con los estándares de estas Normas, los Suscriptores tienen prohibida la utilización de estos certificados para firma de código y contenido, encriptación SSL y firma S/mime y la utilización de clave (key usage) con ese propósito estará deshabilitada para estos certificados.

Los Certificados de Dominio Validado (DV) son emitidos a dominios solamente para proveer cifrado. DigiCert valida que la persona que está solicitando el certificado tenga el control del dominio mediante una Autorización de uso del Dominio o sobre la base de una demostración práctica de que el Solicitante tiene el efectivo control del Nombre de Dominio Calificado. No se realiza ningún tipo de autenticación sobre la organización con respecto a la titularidad del dominio.

Los **certificados de alto nivel de confianza** son certificados para individuos u organizaciones de Clase 3, que proveen un nivel de confianza superior respecto de la identidad del Suscriptor, en comparación con las Clases 1 y 2.

Los **certificados de alto nivel de confianza con Validación Extendida (EV)** son certificados de Clase 3 emitidos por DigiCert con arreglo a los Requerimientos para los Certificados de Validación Extendida (EV).

1.4.2 Usos Prohibidos para los Certificados

Los Certificados pueden ser utilizados en la medida en que los mismos sean consistentes con la ley que resulte de aplicación, en particular solamente con usos permitidos por la legislación aplicable en materia de exportación y/o importación.

Los Certificados de DigiCert y CertiSur no han sido diseñados, orientados ni se autoriza su utilización o reventa para controlar equipos en situaciones peligrosas o para su empleo en aplicaciones que requieren la ausencia total de fallas, tal como la operación de instalaciones nucleares, sistemas de navegación o comunicación de aeronaves, sistemas de control de tráfico aéreo o sistemas de control de armamento, en donde una falla puede derivar en muerte o lesiones a personas o daños serios al medio ambiente. Además, los Certificados de Clase 1 no pueden ser utilizados como prueba de identidad o como soporte del no repudio de identidad o autoridad. Los Certificados en modo Cliente están orientados a ser empleados en aplicaciones cliente y no deben ser empleados como Certificados de Servidor o para organizaciones.

Los Certificados de Autoridad Certificante solamente pueden ser empleados para el desarrollo de las funciones de una Autoridad Certificante. Adicionalmente, los Certificados de Suscriptores usuarios finales no pueden ser usados como Certificados de Autoridad Certificante.

La Symantec Trust Network y sus Participantes no emiten certificados que puedan ser utilizados para operaciones de "hombre en el medio" ("man-in-the-middle" o "MITM"), administración de tráfico, nombres de dominio o direcciones IP, en los cuales el poseedor del certificado no sea el legítimo dueño o posea el control legítimo de dicho dominio o dirección. Esta utilización de los certificados está expresamente prohibida.

Periódicamente, DigiCert reemite las claves ("rekey") de las Autoridades Certificantes Intermedias. Las aplicaciones o plataformas de terceros que poseen una Autoridad Certificante Intermedia embebida como un certificado raíz pueden no funcionar como estaba diseñado, una vez que se haya reemitido la clave de la Autoridad Certificante Intermedia. Por lo tanto, DigiCert no garantiza el empleo de Autoridades Certificantes Intermedias como certificados raíz y recomienda que las Autoridades Certificantes Intermedias no sean embebidas en aplicaciones y/o plataformas

como certificados raíz. DigiCert y CertiSur recomiendan la utilización de las Raíces de las Autoridades Primarias de Certificación como certificados raíz.

1.5 Administración de la Política

1.5.1 Organización Específica de Administración de este Documento

La organización a cargo de la administración de estas Normas es el Departamento Legal de CertiSur S.A. Las consultas al Departamento Legal de CertiSur S.A. deben dirigirse a:
CertiSur S.A.
Av. Santa Fe 788 – 2do. Piso
(C1059ABO) Buenos Aires, República Argentina
Atención: Departamento Legal
Teléfono: (54 11) 4311 2457
Fax: (54 11) 4311 1450
Correo electrónico: legal@certisur.com

1.5.2 Contacto

Gerente de Política de Certificación
Autoridad de Administración de la Política de la Symantec Trust Network
CertiSur S.A.
Av. Santa Fe 788 – 2do. Piso
(C1059ABO) Buenos Aires, República Argentina
Atención: Departamento Legal
Teléfono: (54 11) 4311 2457
Fax: (54 11) 4311 1450
Correo electrónico: legal@certisur.com

La información de contacto para el CA/Browser Forum está disponible en:
https://cabforum.org/leadership/

1.5.2.1 Contacto para Informar una Revocación

Atención: Soporte
CertiSur S.A.
Av. Santa Fe 788 – 2do. Piso
(C1059ABO) Buenos Aires, República Argentina
Atención: Departamento Legal
Teléfono: (54 11) 4311 2457
Fax: (54 11) 4311 1450
Correo electrónico: soporte@certisur.com

Para requerir la revocación de un Certificado se debe remitir un correo electrónico a soporte@certisur.com. El ente que solicita la revocación de un certificado debe informar su

identidad y explicar los motivos por los cuales está solicitando la revocación. DigiCert, CertiSur o una Autoridad de Registro autenticarán cada solicitud y la registrarán con arreglo a lo establecido en la Sección 4.9 de la Política de Certificación de DigiCert y las presentes Normas. DigiCert y/o CertiSur también procederán a la revocación del Certificado si el requerimiento es autenticado como proveniente del Suscriptor o de la Organización vinculada incluida en el Certificado. Si la revocación es solicitada por un tercero, diferente de un representante autorizado del Suscriptor o de la Organización vinculada, DigiCert y/o CertiSur investigarán las razones alegadas para el requerimiento de revocación, antes de tomar las acciones previstas en las Secciones 4.9.1 y 4.9.3

1.5.3 Ente que Determina la Concordancia de las Normas a la Política

La Autoridad de Política de DigiCert (DigiCert Policy Authority o DCPA) es la responsable de determinar la aptitud y aplicabilidad de las presentes Normas.

1.5.4 Procedimiento de Aprobación de estas Normas

La aprobación de las presentes Normas para el Proceso de Certificación y de las subsiguientes modificaciones será efectuada por la Autoridad de Política de DigiCert Las modificaciones pueden ser presentadas en la forma de un documento conteniendo las enmiendas a las Normas para el Proceso de Certificación o bien como una actualización de las mismas. Las versiones corregidas o actualizadas estarán contenidas en la sección Actualizaciones y Notificaciones de Normas del Repositorio de CertiSur localizado en: https://www.certisur.com/repositorio/actualizaciones. Las actualizaciones suplantan cualquier especificación aludida o conflictiva de la versión referenciada de las Normas para el Proceso de Certificación. La Autoridad de Política de DigiCert determinará si los cambios en las presentes Normas requieren una modificación del Identificador de Objeto de la Política de Certificación correspondiente a cada Clase de Certificado.

1.6 Acrónimos y Definiciones

Ver el Apéndice A por la tabla de acrónimos y definiciones

1.6.1 Acrónimos y Definiciones

Ver la Sección 1.6.3 de la Política de Certificación de DigiCert para las referencias relevantes

2. Responsabilidades de Publicación y Repositorio

2.1 Repositorios

CertiSur es responsable por la función del repositorio con respecto a sus propias Autoridades Certificantes y las Autoridades Certificantes de sus Clientes Corporativos (Clientes de los Servicios de Managed PKI).

Después de la revocación de un Certificado de Suscriptor usuario final, CertiSur publica la información de dicha revocación en el repositorio. CertiSur emite Listas de Certificados Revocados (CRL) para sus propias Autoridades Certificantes y para las Autoridades Certificantes de Clientes Corporativos dentro de su Subdominio, con arreglo a lo establecido en estas Normas. Adicionalmente, para los Clientes Corporativos que han contratado los servicios de Protocolo del Estado del Certificado en Línea ("Online Certificate Status Protocol u OCSP"), CertiSur provee dichos servicios en un todo de acuerdo con lo establecido en estas Normas.

2.2 Publicación de Información del Certificado

CertiSur mantiene un repositorio basado en la Web que permite a las Partes Confiadas realizar consultas en línea respecto de la revocación y otra información respecto del estado de un Certificado. CertiSur provee a las Partes Confiadas información respecto de cómo encontrar el repositorio adecuado para comprobar el estado de un Certificado y, en caso de que esté disponible el servicio de Protocolo del Estado del Certificado en Línea ("Online Certificate Status Protocol u OCSP"), como localizar el correspondiente Respondedor ("OCSP Responder").

CertiSur emite Listas de Certificados Revocados y, si están disponibles, provee servicios de Protocolo del Estado del Certificado en Línea ("Online Certificate Status Protocol u OCSP") para sus propias Autoridades Certificantes o para las Autoridades Certificantes de sus Clientes Corporativos dentro de su Subdominio.

CertiSur publica en todo momento una versión actualizada de:

- La Política de Certificación de la Symantec Trust Network
- Estas Normas para el Proceso de Certificación bajo la Symantec Trust Network
- Los Acuerdos del Suscriptor
- Los Acuerdos del Receptor Confiado

DigiCert es responsable de la función de repositorio de las Autoridades Primarias de Certificación de DigiCert y de las Autoridades de Infraestructura y Administrativas de DigiCert que soportan la Symantec Trust Network.

CertiSur es responsable por la función de repositorio de las Autoridades Certificantes CertiSur y las Autoridades Certificantes de sus Clientes Corporativos que emiten Certificados dentro del Subdominio CertiSur de la Symantec Trust Network.

CertiSur publica la Política de Certificación de la Symantec Trust Network, estas Normas para el Proceso de Certificación bajo la Symantec Trust Network, los Acuerdos del Suscriptor y los Acuerdos del Receptor Confiado en el repositorio ubicado en su página web.

2.3 Frecuencia o Periodicidad de Publicación

Las actualizaciones de las presentes Normas para el Proceso de Certificación son publicadas de acuerdo con lo establecido en la Sección 9.12. Las actualizaciones de los Acuerdos del Suscriptor y los Acuerdos del Receptor Confiado son publicadas cuando resulte necesario. La información de la Autoridad Certificante es publicada tan pronto como la misma está disponible. La Symantec Trust Network ofrece Listas de Certificados Revocados que muestran la revocación de los Certificados y servicios de control del estado del Certificado a través del Repositorio de DigiCert. Las Listas de Certificados Revocados para los Certificados de Suscriptor usuarios finales son emitidas, por lo menos, una vez al día. Las Listas de Certificados Revocados para Autoridades Certificantes que solamente emiten Certificados para Autoridades Certificantes son emitidas, por lo menos, una vez al año y también cuando un Certificado de Autoridad Certificante es revocado. Si un Certificado incluido en una Lista de Certificados Revocados expira, puede ser removido de la Lista de Certificados Revocados que se emita después de su expiración.

2.4 Controles de Acceso a los Repositorios

La información publicada en la sección repositorio del sitio web de CertiSur es información accesible para el público. La posibilidad de "sólo lectura" con respecto a dicha información es irrestricta. CertiSur requiere que las personas presten su conformidad al Acuerdo del Receptor Confiado o al Acuerdo de Uso de la Lista de Certificados Revocados, como condición para acceder a información de Certificados, del estado de Certificados o de la Lista de Certificados Revocados. CertiSur ha implementado medidas de seguridad lógicas y físicas para impedir que personas no autorizadas puedan agregar, borrar o modificar datos del repositorio. DigiCert y CertiSur han desarrollado sus repositorios de manera de que solamente puedan ser leídos en el link especificado en la Sección 1.5.4. en donde se encuentran publicados.

3. Identificación y Autenticación

3.1 Nominación

Salvo que esté indicado lo contrario en la Política de Certificación de la Symantec Trust Network, en estas Normas o en el contenido del certificado digital, todos los nombres que aparecen en Certificados emitidos bajo la Symantec Trust Network han sido autenticados.

3.1.1 Tipos de Nombres

Sin perjuicio de que la Symantec Trust Network es ahora propiedad de DigiCert, Inc., certificados generados con anterioridad han sido emitidos con el nombre del anterior propietario. Cualquier certificado emitido con anterioridad que indique como Organización ("O") a "Symantec Corporation" o "VeriSign, Inc." y como Unidad Organizacional ("OU") a la "VeriSign Trust Network", debe interpretarse como DigiCert, Inc. y como Symantec Trust Network, respectivamente.

Los Certificados de las Autoridades Certificantes de la Symantec Trust Network contienen Nombres Distintivos (Distinguished Names) X.501 en los campos Emisor (Issuer) y Sujeto (Subject). Los Nombres Distintivos (Distinguished Names) de las Autoridades Certificantes de la Symantec Trust Network están conformados por los componentes especificados en la Tabla 3 a continuación.

Atributo	Valor
País - Country (C) =	Código ISO de país de de 2 letras (ejemplo "AR", "BO", "CL", "PY", "UY", "VE") o no utilizado.
Organización – Organization (O) =	"DigiCert Inc.", "Symantec Corporation" o CertiSur o el nombre de la organización[8].
Unidad Organizacional - Organizational Unit (OU) =	Los Certificados de las Autoridades Certificantes de DigiCert y de CertiSur pueden contener múltiples atributos en el campo OU. Dichos atributos pueden contener uno o más de lo siguiente: • Nombre de la Autoridad Certificante • Symantec Trust Network • Una declaración con referencia al Acuerdo del Receptor Confiado aplicable y que determina los términos de utilización del Certificado, • Una notificación de copyright, y • Un texto que describe el tipo de Certificado.
Estado o Provincia - State or Province (S) =	No utilizado.
Localidad - Locality (L) =	No utilizado, excepto para la Autoridad Certificante Symantec Commercial Software Publishers, que emplea el valor "Internet."
Nombre Común - Common Name (CN) =	Este Atributo incluye el Nombre de la Autoridad Certificante (si dicho Nombre no está especificado en el atributo OU) o no es utilizado.

Tabla 3 – Atributos del Nombre Distintivo (Distinguished Name) en los Certificados de Autoridades Certificantes

[8] Para una Autoridad Certificante de un Cliente Corporativo, el componente "organización" (O=) debe ser el nombre legal de dicha organización.

Los Certificados de Suscriptor usuario final contienen un nombre distintivo (distinguished name) X.501 en el campo nombre del Sujeto y están conformados por los componentes especificados en la Tabla 4 a continuación.

Atributo	Valor
País - Country (C) =	"AR", "BO", "CL", "PY", "UY", "VE" o similar (Códigos ISO de país compuesto por dos letras) o no utilizado.
Organización - Organization (O) =	El atributo Organización ("Organization") es utilizado de la siguiente forma: • "DigiCert" o "Symantec Corporation" para los Certificados de Respuesta del OCSP y opcionalmente para Certificados para individuos que no estén vinculados a una organización. • Nombre del Suscriptor organizacional en el caso de Certificados para Servidor y Certificados para individuos que estén vinculados a una organización. • No utilizado para Certificados de Dominio Validado (DV)
Unidad Organizacional - Organizational Unit (OU) =	Los Certificados para Suscriptores usuarios finales de CertiSur pueden contener múltiples atributos en el campo OU. Dichos atributos pueden contener uno o más de lo siguiente: • Unidad de negocios del Suscriptor organizacional (en el caso de Certificados para organizaciones o Certificados para individuos que estén vinculados a una organización). • Symantec Trust Network. • Una declaración con referencia al Acuerdo del Receptor Confiado aplicable y que determina los términos de utilización del Certificado, • Una notificación de copyright. • "Authenticated by Symantec"[9] y "Member, Symantec Trust Network" (Autenticado por Symantec y Miembro de la Symantec Trust Network), en el caso de Certificados cuyas solicitudes fueron autenticadas por DigiCert y/o Symantec. • "Domain Validated" ("Dominio Validado") cuando corresponda. • Texto para describir el tipo de Certificado, y • "Sin vinculación con ninguna organización" ("No organization affiliation"), para Certificados de Firma de Código emitidos a individuos
Estado o Provincia - State or Province (S) =	Indica el Estado o Provincia del Suscriptor o no es utilizado. Este es un campo no utilizado para Certificados de Dominio Validado (DV) o Certificados de Clase 1. La mención a Estado o Provincia se incluirá en cualquier certificado, con el alcance que determinan los Requerimientos Básicos del CA/Browser Forum, en los casos en donde no exista un valor con significado para el campo Localidad para el Sujeto del Certificado.
Localidad - Locality (L) =	Indica la Localidad del Suscriptor o no es utilizado. No se utiliza para los Certificados de Dominio Validado (DV) o para los Certificados de Clase 1.
Nombre Común - Common Name (CN) =	Este atributo incluye: • El Nombre del Contestador de OCSP (para los Certificados de Respuesta de OCSP) • Nombre de Dominio o Dirección IP Pública (para los Certificados para Servidor) • Nombre de la organización (para los Certificados de Firma de Código/objeto) • Nombre de la Persona (para Certificados para individuos o para los Certificados de Firma de Código emitidos a individuos). • "Persona Not Validated" (Persona no validada) para los Certificados para individuos de Clase 1[10]

[9] Un Afiliado o cliente que tiene un contrato para desarrollar los servicios de Autoridad de Registro debe indicar el nombre de la organización que desarrolla la autenticación del Suscriptor.

[10] Los clientes de Symantec que han sido aprobados para emitir Certificados de Clase 1 bajo el servicio de Managed PKI al 20 de Marzo de 2014, podrán emitir Certificados para Individuos de Clase 1 con un pseudónimo en el campo

	• Los Certificados para Individuos de Clase 1 pueden omitir este atributo
Dirección de correo electrónico - E-Mail Address (E) =	La Dirección de correo electrónico para los Certificados para individuos de Clase 1 y para los Certificados de Suscriptor de Managed PKI puede figurar. La Dirección de correo electrónico es opcional para los Certificados de firma de correo para Organizaciones de Clase 3.

Tabla 4 – Atributos del Nombre Distintivo (Distinguished Name) en los Certificados para Suscriptores Usuarios Finales

El componente nombre común (CN=) en el nombre distintivo (distinguished name) del Sujeto en los Certificados para Suscriptores usuarios finales es autenticado en el Caso de los Certificados Clases 2 y 3. El nombre común (Common Name) es omitido o puede contener la leyenda "Persona Not Validated" (Persona no validada) para los Certificados de Clase 1.

- El nombre común (Common Name) autenticado incluido en el nombre distintivo del Sujeto de los Certificados para organizaciones es un nombre de dominio o el nombre legal de la organización o unidad dentro de la organización.
- El nombre común (Common Name) autenticado incluido en el nombre distintivo (Distinguished Name) del Sujeto de un Certificado para organizaciones de Clase 3 es el nombre personal generalmente aceptado del representante de la organización, autorizado a emplear la clave privada de la organización y el componente organización (O=) es el nombre legal de la organización.
- El valor del Nombre Común (Common Name) incluido en el nombre distintivo (Distinguished Name) del Sujeto de los Certificados para individuos representa el nombre personal generalmente aceptado del individuo.
- Para todos los Certificados para Servidor, la extensión Nombre Alternativo del Sujeto (Subject Alternative Name) está completada con el valor autenticado incluido en el campo Nombre Común (Common Name) del Nombre de Dominio del Sujeto (nombre de dominio o Dirección IP Pública). La extensión Nombre Alternativo del Sujeto (Subject Alternative Name) puede contener nombres de dominio adicionales o Direcciones IP Públicas, las cuales serán autenticadas de la misma forma que el valor contenido en el Nombre Común (Common Name). Para los nombres de dominio internacionalizados, el Nombre Común (Common Name) estará representado como un valor U Label codificado según Unicode, diseñado para una comprensión por parte de personas y ese Nombre Común (Common Name) será representado en la extensión Nombre Alternativo del Sujeto (Subject Alternative Name) como un valor con sintaxis A Label Punycode diseñado para una comprensión automatizada. Estas diferentes codificaciones del mismo nombre son consideradas como valores equivalentes a los efectos de los requerimientos vinculados con la duplicación de Nombre Alternativo del Sujeto (Subject Alternative Name) y del Nombre Común (Common Name).

Los requerimientos con referencia al contenido y configuración de los Certificados SSL EV (Validación Extendida) están incluidos en el Apéndice B2 de las presentes Normas.

Nombre común (common name), siempre y cuando la mención "Persona Not Validated" (Persona no validada) sea incluida en el campo Unidad Organizacional ("Organizational Unit" o "OU").

Los Certificados de Dominio Validado (DV) contienen un Nombre Distinguido (Distinguished Name) X.501 en el campo Sujeto, que consiste en los componentes especificados en la siguiente tabla:

Atributo	Valor
País - Country (C) =	No utilizado
Organización - Organization (O) =	No utilizado
Unidad Organizacional - Organizational Unit (OU) =	Los Certificados de Dominio Validado (DV) contienen los siguientes atributos OU: • Symantec Trust Network • "Dominio Validado" ("Domain validated")
Estado o Provincia - State or Province (S) =	No utilizado
Localidad - Locality (L) =	No utilizado
Nombre Común - Common Name (CN) =	Nombre de Dominio Registrado
Dirección de correo electrónico - E-Mail Address (E) =	No utilizado

Tabla 5 – Atributos del Nombre Distintivo (Distinguished Name) en los Certificados para Suscriptores Usuarios Finales para Certificados de Dominio Validado (DV)

3.1.1.1 Requerimientos del CA/Browser Forum con Relación a Nombres

Los Certificados SSL de Validación Extendida (EV), de Firma de Código de Validación Extendida (EV) y los Certificados SSL de Dominio Validado (DV) y de Organización Validada (OV) cumplen con los requerimientos del CA/Browser Forum tal como lo establecen la Política de Certificación de DigiCert y las presentes Normas.

3.1.2 Necesidad que los Nombres tengan Significado

Los Certificados para Suscriptores usuarios finales de Clases 2 y 3 contienen nombres con semántica entendible comúnmente, que permiten la determinación de la identidad del individuo o de la organización que es Sujeto del Certificado.

Los Certificados de la Autoridad Certificante de CertiSur contienen nombres con semántica entendible comúnmente, que permiten la determinación de la identidad de la Autoridad Certificante que es Sujeto del Certificado.

3.1.3 Anonimato o Uso de Pseudónimos de Suscriptores

La identidad de los individuos Suscriptores de Certificados de Clase 1 no es autenticada. Los Suscriptores de Clase 1 pueden utilizar pseudónimos. A menos que sea obligatorio por ley o requerido por una Autoridad Gubernamental o Judicial para proteger la identidad de ciertos suscriptores usuarios finales (por ejemplo, en el caso de menores de edad o de información sensible sobre empleados del gobierno), los Suscriptores Clase 2 y Clase 3 no pueden utilizar pseudónimos (nombres diferentes de su verdadero nombre personal o razón social legal, en el caso de organizaciones). Las razones argumentadas para requerir el anonimato en un certificado serán evaluadas por la Autoridad de Política de DigiCert y, si es permitido, el certificado indicará que la identidad ha sido autenticada pero que es protegida.

3.1.4 Reglas para la Interpretación de Formas Variadas de Nombres

No contempladas.

3.1.5 Unicidad de Nombres

DigiCert y CertiSur aseguran que los Nombres Distintivos (Distinguished Names) de los Suscriptores son únicos dentro del dominio de una Autoridad Certificante específica, a través de la utilización de componentes automatizados en el proceso de solicitud del Suscriptor. Es posible que un suscriptor tenga dos o más Certificados con el mismo Nombre Distintivo (Distinguished Name).

3.1.6 Reconocimiento, Autenticación y Rol de Marcas Registradas

Los Solicitantes de Certificado tienen prohibido la utilización de nombres en sus Solicitudes de Certificado que infrinjan Derechos de Propiedad Intelectual de terceros. CertiSur, sin embargo, no verifica si el Solicitante del Certificado posee Derechos de Propiedad Intelectual sobre el nombre que aparece en la Solicitud de Certificado ni arbitra, media o de alguna otra forma resuelve cualquier disputa concerniente a la titularidad o propiedad de cualquier nombre de dominio, nombre comercial, marca registrada o marca de servicio. CertiSur está facultado, sin ninguna responsabilidad hacia cualquier Solicitante de Certificado, para rechazar o suspender cualquier Solicitud de Certificado debido a una disputa de este tipo.

3.2 Validación Inicial de Identidad

3.2.1 Método para Comprobar la Posesión de la Clave Privada

El Solicitante del Certificado debe demostrar que es legítimo poseedor de la clave privada que se corresponde con la clave pública que será incluida en el certificado. El método empleado para comprobar la posesión de la clave privada será el establecido en el estándar PKCS #10, cualquier otra demostración criptográficamente equivalente u otro método aprobado por CertiSur y DigiCert. Este requerimiento no se aplica cuando un par de claves es generado por la Autoridad Certificante en nombre del Suscriptor, por ejemplo cuando claves pregeneradas son instaladas en tarjetas inteligentes (smart cards).

3.2.2 Autenticación de la Identidad de la Organización y del Control del Dominio

Cuando un certificado contiene el nombre de una organización, la identidad de la organización y otra información suministrada por el Solicitante del Certificado en su solicitud (excepto la Información No Verificada del Suscriptor) es confirmada con arreglo a los procedimientos establecidos en la Sección 3.2.2 de la Política de Certificación de DigiCert y en estas Normas.

Como mínimo, DigiCert desarrollará lo siguiente:

- Verificará que la organización existe a través de la utilización de, por lo menos, un servicio prestado por un tercero de validación de identidad o base de datos o, alternativamente, con documentación de la organización emitida por o registrada ante la autoridad gubernamental correspondiente, que confirme la existencia de la organización, con arreglo a los requerimientos de la Sección 3.2 de la Política de Certificación de DigiCert.
- Confirmará, con el contacto apropiado de la Organización de manera telefónica, por correo o procedimiento comparable, cierta información acerca de la organización, que la organización ha autorizado la Solicitud de Certificado y que la persona que ha remitido la solicitud de Certificado en nombre de la Organización está autorizada para ello.

  Cuando el certificado incluya el nombre de un individuo en carácter de representante autorizado de la organización, también se confirmará el empleo de dicho individuo dentro de la organización y que el mismo posee la autoridad requerida para actuar en su nombre.

Cuando se incluye en un certificado un nombre de dominio o una dirección de correo electrónico, DigiCert autentica el derecho de la organización para utilizar ese dominio, ya sea como un nombre de dominio totalmente calificado o como un dominio para correo electrónico. Para Certificados de Organización Validada (OV) y de Validación Extendida (EV), la validación del dominio es ejecutada en todos los casos en forma conjunta con la validación de la Organización. La validación de la titularidad del dominio y su control es confirmada de acuerdo con los procedimientos establecidos en la sección 3.2.2 de la Política de Certificación de DigiCert y en las Normas para el Proceso de Certificación de DigiCert (versión 4.14 o posterior), disponibles en el Repositorio Legal de CertiSur.

DigiCert y CertiSur también desarrollan procedimientos adicionales de control, cuando es necesario, en función de las regulaciones y licencias de exportación dispuestas por la oficina de Industria y Ciencias del Departamento de Comercio de los Estados Unidos de Norte América (BIS).

Para tipos específicos de Certificados se desarrollan procedimientos adicionales, tal como está descripto en la Tabla 6 más abajo.

Tipo de Certificado	***Procedimientos Adicionales***
Certificados de Validación Extendida (EV)	Los procedimientos de DigiCert para la emisión de Certificados SSL de Validación Extendida (EV) están descriptos en la Política de Certificación de DigiCert y en las Normas para el Proceso de Certificación de DigiCert.
Certificados de Firma de Código de Validación Extendida	DigiCert cumple con la versión actualizada de los Lineamientos para la Emisión y Administración de Certificados de Firma de Código de Validación Extendida (EV), la cual puede ser consultada en: https://cabforum.org/ev-code-signing-certificates-guidelines/.
Certificados de Organización Validada (OV) y de Dominio Validado (DV)	Los procedimientos de DigiCert para la emisión de certificados de Organización Validada (OV) y de Dominio Validado (DV) que están especificados a lo largo de estas Normas como Requerimientos del CA/Browser Forum para Certificados de Organización Validada (OV)

	y de Dominio Validado (DV) están descriptos en las Normas para el Proceso de Certificación de DigiCert. Además, DigiCert cumple con la versión actualizada de los Requerimientos Mínimos para la Emisión y Administración de Certificados de Confianza Pública del CA/Browser Forum, los cuales pueden ser consultados en https://cabforum.org/baseline-requi rements-documents/.
Certificado SSL y Certificado para Firma de Código de Validación Extendida (EV) protegido por Hardware	DigiCert verifica que el par de claves haya sido generado en un hardware certificado FIPS 140.
Certificado SSL de Managed PKI para Intranet	DigiCert verifica que el nombre del servidor o la dirección IP asignadas al Dispositivo no sean accesibles desde Internet y que sean propiedad del Suscriptor del Certificado. La utilización de Certificados con una extensión Nombre Alternativo del Sujeto ("SubjectAlternativeName") o el campo Nombre Común del Sujeto ("Subject Common Name") conteniendo una Dirección IP Reservada o un Nombre Interno ha sido considerada obsoleta por el CA/Browser Forum y ha sido eliminada a partir del mes de Octubre de 2016.
Certificado de Firma de Contenido Autenticado	Antes que DigiCert proceda a firmar digitalmente cualquier contenido utilizando un Certificado de este tipo, autentica que el contenido sea el contenido original firmado por la Organización utilizando su Certificado de Firma de Código.
Certificados de Organización de Clase 3 para la Firma de Correos Electrónicos	DigiCert autentica la titularidad del nombre de dominio del correo electrónico por parte de la Organización.

Tabla 6 – Procedimientos de Autenticación Específicos

3.2.2.1 Requerimientos del CA/Browser Forum con Relación a la Verificación de las Organizaciones Solicitantes

Los Certificados SSL de Validación Extendida (EV), de Firma de Código de Validación Extendida (EV) y los Certificados SSL de Dominio Validado (DV) y de Organización Validada (OV) cumplen con los requerimientos del CA/Browser Forum según se establece en La Política de Certificación de DigiCert y en las Normas para el Proceso de Certificación de DigiCert.

3.2.2.2 Requerimientos de Mozilla con Relación a la Verificación de las Organizaciones Solicitantes

Para las solicitudes de Certificados con nombres de dominio internacionalizados ("internationalized domain names" o "IDN") DigiCert desarrolla un proceso para verificar al propietario del nombre de dominio a los fines de detectar casos de engaño mediante la utilización de grafías similares ("homographic spoofing").

DigiCert participa activamente en el CA/Browser Forum suministrando información para la definición de los estándares de los Certificados con nombres de dominio internacionalizados y cumple con los estándares ratificados por esa organización.

3.2.2.3 Validación del Dominio

DigiCert utiliza, para los Certificados emitidos bajo la Symantec Trust Network, los métodos para validar un nombre de dominio documentados en las Normas para el Proceso de Certificación de DigiCert.

3.2.3 Autenticación de la Identidad de un Individuo

La autenticación de la identidad de los individuos difiere según la Clase del Certificado. Los estándares de autenticación mínimos para cada clase de certificados dentro de la Symantec Trust Network se detallan en la Tabla 7 a continuación.

Clase de Certificado	Autenticación de la Identidad
Clase 1	No hay autenticación de identidad. Se realiza una confirmación limitada respecto al acceso del Suscriptor a la dirección de correo electrónico. DigiCert y/o CertiSur desarrollan un procedimiento del tipo "pregunta-respuesta" mediante el cual se envía un correo a la dirección de correo electrónico que será incluida en el certificado, conteniendo una información no predecible, como una contraseña o PIN único, generado en forma aleatoria, dirigido al dueño de la dirección de correo. El dueño de la dirección de correo, quién es el Suscriptor del Certificado, demuestra que tiene el control de la dirección de correo utilizando la información contenida en el correo enviado. Para ello, debe acceder a un Portal Web en donde volcará la información única que se le envió por correo y ejecutará la descarga y posterior instalación del Certificado.
Clase 2	La autenticación de identidad se ejecuta mediante: • Control manual desarrollado por el administrador del cliente organizacional para cada uno de los suscriptores que solicitan un certificado. Para ello el suscriptor recibe el certificado a través de un correo electrónico enviado a la dirección informada durante el proceso de Solicitud, o • Autenticación basada en un sistema de contraseñas, para lo cual se genera un PIN o contraseña de forma aleatoria que el administrador del cliente organizacional le envía por un método alternativo (no en línea) al Suscriptor que está previamente autorizado para poder solicitar el Certificado. El Suscriptor debe suministrar el PIN o contraseña enviado al momento de solicitar el certificado, o • Comparando la información suministrada por el Suscriptor con información contenida en una base de datos o registros de negocios (Registro de clientes o usuarios, como por ejemplo un Directorio LDAP o un Active Directory).
Clase 3	La autenticación de Solicitudes de Certificados para individuos de Clase 3 está basada en la presencia personal (física) del Solicitante del Certificado ante un agente de la Autoridad Certificante o de la Autoridad de Registro o ante un notario público u otra autoridad con atributos comparables, dentro de la jurisdicción del Solicitante del Certificado. El agente, notario u otro funcionario comprueba la identidad del Solicitante del Certificado con un documento de identidad emitido oficialmente y públicamente reconocido, que contenga la fotografía de su titular, tal como un pasaporte, cédula de identidad o licencia de conductor más otra credencial identificatoria.

	La autenticación de las Solicitudes de Certificados de Administrador de Clase 3 está basada en la autenticación de la organización y la confirmación de la identidad y la autorización de la persona que actúa como Administrador. En determinadas circunstancias, DigiCert y/o CertiSur también pueden aprobar Solicitudes de Certificados para sus propios Administradores. Los Administradores son "Personas Confiables" dentro de sus respectivas organizaciones. En este caso, la autenticación de sus Solicitudes de Certificados está basada en la confirmación de su identidad en conexión con su empleo o contratación como proveedor independiente y la ejecución de procedimientos de control de antecedentes. [11] Validación de la Dirección de Correo Electrónico DigiCert verifica, en el caso de los Certificados de Clase 3 Organizacional para correo electrónico, que el suscriptor sea el dueño del dominio base utilizando los métodos descriptos en la Sección 3.2.2 de las Normas para el Proceso de Certificación de DigiCert y permitiendo que el suscriptor incluya en el certificado cualquier dirección de correo electrónico que esté por debajo de ese dominio verificado.

Tabla 7 – Autenticación de la Identidad de Individuos

3.2.4 Información No Verificada del Suscriptor

La Información No Verificada del Suscriptor incluye:

- Unidad Organizacional ("Organization Unit" o "OU") con ciertas excepciones[12]
- El nombre del Suscriptor, en el caso de los Certificados Clase 1
- Cualquier otra información clasificada como no verificada contenida en el Certificado

3.2.5 Validación de Autoridad

DigiCert toma los recaudos razonables para establecer que un Certificado que es requerido en nombre de una Organización es legítimo y ha sido autorizado en forma apropiada. La confirmación de la autorización se deriva normalmente de las acciones tomadas por el Solicitante para confirmar el derecho al uso o el control de los nombres de dominio solicitados, en un todo de acuerdo con los procedimientos establecidos en la Sección 3.2.2 de las Normas para el Proceso de Certificación

[11] DigiCert puede aprobar Certificados de Administrador que están asociados a receptores que no son personas, como un dispositivo o servidor. En estos casos específicos, la autenticación de las Solicitudes de Certificados de Administrador de Clase 3 debe incluir:

- La autenticación de la existencia e identidad del servicio nominado como Administrador en la Solicitud de Certificado.
- La comprobación que el servicio ha sido implementado de manera segura, de una forma que resulte consistente con el desarrollo de las tareas de un Administrador.
- Confirmación de la identidad y autorización de la persona que solicita el certificado de Administrador para el servicio nominado como Administrador en la Solicitud de Certificado.

[12] Los certificados de Dominio Validado y de Organización Validada que certifican el cumplimiento de los Requerimientos del CA/Browser Forum pueden contener valores de Unidad Organizacional ("Organizational Unit") que han sido validados.

de DigiCert. En otras circunstancias, a los efectos de comprobar que un Certificado es debidamente autorizado por la Organización, DigiCert normalmente solicita el nombre de una persona de contacto que sea empleado o funcionario de la misma.

Cuando el nombre de un individuo es asociado en un certificado con el nombre de una Organización, de manera tal de indicar la vinculación o la autorización de ese individuo para actuar en nombre de dicha Organización, CertiSur o una Autoridad de Registro:

- Determinan que la organización existe, utilizando por lo menos un servicio de un tercero de comprobación de identidad o de base de datos o, alternativamente, con documentación organizacional emitida o aceptada formalmente por la autoridad gubernamental que resulte de aplicación, que permita confirmar la existencia de tal organización, y
- Utiliza información contenida en registros de negocios o bases de datos de información comercial (por ejemplo, listados de empleados o clientes) de una Autoridad de Registro que aprueba certificados para sus propios individuos vinculados o confirmando en forma telefónica, por correo postal o procedimiento similar, el empleo dentro de la Organización del individuo que formuló la Solicitud de Certificado y, en los casos en que resulte apropiado, su autoridad para actuar en nombre de la Organización.

3.2.6 Criterios para Interoperabilidad

No aplicable

3.3 Identificación y Autenticación de Solicitudes para Reemisión de Claves

Antes de la expiración de un Certificado de Suscriptor vigente, es necesario que el Suscriptor obtenga un nuevo certificado para mantener la continuidad de su uso. DigiCert y CertiSur generalmente requieren que el Suscriptor genere un nuevo par de claves para reemplazar el par de claves que expirará (técnicamente definido como "reemisión de claves" o "rekey"). Sin embargo, en algunos casos (por ejemplo, en el caso de Certificados para servidor), los Suscriptores pueden solicitar un nuevo certificado con un par de claves existente (técnicamente definido como "renovación").

Hablando genéricamente, ambos términos "reemisión de claves" y "renovación" son comúnmente descriptos como "Renovación de Certificado", partiendo de la base de que el viejo Certificado está siendo reemplazado por un nuevo Certificado y no enfatizando el hecho que se genere o no un nuevo par de claves. Para todas las Clases y tipos de Certificados de la Symantec Trust Network, con la excepción de los Certificados para Servidor de Clase 3, esta distinción no es importante, ya que un nuevo par de claves es siempre generado como parte del proceso de reemplazo de un Certificado para Suscriptor usuario final. Sin embargo, en el caso de los Certificados para Servidor de Clase 3, existe una distinción entre "reemisión de claves" y "renovación", debido a que el par de claves es generado en un servidor web y la mayoría de las herramientas de generación de claves de los servidores web permiten la creación de un nuevo Certificado con un par de claves existente.

3.3.1 Identificación y Autenticación para Reemisión Periódica de Claves

Los procedimientos para la Reemisión de Claves aseguran que la persona u organización que pretende la reemisión del par de claves de un Certificado de Suscriptor usuario final sea efectivamente el Suscriptor del Certificado.

Un procedimiento aceptable es a través de la utilización de una Frase de Comprobación (o equivalente) o la prueba de la posesión de la correspondiente clave privada. Los Suscriptores eligen y remiten con sus solicitudes una Frase de Comprobación. Ante la renovación de un Certificado, si un Suscriptor envía correctamente la Frase de Comprobación (o método equivalente) conjuntamente con la información de Solicitud del Suscriptor y la información de la solicitud (incluyendo la información del Contacto Organizacional y del Contacto Técnico) no ha sufrido cambios y las validaciones previas han sido desarrolladas dentro de los plazos permitidos para la reutilización de datos especificados en los Requerimientos Mínimos y las Normas para la emisión de Certificados de Validación extendida (EV) del CA/Browser Forum, se emitirá automáticamente un nuevo Certificado.

3.3.2 Identificación y Autenticación para Reemisión de Claves Después de la Revocación del certificado

La reemisión de claves después de la revocación no es permitida si:

- La revocación ocurre debido a que el Certificado (distinto de un Certificado de Clase 1) fue emitido a una persona distinta de la nominada como Sujeto del Certificado,
- El Certificado (distinto de un Certificado de Clase 1) fue emitido sin la autorización de la persona nominada como el Sujeto de dicho Certificado,
- La entidad que aprueba la Solicitud de Certificado del Suscriptor descubre o tiene razones para suponer que existe, de hecho, una falsedad de la Solicitud del Certificado, o
- Por cualquier otra razón que tanto DigiCert como CertiSur consideren necesaria para la protección de la Symantec Trust Network.

Sujeto a lo previsto en los párrafos precedentes, la renovación de un Certificado para organizaciones o de una Autoridad Certificante después de la revocación del Certificado, está permitida en la medida en que los procedimientos de renovación permitan asegurar que la organización o Autoridad Certificante que solicita la renovación es, efectivamente, el Suscriptor del Certificado. Los Certificados para organizaciones renovados deben contener el mismo nombre distintivo del Sujeto ("Subject Distinguished Name") que el que contenía el Certificado que pretende ser renovado.

La renovación de Certificados para individuos, después que los mismos han sido revocados, debe asegurar que la persona que solicita la renovación es, efectivamente, el Suscriptor. Un procedimiento aceptable consiste en la utilización de una Frase de Comprobación (o procedimiento equivalente). Salvo este procedimiento u otro procedimiento aprobado por DigiCert y/o CertiSur, los requerimientos para la identificación y autenticación de una renovación de un Certificado después de su revocación son los mismos que se emplean para una Solicitud de Certificado original.

3.4 Identificación y Autenticación de las Solicitudes de Revocación

Antes de la revocación de un Certificado, DigiCert y/o CertiSur verifican 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:

- Envío del Suscriptor de la Frase de Comprobación (o método equivalente) del Suscriptor y revocación automática del Certificado en caso de que la misma concuerde con la Frase de Comprobación (o su equivalente) registrada, para ciertos tipos de certificado. Esta opción puede no estar disponible para todos los clientes.
- Recepción de un mensaje que invoca ser remitido por el Suscriptor que solicita la revocación y contiene una firma digital verificable con referencia al Certificado que pretende ser revocado, y
- Comunicación con el Suscriptor, proveyendo razonable seguridad, en función de la Clase del Certificado, que la persona u organización que requiere la revocación es, efectivamente, el Suscriptor. Dependiendo de las circunstancias, dicha comunicación podrá efectuarse a través de una o más de las siguientes modalidades: llamado telefónico, facsímil, correo electrónico, correo postal o servicio de courier o mensajería.

Los Administradores de DigiCert y CertiSur están facultados para solicitar la revocación de Certificados de Suscriptores usuarios finales dentro del Subdominio CertiSur. DigiCert autentica la identidad de los Administradores mediante el control de acceso empleando SSL y autenticación de cliente, antes de permitirle a los mismos desarrollar las funciones de revocación u otro procedimiento aprobado de la Symantec Trust Network.

Las Autoridades de Registro que utilizan el Módulo de Software de Administración Automática deben remitir en bloque a CertiSur las solicitudes de revocación. Dichas solicitudes son autenticadas mediante un requerimiento firmado digitalmente con la clave privada del dispositivo de hardware de Administración Automática de la Autoridad de Registro.

Las solicitudes para revocar el Certificado de una Autoridad Certificante son autenticadas por DigiCert para asegurarse que tal revocación ha sido solicitada, efectivamente, por la Autoridad Certificante.

4. Requerimientos Operativos del Ciclo de Vida de los Certificados

4.1 Solicitud de Certificados

4.1.1 Personas que Pueden Presentar una Solicitud de Certificado

A continuación, figura un listado de las personas que pueden presentar solicitudes de certificados:

- Cualquier persona que es el Sujeto del Certificado.
- Cualquier representante autorizado de una Organización o entidad.
- Cualquier representante autorizado de una Autoridad Certificante.
- Cualquier representante autorizado de una Autoridad de Registro.

4.1.2 Proceso de Solicitud y Responsabilidades

4.1.2.1 Suscriptores de Certificados Usuarios Finales

Todos los Solicitantes usuarios finales de Certificados deben manifestar su conformidad con el Acuerdo del Suscriptor que resulte aplicable, el cual contiene obligaciones y garantías descriptas en la Sección 9.6.3 y subsiguientes y completar un proceso de solicitud, que consiste en:

- Completar una Solicitud de Certificado y suministrar la información requerida, de manera correcta y veraz.
- Generar o acordar la generación de un par de claves.
- Enviar su clave pública a DigiCert, directamente o a través de una Autoridad de Registro.
- Demostrar que está en posesión y/o bajo control exclusivo de la clave privada que se corresponde con la clave pública que ha enviado a DigiCert.

4.1.2.2 Requerimientos del CA/Browser Forum con Relación a las Solicitudes de Certificado

Los Certificados SSL de Validación Extendida (EV), de Firma de Código de Validación Extendida (EV) y los Certificados SSL de Dominio Validado (DV) y de Organización Validada (OV) cumplen con los requerimientos del CA/Browser Forum según se establece en la Política de Certificación de DigiCert y en las Normas para el Proceso de Certificación de DigiCert.

4.1.2.3 Certificados de Autoridad Certificante y de Autoridad de Registro

Los Suscriptores de Certificados de Autoridad Certificante y de Autoridad de Registro suscriben un acuerdo con CertiSur. Los Solicitantes de Certificado de Autoridad Certificante y de Autoridad de Registro deben presentar documentación identificatoria para demostrar su identidad y proveer la información de contacto durante el proceso de contratación. Durante este proceso de contratación o, a más tardar, antes de la Ceremonia de Generación de Claves para crear el par de claves de la Autoridad Certificante o de la Autoridad de Registro, el solicitante deberá cooperar

con DigiCert y CertiSur a efectos de determinar el nombre distintivo (distinguished name) apropiado y el contenido de los Certificados a ser emitidos a los solicitantes.[13]

4.2 Procesamiento de la Solicitud de Certificado

4.2.1 Desarrollo de las Funciones de Identificación y Autenticación

DigiCert, CertiSur o una Autoridad de Registro deberán realizar la identificación y autenticación de toda la información del Suscriptor requerida con arreglo a lo dispuesto en la Sección 3.2.

4.2.2 Aprobación o Rechazo de las Solicitudes de Certificado

DigiCert, CertiSur o una Autoridad de Registro aprobarán una solicitud de un certificado si los siguientes requisitos han sido cumplidos:

- Identificación y autenticación de manera satisfactoria de toda la información del Suscriptor requerida con arreglo a lo dispuesto en la Sección 3.2.
- El pago ha sido recibido.

DigiCert, CertiSur o una Autoridad de Registro rechazarán una solicitud de un certificado si:

- La identificación y autenticación de toda la información del Suscriptor requerida con arreglo a lo dispuesto en la Sección 3.2. no pudo ser completada, o
- El Suscriptor no aportó en debida forma la documentación de soporte que se le solicitó, o
- El Suscriptor no respondió a las notificaciones enviadas dentro del tiempo establecido, o
- El pago no ha sido recibido, o
- La Autoridad de Registro considera que la emisión del Certificado al Suscriptor puede generar descrédito a la Symantec Trust Network.

4.2.3 Plazo para Procesar las Solicitudes de Certificado

DigiCert y CertiSur comienzan con el procesamiento de las solicitudes de certificado dentro de un plazo razonable desde el momento de su recepción. No existe un plazo determinado para completar el procesamiento de una solicitud, salvo que esté indicado lo contrario en los Acuerdos del Suscriptor que resulte de aplicación, en las Normas para el Proceso de Certificación o cualquier otro Acuerdo aplicable entre los participantes de la Symantec Trust Network. Una solicitud de certificado permanece activa hasta que sea rechazada.

4.2.4 Autorización para la Autoridad Certificante

A partir del 8 de Septiembre de 2017, DigiCert controla los registros “issue” e “issuewild” de CAA. Este control se desarrolla dentro de las 8 horas de la emisión de un Certificado o dentro del

[13] En situaciones excepcionales, pueden existir circunstancias bajo las cuales se emitan certificados de suscriptor directamente desde la raíz. Esta excepción solamente puede ser utilizada en la eventualidad de un certificado para suscriptor con un par de claves de 2048 bits de longitud o menos.

tiempo de vida ("Time to Live" o TTL) del registro de CAA, el que resulte mayor de ambos, salvo en el caso de que el registro CAA haya sido controlado de manera similar en forma previa para la creación de un pre-certificado para cumplir con el protocolo Certificate Transparency que esté incluido en por lo menos 2 listados públicos de Certificate Transparency. El control de CAA puede ser omitido en el caso de Autoridades Certificantes subordinadas que estén técnicamente restringidas.

El fracaso en el acceso a los registros DNS es considerado como el permiso para la emisión del Certificado, en la medida en que dicho fracaso esté demostrado que es consecuencia de una falla producida fuera de la infraestructura de DigiCert, se haya intentado el acceso por lo menos dos veces y la zona de dominio no contenga una cadena de validación DNSSEC a la raíz de ICANN.

DigiCert registra las acciones que desarrolla basadas en los registros de CAA y el impedimento para la emisión de documentos por parte de CAA para su realimentación al CA/Browser Forum.

La Symantec Trust Network y todas las marcas comprendidas bajo la misma reconocen como permiso para la emisión de un Certificado a cualquiera de los siguientes Nombres de Dominio emisores: symantec.com, thawte.com, geotrust.com, rapidssl.com y cualquier Nombre de Dominio Calificado (FQDN) que finalice con el dominio base digitalcertvalidation.com y contenga un prefijo específico de un revendedor autorizado.

4.3 Emisión de Certificados

4.3.1 Acciones Desarrolladas por la Autoridad Certificante Durante la Emisión del Certificado

Un Certificado es generado y emitido por DigiCert después de la aprobación de una Solicitud de Certificado o con posterioridad de la recepción de un requerimiento de una Autoridad de Registro para la emisión del Certificado. DigiCert genera y emite un Certificado al Solicitante del Certificado, sobre la base de la información suministrada en la Solicitud de Certificado, después de aprobar dicha Solicitud de Certificado.

4.3.2 Notificaciones de la Autoridad Certificante al Suscriptor acerca de la Emisión del Certificado

DigiCert o CertiSur, ya sea directamente o a través de una Autoridad de Registro, notificarán a los Suscriptores que ha generado el Certificado y proveerá a los Suscriptores el acceso a los Certificados mediante la notificación de que los mismos están disponibles. Los Certificados serán puestos a disposición de los Suscriptores usuarios finales ya sea permitiéndoles efectuar una descarga de los mismos de una página o sitio Web o a través de un mensaje enviado al Suscriptor que contendrá el Certificado.

4.3.3 Requerimientos del CA/Browser Forum con Relación a la Emisión de Certificados por parte de una Autoridad Certificante Raíz

Los Certificados SSL de Validación Extendida (EV), de Firma de Código de Validación Extendida (EV) y los Certificados SSL de Dominio Validado (DV) y de Organización Validada (OV) cumplen con los requerimientos del CA/Browser Forum según se establece en la Política de Certificación de DigiCert y en las Normas para el Proceso de Certificación de DigiCert.

4.4 Aceptación del Certificado

4.4.1 Conductas que Constituyen Aceptación del Certificado

Las siguientes conductas constituirán aceptación del Certificado:

- Efectuar la descarga del Certificado o instalar el Certificado desde el mensaje al cual se adjunta, constituye la aceptación del Certificado por parte del Suscriptor.
- La ausencia de rechazo del Certificado o la falta de objeción respecto de su contenido, por parte del Suscriptor, constituye la aceptación del mismo.

4.4.2 Publicación del Certificado por parte de la Autoridad Certificante

No aplicable.

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

Las Autoridades de Registro podrás recibir notificación respecto de la emisión de los certificados que ellas aprueban.

4.5 Par de Claves y Uso del Certificado

4.5.1 Clave Privada del Suscriptor y Uso del Certificado

La utilización de la clave privada que se corresponde con la clave pública contenida en el certificado solamente estará permitida una vez que el Suscriptor haya prestado su conformidad al Acuerdo del Suscriptor y aceptado el certificado. El certificado debe ser utilizado de manera legal y con arreglo al Acuerdo del Suscriptor de CertiSur, la Política de Certificación de la Symantec Trust Network y a estas Normas para el Proceso de Certificación. El uso del Certificado tiene que ser consistente con el contenido de la extensión Uso de Claves (KeyUsage) incluido en el certificado (por ejemplo, si la Firma Digital no está habilitada, el certificado no puede ser empleado para firmar).

Los Suscriptores deben proteger sus claves privadas del uso no autorizado y deben discontinuar su utilización después del vencimiento o revocación del certificado. Terceras partes que no sean el

Suscriptor no deben archivar la Clave Privada del Suscriptor, excepto lo previsto en la Sección 4.12.

4.5.2 Clave Pública del Receptor Confiado y Uso del Certificado

Las Partes Confiadas deben aceptar los términos del Acuerdo del Receptor Confiado que resulte de aplicación, como condición para poder confiar en el certificado.

La acción de confiar en un certificado tiene que ser razonable con arreglo a las circunstancias. Si las circunstancias indican la necesidad de seguridades adicionales, la Parte Confiada debe obtener las seguridades que estime razonables para poder contar con dicha confianza.

Antes de cualquier acto que implique confianza, las Partes Confiadas deben, en forma independiente, evaluar:

- La procedencia en el uso de un Certificado para cualquier propósito especificado y determinar si el Certificado podrá ser utilizado, efectivamente, para un propósito que resulte adecuado, que no esté prohibido o de alguna otra forma restringido por estas Normas. Ni DigiCert ni CertiSur son responsables por la evaluación acerca de si el uso de un Certificado es procedente o no.
- Que el certificado esté siendo utilizado en forma consistente con el contenido de la extensión Uso de Claves (KeyUsage) incluido en el certificado (por ejemplo, si la Firma Digital no está habilitada, el certificado no puede ser considerado como confiable para validar una firma del Suscriptor).
- El estado del certificado, como así también el estado de todos los Certificados de Autoridades Certificantes en la Cadena de Certificación que emitió el certificado. Si cualquiera de los Certificados de la Cadena de Certificación ha sido revocado, la Parte Confiada es la exclusiva responsable de investigar si resulta razonable confiar en una firma digital generada por el Suscriptor usuario final del Certificado antes de la revocación del Certificado en la Cadena de Certificación. Esa confianza es asumida bajo el exclusivo riesgo de la Parte Confiada.

Asumiendo que la utilización del certificado es la apropiada, las Partes Confiadas deben utilizar el software y/o hardware que resulten apropiados para desarrollar la verificación de la firma digital u otras operaciones criptográficas que deseen llevar a cabo, como condición para confiar en Certificados relacionados con dichas operaciones. Estas operaciones incluyen la identificación de una Cadena de Certificación y la verificación de las firmas digitales incluidas en todos los Certificados que forman parte de la Cadena de Certificación.

4.6 Renovación del Certificado

La renovación del Certificado es la emisión de un nuevo certificado para el suscriptor sin cambiar la clave pública u otra información en el certificado. La renovación del certificado es soportada para los Certificados de Clase 3, en donde el par de claves es generado en un servidor Web, ya que la mayoría de las herramientas disponibles en dichos servidores permiten la generación de una nueva Solicitud de Certificado desde un par de claves ya existente.

4.6.1 Circunstancias para la Renovación del Certificado

Antes de la expiración del Certificado del Suscriptor vigente, es necesario que el Suscriptor renueve su Certificado a los efectos de mantener la continuidad en el uso del mismo. Un certificado también puede ser renovado una vez que ha expirado.

4.6.2 Individuos que Pueden Solicitar la Renovación

Solamente el suscriptor de un certificado para individuos o un representante autorizado, en el caso de Certificados para organizaciones, pueden solicitar la renovación de un certificado.

4.6.3 Procesamiento de las Solicitudes de Renovación de Certificados

Los procedimientos de renovación aseguran que la persona u organización que está solicitando la renovación de un Certificado de Suscriptor usuario final es, efectivamente, el Suscriptor del Certificado o un individuo autorizado por el mismo. Las Solicitudes de renovación de Certificados dentro de la Symantec Trust Network son procesadas con arreglo a los requisitos establecidos en las Normas para el Proceso de Certificación de DigiCert.

4.6.4 Notificación al Suscriptor de la Emisión de un Certificado Nuevo

La notificación de la emisión de un certificado renovado será realizada al Suscriptor con arreglo a lo previsto en la Sección 4.3.2.

4.6.5 Conducta que Constituye la Aceptación de un Certificado Renovado

La conducta que constituye la aceptación de un certificado renovado es la prevista en la Sección 4.4.1.

4.6.6 Publicación por parte de la Autoridad Certificante del Certificado Renovado

No aplicable.

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

Las Autoridades de Registro podrán recibir notificación respecto de la emisión de los certificados que aprueban.

4.7 Reemisión (Re-Key) del Certificado

La reemisión (rekey) de un certificado es la solicitud para la emisión de un nuevo certificado que certifique una nueva clave pública. La reemisión (rekey) de un Certificado es soportada para todas las Clases de Certificado.

4.7.1 Circunstancias para la Reemisión (Re-Key) del Certificado

Antes de la expiración del Certificado del Suscriptor vigente, es necesario que el Suscriptor reemita (rekey) su Certificado a los efectos de mantener la continuidad en el uso del mismo. Un certificado también puede ser reemitido (rekeyed) una vez que ha expirado.

4.7.2 Individuos que Pueden Solicitar la Certificación de una Nueva Clave Pública

Solamente el Suscriptor de un certificado para individuos o un representante autorizado, en el caso de Certificados para Organizaciones, pueden solicitar la reemisión (rekey) de un certificado.

4.7.3 Procesamiento de las Solicitudes de Reemisión (Re-Key) de Certificados

Los procedimientos de reemisión (rekey) aseguran que la persona u organización que está solicitando la reemisión de un Certificado de Suscriptor usuario final es, efectivamente, el Suscriptor del Certificado o un individuo autorizado por el mismo. Las Solicitudes de Reemisión (rekey) de Certificados dentro de la Symantec Trust Network son procesadas con arreglo a los requisitos establecidos en las Normas para el Proceso de Certificación de DigiCert

4.7.4 Notificación al Suscriptor de la Emisión de un Certificado Nuevo

La notificación al Suscriptor respecto de la reemisión de un certificado es realizada con arreglo a lo previsto en la Sección 4.3.2.

4.7.5 Conducta que Constituye la Aceptación de un Certificado Reemitido (Re-Keyed)

La conducta que constituye la aceptación de un certificado reemitido es la prevista en la Sección 4.4.1.

4.7.6 Publicación por parte de la Autoridad Certificante del Certificado Reemitido (Re-Keyed)

No aplicable.

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

Las Autoridades de Registro podrán recibir notificación respecto 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 implica la solicitud de emisión de un nuevo certificado debido a cambios en la información de un certificado existente (diferente de la clave pública del Suscriptor).

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

4.8.2 Individuos que Pueden Solicitar la Modificación

Ver Sección 4.1.1.

4.8.3 Procesamiento de las Solicitudes de Modificación de Certificados

DigiCert, CertiSur o una Autoridad de Registro desarrollarán la identificación y autenticación de toda la información del Suscriptor requerida con arreglo a los términos de la Sección 3.2.

4.8.4 Notificación al Suscriptor de la Emisión de un Certificado Nuevo

Ver Sección 4.3.2.

4.8.5 Conducta que Constituye la Aceptación de un Certificado Modificado

Ver Sección 4.4.1.

4.8.6 Publicación por parte de la Autoridad Certificante del Certificado Modificado

No aplicable

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

Ver Sección 4.4.3.

4.9 Suspensión y Revocación de Certificados

4.9.1 Circunstancias para la Revocación

DigiCert revocará un Certificado dentro de las 24 horas si uno o más de los siguientes hechos sucede:

1. El Suscriptor requiere, por escrito, que DigiCert revoque el Certificado;
2. El Suscriptor notifica a DigiCert que la solicitud original del Certificado no ha sido autorizada y, por lo tanto, no garantiza su emisión con carácter retroactivo;
3. DigiCert obtiene evidencia que la Clave Privada del Suscriptor que se corresponde con la Clave Pública contenida en el Certificado ha sufrido un Compromiso de Clave, o
4. DigiCert obtiene evidencia que la validación respecto de la autorización del uso del dominio o el control sobre el mismo, con referencia a cualquier Nombre de Dominio Calificado (FQDN) o dirección IP contenidos en el Certificado, no resulta confiable.

DigiCert podrá revocar un Certificado dentro de las 24 horas y revocará un Certificado dentro de cinco (5) días, si uno o más de los siguientes hechos sucede:

1. El Certificado deja de cumplir con los requisitos de las Secciones 6.1.5 y 6.1.6 de los Requerimientos Básicos del CA/Browser Forum;
2. DigiCert obtiene evidencia que el Certificado ha sido utilizado de manera inapropiada;
3. El Suscriptor o la Autoridad Certificante que ha recibido una certificación cruzada ha incumplido una obligación material impuesta por la Política de Certificación, estas Normas o los acuerdos que resulten aplicables;
4. DigiCert confirma la existencia de cualquier circunstancia indicando que el uso de un Nombre de Dominio Calificado (FQDN) o dirección IP contenidos en un Certificado han dejado de ser legalmente permitidos (por ejemplo, un Juzgado o Corte Arbitral ha revocado el derecho del registrante del Nombre de Dominio a utilizar el mismo, un acuerdo de servicios o de licencia entre el registrante del Nombre de Dominio y el Solicitante ha sido rescindido o el registrante del Nombre de Dominio ha fallado en la renovación del registro del mismo);
5. DigiCert confirma que un Certificado WildCard ha sido utilizado para autenticar un Nombre de Dominio Calificado subordinado, de manera fraudulenta;
6. DigiCert confirma que se ha producido un cambio material en la información contenida en el Certificado;
7. DigiCert confirma que el Certificado no fue emitido conforme a los requerimientos del CA/Browser Forum, de la Política de Certificación de DigiCert, de las Normas para el Proceso de Certificación de DigiCert o de las presentes Normas;
8. DigiCert determina o confirma que cualquier información contenida en el Certificado no es veraz;
9. El derecho de DigiCert para emitir Certificados en cumplimiento de los Requerimientos del CA/Browser Forum ha expirado, ha sido revocado o rescindido, salvo que se hayan realizado los acuerdos correspondientes para continuar manteniendo el Repositorio con

información de la Lista de Certificados Revocados o los Servicios de Control del Estado del Certificado;

10. La revocación es requerida en cumplimiento de la Política de Certificación de DigiCert o de las presentes Normas, o
11. DigiCert confirma que existe una demostración o método probado que expone la Clave Privada del Suscriptor a Compromiso, que se hayan desarrollado métodos que permitan su cálculo sobre la base de la Clave Pública (como por ejemplo la debilidad de claves de Debian) o si existe clara evidencia que el método específico utilizado para generar la Clave Privada ha sido defectuoso.

Adicionalmente a las razones detalladas precedentemente, un Certificado de Suscriptor usuario final puede ser revocado por DigiCert, CertiSur o el propio Suscriptor y publicado en una Lista de Certificados Revocados, por alguno de los siguientes motivos:

- El Acuerdo del Suscriptor con el Suscriptor ha expirado,
- La vinculación del Suscriptor con un Cliente Corporativo ha terminado o finalizado por cualquier motivo,
- La vinculación entre una organización que es Suscriptor de un Certificado para organizaciones de Clase 3 y el representante de la organización que controla la clave privada del Suscriptor ha terminado o finalizado por cualquier motivo,
- DigiCert, CertiSur o un Cliente tienen razones para suponer que el Certificado ha sido emitido de una manera que, materialmente, no cumple con los procedimientos requeridos por las Normas para el Proceso de Certificación que resultan de aplicación, el Certificado (distinto de un Certificado de Clase 1) ha sido emitido a una persona diferente de la nominada como Sujeto del Certificado o el Certificado (distinto de un Certificado de Clase 1) ha sido emitido sin la autorización de la persona nominada como Sujeto de dicho Certificado,
- DigiCert, CertiSur o un Cliente tienen razones para suponer que una declaración material contenida en la Solicitud de Certificado es falsa,
- DigiCert, CertiSur o un Cliente determinan que un prerrequisito material para la Emisión del Certificado nunca fue satisfecho ni exceptuado su cumplimiento,
- En el caso de los Certificados para organizaciones de Clase 3, el nombre organizacional del Suscriptor ha cambiado,
- La información contenida en el Certificado, distinta de la Información No Verificada del Suscriptor, es incorrecta o ha cambiado,
- La identidad del Suscriptor no ha sido satisfactoriamente re verificada con arreglo a lo previsto en la Sección 6.3.2,
- En el caso de los Certificados de Firma de Código, si
    - Un Desarrollador de una Aplicación de Software le solicita a la Autoridad Certificante la revocación y una investigación determina que el certificado está siendo empleado para la firma de código malicioso o cualquier otro software no deseado.
    - Un informe es remitido a un Participante de la Symantec Trust Network indicando que el certificado está siendo utilizado para la firma de código malicioso.
- El Suscriptor no ha efectuado el pago dentro del plazo estipulado, o

- La continuidad en el uso de dicho Certificado es perjudicial para la Symantec Trust Network.

A efectos de evaluar si el uso de un Certificado es perjudicial o no para la Symantec Trust Network, DigiCert y CertiSur considerarán, entre otros factores, los siguientes:

- La naturaleza y el número de reclamos recibidos,
- La identidad del o de los reclamantes,
- La legislación en vigencia, relevante para el caso, y
- Las respuestas brindadas por el Suscriptor respecto del perjuicio alegado en el uso del Certificado.

A efectos de evaluar si el uso de un Certificado de Firma de Código es perjudicial o no para la Symantec Trust Network, DigiCert y CertiSur considerarán adicionalmente, entre otros factores, los siguientes:

- El nombre del código firmado,
- El comportamiento del código,
- Los métodos de distribución del código,
- Las declaraciones formuladas a los receptores del código,
- Cualquier declaración adicional formulada con respecto al código,
- Con efecto a partir del 1º de Febrero de 2017, si el Certificado de Firma de Código satisface cualquiera de las razones para revocar un Certificado de Suscriptor descriptas en la Sección 13.1.5 de los Requerimientos Mínimos para la Emisión y Administración de los Certificados de Firma de Código de Confianza Pública, tal como han sido adoptados por Microsoft.

DigiCert siempre revoca un Certificado si la relación que vincula al Sujeto y a la Clave Pública del Sujeto contenida en el Certificado no es más válida o si la Clave Privada asociada ha sido comprometida.

DigiCert procederá a la revocación de un Certificado de Autoridad Certificante Subordinada dentro de siete (7) días, si uno o más de los siguientes hechos sucede:

1. La Autoridad Certificante Subordinada solicita, por escrito, la revocación;
2. La Autoridad Certificante Subordinada notifica a DigiCert que la Solicitud original del Certificado no ha sido autorizada y, por lo tanto, no garantiza su emisión con carácter retroactivo;
3. DigiCert obtiene evidencia que la Clave Privada de la Autoridad Certificante Subordinada que se corresponde con la Clave Pública contenida en el Certificado ha sufrido un Compromiso de Clave o ha dejado de cumplir con los requisitos establecidos en las Secciones 6.1.5 y 6.1.6 de los Requerimientos Básicos del CA/Browser Forum;
4. DigiCert obtiene evidencia que el Certificado de la Autoridad Certificante ha sido utilizado de manera inapropiada;
5. DigiCert confirma que el Certificado de Autoridad Certificante no ha sido emitido de acuerdo con, o que la Autoridad Certificante Subordinada no ha cumplido con las presentes

Normas o la Política de Certificación o las Normas para el Proceso de Certificación que resulten aplicables;

6. DigiCert determina que cualquier información contenida en el Certificado de la Autoridad Certificante no es veraz o resulta falsa;
7. DigiCert o la Autoridad Certificante subordinada dejan de operar por cualquier motivo o razón y no han realizado ningún acuerdo para suministrar soporte de revocación para el Certificado de la Autoridad Certificante;
8. El derecho de DigiCert o de la Autoridad Certificante Subordinada para emitir Certificados en cumplimiento de los Requerimientos del CA/Browser Forum ha expirado, ha sido revocado o rescindido, salvo que se hayan realizado los acuerdos correspondientes para continuar manteniendo el Repositorio con información de la Lista de Certificados Revocados o los Servicios de Control del Estado del Certificado;
9. La revocación es requerida en cumplimiento de la Política de Certificación de DigiCert o de las presentes Normas; o
10. El contenido o formato del Certificado de la Autoridad Certificante supone un riesgo inaceptable para los proveedores de software o aplicaciones o para las Partes Confiadas.

DigiCert revocará un Certificado que contenga una certificación cruzada si la entidad que ha recibido dicha certificación, incluyendo DigiCert, deja de cumplir con las estipulaciones de las correspondientes políticas, señaladas en el Identificador de Objeto (OID) de la Política incluido en la extensión de mapeo de la política incluido en el Certificado que ha sido certificado en forma cruzada.

DigiCert o CertiSur también pueden revocar un Certificado de Administrador si la autoridad del Administrador para actuar como tal se ha terminado o ha concluido por cualquier motivo.

Los Acuerdos del Suscriptor de CertiSur requieren que los Suscriptores usuarios finales notifiquen inmediatamente a CertiSur y/o DigiCert si conocen o sospechan que su clave privada ha sufrido un Compromiso.

DigiCert identificará a un Certificado como inactivo en su base de datos pero no lo publicará en ninguna Lista de Certificados Revocados, si el Suscriptor indica que no utilizará más su Certificado o no desea hacerlo más por razones diferentes a las mencionadas con anterioridad.

4.9.1.1 Requerimientos del CA/Browser Forum con Relación a las Razones para la Revocación

Los Certificados SSL de Validación Extendida (EV), de Firma de Código de Validación Extendida (EV) y los Certificados SSL de Dominio Validado (DV) y de Organización Validada (OV) cumplen con los requerimientos respectivos del CA/Browser Forum según se establece en la Política de Certificación de DigiCert y en las Normas para el Proceso de Certificación de DigiCert.

4.9.2 Persona que Puede Solicitar la Revocación

Los individuos Suscriptores podrán solicitar la revocación de su propio Certificado a través de un representante autorizado de DigiCert, CertiSur o de una Autoridad de Registro. En el caso de certificados para Organizaciones, un representante debidamente autorizado de la organización estará facultado para requerir la revocación de los certificados emitidos para la organización. Un representante debidamente autorizado de DigiCert, CertiSur o de una Autoridad de Registro estará facultado para solicitar la revocación de un Certificado de Administrador de esa Autoridad de Registro. La entidad que aprueba las Solicitudes de Certificados de Suscriptor también estará facultada para revocar o solicitar la revocación de un Certificado de Suscriptor.

Con relación a los Certificados de Firma de Código, DigiCert y los Afiliados que emiten este tipo de certificados suministran a las organizaciones que desarrollan Anti-Malware, Suscriptores, Partes Confiadas, Proveedores de Aplicaciones de Software y demás terceros, precisas instrucciones respecto de cómo deben informar el Compromiso de una Clave Privada, un inadecuado uso del certificado, Certificados utilizados para la firma de Código Sospechoso, ataques para tomar el control de la clave privada u otros tipos de fraude, compromiso, mala utilización, conducta inapropiada o cualquier otro asunto que resulte de material importancia con relación a un certificado. DigiCert y CertiSur publican las instrucciones relevantes en sus respectivas páginas Web.

DigiCert y aquellos Afiliados que emitan Certificados de Firma de Código y que posean la capacidad para revocar un Certificado, procederán a revocar un Certificado de Firma de Código en cualesquiera de las siguientes cuatro circunstancias: (1) el Proveedor de la Aplicación de Software solicita la revocación y DigiCert o su Afiliado no intentan ejecutar un curso de acción alternativo; (2) el suscriptor autenticado solicita la revocación; (3) un tercero suministra información que le permite a la Autoridad Certificante determinar que el certificado ha sido comprometido o está siendo utilizado para un Código Sospechoso; o (4) la Autoridad Certificante determina, de alguna otra forma, que el certificado debe ser revocado. DigiCert y los Afiliados que emiten Certificados de Firma de Código deberán observar el procedimiento para procesar las solicitudes de revocación detallados en la Sección 13.1.5 de los Requerimientos Mínimos para la Emisión y Administración de Certificados de Firma de Código de Confianza Pública.

Solamente DigiCert y CertiSur están facultados para solicitar o iniciar el proceso de revocación de los Certificados emitidos para sus propias Autoridades Certificantes. Las Autoridades de Registro están facultadas, a través de sus representantes debidamente autorizados, a solicitar la revocación de sus propios Certificados y sus Entidades Superiores estarán facultadas para solicitar o iniciar el proceso de revocación de sus Certificados.

Cualquier persona que declare que ha sido testigo de una mala utilización de un certificado o que ha observado una conducta inapropiada, fraude o compromiso de clave con relación a un certificado, puede enviar a DigiCert un Informe de Problema sobre un Certificado, mediante correo electrónico dirigido a: Support@digicert.com. DigiCert desarrollará una investigación y tomará la acción que corresponda con arreglo a los plazos definidos en los Requerimientos Básicos del CA/Browser Forum.

4.9.3 Procedimiento para Solicitar la Revocación

DigiCert procesa una solicitud de revocación de la siguiente forma:

1. DigiCert registra la entidad que realiza la solicitud o informa el problema y las razones por las cuales solicita la revocación basados en los motivos incluidos en la Sección 4.9.1. DigiCert puede también incluir en dicho registro sus propias razones para la revocación;
2. DigiCert puede requerir por un sistema fuera de línea (por ejemplo vía telefónica o facsímil) la confirmación del pedido de revocación a un administrador conocido, en donde resulte aplicable;
3. Si la solicitud es autenticada como proveniente del Suscriptor, DigiCert revocará el Certificado en los tiempos establecidos en la Sección 4.9.1, dependiendo de las razones que motivan el pedido de revocación;
4. Para solicitudes de revocación realizadas por terceros, el personal de DigiCert comenzará el proceso de investigación dentro de las veinticuatro (24) horas de recibidas y decidirá si la revocación resulta apropiada, basándose en los siguientes criterios:
    a. La naturaleza del problema esgrimido,
    b. El número de informes recibido respecto de un Certificado o sitio Web en particular,
    c. La identidad de los denunciantes (por ejemplo, una denuncia realizada por personal policial o judicial, indicando que una página Web está involucrada en actividades ilegales tiene más fuerza que una queja de un consumidor alegando que no ha recibido productos que ha adquirido), y
    d. La legislación que resulte de aplicación.
5. Si DigiCert determina que la revocación es adecuada, el personal de DigiCert procederá a revocar el Certificado y actualizará la correspondiente Lista de Certificados Revocados.

Si DigiCert lo considera adecuado, podrá derivar la información relacionada con una revocación a personal policial o judicial.

DigiCert mantiene internamente la posibilidad de responder a una solicitud de revocación de alta prioridad las veinticuatro horas del día, durante los siete días de la semana.

4.9.3.1 Procedimiento para Solicitar la Revocación de un Certificado de Suscriptor Usuario Final

Un Suscriptor usuario final que solicite la revocación debe notificar dicho requerimiento a DigiCert o al Cliente que aprobó la Solicitud del Certificado del Suscriptor, quienes en cada caso iniciarán el proceso de revocación inmediatamente. Para Clientes Corporativos, el Suscriptor deberá notificar el requerimiento al Administrador de la Empresa quien transmitirá la solicitud de revocación a DigiCert para su procesamiento. La comunicación de dicha solicitud de revocación deberá ser efectuada con arreglo a lo establecido en la Sección 3.4. Los clientes no corporativos deberán comunicar el requerimiento de revocación con arreglo a lo previsto en la Sección 3.4.

Cuando un Cliente Corporativo inicia el proceso de revocación de un Certificado de Suscriptor usuario final bajo su propia iniciativa, el Cliente de Managed PKI instruirá a DigiCert para que revoque el Certificado.

4.9.3.2 Requerimientos del CA/Browser Forum con Relación al Procedimiento para la Revocación de Certificados

Los Certificados SSL de Validación Extendida (EV), de Firma de Código de Validación Extendida (EV) y los Certificados SSL de Dominio Validado (DV) y de Organización Validada (OV) cumplen con los requerimientos respectivos del CA/Browser Forum según se establece en la Política de Certificación de DigiCert y en las Normas para el Proceso de Certificación de DigiCert.

4.9.3.3 Procedimiento para Solicitar la Revocación de un Certificado de Autoridad Certificante o Autoridad de Registro

Una Autoridad Certificante o una Autoridad de Registro que soliciten la revocación de su propio Certificado de Autoridad Certificante o de Autoridad de Registro deben notificar dicho requerimiento a DigiCert. DigiCert entonces procederá a revocar el Certificado. DigiCert o CertiSur también pueden iniciar el proceso de revocación de un Certificado de Autoridad Certificante o de Autoridad de Registro.

4.9.4 Período de Gracia para la Solicitud de Revocación

Las solicitudes de revocación deben ser remitidas tan pronto como resulte posible, dentro de plazos que resulten comercialmente razonables.

4.9.5 Tiempo dentro del cual la Autoridad Certificante debe Procesar la Solicitud de Revocación

DigiCert toma los pasos que resulten comercialmente razonables para procesar las solicitudes de revocación sin demoras. DigiCert procederá a revocar un Certificado de Autoridad Certificante dentro del plazo de una (1) hora, luego de haber recibido claras instrucciones de parte de la Autoridad de Política de DigiCert.

Dentro de las veinticuatro (24) horas de recibido un informe respecto de un problema que afecta a un Certificado, DigiCert procederá a investigar los hechos y circunstancias relacionados con el problema informado y suministrará un informe preliminar de sus recomendaciones, tanto al Suscriptor como a la entidad que reportó el problema.

Luego de revisar los hechos y circunstancias, DigiCert trabajará en conjunto con el Suscriptor y cualquier entidad que haya informado de un problema o cualquier otra información relacionada con la revocación, a los efectos de establecer la pertinencia de la revocación. El período que transcurre desde la recepción del informe del problema o noticia relacionada con la revocación

hasta que la misma sea publicada, no podrá exceder el tiempo definido en la Sección 4.9.1. El tiempo determinado por DigiCert considerará los siguientes criterios:

1. La naturaleza del problema alegado (alcance, contexto, severidad, magnitud, riesgo de daños, etc.);
2. Las consecuencias de la revocación (impactos directos o colaterales sobre Suscriptores y Partes Confiadas);
3. El número de informes de problemas respecto de un Certificado o Suscriptor en particular;
4. La entidad que realizó el reporte del problema (por ejemplo, una denuncia realizada por personal policial o judicial, indicando que una página Web está involucrada en actividades ilegales tiene más fuerza que una queja de un consumidor alegando que no ha recibido productos que ha adquirido), y
5. La legislación que resulte de aplicación.

Bajo circunstancias operativas normales, DigiCert revocará Certificados tan pronto como resulte práctico, luego de validad la solicitud de revocación, cumpliendo con los requisitos establecidos en esta Sección y en la Sección 4.9.1., generalmente dentro de los siguientes plazos:

1. Las solicitudes de revocación de Certificados de Confianza Pública son procesadas dentro de las dieciocho (18) horas de su recepción;
2. Las solicitudes de revocación recibidas con una antelación de dos horas o más a la emisión de una Lista de Certificados Revocados serán procesadas antes que se publique dicha Lista, y
3. Las solicitudes de revocación recibidas con una antelación menor a las dos horas de la emisión de una Lista de Certificados Revocados serán procesadas antes que se publique la Lista subsiguiente.

Con efecto a partir del 1º de Febrero de 2017, DigiCert cumple con los plazos de revocación especificados para casos de código malicioso en la Sección 13.1.5.3 del documento Requerimientos Mínimos para la Emisión y Administración de Certificados de Firma de Código de Confianza Pública, en la Sección, para los Certificados de Firma de Código.

4.9.6 Requerimientos para Controlar la Revocación por Partes Confiadas

Las Partes Confiadas deben controlar el estado de los Certificados sobre los cuales desean confiar. Un método que las Partes Confiadas pueden utilizar para controlar el estado de un Certificado es consultando la Lista de Certificados Revocados más reciente publicada por la Autoridad Certificante que emitió el Certificado en el cual la Parte Confiada desea confiar. Alternativamente, las Partes Confiadas pueden realizar su requerimiento controlando el estado del Certificado utilizando el repositorio basado en la Web que resulte aplicable o mediante la utilización del servicio de Protocolo del Estado del Certificado en Línea ("Online Certificate Status Protocol u OCSP"), si estuviera disponible. Las Autoridades Certificantes deberán proveer a las Partes Confiadas con información respecto de cómo localizar la Lista de Certificados Revocados apropiada, el repositorio basado en la Web o el Respondedor ("OCSP Responder") del servicio de Protocolo del Estado del Certificado en Línea ("Online Certificate Status Protocol u OCSP"), si se encontrara disponible, a los efectos de controlar el estado de revocación de los Certificados.

Debido a las numerosas y variables ubicaciones de repositorios de Listas de Certificados Revocados, las Partes Confiadas están advertidas que deben acceder a la Lista de Certificados Revocados que corresponden utilizando la dirección o direcciones URL que figuran en la extensión Punto de Distribución de la Lista de Certificados Revocados del Certificado. El Respondedor apropiado del Servicio de Protocolo del Estado del Certificado en Línea ("Online Certificate Status Protocol u OCSP") para un Certificado determinado está indicado en la extensión Acceso a la Información de la Autoridad ("Authority Information Access")

4.9.7 Frecuencia de Emisión de la Lista de Certificados Revocados (CRL)

Las Listas de Certificados Revocados de Certificados para Suscriptores usuarios finales son publicadas, como mínimo, diariamente. Las Listas de Certificados Revocados para Certificados de Autoridades Certificantes son publicadas, como mínimo, anualmente pero también cuando es revocado un Certificado de Autoridad Certificante.[14]

Las Listas de Certificados Revocados para Certificados de Autoridades Certificantes Raíz de Firma Autenticada de Contenido ("Authenticates Content Signing" o "ACS") son publicadas anualmente y también cuando es revocado un Certificado de Autoridad Certificante.

Los Certificados cuyo período de vigencia ha expirado pueden ser removidos de la Lista de Certificados Revocados después de la fecha de vencimiento.

4.9.7.1 Requerimientos del CA/Browser Forum con relación a la Emisión de las Listas de Certificados Revocados

La emisión de las Listas de Certificados Revocados para los Certificados SSL de Validación Extendida (EV), de Firma de Código de Validación Extendida (EV) y los Certificados SSL de Dominio Validado (DV) y de Organización Validada (OV) cumple respectivamente con los requerimientos del CA/Browser Forum según se establece en la Política de Certificación de DigiCert y en las Normas para el Proceso de Certificación de DigiCert.

4.9.7.2 Requerimientos de Microsoft con relación a la Emisión de las Listas de Certificados Revocados

La frecuencia de la emisión de la Lista de Certificados Revocados para los Certificados de Firma de Código o de Sello de Tiempo ("TimeStamp") está documentada en las presentes Normas y cumple con la Sección 13.2.2 de los Requerimientos Mínimos para la Emisión y Administración de Certificados de Firma de Código de Confianza Pública, publicados en https://aka.ms/csbr.

[14] La Lista de Certificados Revocados para la Autoridad Certificante "Symantec Class 3 Organizational VIP Device" es emitida solamente cuando un certificado emitido por dicha Autoridad Certificante es revocado.

4.9.8 Período de Latencia Máximo para las Listas de Certificados Revocados

Las listas de Certificados Revocados son incluidas en el repositorio dentro de plazos comercialmente razonables, luego de su generación. Esto es realizado generalmente en forma automática dentro de los minutos posteriores a la generación.

4.9.9 Disponibilidad del Control en Línea de la Revocación y Estado

La información en línea respecto de la revocación y otros datos del estado del Certificado están disponibles a través de un repositorio basado en la web y, cuando es ofrecido, a través del servicio de Protocolo del Estado del Certificado en Línea ("Online Certificate Status Protocol u OCSP"). Adicionalmente a la publicación de Listas de Certificados Revocados, DigiCert suministra información del estado del Certificado a través de funciones de consulta en su Repositorio.

DigiCert también provee información del estado del Certificado a través del Protocolo del Estado del Certificado en Línea (OCSP). Los Clientes Corporativos que contraten los Servicios de OCSP pueden controlar el estado del Certificado a través del uso de dicho Protocolo. La dirección URL para el Respondedor de OCSP que resulte apropiado es notificada al Cliente Corporativo.

DigiCert suministra respuestas del Servicio de Protocolo del Estado del Certificado en Línea (OCSP) para los Certificados de Firma de Código y de Sello de Tiempo por un período de al menos 10 años desde la expiración del certificado. Los números de serie de los certificados revocados permanecen en la Lista de Certificados Revocados por un plazo mínimo de 10 años a contar desde la fecha de expiración del certificado.

4.9.9.1 Requerimientos del CA/Browser Forum con Relación al Protocolo del Estado del Certificado en Línea ("OCSP")

La disponibilidad del servicio de Protocolo del Estado del Certificado en Línea ("Online Certificate Status Protocol u OCSP") para los Certificados SSL de Validación Extendida (EV), de Firma de Código de Validación Extendida (EV) y los Certificados SSL de Dominio Validado (DV) y de Organización Validada (OV) cumple respectivamente con los requerimientos del CA/Browser Forum según se establece en la Política de Certificación de DigiCert y en las Normas para el Proceso de Certificación de DigiCert.

4.9.10 Requerimientos de Control en Línea de la Revocación

Una Parte Confiada debe controlar el estado de un Certificado en el cual desea confiar. Si una Parte Confiada no controla el estado de un Certificado en el cual esa Parte Confiada desea confiar consultando la Lista de Certificados Revocados más reciente que resulte aplicable, la Parte Confiada debe controlar el estado del Certificado consultando el repositorio aplicable o solicitando el estado del Certificado mediante la utilización del adecuado Respondedor de OCSP, cuando el servicio de OCSP estuviera disponible.

4.9.11 Disponibilidad de Otras Formas de Publicación de la Revocación

No aplicable.

4.9.12 Requerimientos Especiales con Relación a Compromiso de Clave

DigiCert emplea todos los esfuerzos que comercialmente resulten razonables para notificar a potenciales Partes Confiadas si descubre o tiene razones para suponer que ha existido un Compromiso de la clave privada de una de sus propias Autoridades Certificantes o de una de las Autoridades Certificantes dentro del subdominio CertiSur.

4.9.13 Circunstancias para la Suspensión

No aplicable

4.9.14 Persona que Puede Solicitar la Suspensión

No aplicable

4.9.15 Procedimiento para Solicitar la Suspensión

No aplicable

4.9.16 Límites al Período de Suspensión

No aplicable

4.10 Servicios Referidos al Estado de los Certificados

4.10.1 Características Operacionales

El estado de los Certificados emitidos bajo la Symantec Trust Network está disponible a través de Listas de Certificados Revocados (CRL) en el sitio Web de DigiCert y a través del Respondedor de OCSP, cuando este servicio está disponible.

4.10.2 Disponibilidad del Servicio

Los servicios referidos al Estado de los Certificados están disponibles las 24 horas del día, durante los 365 días del año y no está prevista ninguna interrupción.

Los servicios referidos al Estado de los Certificados para los Certificados SSL de Validación Extendida (EV), de Firma de Código de Validación Extendida (EV) y los Certificados SSL de

Dominio Validado (DV) y de Organización Validada (OV) cumplen respectivamente con los requerimientos del CA/Browser Forum según se establece en la Política de Certificación de DigiCert y en las Normas para el Proceso de Certificación de DigiCert.

4.10.3 Prestaciones Opcionales

El servicio de Protocolo del Estado del Certificado en Línea ("Online Certificate Status Protocol u OCSP") es una prestación opcional respecto del estado de los Certificados que no está disponible para todos los productos y debe ser específicamente activado para otros productos.

4.11 Finalización de la Suscripción

Un suscriptor puede finalizar la suscripción de un Certificado mediante:

- Dejar que su Certificado expire sin renovarlo o reemitir (rekey) su clave
- Revocar su Certificado antes de su expiración, sin reemplazarlo.

4.12 Depósito de Claves (Key Escrow) y Recupero

Con la excepción de los Clientes Corporativos que utilizan los servicios de Administración de Claves de Managed PKI, ningún participante de la Symantec Trust Network puede ser depositario de claves privadas de Autoridades Certificantes, Autoridades de Registro o Suscriptores usuarios finales.

Los Clientes Corporativos que utilizan los servicios de Administración de Claves de Managed PKI pueden ser depositarios de copias de claves privadas de Suscriptores cuyas Solicitudes de Certificados aprueban. El Cliente Corporativo puede utilizar los servicios de Administración de Claves operados tanto fuera de sus propias instalaciones como del centro de procesamiento seguro de DigiCert. Si el servicio es operado fuera de las instalaciones del Cliente, ni DigiCert ni CertiSur almacenan copia de las claves privadas de los Suscriptores, sin perjuicio de lo cual desarrollan un rol importante en el proceso de recupero de dichas claves.

4.12.1 Depósito de Claves (Key Escrow) y Política y Procedimientos de Recupero

Los Clientes Corporativos que utilizan los servicios de Administración de Claves de Managed PKI o servicio equivalente aprobado por DigiCert, están habilitados para almacenar claves privadas de sus Suscriptores usuarios finales. Las claves privadas almacenadas deben estar resguardadas de manera encriptada utilizando el software de Administración de Claves de Managed PKI. Excepto los Clientes Corporativos que utilizan los servicios de Administración de Claves de Managed PKI o servicio equivalente aprobado por DigiCert, las claves privadas de Autoridades Certificantes o de Suscriptores usuarios finales no pueden ser depositadas en poder de terceros.

Las claves privadas de Suscriptores usuarios finales solamente pueden ser recuperadas mediando las circunstancias permitidas dentro de la Guía del Administrador del Servicio de Administración de Claves de Managed PKI, bajo las cuales:

- Los Clientes Corporativos que utilizan los servicios de Administración de Claves de Managed PKI deben confirmar la identidad de cualquier persona que invoca ser Suscriptor, a los efectos de asegurar que el requerimiento de recupero de la clave privada de ese Suscriptor es efectivamente realizado por el mismo y no por un impostor.
- Los Clientes Corporativos pueden solamente recuperar la clave privada de un Suscriptor sin su previa autorización con propósitos legítimos y legales, como por ejemplo para cumplimentar una orden judicial o proceso administrativo y no para cualquier propósito ilegal, fraudulento u otro fin ilícito, y
- Dicho Cliente Corporativo debe contar con estrictos controles de personal en vigencia que impidan que los Administradores del servicio de Administración de Claves de Managed PKI o cualquier otra persona pueda obtener un acceso no autorizado a las claves privadas almacenadas.

Es recomendable que los Clientes Corporativos que utilizan los servicios de Administración de Claves de Managed PKI:

- Notifiquen a sus Suscriptores que sus claves privadas serán almacenadas
- Proteger las claves almacenadas de los suscriptores de accesos indebidos o no autorizados
- Proteger toda la información, incluyendo las propias claves del administrador, que puede ser utilizada para el recupero de las claves privadas almacenadas
- Recuperar las claves privadas de los suscriptores almacenadas solamente mediando solicitudes de recupero autenticadas y autorizadas
- Revocar el Par de Claves del Suscriptor antes de recuperar la clave de encripción, bajo determinadas circunstancias, como por ejemplo la discontinuación en el uso de un certificado perdido
- No comunicar ninguna información concerniente al recupero de claves a los Suscriptores, excepto cuando un Suscriptor solicita el recupero de su propia clave, y
- No divulgar ni permitir que se divulguen las claves privadas almacenadas o cualquier información relacionada con las mismas a cualquier tercero, salvo que dicho requerimiento esté amparado en una legislación vigente, reglamentación gubernamental o regulación de la propia organización o por orden judicial competente.

4.12.2 Proceso de Encapsulamiento de Claves y Política y Procedimientos de Recupero de las mismas

Las Claves Privadas son resguardadas en forma encriptada en la base de datos del servicio de Administración de Claves. La clave privada de cada Suscriptor es encriptada de manera individual, utilizando su propia clave simétrica triple DES. Se genera, de esta forma, un Registro de Clave Almacenada ("Key Escrow Record" or "KER"). Luego de ello, la clave simétrica triple DES se combina con una clave de sesión aleatoria para conformar una clave de sesión enmascarada ("Mask Session Key" o "MSK"). La clave de sesión enmascarada (MSK) es enviada y almacenada de manera segura en la base de datos del servicio de Managed PKI. La clave de sesión enmascarada (KER), conteniendo la clave privada del usuario final y la clave de sesión aleatoria son

almacenadas en la base de datos del servicio de Administración de Claves y todo el material de claves residual es destruido.

La base de datos del servicio de Managed PKI es operado fuera del Centro de Procesamiento de DigiCert. El Cliente Corporativo puede elegir operar la base de datos del servicio de Administración de Claves en sus propias instalaciones o fuera del Centro de Procesamiento de DigiCert.

El recupero de una clave privada y del certificado digital requiere que el Administrador del Servicio de Managed PKI se conecte de manera segura al Centro de Control de Managed PKI, seleccione el par de claves apropiado que requiere recuperar y oprima el vínculo web "recuperar". Únicamente, después que un administrador aprobado oprimió el vínculo web "recuperar", se puede recobrar la clave de sesión enmascarada (MSK) para ese par de claves desde la base de datos del Servicio de Managed PKI. El servicio de Administración de Claves recupera la clave de sesión de la base de datos y la combina con la clave de sesión enmascarada (MSK) para regenerar la clave simétrica triple DES que fue utilizada originariamente para encriptar la clave privada del usuario final, permitiendo de esta forma el recupero de la misma. Como último paso, un archivo encriptado con el formato PKCS #12 es enviado al administrador para que finalmente se lo remita al correspondiente usuario final.

5. Controles de Instalaciones Físicas, de Administración y Operacionales

5.1 Controles Físicos

DigiCert y CertiSur han implementado la Política de Seguridad de la Información que responde a los requerimientos en materia de seguridad de las presentes Normas para el Proceso de Certificación. El cumplimiento de estas normas está incluido en los requerimientos de la auditoría independiente de DigiCert descriptas en la Sección 8. Un resumen de los requerimientos se describe en las secciones a continuación.

5.1.1 Ubicación y Construcción del Centro de Procesamiento

Todas las operaciones de las Autoridades Certificantes y Autoridades de Registro de la Symantec Trust Network son desarrolladas dentro de un entorno físicamente protegido, diseñado para evitar, prevenir y detectar el uso no autorizado, el acceso o la divulgación de datos o aplicaciones sensibles, perpetrados mediante intrusiones abiertas o encubiertas.

DigiCert cuenta también con instalaciones de recupero ante desastres para sus operaciones de Autoridad Certificante. Estas instalaciones están protegidas mediante diferentes niveles de seguridad física, comparables con los existentes en sus instalaciones primarias.

5.1.2 Acceso Físico

Las actividades sensibles de una Autoridad Certificante y cualquier actividad relacionada con el procesamiento del ciclo de vida de certificados, como por ejemplo autenticación, verificación y emisión, se producen en niveles con restricciones físicas de acceso importantes. El acceso físico es automáticamente registrado y grabado en video. No se permite el ingreso a estas áreas seguras a personas (visitantes o empleados no calificados como personal confiable) no acompañadas por personal confiable.

Los sistemas que firman Certificados y Listas de Certificados revocados están alojados en instalaciones seguras, protegidas con múltiples capas de seguridad física, monitoreo a través de videograbación, controles de acceso doble y el empleo de dos factores de autenticación, incluyendo métodos biométricos. Los dispositivos criptográficos firmantes en línea están protegidos a través del uso de gabinetes cerrados. Los dispositivos criptográficos firmantes fuera de línea están protegidos a través del uso de cajas fuertes, gabinetes y contenedores, cerrados. El acceso a los dispositivos criptográficos firmantes y material relacionado con claves está restringido con arreglo a los requerimientos de segmentación de tareas de DigiCert. La apertura y cierre de los gabinetes o contenedores en estos niveles de seguridad es registrado, con propósitos de auditoría.

5.1.3 Suministro de Energía y Aire Acondicionado

El centro de procesamiento de DigiCert está equipado con sistemas redundantes de:

- Sistemas de generación de energía, para asegurar el suministro ininterrumpido y continuo de electricidad, y
- Sistemas de calefacción, ventilación y/o aire acondicionado, para controlar la temperatura y la humedad relativa ambiente.

5.1.4 Exposición al Agua

DigiCert ha tomado todas las precauciones que resultan razonables para minimizar el impacto de la exposición al agua de sus sistemas.

5.1.5 Prevención y Protección contra el Fuego

DigiCert ha tomado las precauciones que resultan razonables para prevenir y extinguir incendios u otra exposición dañina al fuego o al humo. Las medidas de prevención de protección contra el fuego adoptadas han sido diseñadas para cumplir con las regulaciones locales en materia de seguridad.

5.1.6 Almacenamiento

Todos los elementos de almacenamiento que contienen software de producción o datos, registros de auditoría, archivos o información de resguardo están almacenados dentro de instalaciones de DigiCert o en sitios seguros fuera del mismo, con los controles de acceso apropiados, tanto físicos como lógicos, diseñados para limitar el acceso a personal autorizado y proteger dichos elementos de cualquier daño accidental (por ejemplo inundación, incendio y electromagnetismo).

5.1.7 Material de Desecho

Todos los documentos y materiales sensitivos son destruidos antes de ser desechados. Los elementos utilizados para recoger, almacenar o transmitir información sensitiva son convertidos en ilegibles antes de ser desechados. Los dispositivos criptográficos son destruidos físicamente o inicializados de acuerdo con las instrucciones de los proveedores, antes de ser desechados. Otros elementos desechados son inutilizados de acuerdo con los requerimientos de destrucción normales definidos por DigiCert.

5.1.8 Copias de Resguardo fuera del Centro de Procesamiento

DigiCert efectúa copias de resguardo en forma rutinaria sobre los datos de los sistemas críticos, los registros de auditoría y otra información igualmente sensitiva. Las copias de resguardo ubicadas fuera de sus instalaciones son igualmente almacenadas en forma segura, desde el punto de vista físico, utilizando servicios de almacenamiento contratados con terceros y en las instalaciones de recupero ante desastres de DigiCert.

5.2 Procedimientos de Control

5.2.1 Funciones Confiables

Las Personas Confiables incluyen a todos los empleados, personal contratado o consultores que tienen acceso o controlan operaciones criptográficas o de autenticación que puedan afectar materialmente a:

- La validación o la información de las Solicitudes de Certificado;
- La aceptación, 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 Suscriptores o solicitudes.

Las Personas Confiables incluyen, pero no están limitadas a:

- Personal de atención al cliente,
- Personal de operaciones criptográficas,
- Personal de seguridad,
- Personal de administración de sistemas,
- Personal de ingeniería de diseño, y
- Personal gerencial que está designado para administrar la confiabilidad de la infraestructura.

DigiCert y CertiSur consideran a las categorías de personal identificadas en esta sección como Personas Confiables, que ocupan una Posición de Confianza. Las personas que pretendan convertirse en Personas Confiables obteniendo una Posición de Confianza, deben completar en forma satisfactoria los requerimientos de análisis exigidos por estas Normas.

5.2.2 Cantidad de Personas Requeridas por Tarea

DigiCert y CertiSur han establecido, mantienen y ejecutan una política y procedimientos de control rigurosos para asegurar la segregación de funciones, basada en responsabilidades de trabajo. Las tareas más sensitivas requieren múltiples Personas Confiables.

La política y procedimientos de control se ejecutan de manera tal de asegurar una segregación de funciones basada en responsabilidades de trabajo. Las tareas más sensibles, como el acceso y la administración del hardware criptográfico de una Autoridad Certificante (unidad de firma criptográfica o "cryptographic signing unit") y el material de firma asociado, requiere la operación simultánea de múltiples Personas Confiables.

Estos procedimientos de control interno son ejecutados de manera tal de asegurar que como mínimo, dos Personas Confiables son exigidas para acceder, ya sea física o lógicamente, al dispositivo. El acceso al hardware criptográfico de la Autoridad Certificante está estrictamente restringido a múltiples Personas Confiables para su operación a través de su ciclo de vida, desde su recepción inicial e inspección hasta su destrucción física y/o lógica. Una vez que un módulo es

activado con las claves operacionales, los controles de acceso posteriores aseguran que se mantenga separado el acceso físico y el lógico al dispositivo.

Otras operaciones manuales, tales como la validación y emisión manual de Certificados Clase 3, no emitidos por un sistema automático de validación y generación, requieren la participación de dos (2) Personas Confiables como mínimo o, al menos, la combinación de una Persona Confiable y un proceso de validación y emisión automático. Las operaciones manuales para Recupero de Claves pueden opcionalmente requerir la validación de dos (2) Administradores autorizados.

5.2.3 Identificación y Autenticación para Cada Tarea

El personal que desempeña funciones de Persona Confiable, previamente ha sido sometido a un procedimiento tendiente a su identificación y autenticación individual. Dicho procedimiento contempla, entre otros, la presentación personal del postulante ante los integrantes de las áreas de Relaciones Humanas o de Seguridad, que ya revisten el carácter de Personas Confiables, debiendo acreditar la identidad, primariamente, con los documentos emitidos al efecto por la Autoridad Pública de Registro correspondiente. La identidad es posteriormente confirmada a través de los procedimientos de control de antecedentes mencionados en la Sección 5.3.1.

DigiCert y CertiSur aseguran que el personal ha alcanzado una Posición de Confianza y ha sido aprobado por el personal gerencial correspondiente, antes que a dicho personal:

- Se le emitan dispositivos de acceso y se les permita acceder a las instalaciones correspondientes;
- Se le emitan credenciales electrónicas para acceder y desarrollar funciones específicas en las Autoridades Certificantes, Autoridades de Registro u otros sistemas de procesamiento de información dentro de la Symantec Trust Network.

5.2.4 Roles que Requieren Segmentación de Responsabilidades

Los roles que exigen la Segmentación de responsabilidades incluyen, sin limitarse, las siguientes tareas:

- La validación de la información de las Solicitudes de Certificado.
- La aceptación, rechazo o cualquier otro proceso relacionado con las Solicitudes de Certificado, solicitudes de revocación, solicitudes de recupero o solicitudes de renovación o información de las solicitudes.
- La emisión o revocación de Certificados, incluyendo al personal que tiene acceso a porciones restringidas del Repositorio.
- El manejo de información o solicitudes de un Suscriptor.
- La generación, emisión o destrucción de un Certificado de Autoridad Certificante.
- La puesta en el entorno de producción de una Autoridad Certificante.

5.3 Controles Sobre el Personal

El personal que solicite transformarse en Persona Confiable deberá presentar pruebas de los antecedentes requeridos, calificaciones profesionales y experiencia necesaria para desarrollar de manera satisfactoria y competente las responsabilidades de la tarea que pretende realizar, como así también los comprobantes de cualquier autorización oficial, de existir, necesaria para desarrollar servicios de certificación bajo contratos realizados con el Estado. El control de los antecedentes se repetirá, como mínimo, cada 10 años para todo el personal que ocupe Posiciones de Confianza.

5.3.1 Requerimientos de Antecedentes, Calificaciones Profesionales, Experiencia y Autorizaciones

El personal que solicite transformarse en Persona Confiable deberá presentar pruebas de los antecedentes requeridos, calificaciones profesionales y experiencia necesaria para desarrollar de manera satisfactoria y competente las responsabilidades de la tarea que pretende realizar, como así también los comprobantes de cualquier autorización oficial, de existir, necesaria para desarrollar servicios de certificación bajo contratos realizados con el Estado.

5.3.2 Procedimientos de Control de Antecedentes

DigiCert y CertiSur realizan controles de antecedentes, antes del comienzo del desempeño en una Posición de Confianza, que incluye lo siguiente:

- confirmación de empleos anteriores,
- control de las referencias profesionales,
- confirmación del nivel de educación más alto obtenido o del que resulte relevante, y
- búsqueda de antecedentes judiciales penales y civiles (locales, provinciales y nacionales),

En caso de que alguno de los requerimientos exigidos en esta sección no puedan cumplirse debido a prohibiciones o limitaciones de la legislación local u otras circunstancias, DigiCert y CertiSur utilizarán una técnica investigativa sustituta permitida por la ley, que provea sustancialmente similar información, incluyendo pero no limitándose a obtener controles de antecedentes desarrollados por la dependencia oficial que resultara adecuada.

Los factores que surjan de un control de antecedentes que pueden ser considerados como la base para rechazar candidatos a ocupar Posiciones de Confianza o para tomar acción respecto de una Persona Confiable existente, generalmente incluyen, aunque no están limitados, a los siguientes:

- Declaraciones falsas realizadas por el candidato o la Persona Confiable,
- Referencias laborales altamente desfavorables o no confiables,
- Ciertas penas por delitos penales, y
- Demostraciones de falta de responsabilidad financiera.

Los informes que contienen dicha información son evaluados por personal de recursos humanos y de seguridad, quienes determinan el curso de acción apropiado, en función del tipo, magnitud y frecuencia del comportamiento que surja del control de antecedentes. Dichas acciones pueden

incluir medidas tales como la cancelación de la oferta de empleo realizada a los candidatos para Posiciones de Confianza o la finalización de la tarea de Empleado Confiable.

La utilización de la información emergente del control de antecedentes para tomar dichas acciones está sujeta a las leyes aplicables, nacionales o provinciales.

5.3.3 Requerimientos de Capacitación

DigiCert y CertiSur proveen al personal, inmediatamente después de su ingreso y, más adelante, en forma recurrente, la capacitación necesaria para desarrollar las responsabilidades de su tarea en forma competente y satisfactoria. Se mantienen registros de dichas actividades de capacitación. DigiCert y CertiSur revisan y mejoran en forma periódica sus programas de capacitación internos, tal como resulte necesario.

Los programas de capacitación internos de DigiCert y CertiSur están diseñados a la medida de las responsabilidades individuales e incluyen los siguientes tópicos relevantes:

- Conceptos básicos de una Infraestructura de Clave Pública,
- Responsabilidades de la tarea,
- Procedimientos y Políticas operativas y de seguridad,
- Uso y operación del hardware y software desarrollado,
- Manejo e informes de Incidentes y Compromisos, en material de seguridad, y
- Procedimientos de recupero ante desastres y continuidad de los negocios.

5.3.3.1 Requerimientos del CA/Browser Forum con Relación a Capacitación y Nivel de Conocimiento

Para los Certificados SSL de Validación Extendida (EV), de Firma de Código de Validación Extendida (EV) y los Certificados SSL de Dominio Validado (DV) y de Organización Validada (OV), la capacitación del personal es desarrollada conforme a los requerimientos del CA/Browser Forum según se establece en la Política de Certificación de DigiCert y en las Normas para el Proceso de Certificación de DigiCert.

5.3.4 Frecuencias y Requerimientos en Materia de Capacitación

DigiCert y CertiSur proveen a su personal capacitación recurrente y actualizaciones, con la extensión y frecuencia requeridas para asegurar que dicho personal mantiene el nivel exigido de capacidad para desempeñar las responsabilidades de su tarea, en forma competente y satisfactoria.

5.3.5 Frecuencia y Secuencia en la Rotación de Tareas

No aplicable.

5.3.6 Sanciones Disciplinarias por Acciones No Autorizadas

En caso de comprobarse la ejecución de acciones no autorizadas u otras violaciones a las políticas y procedimientos de DigiCert y CertiSur, se tomarán las sanciones disciplinarias apropiadas. Las sanciones disciplinarias pueden incluir hasta el despido y están proporcionadas a la frecuencia y severidad de las acciones no autorizadas que se hubieran ejecutado.

5.3.7 Requerimientos Respecto del Personal Contratado

En circunstancias limitadas, se puede utilizar personal contratado o consultores para desempeñar Posiciones de Confianza. Resulta de aplicación, para dichos contratados o consultores, el mismo criterio funcional y de seguridad que para los empleados de DigiCert y CertiSur que ocupan una posición comparable.

El personal contratado y los consultores que no hayan completado o aprobado los procedimientos de control de antecedentes especificados en la Sección 5.3.2 pueden acceder a las instalaciones seguras de DigiCert o de CertiSur, solamente si están permanentemente acompañados y directamente supervisados por Personas Confiables.

5.3.8 Documentación Suministrada al Personal

DigiCert y CertiSur le suministran al personal la capacitación requerida y otra documentación que fuera necesaria para que desarrollen las responsabilidades que su tarea exige, en forma competente y satisfactoria.

5.4 Procedimientos Relacionados con los Registros de Auditoría

5.4.1 Tipos de Eventos Registrados

DigiCert, en forma manual o automática, registran los siguientes eventos significativos:

- Eventos de administración del ciclo de vida de una Autoridad Certificante, que incluyen:
  - Generación, resguardo, archivo, recuperación, almacenamiento y destrucción de claves.
  - Cambios en detalles o claves de las Autoridades Certificantes
  - Eventos relacionados con la administración del ciclo de vida de los dispositivos criptográficos.
- Eventos de administración del ciclo de vida de los Certificados de Autoridad Certificante y de Suscriptor, que incluyen:
  - Solicitudes de Certificado, emisión, renovación, reemisión de claves y revocación
  - Procesamiento de solicitudes, aprobadas o rechazadas
  - Cambios en las políticas de creación de certificados
  - Generación y emisión de Certificados y Listas de Certificados Revocados.
- Eventos relacionados con los Empleados Confiables, que incluyen:
  - Intentos de inicio y cierre de sesiones

- Creación, remoción, establecimiento de contraseñas o cambio en los niveles de privilegio de los usuarios privilegiados.
- Cambios de personal.

- Eventos relacionados con seguridad, que incluyen:
  - Intentos de acceso a los sistemas de PKI, exitosos o no
  - Comienzo y finalización de sistemas y aplicaciones
  - Posesión de datos de activación para operaciones de Clave Privada de una Autoridad Certificante
  - Cambios y mantenimiento en la configuración de los sistemas
  - Acciones sobre el sistema de PKI y su seguridad desarrolladas por personal de DigiCert o CertiSur.
  - Lectura, escritura, borrado o destrucción de archivos o registros sensibles en materia de seguridad.
  - Cambios en la configuración de seguridad.
  - Caídas del sistema, fallas de hardware y otras anomalías.
  - Actividad de Firewalls y routers.
  - Entradas y salidas de visitantes a las instalaciones de la Autoridad Certificante.

Los registros de los ingresos de datos incluyen los siguientes elementos:

- Fecha y hora del ingreso
- Número serial o de secuencia del ingreso, para ingresos periódicos automáticos
- Identidad de la entidad que efectúa el ingreso periódico
- Tipo de ingreso.

La información de los registros de las Solicitudes de Certificados para las autoridades de Registro de CertiSur y los Administradores de Clientes Corporativos incluyen:

- Tipo de documento de identidad presentado por el Solicitante del Certificado
- Registro de datos o números únicos de identificación o una combinación resultante (por ejemplo, número de documento nacional de identidad del Solicitante del Certificado) de los documentos de identificación, si resultara de aplicación
- Ubicación de archivo de las copias de las solicitudes y de los documentos identificatorios
- Identidad de la entidad que aceptó la solicitud
- Método empleado para validar los documentos de identidad, de corresponder
- Nombre de la Autoridad Certificante receptora o de la Autoridad de Registro remitente, si fuera aplicable.

Los Certificados SSL de Validación Extendida (EV), de Firma de Código de Validación Extendida (EV) y los Certificados SSL de Dominio Validado (DV) y de Organización Validada (OV) cumplen con los requerimientos del CA/Browser Forum según se establece en la Política de Certificación de DigiCert y en las Normas para el Proceso de Certificación de DigiCert.

5.4.2 Frecuencia de Procesamiento del Registro

El sistema de Autoridades Certificantes está continuamente monitoreado para suministrar alertas en tiempo real acerca de eventos operativos y de seguridad significativos, a los efectos de que sean

analizados por personal de seguridad informática especialmente designado. Las revisiones mensuales de los registros de auditoría incluyen una verificación de que los mismos no hayan sido adulterados y una investigación de cualquier alerta o irregularidad que figure en el mismo. Las acciones tomadas como consecuencia de la revisión del registro también son documentadas.

5.4.3 Período de Disponibilidad del Registro de Auditoría

Los registros de auditoría están disponibles en el lugar en el cual se generan por lo menos durante dos (2) meses a contar desde su procesamiento y son archivados posteriormente con arreglo a lo establecido en la Sección 5.5.2.

5.4.4 Protección del Registro de Auditoría

Los archivos de los registros de auditoría, tanto manuales como electrónicos, están protegidos contra modificaciones, accesos, borrado u otras adulteraciones no autorizadas, a través del uso de controles de acceso, físicos y lógicos.

5.4.5 Procedimientos de Resguardo de los Registros de Auditoría

Diariamente se generan copias de resguardo incrementales de los registros de auditoría mientras que en forma semanal se realiza una copia de resguardo total.

5.4.6 Sistema de Recolección de Auditoría (Interna y Externa)

Los datos de auditoría automáticos son generados y registrados a nivel de los sistemas aplicativos, operativos y de red. Los datos de auditoría generados manualmente son registrados por personal de DigiCert.

5.4.7 Notificación al Sujeto Causante del Evento

Cuando un evento es registrado por el sistema de recolección de auditoría, no está previsto efectuar notificación alguna al individuo, organización o dispositivo causante de la ocurrencia de tal evento.

5.4.8 Evaluaciones de Vulnerabilidad

Los eventos en el proceso de auditoría son registrados, en parte, en un sistema de monitoreo de vulnerabilidades. Las evaluaciones de vulnerabilidad sobre seguridad lógica son desarrolladas, revisadas y controladas después de un análisis del monitoreo de dichos eventos. Dichas evaluaciones están basadas en registros de datos automáticos en línea y se desarrollan diariamente, mensualmente y anualmente. Una evaluación anual de vulnerabilidad sobre seguridad lógica sirve de base para la Auditoría de cumplimiento que se realiza anualmente.

5.5 Archivo de Registros

5.5.1 Tipos de Registros Archivados

DigiCert archiva lo siguiente:

- Todos los registros de auditoría recolectados con arreglo a lo especificado en la Sección 5.4
- La información de las solicitudes de Certificados
- La documentación de soporte de las solicitudes de Certificados, incluyendo los resultados de la Autorización de Autoridad Certificante (CAA)
- La información relacionada con el ciclo de vida de los certificados, como por ejemplo los datos de las solicitudes de revocación, reemisión (rekey) y renovación.

5.5.2 Período de Guarda en Archivo

Los registros asociados con un Certificado deben ser almacenados por lo menos durante el período de tiempo establecido a continuación, contado a partir de la fecha en que el Certificado ha expirado o ha sido revocado:

- Cinco (5) años para Certificados de Clase 1,
- Diez (10) años y seis (6) meses para Certificados de Clases 2 y 3.

5.5.3 Protección de Archivos

DigiCert y CertiSur protegen sus registros archivados compilados de manera tal que solamente Personas Confiables autorizadas puedan acceder a los datos archivados. Los datos archivados electrónicamente están protegidos contra la lectura, modificación, borrado u otra adulteración no autorizada, a través de su archivo en un Sistema Confiable. El medio de almacenamiento de los datos archivados y las aplicaciones necesarias para procesar los datos almacenados son mantenidos para asegurar que los datos archivados puedan estar accesibles durante el lapso de tiempo establecido en estas Normas.

5.5.4 Procedimientos de Resguardo de Archivos

DigiCert efectúa resguardos de sus archivos electrónicos con información sobre los Certificados emitidos, incrementalmente en forma diaria. Las copias de los registros en papel compilados son almacenadas en una instalación segura de recupero ante desastres, fuera del sitio de procesamiento.

5.5.5 Requerimientos de Sellado de Tiempo (Time-Stamp) de los Registros

Los Certificados, Listas de Certificados Revocados y otros datos ingresados en la base de datos de revocación contienen información sobre fecha y hora. No es necesario que dicha información de fecha y hora sea generada criptográficamente.

5.5.6 Sistema de Recolección de Archivos (Internos o Externos)

Los sistemas de recolección de archivos de DigiCert y CertiSur son internos, con la excepción de los Clientes Corporativos que operan como Autoridades de Registro. CertiSur asiste a sus Clientes Corporativos que actúan como Autoridades de Registro en la preservación de sus registros de auditoría. No obstante, tal sistema de recolección de archivos es externo y de dicho Cliente Corporativo que actúa como Autoridad de Registro.

5.5.7 Procedimientos para Obtener y Verificar Información Archivada

Solamente Personal Confiable está habilitado para obtener acceso al archivo. La integridad de la información es verificada cuando la misma es recuperada.

5.6 Cambio de Claves

Los pares de claves de las Autoridades Certificantes de la Symantec Trust Network son retirados de servicio al finalizar el plazo máximo de sus respectivas vidas útiles tal como está definido en las presentes Normas. Los Certificados de Autoridades Certificantes pueden ser renovados en la medida en que el plazo certificado de vida útil acumulado del par de claves de la Autoridad Certificante no exceda el plazo máximo de vida útil del par de claves de la Autoridad Certificante. Los nuevos pares de claves de Autoridades Certificantes deben ser generados cuando resulte necesario, por ejemplo para reemplazar a un par de claves de Autoridad Certificante que ha sido retirado, para suplementar pares de claves activas existentes y para soportar nuevos servicios.

Antes del vencimiento del Certificado de Autoridad Certificante de una Autoridad Certificante Superior, se establecen los procedimientos de cambio de claves para facilitar una transición sin inconvenientes a las entidades dentro de la jerarquía de las Autoridades Certificantes Superiores, del anterior par de claves de la Autoridad Certificante Superior al nuevo par de claves. Los procedimientos de cambio de claves de Autoridades Certificantes de la Symantec Trust Network requieren que:

- Una Autoridad Certificante Superior cese en la emisión de nuevos Certificados de Autoridades Certificantes Subordinadas con una antelación no menor a sesenta (60) días de una fecha ("Fecha de Cese de Emisión") en donde el tiempo de vida útil remanente del par de claves de la Autoridad Certificante Superior es igual al Período de Vigencia del Certificado aprobado para el tipo específico de Certificado emitido por la Autoridad Certificante Subordinada dentro de la jerarquía de la Autoridad Certificante Superior.
- Después que las solicitudes de Certificados para Autoridades Certificantes subordinadas o de Suscriptores usuarios finales recibidos después de la "Fecha de Cese de Emisión" sean validadas satisfactoriamente, los Certificados serán firmados con un nuevo par de claves de Autoridad Certificante.

La Autoridad Certificante Superior continuará emitiendo Listas de Certificados Revocados firmadas con la clave privada original de la Autoridad Certificante Superior hasta que se llegue a la fecha de finalización del plazo de vigencia del último Certificado emitido utilizando el par de claves original.

5.7 Recupero ante Desastres y Compromiso de Claves

5.7.1 Procedimientos para el Manejo de Incidentes y Compromisos

La siguiente información de una Autoridad Certificante es resguardada en archivos seguros fuera del sitio de procesamiento y estará disponible en el evento de un Compromiso o desastre: datos de las Solicitudes de Certificado, registros de auditoría y registros de las bases de datos para todos los Certificados emitidos. Los resguardos de las claves privadas de Autoridades Certificantes serán generados y mantenidos de acuerdo con la Sección 6.2.4. DigiCert mantiene resguardos de similar información para sus propias Autoridades Certificantes como así también de las Autoridades Certificantes de sus Clientes Corporativos dentro del Subdominio CertiSur.

5.7.2 Daño de Recursos Computacionales, Software y/o Datos

En caso de producirse algún daño de los recursos computacionales, software y/o datos, el evento es informado inmediatamente al área de Seguridad de DigiCert y se ponen en vigencia procedimientos de manejo de incidentes. Estos procedimientos establecen mecanismos apropiados para escalar jerárquicamente, investigar el incidente y desarrollar la respuesta adecuada. Si resultara necesario, también se ponen en vigencia los procedimientos de DigiCert relacionados con Compromiso de claves y recupero ante desastres.

5.7.3 Procedimientos ante el Compromiso de la Clave de una Entidad

En caso de sospecharse o conocerse el Compromiso de una clave privada de una Autoridad Certificante de CertiSur, de una Autoridad Certificante de Infraestructura de la Symantec Trust Network o de una Autoridad Certificante de un Cliente de CertiSur, son aplicados inmediatamente los procedimientos de Respuesta ante Compromisos de Claves por parte del Grupo Especial de Respuesta ante Incidentes de Seguridad de DigiCert. Este grupo, que incluye personal de Seguridad, Operaciones Criptográficas, Servicios de Producción y otros representantes del personal gerencial de DigiCert y CertiSur, evalúa la situación, desarrolla un plan de acción e implementa el mismo con la aprobación de las gerencias ejecutivas de DigiCert y CertiSur.

Si es requerida la revocación de un Certificado de Autoridad Certificante, los siguientes procedimientos son llevados a cabo:

- El estado de revocación del Certificado es comunicado a las Partes Confiadas a través del repositorio de DigiCert, de acuerdo con lo establecido en la Sección 4.9.7,
- Se realizan todos los esfuerzos que resulten razonables comercialmente para suministrar notificación adicional de la revocación a todos los Participantes de la Symantec Trust Network que pudieran ser afectados, y
- La Autoridad Certificante generará un nuevo par de claves, de acuerdo con lo previsto en la Sección 5.6, excepto cuando se trate de la finalización de la Autoridad Certificante, según lo establecido en la Sección 5.8.

5.7.4 Capacidad de Continuación de las Operaciones después de un Desastre

DigiCert ha diseñado y mantiene un plan de continuidad de negocios de manera tal que en caso de un evento que implique una interrupción de las operaciones, las funciones críticas puedan ser reasumidas. DigiCert mantiene un Centro de Recupero ante Desastres que está localizado en un lugar geográficamente separado del Centro de Procesamiento principal. En la eventualidad que un desastre generado por el hombre o por causas naturales requiera la cesación permanente de las operaciones en el centro principal de procesamiento de DigiCert, el Grupo de Administración de coordinará con los diferentes grupos funcionales la decisión de declarar formalmente la situación de desastre y administrar el incidente. Una vez que la situación de desastre es declarada, se inicia el proceso de recuperación de los servicios de producción de DigiCert en el Centro de Recupero ante Desastres.

DigiCert ha desarrollado un Plan de Recupero ante Desastres para sus servicios de Managed PKI, incluyendo los servicios de PKI de la Symantec Trust Network. Este Plan identifica las condiciones para su activación y especifica lo que constituye el tiempo de interrupción y de recupero aceptables. Asimismo define los procedimientos que deben emplear los grupos de trabajo para recuperar las operaciones de la Symantec Trust Network utilizando los datos de resguardo y las copias de resguardo de las claves.

Adicionalmente, para los Certificados SSL de Validación Extendida (EV), de Firma de Código de Validación Extendida (EV) y los Certificados SSL de Dominio Validado (DV) y de Organización Validada (OV) el Plan de Recupero ante Desastres cumple con los requerimientos del CA/Browser Forum según se establece en la Política de Certificación de DigiCert y en las Normas para el Proceso de Certificación de DigiCert

El objetivo fijado para la recuperación de la funcionalidad de los servicios críticos de producción es no mayor a las 24 horas.

DigiCert realiza al menos una vez por año calendario una prueba de recuperación ante desastres para asegurar la funcionalidad de los servicios en el Centro de Recupero ante Desastres. Ejercicios formales de continuidad de negocios son llevados a cabo anualmente en donde se prueban y evalúan tipos de escenario adicionales (por ejemplo, pandemia, terremoto, inundación o falta de energía eléctrica).

DigiCert desarrolla esfuerzos significativos para desarrollar, mantener y probar plantes de recuperación de negocios razonables y la planificación de DigiCert para afrontar un desastre o una interrupción de las operaciones es consistente con la mayoría de las mejores prácticas en la materia dentro de la industria.

DigiCert mantiene hardware redundante y copias de resguardo del software de sus sistemas de Autoridad Certificante e Infraestructura, en sus instalaciones de recupero ante desastres. Adicionalmente, las claves privadas de las Autoridades Certificantes tienen copias de resguardo que son mantenidas con el propósito de utilizarlas en el proceso de recupero ante desastres, de acuerdo con lo establecido en la Sección 6.2.4.

DigiCert mantiene copias de resguardo fuera de su Centro de Procesamiento de toda la información relevante de sus Autoridades Certificantes como así también de las Autoridades Certificantes de los Service Centers y Clientes Corporativos dentro del Subdominio CertiSur. Esta información incluye, pero no está limitada a los datos de las Solicitudes de Certificado, los registros de Auditoría con arreglo a lo previsto en la Sección 4.5 y los registros de sus bases de datos, para todos los certificados emitidos.

CertiSur, en su función de Service Center de DigiCert, utiliza las instalaciones de DigiCert para llevar a cabo parte de sus tareas operativas. CertiSur ha diseñado un plan de contingencia, tal como se describe en esta Sección, el cual es aplicado a las tareas que son realizadas localmente por CertiSur. Este plan ha sido diseñado y probado para mitigar los efectos producidos por errores humanos o eventos naturales. El Plan de Recupero ante Desastres se encuentra orientado a restaurar los sistemas de información y los servicios críticos en un plazo acotado de tiempo. El orden de reactivación de los mismos se encuentra determinado por el valor crítico de los servicios.

Es importante destacar que todas las funciones operativas críticas de los Clientes Corporativos de CertiSur S.A. (solicitud, aprobación y emisión, solicitud de revocación, reemplazo y renovación) son cubiertas por el Centro de Procesamiento de DigiCert.

CertiSur mantiene fuera de línea copias de seguridad de la información importante sobre Autoridades Certificantes administradas por CertiSur y de sus servicios de validación, en instalaciones de alta seguridad, externas a los centros operativos. Dicha información incluye registros de la base de datos de los certificados emitidos en el Subdominio CertiSur, registros de acceso a las aplicaciones que son procesadas localmente y registros de auditoría de las tareas que desarrolla el Personal Confiable de CertiSur en sus instalaciones.

5.8 Finalización de una Autoridad Certificante o de una Autoridad de Registro

En caso de que resultara necesario el cese de operaciones de una Autoridad Certificante de la Symantec Trust Network o de una Autoridad Certificante de un Cliente Corporativo, DigiCert realizará todos los esfuerzos que comercialmente resulten razonables para notificar con antelación respecto de dicho cese a Suscriptores, Partes Confiadas y otras entidades afectadas. Cuando sea requerido el cese de actividades de una Autoridad Certificante, DigiCert y, en el caso de una Autoridad Certificante de un Cliente Corporativo, dicho cliente, desarrollarán un plan de finalización a efectos de minimizar los efectos de la interrupción respecto de Clientes, Suscriptores y Partes Confiadas. Dicho plan de finalización debe incluir lo siguiente, según resulte de aplicación:

- Notificación a las partes afectadas por el cese de actividades, tales como Suscriptores, Partes Confiadas y Clientes, informándoles respecto del estado de la Autoridad Certificante,
- Soportar el costo que implique dicha notificación,
- Revocación del Certificado emitido a la Autoridad Certificante por DigiCert,
- La preservación de los archivos y registros de la Autoridad Certificante, durante los plazos establecidos en las presentes Normas,

- La continuidad de los servicios de soporte a Suscriptores y clientes,
- La continuidad de los servicios de revocación, tales como la emisión de las Listas de Certificados Revocados o los servicios de control en línea del estado de los Certificados,
- La revocación de los Certificados no vencidos y que no hubieran sido revocados con anterioridad, de Suscriptores usuarios finales y de Autoridades Certificantes subordinadas, de corresponder.
- El pago de una compensación, si resultara necesario, a los Suscriptores cuyos certificados no vencidos y no revocados con anterioridad sean revocados como consecuencia del plan de finalización o, alternativamente, la emisión de Certificados de reemplazo por parte de una Autoridad Certificante sucesora,
- Eliminación de la clave privada de la Autoridad Certificante y de los dispositivos de hardware que contienen dicha clave privada, y
- Las estipulaciones necesarias para la transición de los servicios de la Autoridad Certificante a la Autoridad Certificante sucesora, de existir.

5.9 Seguridad de Datos

Para la emisión de Certificados SSL de Validación Extendida (EV), Certificados de Firma de Código de Validación Extendida (EV) y Certificados SSL de Organización Validada (OV) o de Dominio Validado (DV), DigiCert cumple con los requerimientos de Seguridad de Datos del CA/Browser Forum, tal como está establecido en la Política de Certificación de DigiCert y en las Normas para el Proceso de Certificación de DigiCert.

6. Controles de Seguridad Técnicos

6.1 Generación e Instalación de Par de Claves

6.1.1 Generación de Par de Claves

La generación del par de claves de una Autoridad Certificante es desarrollada por múltiples individuos confiables, preseleccionados y entrenados, que utilizan Sistemas Confiables y procesos que proveen la seguridad y fortaleza criptográfica requerida para las claves generadas. Para las Autoridades Primarias de Certificación y las Autoridades Certificantes Raíz Emisoras, los módulos criptográficos utilizados para la generación de claves cumplen con los requerimientos de los estándares FIPS 140-2 nivel 3. Para otras Autoridades Certificantes, incluyendo las Autoridades Certificantes de CertiSur y Autoridades Certificantes de Clientes de Managed PKI, los módulos criptográficos empleados cumplen, como mínimo, con los requerimientos de los estándares FIPS 140-2 nivel 2.

Todos los pares de claves de Autoridades Certificantes son generados en Ceremonias de Generación de Claves planificadas con anterioridad. Las actividades desarrolladas en cada ceremonia de generación de claves son registradas, fechadas y firmadas por todos los individuos participantes. Estos registros son resguardados para propósitos de auditoría y seguimiento, por el período de tiempo que el personal gerencial de DigiCert estime apropiado.

La generación del par de claves de Autoridades de Registro es generalmente desarrollada por la Autoridad de Registro, utilizando módulos criptográficos certificados, según estándares FIPS 140-2 nivel 1, provistos con su software de navegación (browser).

Los Clientes Corporativos generan el par de claves utilizado por sus servidores de Administración Automática. CertiSur recomienda que la generación del par de claves para el servidor de Administración Automática sea realizada utilizando un módulo criptográfico certificado, según estándares FIPS 140-2 nivel 2.

La generación del par de claves de un Suscriptor usuario final es generalmente desarrollada por el Suscriptor. Para los Certificados de Clase 1, Certificados de Clase 2 y Certificados de Clase 3 de firma de código y objeto, el Suscriptor utiliza normalmente, para la generación de claves, un módulo criptográfico certificado, según estándares FIPS 140-2 nivel 1, provisto con su software de navegación (browser). Para Certificados para servidor, el suscriptor utiliza normalmente la herramienta de generación de claves provista con su software de servidor web.

Para las Solicitudes de Certificado de Firma de Contenido Autenticado, DigiCert genera un par de claves en nombre del Suscriptor utilizando semillas aleatorias generadas en un módulo criptográfico que, como mínimo, cumple con los requerimientos del estándar FIPS 140-2 nivel 3.

6.1.2 Entrega de la Clave Privada al Suscriptor

El par de claves de un Suscriptor usuario final es generado por el Suscriptor usuario final, por lo tanto la entrega de la clave privada al Suscriptor no resulta de aplicación. Para las Solicitudes de

Certificado de Firma de Contenido Autenticado, tampoco resulta de aplicación la entrega de la clave privada al Suscriptor.

Cuando el par de claves de un Suscriptor usuario final o de una Autoridad de Registro es pregenerado por DigiCert en dispositivos externos, tales como tokens o tarjetas smart cards, estos dispositivos son distribuidos al Suscriptor usuario final o a la Autoridad de Registro utilizando un servicio de entrega seguro y un contenedor que le permite detectar al receptor una eventual violación de dicho contenedor. Los datos requeridos para la activación del dispositivo son comunicados a la Autoridad de Registro o al Suscriptor usuario final utilizando un procedimiento totalmente separado del anterior. La distribución de dichos dispositivos es controlada y registrada por DigiCert.

Cuando el par de claves de un Suscriptor usuario final es pregenerado por un Cliente Corporativo en dispositivos externos, tales como tokens o tarjetas smart cards, estos dispositivos son distribuidos al Suscriptor usuario final utilizando un servicio de entrega seguro y un contenedor que le permite detectar al receptor una eventual violación de dicho contenedor. Los datos requeridos para la activación del dispositivo son comunicados al Suscriptor usuario final utilizando un procedimiento totalmente separado del anterior. La distribución de dichos dispositivos es controlada y registrada por el Cliente Corporativo.

Para Clientes Corporativos que utilizan el Servicio de Recupero de Claves provisto por el Key Manager de Managed PKI, el Cliente puede generar el par de claves de encriptación (en nombre de los Suscriptores cuyas Solicitudes de Certificado el Cliente aprueba) y transmitir dicho par de claves a los Suscriptores, a través de un archivo PKCS #12, protegido con una contraseña.

Los Certificados para Servidor SSL y los certificados para firma de correo electrónico S/MIME no son distribuidos como un archivo PKCS #12. Los Certificados para firma de correo electrónico S/MIME pueden ser distribuidos como un archivo PKCS #12 utilizando canales seguros y contraseñas suficientemente seguras, enviadas por un medio separado del archivo conteniendo el certificado.

6.1.3 Entrega de la Clave Pública al Emisor del Certificado

Los Suscriptores usuarios finales y las Autoridades de Registro remiten sus claves públicas a DigiCert para su certificación electrónica, a través de un archivo PKCS #10 Solicitud de Firma de un Certificado (Certificate Signing Request o CSR) u otro paquete firmado digitalmente, en una sesión segura por la utilización del protocolo SSL. En el caso que el par de claves de una Autoridad Certificante, de una Autoridad de Registro o de un Suscriptor usuario final es generado por DigiCert, este requerimiento no resulta de aplicación.

6.1.4 Entrega de la Clave Pública de la Autoridad Certificante a Partes Confiadas

DigiCert posibilita que los Certificados de Autoridad Certificante de las Autoridades Primarias de Certificación y sus Autoridades Certificantes raíces estén disponibles para Suscriptores y Partes Confiadas a través de su inclusión en el software de navegación (browser). En la medida en que

sean generados nuevos Certificados de Autoridades Primarias de Certificación y Autoridades Certificantes raíces, DigiCert entrega dichos Certificados a los fabricantes, para su inclusión en las nuevas versiones o actualizaciones de sus navegadores.

DigiCert y CertiSur generalmente proveen al Suscriptor usuario final la totalidad de la cadena de certificación (incluyendo la Autoridad Certificante emisora y cualquiera de las Autoridades Certificantes en la cadena), al emitir el Certificado.

6.1.5 Longitudes de Clave

Los pares de claves tienen que contar con una longitud suficiente como para prevenir que terceros puedan determinar la clave privada de dichos pares de claves mediante la utilización de criptoanálisis, durante el período de tiempo en el que se espera que dichos pares de claves sean utilizados. El Estándar de DigiCert para la longitud mínima de claves es la utilización de pares de claves con una fortaleza mínima equivalente a 2048 bits RSA para las Autoridades Primarias de Certificación y las Autoridades Certificantes. La tabla siguiente incluye los pares de claves de las Raíces DigiCert y su fortaleza:

Algoritmo de Clave Pública	***Algoritmo de Firma***	***Clase***	***Generación***
2048 bits RSA	SHA 1	Autoridades Primarias de Certificación Clases 1, 2 y 3	Autoridades Primarias de Certificación G3
		Autoridad Primaria de Certificación Clase 3	Autoridad Primaria de Certificación G5
	SHA 256	Autoridad Primaria de Certificación Raíz Universal Clases 1, 2 y 3	Autoridades Primarias de Certificación G6
384 bits ECC	SHA 384	Autoridades Primarias de Certificación Clases 1, 2 y 3(*)	Autoridades Primarias de Certificación G4
4096 bits RSA	SHA 384	Autoridad Primaria de Certificación Clase 3	Autoridad Primaria de Certificación G6
2048_256 bits DSA	SHA 256	Autoridades Primarias de Certificación Clases 1, 2 y 3	Autoridades Primarias de Certificación G7
(*) Hay dos Raíces G4 de Clase 3: una con la marca VeriSign (legada) y otra con la marca Symantec			

Tabla 8: Autoridades Certificantes Raíz de DigiCert y Longitud de Claves

Todos los Certificados de todas las clases de Autoridades Primarias de Certificación y Autoridades Certificantes de la Symantec Trust Network y de CertiSur, de Autoridades de Registro y de entidades finales utilizan los estándares SHA-2 para los algoritmos de hash de firmas digitales y ciertas versiones del Centro de Procesamiento de DigiCert soportan el uso del algoritmo de hash bajo el estándar SHA-256 y SHA-384 para los Certificados de Suscriptores usuarios finales. El algoritmo SHA-1 puede ser empleado para soportar aplicaciones legadas y otros casos, diferentes de Certificados de Servidor SSL y Certificados de Validación Extendida de Firma de Código y siempre que tal uso no sea contrario a los procedimientos y políticas definidos por el CA/Browser Forum y Proveedores de Aplicaciones de Software relacionados.

6.1.5.1 Requerimientos del CA/Browser Forum con Relación al Tamaño de Claves

Los Certificados SSL de Validación Extendida (EV), de Firma de Código de Validación Extendida (EV) y los Certificados SSL de Dominio Validado (DV) y de Organización Validada (OV) cumplen con los requerimientos del CA/Browser Forum según se establece en la Política de Certificación de DigiCert y en las Nomas para el Proceso de Certificación de DigiCert[15].

Los Certificados de la Autoridad Certificante Raíz de DigiCert cumplen con los siguientes requerimientos, en relación al tipo de algoritmo y tamaño de clave:

	Período de vigencia comenzando el o antes del 31 de Diciembre de 2010	***Período de vigencia comenzando después del 31 de Diciembre de 2010***
Algoritmo de Hash	MD5 No Recomendado SHA-1, SHA-256, SHA-384 o SHA-512	SHA-1*, SHA-256, SHA-384 o SHA-512
Longitud mínima del módulo RSA (bits)	2048**	2048
Longitud mínima del módulo DSA (bits)	No Disponible	2048
Curva ECC	NIST P-256, P-384 o P-521	NIST P-256, P-384 o P-521

Tabla 9 – Algoritmos y Tamaño de Claves para Certificados de Autoridad Certificante Raíz

Los Certificados de Autoridades Certificantes Subordinadas de DigiCert cumplen con los siguientes requerimientos, en relación al tipo de algoritmo y tamaño de clave:

	Período de vigencia comenzando el o antes del 31 de Diciembre de 2010 y finalizando en o antes del 31 de Diciembre de 2013	***Período de vigencia comenzando después del 31 de Diciembre de 2010 o finalizando después del 31 de Diciembre de 2013***
Algoritmo de Hash	SHA-1, SHA-256, SHA-384 o SHA-512	SHA-1*, SHA-256, SHA-384 o SHA-512
Longitud mínima del módulo RSA (bits)	1024	2048
Longitud mínima del módulo DSA (bits)	2048	2048
Curva ECC	NIST P-256, P-384 o P-521	NIST P-256, P-384 o P-521

Tabla 10 – Algoritmos y Tamaño de Claves para Certificados de Autoridad Certificante Subordinada

Las Autoridades Certificantes DigiCert solamente emiten certificados para Suscriptores con claves que contienen los siguientes tipos de algoritmo y tamaño:

[15] Los certificados de la Symantec Trust Network que posean pares de claves no estándar o tamaño de claves inferior a 2048 bits están autorizados para ser utilizados dentro de un grupo seleccionado o dentro de un ecosistema cerrado.

	Período de vigencia finalizando en o antes del 31 de Diciembre de 2013	*Período de vigencia finalizando después del 31 de Diciembre de 2013*
Algoritmo de Hash	SHA-1*, SHA-256, SHA-384 o SHA-512	SHA-1*, SHA-256, SHA-384 o SHA-512
Longitud mínima del módulo RSA (bits)	1024	2048
Longitud mínima del módulo DSA (bits)	2048	2048
Curva ECC	NIST P-256, P-384 o P-521	NIST P-256, P-384 o P-521

Tabla 11 – Algoritmos y Tamaño de Claves para Certificados de Suscriptores

*SHA-1 puede ser utilizado con claves RSA de acuerdo con los criterios definidos en la Sección 7.1.3 de los Requerimientos Básicos para la Emisión y Administración de Certificados de Confianza Pública del CA/Browser Forum y en la Política de Raíz de Mozilla, versión 2.5 o superior, en donde resulte aplicable.
**Un Certificado de una Autoridad Certificante Raíz emitido antes del 31 de Diciembre de 2010 con un tamaño de clave RSA menor a 2048 bits aún puede ser utilizado como raíz de confianza de Certificados de Suscriptor emitidos con arreglo a estos requerimientos.

Las Autoridades Certificantes de DigiCert se reservan el derecho de rechazar una solicitud de certificado si la Clave Pública incluida en la misma no cumple con la longitud mínima de clave de los algoritmos tal como se establece en esta Sección.

6.1.6 Generación de Parámetros de Clave Pública y Control de Calidad

No aplicable.

6.1.7 Propósitos del Uso de Claves (según la Extensión Uso de Claves del Estándar X.509 v3)

Ver Sección 7.1.2.1.

6.2 Protección de Claves Privadas y Controles de Ingeniería de los Módulos Criptográficos

DigiCert ha implementado una combinación de controles físicos, lógicos y de procedimiento para reforzar la seguridad de las claves privadas de las Autoridades Certificantes de DigiCert, CertiSur y de los Clientes Corporativos. A los Suscriptores se les exige, por contrato, que tomen las necesarias precauciones para prevenir la pérdida, divulgación a terceros, modificación o uso no autorizado de las claves privadas.

6.2.1 Estándares y Controles de los Módulos Criptográficos

Para la generación de los pares de claves de las Autoridades Primarias de Certificación y las Autoridades Certificantes Raíz Emisoras y el resguardo de las claves privadas de las Autoridades Certificantes, DigiCert utiliza módulos de hardware criptográfico que están certificados o que cumplen con los requerimientos del estándar FIPS 140-2 Nivel 3. DigiCert y CertiSur recomiendan que los Clientes Corporativos que actúan como Autoridades de Registro desarrollen todas las operaciones criptográficas de Administración Automática de la Autoridad de Registro en un módulo criptográfico que esté catalogado como mínimo como FIPS 140-2, nivel 2.

6.2.2 Control por parte de Múltiples Personas de Claves Privadas (m sobre n)

DigiCert ha implementado mecanismos técnicos y de procedimientos que requieren la participación de múltiples individuos confiables para desarrollar operaciones criptográficas sensibles de una Autoridad Certificante. DigiCert utiliza secretos particionados para dividir los datos de activación necesarios para hacer uso de la clave privada de una Autoridad Certificante entre distintas partes, denominados "Secretos Compartidos", que son mantenidos por individuos entrenados y confiables, denominados "Depositarios". Una cantidad mínima de "Secretos Compartidos" (m), sobre el número total de "Secretos Compartidos", creados y distribuidos para un módulo de hardware criptográfico en particular (n), es requerida para activar la clave privada de la Autoridad Certificante resguardada en el módulo.

El umbral mínimo de particiones requeridas para firmar un certificado de Autoridad Certificante es de tres (3). Debe destacarse que el número de secretos distribuidos para los dispositivos de recupero ante desastres puede ser menor que el número distribuido para los dispositivos operacionales, mientras que la cantidad mínima requerida de secretos permanece en idéntico nivel. Los Secretos Compartidos son protegidos con arreglo a lo previsto en estas Normas.

6.2.3 Depósito en Poder de Terceros de Claves Privadas

Las claves privadas de las Autoridades Certificantes no son depositadas en manos de terceros. El depósito en terceros de claves privadas de Suscriptores usuarios finales está detallado en la Sección 4.12.

6.2.4 Copias de Resguardo de Claves Privadas

DigiCert generan copias de resguardo de las claves privadas de las Autoridades Certificantes, para tareas rutinarias de recuperación o en caso de necesidad de recupero ante desastres. Dichas claves son almacenadas de manera encriptada dentro de módulos de hardware criptográfico y dispositivos para el almacenamiento de claves asociados. Los módulos criptográficos utilizados para el almacenamiento de la clave privada de Autoridades Certificantes cumplen con las exigencias establecidas en las presentes Normas. Las claves privadas de Autoridades Certificantes son copiadas en módulos criptográficos de resguardo que cumplen con lo establecido en las presentes Normas.

Los módulos que contienen las copias de resguardo de las claves privadas de Autoridades Certificantes están sujetos a los requerimientos establecidos por las presentes Normas. Los módulos conteniendo las copias necesarias para recupero ante desastres de las claves privadas de Autoridades Certificantes están sujetos a los requerimientos establecidos por las presentes Normas.

Ni DigiCert ni CertiSur almacenan copia de las claves privadas de Autoridades de Registro. Para copias de resguardo de las claves privadas de Suscriptores usuarios finales, ver las Secciones 6.2.3 y 4.12. Para las Solicitudes de Certificados de Firma de Contenido Autenticado, DigiCert no almacena copias de resguardo de las claves privadas de los Suscriptores.

6.2.5 Archivo de Claves Privadas

Cuando los pares de claves de las Autoridades Certificantes de la Symantec Trust Network alcanzan el final del período de vida útil, dichas claves privadas son almacenadas de manera segura por un período de, como mínimo, cinco (5) años, utilizando módulos criptográficos que cumplen con los requerimientos de las presentes Normas. Estos pares de claves de Autoridades Certificantes no pueden ser utilizados para ningún tipo de firma después de la correspondiente fecha de expiración del Certificado de la Autoridad Certificante al cual pertenecen, salvo que el Certificado de la Autoridad Certificante haya sido renovado en los términos establecidos por las presentes Normas.

Ni DigiCert ni CertiSur archivan copias de las claves privadas de las Autoridades de Registro y de Suscriptores.

6.2.6 Transferencia de Claves Privadas Desde o Hacia Módulos Criptográficos

Los pares de claves de Autoridades Certificantes son generados en los módulos de hardware criptográfico en los cuales las claves serán utilizadas. Adicionalmente, se realizan copias de dichos pares de claves de Autoridades Certificantes para tareas rutinarias de recuperación o en caso de necesidad de recupero ante desastres. Cuando se transfieren copias de resguardo de pares de claves de Autoridades Certificantes a otro módulo de hardware criptográfico, dichos pares de claves son transportados entre los módulos en forma encriptada.

6.2.7 Resguardo de Claves Privadas en Módulos Criptográficos

Las claves privadas de las Autoridades Certificantes o de las Autoridades de Registro están resguardadas en módulos criptográficos de manera encriptada.

6.2.8 Métodos de Activación de Claves Privadas

Todos los participantes del Subdominio CertiSur tienen la obligación de proteger los datos de activación de sus claves privadas contra pérdida, robo, modificación, divulgación no autorizada a terceros o uso no autorizado.

6.2.8.1 Certificados de Clase 1

El Requerimiento Estándar para la protección de la clave privada de Clase 1 es que los Suscriptores tomen las medidas que resulten económicamente razonables para la protección física de la estación de trabajo del Suscriptor, a efectos de prevenir el uso de dicha estación de trabajo y su clave privada asociada sin la autorización del Suscriptor. Adicionalmente, DigiCert y CertiSur recomiendan que los Suscriptores utilicen contraseñas, de acuerdo con la Sección 6.4.1 o medidas de seguridad de fortaleza equivalente, para autenticar al Suscriptor antes de la activación de la clave privada, que incluyen, por ejemplo, una contraseña para operar la clave privada, una contraseña de acceso a Windows o de protector de pantalla o usuario y contraseña de acceso a la red.

6.2.8.2 Certificados de Clase 2

El Requerimiento Estándar para la protección de la clave privada de Clase 2 es que los Suscriptores:

- Utilicen una contraseña con arreglo a lo previsto en la Sección 6.4.1 o medidas de seguridad de fortaleza equivalente, para autenticar al Suscriptor antes de la activación de la clave privada que incluye, por ejemplo, una contraseña para operar la clave privada, una contraseña de acceso a Windows o de protector de pantalla, y
- Tomen las medidas que resulten económicamente razonables para la protección física de la estación de trabajo del Suscriptor, a efectos de prevenir el uso de dicha estación de trabajo y su clave privada asociada sin la autorización del Suscriptor.

Cuando están desactivadas, las claves privadas deben ser mantenidas solamente de manera encriptada.

6.2.8.3 Certificados de Clase 3 que no sean Certificados de Administrador

El Requerimiento Estándar para la protección de la clave privada de Clase 3 (siempre que no se trate de Administradores) es que los Suscriptores:

- Usen una tarjeta smart card, un dispositivo biométrico de acceso o medidas de seguridad de similar fortaleza para autenticar al Suscriptor antes de la activación de la clave privada, y
- Tomen las medidas que económicamente resulten razonables para la protección física de la estación de trabajo del Suscriptor, para prevenir el uso de la estación de trabajo o servidor y su clave privada asociada, sin la autorización del Suscriptor.

Se recomienda la utilización de una contraseña en forma conjunta con una tarjeta smart card o dispositivo biométrico de acceso, de acuerdo con lo previsto en la Sección 6.4.1. Cuando están desactivadas, las claves privadas deben ser mantenidas solamente de manera encriptada.

DigiCert requiere de una declaración de parte del Suscriptor, afirmando que utilizará una de las siguientes opciones a los efectos de generar y proteger la Clave Privada de un Certificado de Firma de Código:

1. Un Módulo de Plataforma Confiable ("Trusted Platform Module" o TPM) que genere y almacene de manera segura el par de claves y que pueda documentar la protección de la clave privada del Suscriptor a través de una confirmación de clave del módulo.
2. Un módulo criptográfico con características de diseño físicas certificadas de conformidad con arreglo a, por lo menos, FIPS 140-2, Common Criteria EAL 4+ o equivalente.
3. Otro tipo de dispositivo de almacenamiento de hardware con características físicas de diseño de una tarjeta de memoria digital segura (SD Card) o un token USB (no necesariamente certificado con arreglo a FIPS 140-2 o Common Criteria EAL 4+). En este caso, el Suscriptor debe también garantizar que mantendrá el dispositivo de memoria físicamente separado del dispositivo en donde ejecuta las funciones de firma, hasta el momento en que va a comenzar la sesión de firmado.

DigiCert y CertiSur recomiendan que los Suscriptores protejan las claves privadas utilizando los métodos descriptos en los puntos 1 y 2 precedentemente, por encima de la utilización del método descripto en el punto 3. Asimismo, obligan al Suscriptor a proteger las claves privadas con arreglo a lo establecido en la Sección 10.3.2(2) de los Requerimientos Mínimos para la Emisión y Administración de Certificados de Firma de Código de Confianza Pública.

El Servicio de Aplicación Segura de Symantec ("Symantec Secure App Service" o SAS) permite asegurar que la clave privada del Suscriptor es generada, almacenada y utilizada en un ambiente seguro, que posee controles para evitar su robo o mal uso. Este Servicio obliga a la utilización de un factor de autenticación robusto para acceder y autorizar la Firma de Código, obteniendo la confirmación de parte del Suscriptor que mantendrá almacenados de manera segura los dispositivos o tokens requeridos para el acceso mediante un factor de autenticación múltiple. Los sistemas empleados para el procesamiento de los Servicios de Firma no son utilizados para la navegación Web, procesan regularmente una solución de antivirus actualizada a los efectos de escanear el servicio por posibles infecciones de virus y cumple con los Lineamientos de Seguridad de Redes del CA/Browser Forum, en carácter de "Tercer Parte Delegada".

6.2.8.4 Claves Privadas de Administradores (Clase 3)

El Requerimiento Estándar para la protección de la clave privada de Administradores es que ellos:

- Usen una tarjeta smart card o dispositivo biométrico de acceso y contraseña, de acuerdo con la Sección 6.4.1, o medidas de seguridad de similar fortaleza, para autenticar al Administrador antes de la activación de la clave privada que incluyen, por ejemplo, una contraseña para operar la clave privada, una contraseña de acceso a Windows o del protector de pantalla o usuario y contraseña de acceso a la red, y
- Tomen las medidas que económicamente resulten 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.

En los casos en que los controles técnicos no restrinjan la emisión de certificados bajo dominios pre aprobados, DigiCert y CertiSur exigen que los Administradores utilicen en forma conjunta con una contraseña, una tarjeta smart card o dispositivo biométrico de acceso o medidas de seguridad de similar fortaleza, de acuerdo con la Sección 6.4.1 para autenticar al Administrador antes de la activación de la clave privada que puede generar la emisión de certificados que resultarán confiables a través de la distribución de los Certificados Raíz por parte de los Proveedores de Aplicaciones de Software.

Cuando están desactivadas, las claves privadas deben ser mantenidas solamente de manera encriptada.

6.2.8.5 Autoridades de Registro de Clientes Corporativos que Utilizan un Módulo Criptográfico (con Administración Automática o con Key Manager de Managed PKI)

El Requerimiento Estándar para la protección de la clave privada de Administradores que utilizan un módulo criptográfico requiere que ellos:

- Usen el modulo criptográfico conjuntamente con una contraseña, de acuerdo con la Sección 6.4.1 para autenticar al Administrador antes de la activación de la clave privada, y
- Tomen las medidas que económicamente resulten razonables para la protección física de la estación de trabajo que aloja al lector del módulo criptográfico, para prevenir 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 Claves Privadas en Posesión de Centros de Procesamiento (Clases 1 a 3)

La clave privada de una Autoridad Certificante será activada por un número mínimo de Depositarios que suministran sus datos de activación (almacenados en dispositivos seguros) de acuerdo con la Sección 6.2.2. Una vez que la clave privada es activada, la misma se mantendrá en esa situación por un período de tiempo indefinido hasta que es desactivada al sacar de línea a la Autoridad Certificante. De idéntica forma, un número mínimo de Depositarios que suministran sus datos de activación es necesario para activar la clave privada de una Autoridad Certificante fuera de línea. Una vez que la clave privada es activada, la misma estará activa solamente para una sesión.

6.2.9 Método de Desactivación de Claves Privadas

Las claves privadas de las Autoridades Certificantes de la Symantec Trust Network son desactivadas en caso de ser removidas del dispositivo de lectura. Las claves privadas de las Autoridades de Registro (utilizadas para la autenticación de las solicitudes de Autoridades de Registro) son desactivadas al desconectarse del sistema. Las Autoridades de Registro están obligadas a desconectar sus estaciones de trabajo del sistema, antes de abandonar el lugar en el cual desempeñan sus tareas.

Los claves privadas de los Administradores de Clientes Corporativos, Autoridades de Registro y Suscriptores usuarios finales deben ser desactivadas después de cada operación, después de desconectarse de sus sistemas o después de remover la tarjeta smart card del dispositivo de lectura, dependiendo del mecanismo de autenticación empleado por el usuario. En todos los casos, los Suscriptores usuarios finales tienen la obligación de proteger adecuadamente sus claves privadas, de acuerdo con lo establecido en las presentes Normas. Las claves privadas asociadas con los Certificados de Firma de Código de Contenido Autenticado deben ser borradas inmediatamente luego de que han sido utilizadas para la firma de código.

6.2.10 Método de Destrucción de Claves Privadas

Cuando resulte necesario, DigiCert destruye las claves privadas de Autoridades Certificantes de una manera que, razonablemente, permita asegurar que no quedan partes residuales de la clave que pudieran posibilitar la reconstrucción de la misma. DigiCert utiliza la función de inicialización de sus módulos de hardware criptográfico y otros medios apropiados para asegurar la completa destrucción de las claves privadas de Autoridades Certificantes. Cuando se desarrollan, las actividades vinculadas con la destrucción de claves de Autoridades Certificantes son monitoreadas. La clave privada asociada con un Certificado de Firma de Código de Contenido Autenticado es borrada inmediatamente luego de que ha sido utilizada para la firma de código.

6.2.11 Clasificación de los Módulos Criptográficos

Ver Sección 6.2.1.

6.3 Otros Aspectos de la Administración del Par de Claves

6.3.1 Archivo de Claves Públicas

Los Certificados de las Autoridades Certificantes de la Symantec Trust Network y de las Autoridades de Registro y Suscriptores usuarios finales tienen copias de resguardo y son archivados, como parte de los procedimientos de resguardo rutinarios de DigiCert.

6.3.2 Períodos de Vigencia de los Certificados y de los Pares de Claves

El Período de Vigencia de un Certificado finaliza cuando éste expira o es revocado. El Período de Vigencia del par de claves es el mismo que el Período de Vigencia de los Certificados asociados, excepto que las claves privadas pueden continuar siendo utilizadas para desencriptar y las claves públicas pueden continuar siendo utilizadas para verificación de firmas. Los Períodos de Vigencia máximos para los Certificados de DigiCert, para todos los certificados emitidos a partir de la fecha de vigencia de las presentes Normas para el Proceso de Certificación están establecidos en la Tabla

12 más abajo[16]. Los Certificados de Suscriptores usuarios finales que son renovaciones de certificados existentes, pueden tener un período de vigencia mayor (hasta un máximo de 3 meses mayor).

Además, las Autoridades Certificantes de la Symantec Trust Network dejarán de emitir nuevos Certificados a partir de una fecha que resulte apropiada (60 días más el período máximo de validez de los Certificados emitidos), con antelación al vencimiento del Certificado de la Autoridad Certificante, de modo tal que ningún Certificado emitido a una Autoridad Certificante Subordinada expire después de la finalización de la vigencia de cualquier Certificado de una Autoridad Certificante Superior.

Certificado Emitido por:	***Período de Vigencia***
Autoridad Primaria de Certificación auto firmada (2048 bits RSA)	Hasta 25 años
Autoridad Primaria de Certificación auto firmada (256 bits ECC)	Hasta 25 años
Autoridad Primaria de Certificación auto firmada (384 bits ECC)s	Hasta 25 años
Autoridad Primaria de Certificación a una Autoridad Certificante Intermedia fuera de línea	Generalmente 10 años, pero hasta 15 años después de la renovación
Autoridad Primaria de Certificación a una Autoridad Certificante en línea	Generalmente 5 años, pero hasta 10 años después de la renovación[17]
Autoridad Certificante Intermedia fuera de línea a una Autoridad Certificante en línea	Generalmente 5 años, pero hasta 10 años después de la renovación[18]
Autoridad Certificante en línea a un Suscriptor usuario final	Normalmente hasta 3 años, pero bajo las condiciones descriptas a continuación, los Certificados pueden ser renovados una única vez hasta 6 años[19]. Después de los 6 años, es necesaria una nueva solicitud.
Autoridad Certificante en línea a un Suscriptor Organizacional Entidad Final	Con arreglo a la restricción establecida en la Sección 6.3.2.1 más abajo, normalmente hasta 6 años[20,] bajo las condiciones descriptas a

[16] Las excepciones individuales para Suscriptores usuarios finales deben ser aprobadas por DigiCert para períodos de validez que excedan los límites establecidos en la Sección 6.3.2 y están estrictamente limitados a certificados que utilizan algoritmos de encriptación fuerte o tamaños de clave más largos, como por ejemplo el uso de algoritmos SHA 2 o ECC (Criptografía de Curvas Elípticas) y/o claves de 4096 bits o superiores. A los efectos del análisis de la aprobación, se pueden imponer requerimientos adicionales en materia de protección de la clave privada, como por ejemplo la generación y guarda en un dispositivo de Hardware.

[17] La Autoridad Certificante Administrativa de Clase 3 de OnSite, la Autoridad Certificante Administrativa Operacional de Clase 3 de Secure Server y la Autoridad Certificante Administrativa de Clase 3 de OnSite Enterprise – G2 de Symantec tienen un período de vigencia superior a los 10 años para soportar los sistemas legados y serán revocadas cuando resulte apropiado.

[18] Si se emiten certificados para suscriptores usuarios finales de 6 años de validez, el período de vigencia del certificado de la Autoridad Certificante en línea será de 10 años, sin opción para su renovación. La reemisión (rekey) de la Autoridad Certificante es mandatorio después de transcurridos 5 años.

[19] Si se emiten certificados para suscriptores usuarios finales de 6 años de validez, el período de vigencia del certificado de la Autoridad Certificante en línea será de 10 años, sin opción para su renovación. La reemisión (rekey) de la Autoridad Certificante es mandatorio después de transcurridos 5 años.

[20] El Nombre Distintivo ("Distinguished Name") de los certificados emitidos con un plazo de vigencia de más de 2 años es re verificado, como mínimo, después de transcurridos 2 años desde la fecha de emisión del certificado.

Certificado Emitido por:	*Período de Vigencia*
	continuación sin posibilidad de renovación o reemisión (rekey). Después de los 6 años, es necesaria una nueva solicitud.

Tabla 12 – Períodos de Vigencia de los Certificados

Con las excepciones consideradas en esta sección, los Participantes del Subdominio CertiSur deben finalizar cualquier uso de sus pares de claves después de la finalización de sus respectivos períodos de vigencia.

Los Certificados emitidos por Autoridades Certificantes a Suscriptores usuarios finales pueden tener Períodos de Vigencia mayores de tres (3) años y hasta cinco (6) años, si se cumplimentan los siguientes requerimientos:

- En el caso de la protección del par de claves del Suscriptor de Certificados para Organizaciones en relación con su entorno operacional, la administración es efectuada con la protección ampliada que brinda un centro de procesamiento. En el caso de Certificados para Individuos, el par de claves del Suscriptor debe estar almacenado en un dispositivo de hardware, tal como una tarjeta smart card,
- Se les exige a los Suscriptores que como máximo cada tres (3) años cumplan con los requerimientos de autenticación establecidos en la Sección 3.2.3,

Si un Suscriptor no puede completar satisfactoriamente los procedimientos de autenticación o no puede demostrar satisfactoriamente que está en posesión de la clave privada según el requerimiento mencionado anteriormente, la Autoridad Certificante automáticamente revocará el Certificado del Suscriptor.

DigiCert también opera la “Autoridad Certificante Symantec de Clase 3 International Server”, la “Autoridad Certificante Thawte SGC” y la “Autoridad Certificante de Clase 3 de Open Financial Exchange”, que son Autoridades Certificantes en línea firmadas por una Autoridad Primaria de Certificación. La validez de estas Autoridades Certificantes puede exceder los plazos de vigencia descriptos en la Tabla 12 más arriba, a los efectos de asegurar la continuidad en la interoperabilidad de los certificados que ofrecen las funcionalidades SGC y OFX.

6.3.2.1 Requerimientos del CA/Browser Forum con relación a los Períodos de Validez de los certficados

Los Certificados SSL de Validación Extendida (EV), de Firma de Código de Validación Extendida (EV) y los Certificados SSL de Organización Validada (OV) y de Dominio Validado (DV) cumplen con los requerimientos del CA/Browser Forum según se establece en la Política de Certificación de DigiCert y en las Normas para el Proceso de Certificación de DigiCert.

6.4 Datos de Activación

6.4.1 Generación e Instalación de los Datos de Activación

Los datos de activación (Secretos Compartidos) utilizados para proteger los dispositivos que contienen las claves privadas de las Autoridades Certificantes de la Symantec Trust Network son generados con arreglo a los requerimientos establecidos por la Sección 6.2.2 y la Guía de la Ceremonia de Generación de Claves. La creación y distribución de los Secretos Compartidos es registrada.

Las Autoridades de Registro deben seleccionar contraseñas fuertes para proteger sus claves privadas. Los lineamientos de DigiCert y CertiSur para la selección de contraseñas requieren que las mismas:

- sean generadas por el usuario;
- estén compuestas como mínimo de quince (15) caracteres;
- contengan como mínimo un carácter alfabético y un carácter numérico;
- contengan como mínimo un carácter en minúscula;
- no contengan caracteres repetidos;
- no sean iguales al nombre de usuario del operador; y
- no contengan una secuencia parcial de caracteres idéntica a la contenida dentro del nombre de usuario del operador.

DigiCert y CertiSur recomiendan enfáticamente que los Administradores de Clientes Corporativos, las Autoridades de Registro y los Suscriptores usuarios finales seleccionen contraseñas que cumplan con los mismos requerimientos. Asimismo, recomiendan la utilización de mecanismos de autenticación con dos factores (por ejemplo, dispositivo de hardware y contraseña, dispositivo biométrico y de hardware o dispositivo biométrico y contraseña), para la activación de claves privadas.

6.4.2 Protección de los Datos de Activación

Los Depositarios de DigiCert están obligados a proteger sus Secretos Compartidos y firman un acuerdo mediante el cual toman conocimiento de sus responsabilidades como Depositarios.

Las Autoridades de Registro están obligadas a almacenar sus claves privadas de Administrador/Autoridad de Registro de manera encriptada, utilizado protección con contraseña y configurando su navegador en la opción de “seguridad alta”.

DigiCert y CertiSur recomiendan enfáticamente que los Administradores de Clientes, Autoridades de Registro y Suscriptores usuarios finales almacenen sus claves privadas de manera encriptada y protejan sus claves privadas a través de la utilización de dispositivos de hardware y/o contraseñas fuertes. Se recomienda, asimismo, la utilización de mecanismos de autenticación con dos factores (por ejemplo, dispositivo de hardware y contraseña, dispositivo biométrico y de hardware o dispositivo biométrico y contraseña).

6.4.3 Otros Aspectos de los Datos de Activación

6.4.3.1 Transmisión de los Datos de Activación

En la medida en que los datos de activación de claves privadas sean transmitidos, los Participantes de la Symantec Trust Network deben emplear métodos que protejan contra pérdida, robo, modificación, publicación o uso no autorizado por parte de terceros de dichas claves privadas. En la medida en que se utilicen como datos de activación para un Suscriptor usuario final la combinación de nombre de usuario y contraseña o contraseña de red para Windows, la transferencia de dichas contraseñas a través de una red de comunicación debe estar protegida contra el acceso no autorizado de terceros.

6.4.3.2 Destrucción de los Datos de Activación

Los datos de activación de las claves privadas deben ser destruidos utilizando métodos que protejan contra pérdida, robo, modificación, publicación o uso no autorizado por parte de terceros de las claves privadas protegidas por dichos datos de activación. Una vez que haya transcurrido el plazo de guarda establecido en la Sección 5.5.2, DigiCert destruirá los datos de activación a través del empleo de sobre escritura o de su destrucción física.

6.5 Controles de Seguridad Computacionales

DigiCert y CertiSur desarrollan todas las funciones de Autoridad Certificante y de Autoridad de Registro empleando Sistemas Confiables que cumplen con los requerimientos de las Normas para el Proceso de Certificación de DigiCert.

6.5.1 Requerimientos Técnicos de Seguridad Computacionales Específicos

DigiCert asegura que los sistemas que mantienen el software de Autoridad Certificante y los archivos de datos son Sistemas Confiables, que impiden accesos no autorizados. Adicionalmente, limita los accesos a los servidores de producción a aquellos individuos que resulte necesario que cuenten con dicho acceso conforme a sus funciones. Los usuarios de aplicaciones generales no tienen cuentas de usuario en los servidores de producción.

La red de producción de DigiCert está segmentada de manera lógica de otros componentes. Esta segmentación impide el acceso a la red, excepto a través de procesos aplicativos definidos. Se utilizan firewalls para proteger la red de producción de intrusiones internas y externas y se limita la naturaleza y origen de las actividades de la red que puedan acceder a los sistemas de producción.

DigiCert y CertiSur exigen la utilización de contraseñas que cuenten con un número mínimo de caracteres y una combinación de caracteres especiales y alfanuméricos.

El acceso directo a las bases de datos de DigiCert que soportan las operaciones de las Autoridades Certificantes está limitado a Personas Confiables, que desarrollan tareas dentro del grupo de

operaciones y producción y para el ejercicio de cuyas funciones es imprescindible contar con dicho acceso.

6.5.1.1 Requerimientos del CA/Browser Forum con Relación a los Sistemas de Seguridad

Los Certificados SSL de Validación Extendida (EV), de Firma de Código de Validación Extendida (EV) y los Certificados SSL de Dominio Validado (DV) y de Organización Validada (OV) cumplen con los requerimientos del CA/Browser Forum según se establece en la Política de Certificación de DigiCert y en las Normas para el Proceso de Certificación de DigiCert.

6.5.2 Calificación de Seguridad Computacional

No contemplada.

6.6 Controles Técnicos del Ciclo de Vida

6.6.1 Controles de Desarrollo de Sistemas

Las aplicaciones son desarrolladas e implementadas por DigiCert y CertiSur, con arreglo a sus estándares de desarrollo de sistemas y administración de cambios. DigiCert y CertiSur también suministran software a sus Clientes Corporativos para desarrollar las funciones de Autoridad de Registro y ciertas funciones de Autoridad Certificante. Dicho software es desarrollado de acuerdo con los estándares de desarrollo de sistemas de DigiCert y CertiSur

DigiCert desarrolla software que al ser cargado por primera vez provee un método para verificar en el sistema que dicho software, originado en DigiCert, no ha sido modificado antes de su instalación y es la versión indicada para su utilización.

6.6.2 Controles de Administración de Seguridad

DigiCert cuenta con mecanismos o políticas en vigencia para controlar y monitorear la configuración de sus sistemas de Autoridad Certificante. DigiCert crea un hash de todos los paquetes de software y de las actualizaciones de dicho software. Este hash es utilizado para verificar manualmente la integridad de dicho software. Al finalizar la instalación y en forma diaria a partir de allí, DigiCert valida la integridad de sus sistemas de Autoridad Certificante.

6.6.3 Controles de Seguridad del Ciclo de Vida

No contempladas.

6.7 Controles de Seguridad de Red

DigiCert y CertiSur protegen las comunicaciones de información sensible a través de la utilización de encriptación y firmas digitales.

6.8 Estampado de Sello de Tiempo ("Time-Stamping")

Los Certificados, las Listas de Certificados Revocados y otros registros de revocaciones en las bases de datos deberán contener información de fecha y hora. Esta información de tiempo no requiere estar basada en dispositivos criptográficos.

7. Configuración de Certificados, Listas de Certificados Revocados y del Protocolo del Estado del Certificado en Línea ("Online Certificate Status Protocol u OCSP")

7.1 Configuración de Certificados

Los Certificados de DigiCert en términos generales cumplimentan: (a) la Recomendación X.509 de ITU-T (2005): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, Agosto de 2005 y (b) RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, Mayo de 2008 ("RFC 5280")[21]. Según como resulte aplicable en función del tipo de Certificado, los Certificados de la Symantec Trust Network cumplen con la versión actualizada de los Requerimientos Básicos del CA/Browser Forum para la Emisión y Administración de Certificados de Confianza Públicos. La gerencia de DigiCert puede realizar excepciones a esta política, en casos específicos, para mitigar impactos inminentes y materiales a clientes, socios de negocio, partes confiadas y otras partes que componen el ecosistema de certificados, en la medida en que no existan alternativas de implementación prácticas para resolver el problema. Cada una de estas excepciones, aprobadas por la gerencia, son documentadas, controladas e informadas como parte de los procesos de auditoría.

Como mínimo, los Certificados X.509 contienen los campos básicos y los valores prescriptos indicados o los valores restrictivos (value constraints) tal como se muestra en la Tabla 13 a continuación:

Campo	*Valor o Valor restrictivo (Value constraint)*
Número de Serie	Valor único por Nombre Distintivo (Distinguished Name) del Emisor que contiene como mínimo 64 bits de entropía como salida de un CSPRNG
Algoritmo de Firma	Nombre del algoritmo (Object Identifier) utilizado para firmar el Certificado (Ver la Sección 7.1.3)
Nombre Distintivo (Distinguished Name) del Emisor	Ver la Sección 7.1.4
Válido desde	Basado en Universal Coordinate Time (UCT). Sincronizado con el Reloj Maestro del Observatorio Naval de los Estados Unidos de Norte América. Codificado de acuerdo con el RFC 5280.
Válido hasta	Basado en Universal Coordinate Time (UCT). Sincronizado con el Reloj Maestro del Observatorio Naval de los Estados Unidos de Norte América. Codificado de acuerdo con el RFC 5280
Nombre Distintivo (Distinguished Name) del Sujeto	Ver la Sección 7.1.4
Clave Pública del Sujeto	Codificado con arreglo el RFC 5280
Firma	Generada y codificada con arreglo el RFC 5280

Tabla 13 – Campos Básicos de la Configuración de Certificados

[21] Si bien los certificados de la Symantec Trust Network cumplen con el RFC 5280, ciertas provisiones limitadas pueden no ser soportadas.

7.1.1 Número (s) de Versión

Los Certificados de DigiCert son Certificados X.509 v3, aunque está permitido que algunos Certificados Raíz sean Certificados X.509 Versión 1 para soportar sistemas legados. Los Certificados de Autoridades Certificantes serán Certificados de Autoridad Certificante X.509 Versión 1 o Versión 3. Los certificados para Suscriptores usuarios finales serán Certificados X.509 v3.

7.1.2 Extensiones de los Certificados

DigiCert completa los Certificados X 509 v3 de la Symantec Trust Network con las extensiones requeridas por las Secciones 7.1.2.1 a 7.1.2.8. Las extensiones privadas son permitidas pero su utilización no está garantizada bajo la Política de Certificación de DigiCert y las presentes Normas para el Proceso de Certificación, a menos que específicamente estén incluidas por referencia.

Los requerimientos de las extensiones de los Certificados para Servidor SSL de Validación Extendida (EV) están descriptos en el Apéndice B2 de las presentes Normas.

7.1.2.1 Extensión Uso de Claves (Key Usage)

Los Certificados X 509 v3 son completados con arreglo a lo establecido en el RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, Mayo de 2008. El campo criticidad (criticality) de esta extensión está marcado generalmente como TRUE para Certificados de Autoridades Certificantes y para los Certificados de Suscriptores usuarios finales.

Nota: No es mandatorio que el bit de no repudio ("non-Repudiation bit")[22] esté establecido en estos Certificados, debido a que la industria relacionada con Infraestructuras de Clave Pública ("PKI") no ha llegado aún a un consenso respecto de cuál es el significado de este bit de no repudio. Hasta que ese consenso no se alcance, el bit de no repudio podría no tener significado alguno para potenciales Partes Confiadas. Además, la mayoría de las aplicaciones utilizadas normalmente no siempre respetan el sentido del bit de no repudio. Por lo tanto, establecer este bit no ayudaría a las Partes Confiadas a tomar una decisión veraz. Consecuentemente, las presentes Normas no exigen que el bit de no repudio esté establecido. Puede estar establecido en el caso de los Certificados emitidos bajo el servicio de Administración de Claves de Managed PKI con doble par de claves de firma, o si de otra forma es requerido. Cualquier disputa relacionada con el no repudio que surja de la utilización de un Certificado es materia exclusiva entre el Suscriptor y las Partes Confiadas. Ni DigiCert ni CertiSur incurrirán en responsabilidad alguna en relación con este asunto.

[22] El bit de no repudio ("non-Repudiation bit") también puede ser denominado como Compromiso de Contenido ("ContentCommitment") en los Certificados Digitales, de acuerdo con el estándar X.509.

7.1.2.2 Extensión Políticas de Certificación (Certificate Policies)

La extensión Políticas de Certificación (CertificatePolicies) de los Certificados X.509 v3 está completada con el identificador de objeto apropiado para la Política de Certificación de la Symantec Trust Network, de acuerdo con lo previsto en la Sección 7.1.6 y con los calificadores de política establecidos en la Sección 7.1.8. El campo criticidad (criticality) de esta extensión está marcado como FALSE.

7.1.2.2.1 Requerimientos del CA/Browser Forum con Relación a la Extensión Políticas de Certificación (Certificate Policies)

Los Certificados SSL de Validación Extendida (EV), de Firma de Código de Validación Extendida (EV) y los Certificados SSL de Dominio Validado (DV) y de Organización Validada (OV) cumplen con los requerimientos del CA/Browser Forum según se establece en la Política de Certificación de DigiCert y en las Normas para el Proceso de Certificación de DigiCert.

7.1.2.3 Extensión Nombres Alternativos del Sujeto (Subject Alternative Names)

La extensión Nombre Alternativo del Sujeto (subjectAltName) de los Certificados X.509 v3 está completada con acuerdo al RFC 5280, con la excepción de aquellos certificados emitidos bajo cuentas de Managed PKI Lite Public, que pueden excluir opcionalmente la dirección de correo electrónico en este campo. El campo criticidad (criticality) de esta extensión está marcado como FALSE.

Para todos los Certificados para Servidor, la extensión Nombre Alternativo del Sujeto (subjectAltName) está completada con el valor autenticado incluido en el campo Nombre Común (Common Name) del Nombre de Dominio del Sujeto (nombre de dominio o Dirección IP Pública). La extensión Nombre Alternativo del Sujeto (subjectAltName) puede contener nombres de dominio o direcciones IP Públicas autenticados. Para los nombres de dominio internacionalizados, el Nombre Común (Common Name) estará representado como un valor U Label codificado según Unicode, diseñado para una comprensión por parte de personas y ese Nombre Común (Common Name) será representado en la extensión Nombre Alternativo del Sujeto (Subject Alternative Name) como un valor con sintaxis A Label Punycode diseñado para una comprensión automatizada. Estas diferentes codificaciones del mismo nombre son consideradas como valores equivalentes a los efectos de los requerimientos vinculados con la duplicación de Nombre Alternativo del Sujeto (Subject Alternative Name) y del Nombre Común (Common Name).

7.1.2.4 Extensión Restricciones Básicas (Basic Constraints)

La extensión Restricciones Básicas (BasicConstraints) de los Certificados de DigiCert X.509 v3 de Autoridades Certificantes tiene el campo Autoridad Certificante completado como TRUE. La extensión Restricciones Básicas (BasicConstraints) de los Certificados de Suscriptores usuarios finales tiene el campo Autoridad Certificante completado como FALSE. El campo criticidad (criticality) de esta extensión está marcado como TRUE para los Certificados de Autoridades

Certificantes pero puede estar marcado como TRUE o como FALSE para los Certificados de Suscriptores usuarios finales.

Los Certificados de Autoridades Certificantes de DigiCert X.509 v3 están emitidos para contar con un campo Restricción de Longitud de Cadena ("pathLenConstraint") de la extensión Restricciones Básicas (BasicConstraints) marcado con el número máximo de Certificados de Autoridad Certificante que pueden seguir a continuación de este Certificado en una cadena de certificación. Los Certificados de Autoridades Certificantes emitidos a las Autoridades Certificantes en línea de Clientes Corporativos emitiendo Certificados para Suscriptores usuarios finales, contienen un campo Restricción de Longitud de Cadena ("pathLenConstraint") marcado con un valor de "0", indicando que solamente un Certificado de Suscriptor usuario final puede seguir a continuación en la cadena de certificación. Los Certificados de Suscriptor usuario final no contienen el atributo de Restricción de Longitud de Cadena ("pathLenConstraint")

7.1.2.5 Extensión Uso de Claves Extendido (Extended Key Usage)

Por defecto, la extensión Uso de Claves Extendido (ExtendedKeyUsage) está marcada como una extensión no crítica. Los Certificados de Autoridades Certificantes dentro de la Symantec Trust Network pueden incluir la extensión Uso de Claves Extendido como una forma de restringir técnicamente la utilización de los certificados que emiten. Los Certificados de DigiCert pueden contener la extensión Uso de Claves Extendido (ExtendedKeyUsage), alineados con los bits de garantía de confianza de Proveedores de Aplicaciones de Software y casos de uso en Infraestructuras de Clave Pública (PKI) Privadas. Todos los Certificados emitidos después del 1º de Febrero de 2017 para Suscriptores usuarios finales contienen una extensión Uso de Claves Extendido (ExtendedKeyUsage), con el propósito para el cual dicho certificado fue emitido al usuario final y no contienen el valor anyEKU.

Las Autoridades Certificantes Subordinadas creadas luego del 1º de Enero de 2019 para Certificados de Confianza Pública, con la excepción de los certificados firmados en forma cruzada que comparten una clave privada con una correspondiente a un certificado raíz, contienen la extensión Uso de Claves Extendido (ExtendedKeyUsage) y no pueden incluir como identificador del propósito de clave el valor anyEKU. DigiCert no incluye más el identificador del propósito de clave serverAuth y el identificador del propósito de clave emailProtection en el mismo certificado.

Los Certificados de Autoridades Certificantes Subordinadas con Restricciones Técnicas de DigiCert incluyen una extensión Uso de Claves Extendido (ExtendedKeyUsage) especificando todos los usos extendidos de claves autorizados para los cuales puede emitir certificados ese Certificado de Autoridad Certificante Subordinada. El identificador del propósito de clave anyEKU no aparece en la extensión Uso de Claves Extendido (ExtendedKeyUsage) de los certificados de Confianza Pública.

7.1.2.6 Extensión Puntos de Distribución de la Lista de Certificados Revocados (CRL Distribution Points)

La mayor parte de los Certificados X.509 v3 de DigiCert para Suscriptores usuarios finales y para Autoridades Certificantes Intermedias incluyen la extensión Puntos de Distribución de la Lista de Certificados Revocados (cRLDistributionPoints), conteniendo la dirección URL en donde una Parte Confiada puede obtener la Lista de Certificados Revocados para controlar el estado de los Certificados de la Autoridad Certificante. El campo criticidad (criticality) de esta extensión está marcado como FALSE. Las direcciones URL cumplen con los requerimientos de Mozilla para excluir el protocolo LDAP y pueden aparecer múltiples veces dentro de la extensión Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints).

7.1.2.7 Extensión Identificador de Clave de la Autoridad (Authority Key Identifier)

DigiCert completa generalmente la extensión Identificador de Clave de la Autoridad (Authority Key Identifier) de los Certificados X.509 v3 de Suscriptores usuarios finales y Certificados de las Autoridades Certificantes Intermedias. Cuando el certificado del emisor contiene la extensión Identificador de Clave del Sujeto (Subject Key Identifier), el Identificador de Clave de la Autoridad (Authority Key Identifier) está compuesto por el hash de 160 bits SHA-1 de la clave pública de la autoridad Certificante que emite el Certificado. De lo contrario, la Extensión Identificador de Clave de la Autoridad Certificante (Authority Key Identifier) incluye el nombre distintivo (distinguished name) y el número de serie de la Autoridad Certificante emisora. El campo criticidad (criticality) de esta extensión está marcado como FALSE.

7.1.2.8 Extensión Identificador de Clave del Sujeto (Subject Key Identifier)

Cuando DigiCert completa los Certificados X.509 v3 bajo la Symantec Trust Network con una extensión Identificador de Clave del Sujeto (subjectKeyIdentifier), el Identificador de clave (keyIdentifier) es generado en base a la clave pública del Sujeto del Certificado de acuerdo con uno de los métodos descriptos en el RFC 5280. Cuando esta extensión es utilizada, el campo criticidad (criticality) de esta extensión está marcado como FALSE.

7.1.3 Identificadores de Objeto Algoritmo (Algorithm Object Identifiers)

Los Certificados de DigiCert están firmados utilizando alguno de los siguientes algoritmos:

- ***sha256withRSAEncryption*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

- ***ecdsa-with-Sha256*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2}

- ***ecdsa-with-Sha384*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 3}

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

Las firmas de los Certificados generadas utilizando estos algoritmos cumplen con el RFC 3279. La encripción ***sha256WithRSA*** se utilizará por encima de la encripción ***sha-1WithRSA*** [23].

7.1.4 Formas de Nombres

DigiCert completa los Certificados bajo la Symantec Trust Network con un Nombre Distintivo (Distinguished Name) del Emisor y del Sujeto con arreglo a lo establecido en la Sección 3.1.1. El Nombre del Emisor será incluido en cada Certificado emitido con la indicación de País, Nombre Organizacional y el Nombre Común de la Autoridad Certificante Emisora.

Además, DigiCert puede incluir en los Certificados para Suscriptores usuarios finales un campo adicional Unidad Organizacional (Organizational Unit) que contiene una notificación estableciendo que los términos de uso del Certificado están determinados en una dirección URL donde poder acceder al Acuerdo del Receptor Confiado que resulta aplicable. Este campo Unidad Organizacional debe figurar si en la extensión de Políticas de Certificación no está incluido un marcador al Acuerdo del Receptor Confiado que resulte aplicable.

7.1.5 Restricciones de Nombres

Sin especificación.

7.1.6 Identificador de Objeto de Políticas de Certificación (Certificate Policy Object Identifier)

Cuando la extensión Políticas de Certificación (Certificate Policies) es utilizada, los Certificados contienen un Identificador de Objeto para la Política de Certificación (Certificate Policy Object Identifier) correspondiente a la Clase de Certificado apropiada, tal como está establecido en la Política de Certificación de la Symantec Trust Network Sección 1.2. Para los Certificados anteriores, emitidos antes de la publicación de la Política de Certificación de la Symantec Trust Network, que incluyen la extensión Política de Certificación (Certificate Policies), los Certificados remiten a las Normas para el Proceso de Certificación de la Symantec Trust Network.

7.1.6.1 Requerimientos del CA/Browser Forum con Relación a la Identificación de Objeto de Políticas de Certificación (Certificate Policies)

Los Certificados SSL de Validación Extendida (EV), de Firma de Código de Validación Extendida (EV) y los Certificados SSL de Dominio Validado (DV) y de Organización Validada (OV)

[23] La encripción ***SHA-1WithRSA*** es utilizada solamente, previa aprobación, a los efectos de preservar la continuidad de funcionamiento de aplicaciones legadas.

cumplen con los requerimientos del CA/Browser Forum según se establece en la Política de Certificación de DigiCert y en las Normas para el Proceso de Certificación de DigiCert.

7.1.7 Uso de la Extensión Restricciones de Política (Policy Constraints)

Sin especificación.

7.1.8 Sintaxis y Semántica de los Calificadores de Política (Policy Qualifiers)

DigiCert completa generalmente los Certificados X.509 v3 bajo la Symantec Trust Network con un calificador de política (policy qualifier) dentro de la extensión Políticas de Certificación (CertificatePolicies). Normalmente, dichos Certificados contienen un calificador de puntero de Normas para el Proceso de Certificación (CPS pointer qualifier) que apunta hacia el Acuerdo del Receptor Confiado que resulta de aplicación o a las Normas para el Proceso de Certificación de CertiSur. Adicionalmente, algunos Certificados contienen un Calificador de Notificación al Usuario (User Notice Qualifier) que apunta hacia el Acuerdo del Receptor Confiado que resulta de aplicación.

7.1.9 Procesamiento de la Semántica para la Extensión Política de Certificación Crítica (Critical Certificate Policy)

Sin especificación.

7.2 Configuración de la Lista de Certificados Revocados (CRL)

Como resulte de aplicación según el tipo de Certificado, las correspondientes Listas de Certificados Revocados están de acuerdo con la versión vigente de los Requerimientos Básicos para la Emisión y Administración de Certificados de Confianza Pública, emitido por el CA/Browser Forum.

Las Listas de Certificados Revocados Versión 2 cumplen con la RFC 5280 y contienen los campos básicos y los contenidos especificados en la Tabla 14 a continuación:

Campo	*Valor o Valor restrictivo*
Versión	Ver Sección 7.2.1.
Algoritmo de firma	Algoritmo empleado para firmar la Lista de Certificados Revocados (CRL) de acuerdo con el RFC 3279. Ver Sección 7.1.3.
Emisor	Entidad que ha firmado y emitido la Lista de Certificados Revocados (CRL).
Día y Hora de Vigencia	Día y hora de la emisión de la Lista de Certificados Revocados (CRL). Las Listas de Certificados Revocados (CRL) entran en vigencia en el momento de su emisión.
Próxima Actualización	Día y hora en que será emitida la siguiente Lista de Certificados Revocados (CRL). La frecuencia de emisión de las Listas de Certificados Revocados está de acuerdo con los requerimientos establecidos por la Sección 4.9.7.
Certificados Revocados	Listado de los certificados revocados, incluyendo el Número de Serie del Certificado Revocado y la Fecha de Revocación.

Tabla 14 – Campos Básicos de la Configuración de la Lista de Certificados Revocados (CRL)

7.2.1 Números de Versión

DigiCert soporta Listas de Certificados Revocados X.509 Versión 1 y Versión 2. Las Listas de Certificados Revocados Versión 2 cumplen con los requerimientos del RFC 5280.

7.2.2 Extensiones de Lista de Certificados Revocados (CRL) y de Ingreso a la Lista de Certificados Revocados (CRL Entry)

Sin especificación.

7.3 Configuración del Protocolo del Estado del Certificado en Línea ("Online Certificate Status Protocol u OCSP")

El Protocolo del Estado del Certificado en Línea ("Online Certificate Status Protocol u OCSP") es el medio para obtener información en tiempo oportuno respecto del estado de revocación de un certificado en particular. DigiCert valida:

- Los Certificados de Clientes Corporativos de Clase 2 con el servicio de OCSP para Empresas, en un todo de acuerdo con el RFC 2560, y
- Los Certificados de Clientes Corporativos de Clase 2 y los Certificados para organizaciones de Clase 3 utilizando el servicio de Validación Global de Confianza de Symantec ("Trusted Global Validation" o "TGV"), en un todo de acuerdo con el RFC 6960, excluyendo soporte de cifrado requerido por el cliente.

Requerimientos del CA/Browser Forum en relación a la Firma de la Respuesta OSCP

Para los Certificados SSL de Validación Extendida (EV), de Firma de Código de Validación Extendida (EV) y los Certificados SSL de Dominio Validado (DV) y de Organización Validada (OV), DigiCert suministra respuestas de OCSP de conformidad con los Requerimientos del CA/Browser Forum, según se establece en la Política de Certificación de DigiCert y en las Normas para el Proceso de Certificación de DigiCert.

7.3.1 Números de Versión

La versión 1 de la especificación del Protocolo del Estado del Certificado en Línea ("Online Certificate Status Protocol u OCSP") tal como está definida por las RFC2560, RFC5019 y RFC 6960 es soportada, excluyendo cifrados requeridos por el cliente.

7.3.2 Extensiones del Protocolo del Estado del Certificado en Línea ("Online Certificate Status Protocol u OCSP")

El Servicio del protocolo de Validación Global de Confianza de Symantec ("Trusted Global Validation" o "TGV") utiliza sello de tiempo (timestamp) seguro y períodos de validez para establecer la vigencia actual de cada respuesta de OCSP. DigiCert no utiliza la extensión "nonce" (número criptográfico aleatorio) para establecer la vigencia actual de cada respuesta de OCSP y los clientes no deben esperar un valor en la extensión "nonce" en la respuesta a una solicitud, aún cuando la misma contenga un valor en dicha extensión. En cambio, los clientes deben utilizar la hora local a los efectos de establecer la vigencia de una respuesta.

8. Auditorías de Cumplimiento y Otras Evaluaciones

Anualmente, se desarrolla una auditoría WebTrust "Principios y Criterios para Autoridades Certificantes" versión 2.0 o posterior y, cuando resulte de aplicación, alguna de las siguientes Auditorías WebTrust: "Principios y Criterios para Autoridades Certificantes – Requisitos Básicos sobre Certificados SSL y Seguridad de Red", versión 2.2 o posterior, "Principios y Criterios para Autoridades Certificantes – Requisitos Básicos sobre Certificados SSL de Validación Extendida (EV)", versión 1.4.5 o posterior y/o "Principios y Criterios para Autoridades Certificantes – Requisitos Básicos sobre Certificados de Firma de Código de Validación Extendida (EV)", sobre el Centro de Procesamiento de Datos de DigiCert y las operaciones de administración de claves que soportan los servicios de Autoridades Certificantes de Confianza Pública de DigiCert y de Managed PKI, incluyendo las Autoridades Certificantes Raíz de la Symantec Trust Network, las Autoridades Certificantes Clase 3 para organizaciones, Autoridades Certificantes de Clase 2 para organizaciones e individuos y Autoridades Certificantes Clase 1 para individuos, tal como está especificado en la Sección 1.3.1. DigiCert y/o CertiSur están facultados para requerir que los Clientes Corporativos lleven a cabo una Auditoría de Cumplimiento con arreglo a estas Normas y programas de auditoría para estos tipos de Clientes.

Además de las Auditorías de Cumplimiento, DigiCert y/o CertiSur están facultados para desarrollar otras revisiones e investigaciones para asegurar la confiabilidad del Subdominio CertiSur de la Symantec Trust Network, que incluyen, pero no están limitadas a:

- Una Revisión de Prácticas y Seguridad de un Afiliado o un Cliente, antes que se le autorice para iniciar las operaciones. Esta revisión consiste en un análisis de las instalaciones físicas, los documentos de seguridad, las Normas para el Proceso de Certificación, los Acuerdos relacionados con la Symantec Trust Network, la Política de Privacidad y los Planes de Validación, a los efectos de asegurar que se cumplan con los Requerimientos Estándar dentro de la Symantec Trust Network. DigiCert no delega en Afiliados o terceras partes la validación de dominios o direcciones IP.
- DigiCert y/o CertiSur están facultados, a su sola y exclusiva discreción, para efectuar en cualquier momento una Auditoría Investigativa o Investigación sobre su propia operación o sobre la operación de un Cliente, en caso de que tengan razones para suponer que la entidad auditada ha fallado en el cumplimiento de los Requerimientos Estándar dentro de la Symantec Trust Network, ha sufrido un incidente o Compromiso de seguridad o ha actuado o dejado de actuar de modo tal que dicha falla de la entidad auditada, el incidente o Compromiso o la actuación o falta de ella signifique una amenaza real o potencial a la seguridad o integridad de la Symantec Trust Network.
- DigiCert y/o CertiSur están facultados para efectuar Revisiones Complementarias de Administración del Riesgo sobre un Cliente, luego de detectar resultados incompletos o excepcionales en una Auditoría de Cumplimiento o como parte del proceso de evaluación de administración del riesgo, en el curso normal de los negocios.

DigiCert y CertiSur están facultados para delegar la ejecución de dichas auditorías, revisiones e investigaciones en una firma de auditoría. Las entidades sujetas a auditoría, revisión o investigación deben proveer razonable cooperación a DigiCert, CertiSur y al personal responsable de la ejecución de la auditoría, revisión o investigación.

Requerimientos del CA/Browser Forum con Relación a Auditorías Internas

Para los Certificados SSL de Validación Extendida (EV), de Firma de Código de Validación Extendida (EV) y los Certificados SSL de Dominio Validado (DV) y de Organización Validada (OV) DigiCert realiza auditorías internas de conformidad con los Requerimientos del CA/Browser Forum, según se establece en la Política de Certificación de DigiCert y en las Normas para el Proceso de Certificación de DigiCert.

8.1 Periodicidad y Circunstancias de las Evaluaciones

Las Auditorías de Cumplimiento son desarrolladas como mínimo en forma anual y su costo está a cargo exclusivo de la entidad auditada. Las auditorías son ejecutadas sobre una secuencia ininterrumpida de períodos auditados y cada uno de esos períodos no puede exceder el año de duración. El plazo que cubre la auditoría es el lapso que transcurre entre el primer día (comienzo) y el último día (finalización) de operaciones cubierto por los auditores en su tarea.

8.2 Identidad y Calificaciones del Auditor

Las Auditorías de Cumplimiento de las Autoridades Certificantes de DigiCert son desarrolladas por profesionales o firmas de auditoría que:

- Demuestren la aptitud y certificaciones necesarias como para conducir una Auditoría WebTrust para Autoridades Certificantes, versión 2.0 o posterior.
- Demuestren acabado conocimiento acerca de la tecnología de infraestructura de clave pública, técnicas y herramientas de seguridad de información, auditoría de seguridad y funciones de certificación hacia terceros, y
- Estén inscriptos en el Instituto Americano de Contadores Públicos Certificados ("American Institute of Certified Public Accountants o AICPA), cuya inscripción esté sujeta al cumplimiento de determinados requisitos, en materia de conocimientos técnicos y control de calidad de las tareas asignadas, tales como revisiones puntuales, evaluaciones de conocimiento, estándares en la asignación de tareas a los profesionales competentes y capacitación continua de los mismos.
- Estén obligados por una ley específica, regulación gubernamental o código de ética profesional, y
- Cuenten con una póliza de seguro profesional por errores y/u omisiones con una cobertura equivalente a, por lo menos, un millón de dólares estadounidenses.

8.3 Relación del Auditor con la Entidad Auditada

Las Auditorías de Cumplimiento de las operaciones de DigiCert son desarrolladas por un profesional o firma de auditoría independiente.

8.4 Temas cubiertos por la Evaluación

El alcance de la auditoría anual Web Trust o similar, para Autoridades Certificantes de DigiCert incluye controles de la infraestructura de Autoridades Certificantes, de las operaciones de administración de claves de las Autoridades Certificantes de Infraestructura y Administrativas, de las operaciones vinculadas con la administración del ciclo de vida de los certificados y sobre la publicación de las prácticas de negocio relacionadas con las operaciones de las Autoridades Certificantes.

Auditorías de Autoridades de Registro (Clases 1 y 2)

Los clientes Corporativos que aprueban la emisión de Certificados de Clase 1 y Clase 2 pueden realizar una auditoría anual de cumplimiento. Ante un requerimiento de DigiCert y/o CertiSur o una Entidad Superior (diferente de DigiCert) los clientes Corporativos pueden realizar una auditoría a los efectos de detectar cualquier excepción o irregularidad a las políticas de la Symantec Trust Network y los pasos observados para solucionar las irregularidades.

Auditoría de una Autoridad de Registro (Clase 3)

Los clientes Corporativos que aprueban la emisión de Certificados de Servidor SSL de Clase 3 deben realizar una auditoría anual de cumplimiento de sus obligaciones bajo la Symantec Trust Network[24]. Ante un requerimiento de DigiCert y/o CertiSur o una Entidad Superior (diferente de DigiCert) los clientes Corporativos pueden realizar una auditoría a los efectos de detectar cualquier excepción o irregularidad a las políticas de la Symantec Trust Network y los pasos observados para solucionar las irregularidades.

Auditoría de DigiCert y de CertiSur (Clases 1 a 3)

DigiCert y CertiSur, de corresponder, son auditados con arreglo a los procedimientos establecidos por las Prácticas de Contadores Públicos Certificados para los Informes de Control de las Organizaciones de Servicio, en relación a los riesgos asociados con la operación de Organizaciones de Servicio. Su Auditoría de Cumplimiento es la Auditoría WebTrust para Autoridades Certificantes o una auditoría de estándares similares aprobada por DigiCert y que incluye un Informe de las Políticas y Procedimientos de la Operación y una Prueba de la Efectividad Operacional.

Las operaciones de CertiSur en su carácter de Autoridad de Registro dentro de la Symantec Trust Network, en caso de corresponder, son auditadas con arreglo a los Procedimientos Aprobados por el Consejo Profesional de Ciencias Económicas de la Ciudad Autónoma de Buenos Aires e incluyen los procedimientos establecidos para una Auditoría WebTrust para Autoridades Certificantes o similar, en lo que resulta de aplicación.

[24] DigiCert realiza todas las tareas de identificación y autenticación de los Certificados para Servidor SSL de Clase 3, autorizados para su emisión por parte de Clientes Corporativos.

8.5 Acciones Tomadas como Consecuencia de Deficiencias

Las excepciones significativas o deficiencias identificadas durante la Auditoría de Cumplimiento de las operaciones de DigiCert determinarán una serie de acciones a tomar. Esta determinación será realizada por el personal gerencial de DigiCert, sobre la base de la información proporcionada por el auditor. El personal gerencial de DigiCert es responsable por el desarrollo y la implementación de un plan de acción correctivo. Si DigiCert determina que dichas excepciones o deficiencias significan una amenaza inmediata a la seguridad o integridad de la Symantec Trust Network se desarrollará, dentro de un plazo de 30 días, un plan de acción correctivo el que será implementado dentro de un período que resulte comercialmente razonable. En el caso de excepciones o deficiencias más leves, el personal gerencial de DigiCert evaluará la significatividad de dichos puntos y determinará el curso de acción apropiado.

8.6 Comunicación de Resultados

DigiCert publica su Informe Anual de Auditoría en un plazo no mayor a los tres (3) meses de finalizado el período auditado. En la eventualidad de que exista una demora superior a los tres (3) meses, DigiCert publicará una carta explicativa, suscripta por un auditor calificado. Una copia del informe de auditoría Web Trust, o similar, para Autoridades Certificantes de DigiCert se encuentra en el Repositorio localizado en: https://www.digicert.com/legal-repository.

9. Otros Asuntos y Cuestiones Legales

9.1 Costos

9.1.1 Costos de la Emisión o Renovación de Certificados

DigiCert y/o CertiSur están facultados para cobrar aranceles a los Suscriptores usuarios finales, en concepto de emisión, administración y renovación de Certificados.

9.1.2 Costos de Acceso a los Certificados

Ni DigiCert ni CertiSur perciben arancel alguno como condición para que los Certificados estén disponibles para Partes Confiadas, ya sea en un repositorio o de otra forma.

9.1.3 Costos de la Revocación o de Acceso a la Información del Estado

Ni DigiCert ni CertiSur cobran arancel alguno como condición para que las Listas de Certificados Revocados requeridas bajo estas Normas estén disponibles, en un repositorio o de otra forma, para Partes Confiadas. DigiCert y/o CertiSur pueden percibir, sin embargo, un arancel por proveer Listas de Certificados Revocados adaptadas a necesidades específicas, servicios de Protocolo del Estado del Certificado en Línea ("Online Certificate Status Protocol u OCSP") u otros servicios de valor agregado relacionados con la revocación de Certificados o la información del estado de los Certificados. DigiCert no permite el acceso a la información sobre la revocación, información respecto del estado de Certificados o de time stamping en su repositorio, a terceros que suministren productos o servicios que utilizan dicha información respecto del estado del Certificado, sin el previo consentimiento expreso y por escrito.

9.1.4 Costos de Otros Servicios

Ni DigiCert ni CertiSur perciben arancel alguno para acceder a las presentes Normas para el Proceso de Certificación. Cualquier uso realizado con propósitos diferentes a la simple lectura del documento, como por ejemplo la reproducción, redistribución, modificación o creación de trabajos derivados, está sujeto a un acuerdo de licencia con la entidad que sea titular de los derechos de propiedad intelectual del documento.

9.1.5 Política de Reembolso

Dentro del Subdominio CertiSur está en vigencia la siguiente política de reembolso (reproducida en https://www.certisur.com/repositorio/Reembolso/):

> DigiCert y CertiSur se rigen por rigurosas normas y procedimientos en la ejecución de las operaciones de certificación y en la emisión de certificados. No obstante ello, si por cualquier razón un suscriptor no está completamente satisfecho con el certificado que se le ha emitido, el suscriptor puede solicitar que CertiSur le

revoque el certificado dentro de los treinta (30) días corridos posteriores a su emisión y le reembolse el costo del mismo. Después de finalizado este período inicial de treinta (30) días corridos, un suscriptor puede solicitar que CertiSur le revoque el certificado y le reembolse el costo del mismo, sólo si CertiSur ha incumplido con una obligación material bajo estas Normas para el Proceso de Certificación, relacionada con el suscriptor o con el certificado del suscriptor. Después que CertiSur revoque el certificado del suscriptor, acreditará oportunamente la cuenta de la tarjeta de crédito del suscriptor (si éste fue el medio de pago del certificado) o pondrá a disposición de éste un cheque, por el monto total de los costos pagados por el certificado. Para solicitar un reembolso, llame al sector de Atención al Cliente al teléfono (54 11) 4311 2457. Esta política de reembolso no constituye una indemnización, por no resultar procedente indemnización alguna en los presentes casos.

9.2 Responsabilidad Financiera

9.2.1 Cobertura de Seguro

Se recomienda que los Clientes Corporativos cuenten con una cobertura de seguro por un monto que resulte comercialmente razonable, para cubrir errores u omisiones, ya sea a través de la contratación de un seguro específico o la constitución de un fondo específico de cobertura. DigiCert y CertiSur mantienen una cobertura de seguro por errores u omisiones, contratado con una compañía aseguradora autorizada.

9.2.2 Otros Activos

Los Clientes Corporativos deben contar con recursos financieros suficientes como para mantener sus operaciones y desarrollar sus tareas y deben estar en condiciones razonables de asumir el riesgo de su responsabilidad frente a Suscriptores y Partes Confiadas.

9.2.3 Cobertura de Garantía Extendida

No contemplada.

9.3 Confidencialidad de la Información

9.3.1 Alcance de la Información Confidencial

Los siguientes registros de los Suscriptores son mantenidos en forma confidencial y privada, sujeto a lo dispuesto por la Sección 9.3.2 (“Información Confidencial o Privada”):

- Registros de solicitudes de Autoridad Certificante, independientemente de que hayan sido aprobadas o rechazadas,
- Registro de Solicitudes de Certificado,
- Claves privadas mantenidas en poder de Clientes Corporativos que utilizan el Key Manager de Managed PKI y la información necesaria para recuperar dichas claves privadas,

- Registros de transacciones (los registros de las transacciones como así también los registros de auditoría de dichas transacciones),
- Registros de auditoría de la Symantec Trust Network generados o retenidos por DigiCert, CertiSur o un Cliente,
- Informes de auditoría generados por DigiCert, CertiSur o por un Cliente (en la medida en que esos informes son mantenidos) o sus respectivos auditores (internos o externos),
- Planes de contingencia y de recupero ante desastres, y
- Medidas de seguridad para el control de las operaciones del hardware y software de DigiCert y la administración del servicio de Certificados y servicios de solicitudes especificados.

9.3.2 Información Fuera del Alcance de la Información Confidencial

Los Certificados, la información de la revocación o estado de los Certificados, los repositorios de DigiCert y CertiSur y la información contenida en los mismos no son considerados como Información Confidencial o Privada. La información que no esté expresamente reconocida como Información Confidencial o Privada según lo previsto en la Sección 9.3.1 no será considerada como confidencial ni como privada. Esta sección está sujeta a las leyes que resulten de aplicación en materia de privacidad.

9.3.3 Responsabilidad para Proteger la Información Confidencial

DigiCert y CertiSur aseguran la información privada, de modo de evitar cualquier compromiso o acceso a terceros de dicha información.

9.4 Privacidad de la Información Personal

9.4.1 Plan de Privacidad

CertiSur ha implementado una política de privacidad, la cual aparece publicada en: https://www.certisur.com/repositorio/DeclaracionPrivacidad.html, con arreglo a lo establecido en La Sección 9.4.1 de la Política de Certificación.

9.4.2 Información Considerada como Privada

Cualquier información acerca de los Suscriptores que no está públicamente disponible a través de su inclusión en un certificado emitido, un directorio de certificados o una Lista de Certificados Revocados en línea es considerada y tratada como privada.

9.4.3 Información No Considerada como Privada

Sujeto a cualquier regulación de la legislación local, toda la información que está públicamente disponible en un certificado no es considerada como privada.

9.4.4 Responsabilidad para Proteger la Información Privada

DigiCert y CertiSur aseguran la información privada de modo tal de evitar cualquier compromiso o acceso a terceros de dicha información y cumplen con toda la legislación local en materia de privacidad.

9.4.5 Notificación y Consentimiento para el Uso de Información Privada

Salvo que esté establecido lo contrario en las presentes Normas, en la Política de Privacidad que resulte aplicable o en un acuerdo específico, la información privada no puede ser utilizada sin el consentimiento de la parte a la cual dicha información le concierne. Esta sección está sujeta a las leyes que resulten de aplicación en materia de privacidad.

9.4.6 Divulgación como Consecuencia de un Proceso Judicial o Administrativo

DigiCert y CertiSur están facultados para divulgar Información Confidencial o Privada si consideran de buena fe que:

- la divulgación es necesaria como respuesta a citaciones u órdenes judiciales
- la divulgación es necesaria como respuesta a procesos judiciales, administrativos u otros procesos legales, durante una acción civil o administrativa, tales como citaciones, interrogatorios, solicitud de pruebas, etc.

Esta sección está sujeta a las leyes que resulten de aplicación en materia de privacidad.

9.4.7 Otras Circunstancias de Divulgación de Información

No contempladas.

9.5 Derechos de Propiedad Intelectual

Los temas concernientes a los Derechos de Propiedad Intelectual entre los Participantes del Subdominio CertiSur, con excepción de los Suscriptores y las Partes Confiadas, se rige por los acuerdos que resulten de aplicación entre tales Participantes del Subdominio CertiSur. Las subsecciones que conforman la Sección 9.5 que figuran a continuación son aplicables a los Derechos de Propiedad Intelectual en relación con Suscriptores y Partes Confiadas.

9.5.1 Derechos de Propiedad en Certificados y en Información de Revocación

Las Autoridades Certificantes mantienen en forma exclusiva todos los Derechos de Propiedad Intelectual de los Certificados que emiten y de la información de revocación de los mismos. DigiCert, CertiSur y los Clientes permiten la reproducción o distribución de Certificados, en forma

no exclusiva y gratuita, en la medida en que sean reproducidos en su totalidad y el uso de los Certificados esté sujeto al Acuerdo del Receptor Confiado referenciado en el Certificado. CertiSur y los Clientes permiten la utilización de la información de revocación, a efectos de ejecutar las funciones de la Parte Confiada y sujeto al Acuerdo de Uso de la Lista de Certificados Revocados aplicable, al Acuerdo del Receptor Confiado o a cualquier otro acuerdo que resulte de aplicación.

9.5.2 Derechos de Propiedad de las Normas para el Proceso de Certificación

Los Participantes de la Symantec Trust Network reconocen que DigiCert y CertiSur mantienen en forma exclusiva todos los Derechos de Propiedad Intelectual con respecto a las presentes Normas para el Proceso de Certificación.

9.5.3 Derechos de Propiedad en Nombres

Un Solicitante de Certificado mantiene en forma exclusiva todos los derechos que posee, de existir, sobre cualquier marca comercial, marca de servicio o nombre comercial contenido en cualquier Solicitud de Certificado y nombre distintivo contenido en cualquier Certificado emitido para dicho Solicitante de Certificado.

9.5.4 Derechos de Propiedad en Claves y Componentes de Claves

El par de claves correspondiente a los Certificados de Autoridades Certificantes y Suscriptores usuarios finales son propiedad de las Autoridades Certificantes y Suscriptores usuarios finales que son los respectivos Sujetos de dichos Certificados, supeditado a los derechos de los Clientes Corporativos que utilizan el Servicio de Key Manager de Managed PKI, independientemente del medio físico dentro del cual esté guardado y protegido y dichas personas retienen todos los Derechos de Propiedad Intelectual con respecto a dicho par de claves. No obstante lo mencionado, las claves públicas raíz de DigiCert y los Certificados raíz que las contienen, incluyendo todas las claves públicas de las Autoridades Primarias de Certificación y los Certificados auto firmados, son propiedad de DigiCert. DigiCert licencia a productores de software y hardware para que reproduzcan tales Certificados raíz insertando copias en dispositivos de hardware o software confiables. Finalmente, Los Secretos Compartidos de la clave privada de una Autoridad Certificante son propiedad de la Autoridad Certificante y dicha Autoridad Certificante mantiene en forma exclusiva todos los Derechos de Propiedad Intelectual relacionados con dichos Secretos Compartidos, incluso a pesar de que ellos no puedan obtener la posesión física de tales Secretos o de la Autoridad Certificante de parte de DigiCert.

9.6 Declaraciones y Garantías

9.6.1 Declaraciones y Garantías de una Autoridad Certificante

DigiCert y CertiSur garantizan que:

- No existen, de hecho, informaciones falsas en el Certificado que sean de conocimiento u originadas en las entidades que aprueban la Solicitud de Certificado o emiten el Certificado,
- No existen errores en la información contenida en el Certificado que hayan sido introducidos por las entidades al aprobar la Solicitud de Certificado o al emitir el Certificado, como resultado de un accionar irrazonable en el cumplimiento de los deberes inherentes a la administración de la Solicitud de Certificado y a la generación del Certificado,
- Sus Certificados cumplen con todos los requerimientos materiales de estas Normas para el Proceso de Certificación, y
- Los servicios de revocación y el uso de un repositorio se efectúan de acuerdo con las presentes Normas para el Proceso de Certificación, en todos sus aspectos relevantes.

Los Acuerdos del Suscriptor pueden incluir declaraciones y garantías adicionales.

9.6.1.1 Requerimientos del CA/Browser Forum con Relación a Garantías y Obligaciones

Los Certificados SSL de Validación Extendida (EV), de Firma de Código de Validación Extendida (EV) y los Certificados SSL de Dominio Validado (DV) y de Organización Validada (OV) cumplen con los requerimientos del CA/Browser Forum según se establece en la Política de Certificación de DigiCert y en las Normas para el Proceso de Certificación de DigiCert

9.6.2 Declaraciones y Garantías de una Autoridad de Registro

Las Autoridades de Registro garantizan que:

- No existen, de hecho, informaciones falsas en el Certificado que sean de conocimiento u originadas en las entidades que aprueban la Solicitud de Certificado o emiten el Certificado,
- No existen errores en la información contenida en el Certificado que hayan sido introducidos por las entidades al aprobar la Solicitud de Certificado o al emitir el Certificado, como resultado de un accionar irrazonable en el cumplimiento de los deberes inherentes a la administración de la Solicitud de Certificado y a la generación del Certificado,
- Sus Certificados cumplen con todos los requerimientos materiales de estas Normas para el Proceso de Certificación, y
- Los servicios de revocación, cuando resulten de aplicación, y el uso de un repositorio se efectúan de acuerdo con las presentes Normas para el Proceso de Certificación, en todos sus aspectos relevantes.

Los Acuerdos del Suscriptor pueden incluir declaraciones y garantías adicionales.

9.6.3 Declaraciones y Garantías de un Suscriptor

Los Suscriptores garantizan que:

- Cada firma digital generada utilizando la clave privada que se corresponde con la clave pública contenida en el Certificado es la firma digital del Suscriptor y el Certificado ha sido aceptado y está vigente (no ha expirado ni ha sido revocado) al momento de generar la firma digital,
- La clave privada está protegida y ningún tercero no autorizado a tenido acceso jamás a la clave privada del Suscriptor,
- Todas las declaraciones formuladas por el Suscriptor en la Solicitud de Certificado que remitió son veraces,
- Toda la información suministrada por el Suscriptor y contenida en el Certificado es veraz,
- El Certificado es utilizado exclusivamente con propósitos autorizados y legales, consistentes con las presentes Normas, y
- El Suscriptor es un Suscriptor usuario final y no una Autoridad Certificante y no utiliza la clave privada que se corresponde con la clave pública contenida en el Certificado para firmar digitalmente cualquier Certificado o cualquier otro formato de certificación de clave pública, o Lista de Certificados Revocados, como una Autoridad Certificante o de cualquier otra forma.

Los Acuerdos del Suscriptor pueden incluir declaraciones y garantías adicionales.

9.6.4 Declaraciones y Garantías de una Parte Confiada

Los Acuerdos del Receptor Confiado exigen que las Partes Confiadas reconozcan que cuentan con información suficiente como para tomar una decisión informada respecto del nivel de confianza que quieran depositar en la información contenida en un Certificado, que ellas son las exclusivas responsables de decidir si confían o no en dicha información y que asumirán las consecuencias legales de su incumplimiento al desarrollar las obligaciones que las presentes Normas le imponen a las Partes Confiadas.

Los Acuerdos del Receptor Confiado pueden incluir declaraciones y garantías adicionales.

9.6.5 Declaraciones y Garantías de Otros Participantes

No contempladas

9.7 Exclusión de Garantías

Con el alcance permitido por la ley aplicable, los Acuerdos del Suscriptor y los Acuerdos del Receptor Confiado excluyen cualquier posible garantía de DigiCert y/o CertiSur, incluyendo cualquier garantía de comerciabilidad o aplicabilidad para un propósito en particular.

9.8 Limitaciones de Responsabilidad

En la medida en que DigiCert y Certisur hayan emitido y administrado un Certificado en cumplimiento de la Política de Certificación y las Normas para el Proceso de Certificación, no tendrán responsabilidad alguna hacia el Suscriptor, cualquier Receptor Confiado o cualquier tercero, con relación a cualquier daño o pérdida sufrida como consecuencia del uso o confianza depositada en dicho Certificado.

Con el alcance permitido por la ley aplicable, los Acuerdos del Suscriptor y los Acuerdos del Receptor Confiado de CertiSur limitan la responsabilidad de DigiCert y CertiSur. Las limitaciones de responsabilidad suponen la exclusión de responsabilidad por daños y perjuicios fortuitos o imprevistos, directos o indirectos y los daños consiguientes. Dichos Acuerdos también incluyen los topes máximos que figuran a continuación, respecto de la responsabilidad de CertiSur por daños y perjuicios, concernientes a un Certificado específico:

Clase	*Tope Máximo de Responsabilidad*
Clase 1	El equivalente en moneda local a Cien Dólares Estadounidenses (u$s 100,00)
Clase 2	El equivalente en moneda local a Cinco Mil Dólares Estadounidenses (u$s 5.000,00)
Clase 3	El equivalente en moneda local a Cien Mil Dólares Estadounidenses (u$s 100.000,00)

Tabla 15 – Topes Máximos de Responsabilidad

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

La responsabilidad (y/o limitación de la misma) de los Clientes Corporativos actuando como Autoridades de Registro y la aplicable Autoridad Certificante será la establecida en los Acuerdos suscriptos entre ellos.

La responsabilidad de las Partes Confiadas (y/o limitación de la misma) será la establecida en los Acuerdos del Receptor Confiado que resultan aplicables.

La limitación de responsabilidad de DigiCert con respecto a los Certificados de Validación Extendida (EV) está descripta en el Acuerdo del Receptor Confiado y Limitación de Garantías de DigiCert, disponible en https://www.digicert.com/legal-repository.

9.9 Indemnizaciones

9.9.1 Indemnizaciones por Parte de los Suscriptores

Con el alcance permitido por la ley aplicable, los Suscriptores deberán indemnizar a DigiCert y/o CertiSur por:

- Falsedad o tergiversación de hecho por parte del Suscriptor en la Solicitud de Certificado del Suscriptor,

- Omisión por parte del Suscriptor de revelar un hecho relevante en la Solicitud de Certificado, si la falsedad u omisión fue realizada negligentemente o con la intención de engañar a cualquier persona,
- Errores del Suscriptor en la protección de la clave privada del Suscriptor, en la utilización de un Sistema Confiable o de cualquier otra forma en la toma de las precauciones necesarias para prevenir el compromiso, pérdida, divulgación, modificación o uso no autorizado de la clave privada del Suscriptor, o
- El uso de parte del Suscriptor de un nombre (incluyendo sin limitación alguna el nombre común, el nombre de dominio o una dirección de correo electrónico) que infrinja los Derechos de Propiedad Intelectual de terceros.

Los Acuerdos del Suscriptor que resultan aplicables pueden incluir obligaciones de indemnizaciones adicionales.

9.9.2 Indemnizaciones por Parte de Partes Confiadas

Con el alcance permitido por la ley aplicable, las Partes Confiadas deberán indemnizar a DigiCert y/o a CertiSur por:

- Falla de la Parte Confiada en el cumplimiento de las obligaciones de una Parte Confiada,
- La confianza de la Parte Confiada en un Certificado que no resulta razonable bajo las circunstancias, o
- La omisión o falla de la Parte Confiada en verificar el estado de ese Certificado para determinar si el Certificado había expirado o había sido revocado.

Los Acuerdos del Receptor Confiado que resultan aplicables pueden incluir obligaciones de indemnizaciones adicionales.

9.9.3 Indemnizaciones de Proveedores de Aplicaciones de Software

Sin perjuicio de cualquier limitación de su responsabilidad hacia Suscriptores o Partes Confiadas, la Autoridad Certificante reconoce y acepta que los Proveedores de Aplicaciones de Software que tengan un acuerdo vigente de distribución de Certificados Raíz respecto de una Autoridad Certificante Raíz de DigiCert no asumen ninguna obligación ni potencial responsabilidad de la Autoridad Certificante bajo estas Normas o que pueda existir de alguna otra forma, como consecuencia de la emisión o mantenimiento de Certificados o la confianza depositada en ellos por Partes Confiadas o terceros.

Por lo tanto, la Autoridad Certificante defenderá, indemnizará y mantendrá indemne a cada Proveedor de Aplicaciones de Software por cualquier reclamo, daño y pérdida sufrida por el mismo relacionados con un Certificado emitido por la Autoridad Certificante, sin importar la causa de la acción o interpretación legal involucrada. Sin embargo, esta cláusula no es aplicable a cualquier reclamo, daño o pérdida sufrida por dicho Proveedor relacionados con un Certificado emitido por la Autoridad Certificante, cuando dicho reclamo, daño o pérdida haya sido causado directamente por el software del Proveedor que haya indicado como no confiable un Certificado que es válido o indicado como confiable un certificado que: (1) haya expirado, o (2) ha sido revocado (solamente

en caso en que el estado de revocación esté disponible en línea de parte de la Autoridad Certificante y el Proveedor falló en la verificación de tal estado o ignoró la indicación de revocado).

9.10 Vigencia y Finalización

9.10.1 Vigencia

Estas Normas para el Proceso de Certificación entran en vigencia a partir de su publicación en el Repositorio de CertiSur Las enmiendas a estas Normas para el Proceso de Certificación entrarán en vigencia a partir del momento de su publicación en el Repositorio de CertiSur.

9.10.2 Finalización

Estas Normas para el Proceso de Certificación, tal como son modificadas de tanto en tanto, mantendrán su vigencia hasta que sean reemplazadas por una nueva versión.

9.10.3 Efectos de la Finalización y Supervivencia

Sin perjuicio de la finalización de la vigencia de las presentes Normas para el Proceso de Certificación, todos los Participantes del Subdominio CertiSur estarán obligados por sus términos con relación a todos los certificados emitidos, por el plazo de vigencia restante de dichos certificados.

9.11 Avisos y Comunicaciones Individuales entre los Participantes

A menos que esté especificado de otra forma en los acuerdos entre las partes, los Participantes del Subdominio CertiSur deberán utilizar todos los métodos de comunicación con las otras partes que resulten comercialmente razonables, teniendo en consideración la criticidad y el tema sujeto de la comunicación.

9.12 Cambios en las Regulaciones

9.12.1 Procedimientos de Cambio en las Regulaciones

Los cambios a estas Normas para el Proceso de Certificación pueden ser realizados por el Departamento Legal de CertiSur S.A. Los cambios pueden ser realizados en la forma de un documento conteniendo las enmiendas a las Normas o directamente una actualización del documento completo. Los documentos conteniendo las enmiendas o las versiones actualizadas estarán publicadas en el Repositorio de CertiSur localizado en: https://www.certisur.com/repositorio/actualizaciones. Las actualizaciones sustituyen cualquier provisión especificada o conflictiva de la versión referenciada de las Normas. La Autoridad de Política de Certificación de DigiCert determinará si los cambios en las presentes Normas

requerirán un cambio en la extensión Identificador de Objeto para la Política de Certificación (Certificate Policy Object Identifier) correspondiente a cada Clase de Certificado.

9.12.2 Mecanismo de Notificación y Plazos

CertiSur se reserva el derecho de efectuar cambios a las Normas para el Proceso de Certificación sin mediar notificación, por modificaciones que no resulten sustanciales incluyendo, sin limitaciones, correcciones de errores tipográficos, cambios de direcciones URL o cambios en la información de contactos. La decisión de CertiSur de calificar a una modificación como material o no está sujeta a la exclusiva discrecionalidad de CertiSur.

Todos los cambios propuestos a estas Normas serán publicados en el Repositorio de CertiSur localizado en: https://www.certisur.com/repositorio/actualizaciones.

Sin perjuicio que cualquier disposición de las presentes Normas para el Proceso de Certificación estipule lo contrario, si CertiSur considera que resulta necesario efectuar modificaciones materiales a las mismas para detener o prevenir una falla de seguridad de la Symantec Trust Network, del Subdominio CertiSur o de cualquier otra porción de la Symantec Trust Network, CertiSur estará facultado para efectuar dichas modificaciones, mediante su publicación en el Repositorio de CertiSur. Dichas modificaciones entrarán en vigencia inmediatamente desde el momento de su publicación. Dentro de un plazo razonable a partir de su publicación, CertiSur comunicará dichos cambios a los Participantes del Subdominio CertiSur.

Como mínimo, CertiSur actualizará las presentes Normas con una frecuencia anual, en cumplimiento de las disposiciones del CA/Browser Forum.

9.12.2.1 Período para Comentarios

Excepto que esté previsto lo contrario, el período para comentarios para cualquier enmienda material a las Normas para el Proceso de Certificación será de quince (15) días, que comenzarán en la fecha en que la modificación sea incluida en el Repositorio de CertiSur. Cualquier Participante del Subdominio CertiSur estará facultado para enviar comentarios al Departamento Legal de CertiSur S.A. hasta la finalización del período para comentarios.

9.12.2.2 Mecanismo para el Tratamiento de Comentarios

El Departamento Legal de CertiSur S.A. considerará cualquier comentario respecto de las modificaciones propuestas. CertiSur podrá: (a) posibilitar que la modificación propuesta se transforme en efectiva sin cambios, (b) modificar los cambios propuestos y publicarlos como si se tratara de una nueva enmienda, o (c) descartar las modificaciones propuestas. CertiSur está facultado para descartar cualquier modificación propuesta, mediante notificación en la sección Actualizaciones y Notificaciones del Repositorio de CertiSur. Salvo que las enmiendas propuestas sean modificadas o rechazadas, se transformarán en efectivas al finalizar el período para comentarios.

9.12.3 Modificaciones que Exigen Cambios en el Identificador de Objeto de la Política de Certificación (Certificate Policy OID)

Si la Autoridad de Política de Certificación de DigiCert determina que es necesario un cambio en la extensión Identificador de Objeto para la Política de Certificación (Certificate Policy Object Identifier), la enmienda contendrá un nuevo Identificador de Objeto para la Política de Certificación (Certificate Policy Object Identifier) correspondiente a cada Clase de Certificado. De otra forma, las modificaciones no requerirán cambio alguno en la extensión Identificador de Objeto para la Política de Certificación (Certificate Policy Object Identifier).

9.13 Procedimientos para la Resolución de Disputas

9.13.1 Disputas entre DigiCert, Afiliados y Clientes

Las disputas entre los Participantes del Subdominio CertiSur deberán ser resueltas con arreglo a las disposiciones del acuerdo aplicable entre las partes.

9.13.2 Disputas con Suscriptores Usuarios Finales o Partes Confiadas

Con el alcance permitido por la ley aplicable, los Acuerdos del Suscriptor y los Acuerdos del Receptor Confiado de CertiSur incluyen una cláusula de resolución de disputas. Las disputas que involucren a CertiSur requieren un período inicial de negociación de sesenta (60) días, a continuación del cual se podrá iniciar un proceso judicial en los Tribunales Comerciales de la Ciudad Autónoma de Buenos Aires, República Argentina, en caso de que el demandante sea una persona jurídica residente en la República Argentina. En el caso de residentes de otros países, se podrá iniciar un proceso arbitral ante la Cámara Internacional de Comercio ("International Chamber of Commerce o ICC"), con arreglo a las Reglas de Conciliación y Arbitraje de dicha Cámara.

9.14 Ley Aplicable

Sujeto a cualquier limitación existente en la ley aplicable, las leyes de la República Argentina regirán la obligatoriedad, redacción, interpretación y validez de las presentes Normas para el Proceso de Certificación, independientemente de cualquier previsión contractual u otra opción de legislación y sin el requerimiento de establecer un nexo comercial en la República Argentina. Esta elección de la ley aplicable es realizada a efectos de asegurar la uniformidad de los procedimientos e interpretaciones para todos los Participantes del Subdominio CertiSur, sin importar en donde éstos se encuentren localizados.

Esta disposición con relación a la ley aplicable tiene efecto solamente con respecto a las presentes Normas para el Proceso de Certificación. Los Acuerdos que incorporan a las presentes Normas por referencia pueden contener sus propias disposiciones en materia de ley aplicable, en la medida en que esta Sección rija la obligatoriedad, redacción, interpretación y validez de los términos de

estas Normas en forma separada e independiente de las restantes disposiciones de cualesquiera de dichos acuerdos, sujeto a las limitaciones existentes en la ley aplicable.

9.15 Cumplimiento de la Ley Aplicable

Las presentes Normas para el Proceso de Certificación están sujetas a la legislación aplicable, nacional, provincial, local o extranjera, reglas, regulaciones, ordenanzas, decretos y otras regulaciones gubernamentales incluyendo, pero no limitándose, a restricciones respecto de la exportación e importación de hardware, software o información técnica.

9.16 Misceláneos

9.16.1 Acuerdo Completo

No aplicable.

9.16.2 Asignación

No aplicable.

9.16.3 Divisibilidad

En caso de que una cláusula o provisión de las presentes Normas sea declarada como inaplicable por un juez o cualquier otro tribunal que tenga jurisdicción, las cláusulas restantes de las presentes Normas continuarán en vigencia.

9.16.4 Aplicabilidad (Honorarios de Letrados y Renuncia de Derechos)

No aplicable.

9.16.5 Fuerza Mayor

Con el alcance permitido por la ley aplicable, los Acuerdos del Suscriptor y los Acuerdos del Receptor Confiado de CertiSur incluyen una cláusula que protege a DigiCert y a CertiSur en caso de fuerza mayor.

9.17 Otras Disposiciones

No contempladas.

Apéndice A – Acrónimos y Definiciones

Tabla de Acrónimos

Acrónimo	*Término*
AC	Autoridad Certificante.
AICPA	Instituto Americano de Contadores Públicos Certificados (American Institute of Certified Public Accountants)
ANSI	Instituto Americano de Estándares (American National Standards Institute).
APC	Autoridad Primaria de Certificación (Primary Certification Authority o PCA).
AR	Autoridad de Registro (Registration Authority o RA).
BIS	United States Bureau of Industry and Science del Departamento de Comercio de los Estados Unidos
ccTLD	Código de País de Dominio de Primer Nivel (Country Code Top-Level Domain)
CP	Política de Certificación (Certificate Policy)
CPS	Normas para el Proceso de Certificación (Certification Practice Statement).
CRL	Lista de Certificados Revocados (Certificate Revocation List).
CSPRNG	Generador de números pseudoaleatorios asegurado criptográficamente (Criptographically Secure Pseudo-Random Number Generator)
DBA	Nombre de Fantasía o Denominación de Marca utilizado por una organización en reemplazo de su Denominación según Estatuto de conformación (doing business as)
DCPA	Autoridad de Política de DigiCert (DigiCert Policy Authority)
DNS	Sistema de Nombres de Dominio (Domain Name System)
EV	Validación Extendida (Extended Validation)
FCA	Firma de Contenido Autenticado (Authenticated Content Signing o ACS)
FIPS	United State Federal Information Processing Standards.
IANA	Autoridad de Asignación de Números de Internet (Internet Assigned Numbers Authority)
FQDN	Nombre de Dominio Calificado (Fully Qualified Domain Name)
ICC	Cámara Internacional de Comercio (International Chamber of Commerce).
ICCANN	Corporación de Internet para la Asignación de Nombres y Números (Internet Corporation for Assigned Names and Numbers)
IM	Mensajería Instantánea (Instant Messaging)
ISO	Organización Internacional para la Estandarización (International Organization for Standardization)
KRB	Conjunto de Recupero de Clave (Key Recovery Block).
LSVA	Análisis lógico de vulnerabilidades de seguridad (Logical security vulnerability assessment).
NIST	Instituto Nacional de Estándares y Tecnología del Gobierno de los Estados Unidos de Norte América (National Institute of Standards and Technology)
OCSP	Protocolo de Estado del Certificado en Línea (Online Certificate Status Protocol).
OID	Identificador de Objeto (Object Identifier)
PIN	Número de Identificación Personal (Personal Identification Number).
PKCS	Estándar Criptográfico de Clave Pública (Public-Key Cryptography Standard).
PKI	Infraestructura de Clave Pública (Public Key Infrastructure).
QGIS	Fuente Gubernamental de Información Calificada (Qualified Government Information Source)
QIIS	Fuente Independiente de Información Calificada (Qualified Independent Information Source)
RFC	Request for comment.
S/MIME	Secure multipurpose Internet mail extensions.
SSL	Secure Sockets Layer.

Acrónimo	*Término*
STN	Symantec Trust Network.
TLD	Cominio de Primer Nivel (Top-Level Domain)
TLS	Transport Layer Security

Definiciones

Término	*Definición*
Acuerdo de Managed PKI	Acuerdo bajo el cual una organización se convierte en Cliente de Managed PKI y acepta estar obligado por los términos de las presentes Normas para el Proceso de Certificación.
Acuerdo de Uso de la Lista de Certificados Revocados (CRL)	Contrato mediante el cual se establecen los términos y condiciones bajo los cuales pueden ser utilizadas una Lista de Certificados Revocados o la información contenida en dicha Lista.
Acuerdo del Receptor Confiado (Relying Party Agreement o RPA)	Contrato utilizado por una Autoridad Certificante para establecer los términos y condiciones bajo los cuales un individuo o una organización actúan como una Parte Confiada.
Acuerdo del Suscriptor	Contrato utilizado por una Autoridad Certificante o una Autoridad de Registro para establecer los términos y condiciones bajo los cuales un individuo o una organización actúan como Suscriptor.
Administración Automática	Procedimiento mediante el cual las Solicitudes de Certificado son aprobadas automáticamente siempre que la información de la solicitud concuerde con información contenida en una base de datos.
Administrador	Persona Confiable que pertenece a una organización que actúa como Processing Center, Service Center o Cliente Corporativo desarrollando tareas de validación y otras funciones de Autoridad Certificante o Autoridad de Registro.
Administrador de Key Manager	Persona Confiable que desarrolla tareas de generación y recupero de claves para un Cliente de Managed PKI que utiliza el servicio de Key Manager de Managed PKI.
Administrador de Managed PKI	Persona Confiable que desarrolla tareas de validación y otras funciones de Autoridad de Registro para un Cliente de Managed PKI.
Afiliado	Tercero confiable, líder en su género (por ejemplo en tecnología, telecomunicaciones o servicios financieros), que ha celebrado un acuerdo con DigiCert para ser el canal de distribución y de servicios para la Symantec Trust Network, dentro de un territorio especificado. En el contexto del CA/Browser Forum, el término Afiliado se refiere a: (i) una coporación, un socio, un joint venture u otra entidad controlada o controlante o con un control en común con otra entidad. (ii) una agencia, subdivisión política, departamento o cualquier entidad que opere bajo el control directo de una agencia de gobierno.
Auditor Calificado	Persona física o Entidad Legal que reúne los requisitos establecidos en la Sección 8.2.
Auditoría de Cumplimiento	Revisión periódica que realiza un Processing Center, un Service Center o un Cliente Corporativo para determinar su conformidad con los Requerimientos Estándar dentro de la STN que le resulten aplicables.
Auditoría Investigativa/ Investigación	Auditoría o investigación llevada a cabo por DigiCert o CertiSur, debido a que DigiCert o CertiSur tienen razones para suponer que una entidad ha incumplido los Requerimientos Estándar de la STN o ha ocurrido un incidente o Compromiso relacionado con esa entidad o una amenaza real o potencial para la seguridad de la STN en virtud del comportamiento de dicha entidad.
Autenticación Manual	Procedimiento mediante el cual un Administrador revisa y aprueba, una por una, las Solicitudes de Certificado, utilizando una interfaz web.
Autoridad Certificante (Certification Authority o CA)	Entidad autorizada para emitir, administrar, revocar y renovar Certificados dentro de la Symantec Trust Network (STN).
Autoridad Certificante Emisora	En relación a un Certificado en particular, la Autoridad Certificante que emitió dicho Certificado. Puede tratarse de una Autoridad Certificante Raíz o de una Autoridad Certificante Subordinada.
Autoridad Certificante en línea (Online CA)	Autoridades Certificantes que se encuentran en línea firmando Certificados de Suscriptores, de modo tal de prestar un servicio continuo de firma.
Autoridad Certificante fuera de línea (Offline CA)	Autoridades Primarias de Certificación, Autoridades Certificantes Emisoras Raíz u otras Autoridades Certificantes Intermedias designadas dentro de la Symantec Trust Network que son mantenidas fuera de línea por razones de seguridad, a los efectos

Término	Definición
	de protegerlas de eventuales ataques de intrusos, a través de una red. Estas Autoridades Certificantes no firman directamente Certificados de Suscriptores usuarios finales.
Autoridad Certificante Intermedia (Intermediate CA)	Autoridad Certificante cuyo Certificado está ubicado en la Cadena de Certificación entre el Certificado de la Autoridad Certificante raíz y el Certificado de la Autoridad Certificante que emite los Certificados para Suscriptores.
Autoridad Certificante Raíz	Autoridad Certificante de máximo nivel cuyo Certificado Raíz es distribuido por los Proveedores de Software Aplicativo y que emite los Certificados de Autoridades Certificantes Subordinadas.
Autoridad Certificante Subordinada	Una Autoridad Certificante cuyo Certificado está firmado por una Autoridad Certificante Raíz u otra Autoridad Certificante Subordinada.
Autoridad de Política de DigiCert (DCPA)	Organización responsable, dentro de la estructura de DigiCert, de promulgar o aprobar Políticas de Certificación o Normas para el Proceso de Certificación en la Symantec Trust Network.
Autoridad de Registro (Registration Authority o RA)	Entidad autorizada por una Autoridad Certificante para asistir a los Solicitantes de Certificados en las tareas de requerir Certificados y para aprobar o rechazar Solicitudes de Certificados, revocar Certificados o renovar Certificados.
Autoridad de Registro Organizacional (Enterprise RA)	Cliente de Managed PKI para SSL que puede solicitar múltiples Certificados de Validación Extendida (EV) para Dominios y Organizaciones que han sido verificados por DigiCert para un tercer nivel de dominio o superior, y que contienen el nombre de dominio que ha sido verificado por DigiCert en el Certificado de Validación Extendida (EV) original, en un todo de acuerdo con los requerimientos de las presentes Normas
Autoridad Primaria de Certificación (Primary Certification Authority o PCA)	Autoridad Certificante que actúa como una Autoridad Certificante raíz de una Clase específica de Certificados y emite los Certificados de las Autoridades Certificantes subordinadas a ella.
Autorización de Dominio	Carta u otra documentación suministrada por un Registrante del Nombre de Dominio confirmando la legitimidad de un Solicitante para solicitar un Certificado con un Espacio de Nombre de Dominio específico.
Autorizante del Certificado	Persona física que es empleado o agente autorizado del Solicitante que manifiesta su autoridad para representar al Solicitante de un Certificado de Validación Extendida (EV) a los efectos de: (i) Actuar como Solicitante del Certificado y autorizar a otros empleados o terceros a actuar en carácter de Solicitante del Certificado, y (ii) aprobar Solicitudes de Certificados de Validación Extendida (EV) remitidos por otros Solicitantes.
Cadena de Certificación	Lista ordenada de Certificados conteniendo un Certificado de Suscriptor de usuario final y los Certificados de las Autoridades Certificantes, que termina en un Certificado raíz.
Ceremonia de Generación de Claves	Procedimiento mediante el cual se genera el par de claves de una Autoridad Certificante o una Autoridad de Registro, la clave privada es transferida a un módulo criptográfico, se genera una copia de seguridad (back-up) de esta clave privada y/o se certifica la correspondiente clave pública.
Certificación	Carta o Informe certificando que la Información del Sujeto de un Certificado es correcta, firmada por un contador, abogado, agente gubernamental o cualquier otro tercero confiable en el cual usualmente se deposite confianza para certificar este tipo de información.
Certificación Cruzada	Certificado utilizado para establecer una relación de confianza entre dos Autoridades Certificantes Raíz.
Certificado	Mensaje que, como mínimo, indica un nombre o identifica a la Autoridad Certificante identifica al Suscriptor, contiene la Clave Pública del Suscriptor, establece el Período de Vigencia del Certificado, contiene el número de serie del Certificado y está firmado digitalmente por la Autoridad Certificante allí identificada.
Certificado (minorista)	Certificado emitido por DigiCert, actuando como Autoridad Certificante, a individuos u organizaciones que le solicitan el mismo, uno por uno, en el sitio web de DigiCert o CertiSur
Certificado Confiable Públicamente	Certificado que resulta confiable como resultado del hecho que su correspondiente Certificado Raíz está distribuido como raíz de confianza en los softwares aplicativos más difundidos.

Término	*Definición*
Certificado de Administrador	Certificado emitido a un Administrador que puede ser utilizado solamente para desarrollar funciones de Autoridad Certificante o de Autoridad de Registro.
Certificado de Prueba	Certificado con una período de validez máxima de treinta (30) días, que: i) incluye una extensión crítica que especifica el OID del CA/Browser Forum como Certificado de Prueba, o ii) es emitido por una Autoridad Certificante que no está bajo una cadena de un certificado raìz sujeto a las presentes Normas.
Certificado de Validación Extendida (EV)	Certificado digital que contiene información especificada en los Requerimientos de Validación Extendida (EV Guidelines) yque ha sido validado con arreglo a dichos Requerimientos.
Certificado de Validación Extendida (EV) Organizacional	Certificado de Validación Extendida (EV) que un Cliente del servicio de Managed PKI para SSL autoriza a DigiCert a emitir, en un tercer nivel de dominio o superior, y que contiene el nombre de dominio que ha sido verificado por DigiCert
Certificado Raíz	El Certificado auto firmado emitido por la Autoridad Certificante Raíz para identificarse y facilitar la verificación de los Certificados emitidos por sus Autoridades Certificantes Subordinadas.
Certificado Válido	Un Certificado que cumple positivamente con los procedimientos de validación especificados en la RFC 5280.
Certificado Wildcard	Un Certificado conteniendo un asterisco (*) en la última posición a la izquierda de cualquier Nombre de Dominio Calificado de un Sujeto.
Clase	Un nivel especificado de confianza, tal como se define en estas Normas. Ver Sección 1.1.
Clave Privada	Clave de un Par de Claves que es mantenida en secreto por el poseedor del Par de Claves y que es utilizada para generar Firmas Digitales y/o desencriptar registros o archivos digitales que fueron encriptados con la Clave Pública asociada.
Clave Pública	La clave de un Par de Claves que puede ser difundida públicamente por el poseedor de la correspondiente Clave Privada y que es utilizada por una Parte Confiada para verificar Firmas Digitales que ha sido creadas por el poseedor de la correspondiente Clave Privada y/o encriptar mensajes que puedan solamente ser desencriptados por el poseedor de la correspondiente Clave Privada.
Client Service Center	Service Center que es administrado por un Afiliado que provee Certificados para clientes, tanto en la línea de negocios minorista como para Clientes Corporativos.
Cliente Corporativo	Organización que es Cliente de Managed PKI o de cualquier otro servicio dentro de la Symantec Trust Network.
Compromiso	Violación (o sospecha de que ella puede haberse producido) de una política de seguridad que pueda implicar el conocimiento no autorizado o la pérdida de control sobre información sensitiva o confidencial. Con respecto a una clave privada, Compromiso significa la pérdida, robo, conocimiento por parte de un tercero, modificación, uso no autorizado o cualquier otra violación de la seguridad de esa clave privada.
Compromiso de Clave	Se dice que una Clave Privada ha sido comprometida si su valor ha sido revelado a una persona no autorizada, una persona no autorizada ha tenido acceso a la misma o existe una técnica en los hechos que una persona no autorizada puede utilizar a los efectos de descubrir su valor.
Condiciones de uso	Especificaciones con respecto a los resguardos de seguridad yusos aceptables de un Certificado emitido con arreglo a estas Normas, en la medida en que el Solicitante o Suscriptor esté vinculado con la Autoridad Certificante.
Conjunto de Recupero de Clave (Key Recovery Block o KRB)	Estructura de datos que contiene una clave privada de un Suscriptor, encriptada mediante la utilización de una clave de encriptación. Los Conjuntos de Recupero de Clave (KRB) son generados utilizando el software de Key Manager de Managed PKI.
Contacto del Dominio	Registrante del Nombre de Dominio, Contacto Técnico o Contacto Corporativo (o su equivalente en un registrante de nombre de dominio de primer nivel de un país) tal como aparece en los datos del registro WHOIS del Nombre de Dominio Base o en un Registro de Servicio de DNS SOA.
Contestador del Protocolo del Estado del Certificado en Línea (OCSP Responder)	Servidor en línea operado bajo la autoridad de la Autoridad Certificante y conectado a su Repositorio, a los efectos de procesar las solicitudes del estado de los Certificados. Ver también Protocolo del Estado del Certificado en Línea (Online Certificate Status Protocol u OCSP).

Término	*Definición*
Control Center de Managed PKI	Interfaz web que permite a los Administradores de Managed PKI desarrollar la tarea de Autenticación Manual de las Solicitudes de Certificado
Datos del Certificado	Solicitudes de Certificados yotros datos relacionados con el mismo, ya sea obtenidos del Solicitante o de otra forma, en poder o control de la Autoridad Certificante o a los cuales la Autoridad Certificante tenga acceso.
Derechos de Propiedad Intelectual	Alude a la titularidad de la propiedad, tales como derechos de autor, patente industrial, secreto comercial, marca registrada o cualquier otro derecho vinculado con la propiedad intelectual.
Desarrollador de Software de Navegación	Desarrollador de software de navegación (browser) sobre Internet u otras aplicaciones que muestra o utiliza certificados y distribuye certificados raíz, tal como KDE, Microsoft Corporation, Mozilla Corporation, Opera Software ASA y Red Hat, Inc.,
Dirección IP Reservada	Una dirección IPv4 o IPv6 que la Autoridad de Asignación de Números de Internet (Internet Assigned Numbers Authority o IANA) ha marcado como reservada: http://www.iana.org/assgnments/ipv4-address-space/ipv4-address-space.xml http://www.iana.org/assgnments/ipv6-address-space/ipv6-address-space.xml
Dispositivo Criptográfico Seguro Generador de Números Pseudoaleatorios (CSPRNG)	Dispositivo generador de números aleatorios destinados a ser empleados en un sistema criptográfico.
Empresa Madre	Compañía dueña o accionista mayoritaria de una empresa Subsidiaria, tal como puede verificarse en una Base de Datos Privada Calificada o a través de los correspondientes Estados Contables certificados por un Contador Público Matriculado o equivalente.
Enterprise Service Center	Línea de negocios a cargo de un Afiliado, consistente en proveer a clientes (empresas u organizaciones) servicios de Managed PKI.
Entidad de Registro	Oficina del Gobierno que registra la información de las empresas en relación a su conformación o a la autorización para ejercer el comercio, bajo una licencia, aprobación u otra certificación. Una Entidad de Registro puede ser, aunque no está limitado a, la Inspección General de Justicia, el Registro Público de Comercio, la oficina que autoriza el funcionamiento de una entidad financiera, como por ejemplo el Banco Central o la Superintendencia de Bancos o la oficina que autoriza el funcionamiento de una compañía de seguros, como la Superintendencia de Seguros.
Entidad Gubernamental	Entidad legal, agencia, departamento, ministerio, secretaría, sucursal o cualquier oficina similar del gobierno de un país o subdivisión política dentro de dicho país, como por ejemplo una provincia, estado, ciudad, municipio, etc.
Entidad Legal	Una empresa, asociación, corporación, fideicomiso, sociedad, entidad gubernamental u otra entidad que es legítima dentro del sistema legal de un país.
Entidad Superior	Organización por encima de otra entidad dentro de la jerarquía de la Symantec Trust Network (jerarquía de Clase 1, 2 o 3).
Espacio de Nombre de Dominio	Conjunto de todos los posibles Nombres de Dominio que están subordinados a un nodo dentro del Sistema de Nombres de Dominio.
Especialista en Validación	Persona que desarrolla las tareas de verificación de la información especificadas en las presentes Normas.
Estado Soberano	Estado o País que administra su propio gobierno yno es dependiente o está sujeto a otro poder.
Fecha de Expiración	Fecha asociada a la frase “No después de” (Not After) en un Certificado y que define la finalización del Período de Vigencia de un Certificado
Firmante Autorizado	Persona física o agente autorizado del Solicitante de Certificado de Validación Extendida (EV) que ha manifestado su autoridad para representar al Solicitante y que tiene dicha autoridad para firmar los Acuerdos del Suscriptor en su representación.
Frase de Comprobación	Párrafo secreto elegido por el Solicitante del Certificado durante el proceso de solicitar un Certificado. Una vez que el Certificado es emitido, el Solicitante del Certificado se convierte en un Suscriptor y la Autoridad Certificante o la Autoridad de Registro podrán usar la Frase de Comprobación para autenticar al Suscriptor cuando éste desee revocar o renovar su Certificado.
Funcionario Responsable	Empleado de una Organización Privada, Entidad Gubernamental o Comercio que es propietario, socio, gerente, director o funcionario, tal como es identificado por la

Término	Definición
	denominación de su puesto o cargo, o un empleado, proveedor o agente autorizado de dicha entidad u organización a los efectos de ejecutar tareas relacionadas con la solicitud, emisión y uso de Certificados de Validación Extendida (EV).
Guía del Administrador del Servicio de Key Management de Managed PKI	Documento que establece los requerimientos operativos y los procedimientos que deben observar los Clientes de Managed PKI al utilizar los servicios de Key Manager.
Guión de Generación de Claves	Plan documentado de los procedimientos para la generación de un Par de Claves de una Autoridad Certificante.
Identificador de Objeto (Object Identifier)	Identificador único numérico o alfanumérico registrado bajo el estándar aplicable de la Organización Internacional para la Estandarización (International Organization for Standardization o ISO) para un objeto específico o para una clase de objetos.
Individuo Vinculado	Persona vinculada a un Cliente Corporativo (i) como gerente, director, empleado, socio, contratista, proveedor, personal temporario o relacionada de otra forma con la organización (ii) como miembro de una comunidad de interés reconocida por CertiSur, o (iii) como individuo que mantiene una relación con la organización y de la cual la organización tiene registros de negocios u otros elementos que permiten asegurar adecuadamente la identidad de esa persona.
Información Confidencial o Privada	Dato que debe permanecer de manera confidencial y privada en función de lo previsto en la Sección 9.3.
Información de Identidad del Sujeto	Información que identifica al Sujeto del Certificado. La Información de Identidad del Sujeto no incluye el nombre de dominio especificado en la extensión subjetAltName o en el campo Nombre Común (commonName).
Información No Verificada del Suscriptor	Datos suministrados por un Solicitante de Certificado a una Autoridad Certificante o a una Autoridad de Registro e incluidos en el Certificado, que no han sido confirmados por la Autoridad Certificante o la Autoridad de Registro y sobre los cuales la Autoridad Certificante o la Autoridad de Registro no afirman nada salvo que los mismos fueron provistos por el Solicitante del Certificado.
Informe de Auditoría	Dictamen emitido por un Auditor Calificado expresando su opinión acerca de si los procesos y controles llevados a cabo por una entidad cumplen con las disposiciones obligatorias de las presentes Normas.
Informe de Problemas de un Certificado	Reporte de sospechas sobre Compromiso de Claves, uso inapropiado de un Certificado u otros tipos de fraude, compromiso, uso inadecuado o comportamiento incorrecto con relación a Certificados.
Infraestructura de Clave Pública (Public Key Infrastructure o PKI)	Arquitectura, organización, técnicas, normas y procedimientos que soportan colectivamente la implementación y operación de un sistema criptográfico de clave pública basado en Certificados. La Symantec Trust Network es una Infraestructura de Clave Pública compuesta por sistemas que de manera concurrente proveen e implementan los servicios dentro de la Symantec Trust Network.
Key Manager de Managed PKI	Solución de recupero de claves para aquellos Clientes de Managed PKI que optaron por implementar el servicio de recupero de claves, bajo un Acuerdo de Managed PKI específico.
Lista de Certificados Revocados (Certificate Revocation List o CRL)	Lista emitida periódicamente y también debido a una exigencia operacional, firmada digitalmente por una Autoridad Certificante, que identifica a los Certificados que han sido revocados con anterioridad a sus respectivas fechas de vencimiento, en un todo de acuerdo con lo previsto en la Sección 3.4. La lista incluye generalmente el nombre del emisor de la Lista de Certificados Revocados, la fecha de emisión, la fecha de emisión programada de la próxima Lista de Certificados Revocados, los números de serie de los Certificados revocados y la fecha exacta y los motivos de la revocación.
Managed PKI	Servicio de DigiCert, consistente en una prestación totalmente integrada de administración de una Infraestructura de Clave Pública, ofrecido por CertiSur. Este servicio posibilita que los Clientes Corporativos de CertiSur distribuyan Certificados a individuos, como por ejemplo empleados, socios comerciales, proveedores y clientes como así también a dispositivos (por ejemplo, servidores, routers y firewalls). Managed PKI le permite a las empresas asegurar los servicios de mensajería,

Término	Definición
	intranets[25], extranets, redes privadas virtuales (VPN) y aplicaciones de comercio electrónico.
Método de comunicación confiable	Forma de comunicación, tal como dirección de correo postal o de envío por Courier, número telefónico o dirección de correo electrónico, que ha sido verificada utilizando una fuente diferente del Representante del Solicitante.
No repudio	Atributo de una comunicación, que provee protección contra una parte que niega falsamente el origen de una comunicación, niega que la misma fue remitida o niega su emisión. La negación del origen incluye la negación de una comunicación originada por la misma fuente dentro de una secuencia de uno o más mensajes previos, incluso si la identidad asociada con el remitente es desconocida. Nota: Solamente un fallo de un Juez, una Corte, un tribunal arbitral u otro tribunal pueden dictaminar el no repudio. Por ejemplo, una firma digital verificada mediante la utilización de un Certificado perteneciente a la Symantec Trust Network puede suministrar una prueba que permite la determinación de no repudio de parte de un tribunal, pero no constituye por sí misma la determinación de no repudiabilidad.
Nombre de Dominio	Etiqueta asignada a un nodo en el Sistema de Nombres de Dominio
Nombre de Dominio Autorizado	Nombre de Dominio utilizado para obtener autorización para la emisión de un Certificado para un determinado Nombre de Dominio Calificado (FQDN). DigiCert puede utilizar un Nombre de Dominio Calificado (FQDN) informado por un Registro de DNS de Nombres de Dominio como un Nombre de Dominio a los efectos de validar dicho dominio. Si el Nombre de Dominio contiene un caracter asterisco (wildcard), DigiCert eliminará todas las porciones a la izquierda del Nombre de Dominio solicitado. DigiCert puede eliminar ninguno o los niveles necesarios hasta encontrar, desde la izquierda hacia la derecha, un nombre de dominio base y puede utilizar cualquiera de los valores intermedios a los efectos de la validación del dominio.
Nombre de Dominio Base	Porción de un Nombre de Dominio Calificado (FQDN) que es solicitado para un Certificado, que constituye el primer nodo del Nombre de Dominio hacia la izquierda de un sufijo controlado por un registro o un sufijo público, más la porción correspondiente a dicho sufijo. Para los casos de Nombres de Dominio Calificados (FQDN), en donde el nodo que aparece en el extremo derecho es un Dominio de Primer Nivel Genérico (gTLD) asignado a un propietario con arreglo a las directivas de ICANN, dicho Dominio de Primer Nivel puede ser utilizado como Nombre de Dominio Base.
Nombre de Dominio (Fully-Qualified Domain Name)	Nombre de Dominio que incluye las etiquetas de todos los nodos superiores en el Sistema de Nombres de Dominio.
Nombre de Dominio No Registrado	Nombre de Dominio que no es un Nombre de Dominio Registrado
Nombre de Dominio Registrado	Nombre de Dominio que ha sido registrado por un Registrador de Nombres de Dominio.
Nombre Interno	Cadena de caracteres (no una dirección IP) en el campo Nombre Común (Common Name) o Nombre Alternativo del Sujeto (Subject Alternative Name), dentro de un Certificado, que no puede ser verificado como único globalmente al momento de emisión del certificado, debido a que no finaliza con un Dominio de Nivel Superior (Top Level Domain) registrado en la Base de Datos de Raíces (Root Zone) del IANA (Internet Assigned Numbers Authority).
Normas para el Proceso de Certificación (Certification Practice Statement o CPS)	Conjunto de normas que DigiCert o un Afiliado emplean para aprobar o rechazar Solicitudes de Certificados y para emitir, administrar y revocar Certificados y que deben emplear sus Clientes Corporativos.

[25] La utilización de Certificados de Servidor SSL o de Firma de Código con una extensión Nombre Alternativo del Sujeto ("SubjectAlternativeName") o el campo Nombre Común del Sujeto ("Subject commonName") conteniendo una Dirección IP Reservada o un Nombre Interno ha sido considerada obsoleta por el CA/Browser Forum y ha sido eliminada a partir del mes de Octubre de 2016. Cualquier certificado con estas características emitido después de esa fecha deberá tener fecha de vencimiento 1° de Noviembre de 2015 o anterior. Los certificados emitidos con anterioridad que contenían fechas de vencimiento posteriores al 1° de Octubre de 2016 han sido revocados con efecto a partir del 1° de Octubre de 2016.

Término	*Definición*
Objetivos de Control de la Administración de Certificados	Criterio que una entidad debe cumplir para satisfacer una Auditoría de Cumplimiento.
OID de Validación Extendida (EV)	Número de identificación, denominado "Identificador de Objeto" (Object Identifier), incluido en el campo Política de Certificación de un Certificado de Validación Extendida (EV) que: (i) indica que Norma de Política de Certificación de una Autoridad Certificante está relacionada con dicho Certificado, y (ii) señala al Certificado como que se trata de un Certificado de Validación Extendida (EV), mediando un acuerdo preexistente con uno o más Proveedores de Software Aplicativo.
Organización Internacional	Organización fundada en base a un documento constitutivo, por ejemplo un Tratado, una Convención o documento similar, firmado por o en nombre de, como mínimo, dos o más gobiernos de Estados Soberanos.
Organización vinculada	En el contexto del CA/Browser Forum, el término "organización vinculada" se refiere a: • Una empresa, corporación, joint venture u otra entidad que controla o es controlada por otra o que tiene un control en común con una tercera entidad, o • Una Agencia, Departamento, Oficina u otra subdivisión política o cualquier otra entidad que opere bajo las órdenes directas de una Entidad Gubernamental
País	Estado Soberano, tal como se define en las Directivas
Par de Claves (Key Pair)	Clave Privada y su correspondiente Clave Pública.
Parte Confiada	Individuo u organización que actúa basándose en la confianza en un Certificado y/o en una firma digital.
Partición de Secreto	Procedimiento de dividir la clave privada de una autoridad Certificante o los datos de activación necesarios para operar la clave privada de una Autoridad Certificante, a fin de efectivizar el control por parte de múltiples personas de las operaciones de la clave privada de una Autoridad Certificante, según lo establecido en la Sección 6.2.2.
Participante de la Symantec Trust Network	Individuo u organización que desempeña una o más funciones de las enumeradas a continuación, dentro de la Symantec Trust Network: DigiCert, un Afiliado, un Cliente, un Service Center, un Revendedor, un Suscriptor o una Parte Confiada.
Participantes del Subdominio CertiSur	Individuo u organización que es uno o más de los enumerados a continuación, dentro del Subdominio CertiSur de la Symantec Trust Network: CertiSur, un Cliente, un Revendedor, un Suscriptor o una Parte Confiada.
Período Operacional	Lapso durante el cual está en vigor un Certificado, que comienza en la fecha y hora de su emisión (o en un momento posterior, si así está específicamente indicado en el Certificado) y finaliza en la fecha y hora en que el Certificado expira o es revocado previamente a su vencimiento.
Persona Confiable	Empleado, personal contratado o consultor de una entidad, dentro de la Symantec Trust Network, responsable de administrar la confiabilidad estructural de esa entidad, sus productos y servicios, sus instalaciones y/o sus normas, tal como se describe en la Sección 5.2.1.
PKCS #10	Estándar Criptográfico de Clave Pública nro.10, desarrollado por RSA Security Inc., que define una estructura para la Solicitud de Firma de un Certificado (Certificate Signing Request o CSR).
PKCS #12	Estándar Criptográfico de Clave Pública nro.12, desarrollado por RSA Security Inc., que define un medio seguro para transmitir claves privadas.
Plazo de Vigencia	Lapso de tiempo que transcurre entre la fecha en que el Certificado es emitido y la Fecha de Expiración.
Política de Certificación (Certificate Policy o CP)	Documento de DigiCert que gobierna la Symantec Trust Network ("Symantec Trust Network Certificate Policies") que constituye la norma principal que regula la Symantec Trust Network (STN).
Posición de Confianza	Función dentro de una entidad de la Symantec Trust Network que debe ser ocupada por una Persona Confiable.
Proceso de Administración de Certificados	Procesos, normas y procedimientos asociados con el uso de claves, software y hardware, por medio de los cuales una Autoridad Certificante verifica los datos de los

Término	Definición
	Certificados, emite los Certificados, mantiene un Repositorio y revoca los Certificados.
Processing Center	Organización (DigiCert o ciertos Afiliados) que construye instalaciones altamente seguras para albergar, entre otras cosas, los módulos criptográficos utilizados para la emisión de los Certificados. En las líneas de negocios de Consumer y Web Site Service Center, los Processing Centers actúan como Autoridades Certificantes dentro de la Symantec Trust Network y desarrollan todos los servicios del ciclo de vida de los Certificados, tales como emisión, administración, revocación y renovación de Certificados. En la línea de negocios de Enterprise Service Center, los Processing Centers suministran servicios del ciclo de vida de los Certificados en nombre de sus Clientes Corporativos o Service Centers subordinados a ellos.
Protocolo del Estado del Certificado en Línea (Online Certificate Status Protocol u OCSP)	Un protocolo que permite suministrar a Partes Confiadas la información en tiempo real acerca del estado de un Certificado.
Proveedor de Software	Proveedor de software de Internet u otra aplicación confiable que muestra o utiliza certificados e incorpora certificados raìz.
Puerto Autorizado	Alguno de los siguientes puerto: 80 (http), 443 (http), 115 (sftp), 25 (smtp) y 22 (ssh).
Registrador de Nombres de Dominio	Persona o entidad que registra Nombres de Dominio bajo el auspicio o mediante el acuerdo con: (i) La Corporación para la Asignación de Nombres y Números de Internet (Internet Corporation for Assigned Names and Numbers o ICANN), (ii) una Autoridad o Registro de Nombres de Dominio nacional, o (iii) un Centro de Información de Redes (Network Information Center o NIC), incluyendo sus afiliados, contratados, delegados, sucesores o cesionarios.
Registrante del Nombre de Dominio	Normalmente conocido como el "Propietario" de un Nombre de Dominio, pero más adecuadamente la o las personas registradas con el Registrador de Nombres de Dominio como poseedores del derecho a controlar como es utilizado un Nombre de Dominio y, a su vez, como la persona física o Entidad Legal que figura como "Regis trante" por el servicio WHOIS del Registrador de Nombres de Dominio
Repositorio	Base de datos en línea conteniendo documentos que rigen la Infraestructura de Clave Pública públicamente disponibles, como las políticas de Certificación y las Normas para el Proceso de Certificación e información respecto del estado de los Certificados, ya sea a través de una Lista de Certificados Revocados o mediante una respuesta del Protocolo del Estado del Certificado en Línea (OCSP).
Repositorio de CertiSur	Base de datos accesible vía Web que cuenta con información relevante sobre la Symantec Trust Network y el Subdominio CertiSur de la misma.
Representante del Solicitante	Persona física que es el Solicitante, empleado del Solicitante o agente autorizado que manifiesta su autoridad para representar al Solicitante a los efectos de: (i) firmar y remitir o aprobar una solicitud de certificado en representación del Solicitante, y/o (ii) firmar y remitir un Acuerdo del Suscriptor en representación del Solicitante, y/o (iii) tomar conocimiento y aceptar las Condiciones de Uso del Certificado en representación del Solicitante, cuando se trate de una organización o individuo vinculado con la Autoridad Certificante. En el contexto de una Solicitud de Certificado de Validación Extendida (EV) Persona física empleada por el Solicitante de un Certificado de Validación Extendida (EV) para: (i) firmar y remitir o aprobar la Solicitud de Certificado de Validación Extendida (EV) en representación del Solicitante y/o (ii) firmar y remitir un Acuerdo del Suscriptor en representación del Solicitante.
Requerimientos Estándar dentro de la Symantec Trust Network	Exigencias en materia legal, técnica y de negocios, para emitir, administrar, revocar, renovar y utilizar Certificados dentro de la Symantec Trust Network.
Revendedor	Entidad que comercializa servicios dentro de mercados específicos, en nombre de DigiCert o de un Afiliado.
Revisión Complementaria de Administración del Riesgo	Control de un ente, por parte de DigiCert o de CertiSur, después de detectarse situaciones excepcionales o controles incompletos en el transcurso de una Auditoría de Cumplimiento o como parte del proceso normal de evaluación de riesgos, en el curso ordinario de los negocios.

Término	Definición
Revisión de Seguridad y Normas de Procedimiento	Control realizado por DigiCert a un Afiliado, antes de autorizarlo a iniciar su funcionamiento operativo.
RSA	Sistema criptográfico de clave pública inventado por Rivest, Shamir y Adleman.
Secreto Compartido	Porción de la clave privada de una Autoridad Certificante o una porción de los datos de activación necesarios para operar la clave privada de una Autoridad Certificante, con arreglo a las disposiciones de un acuerdo de Secreto Compartido.
Secure Sockets Layer (SSL)	Método estándar del mercado para proteger las comunicaciones web, desarrollado por Netscape Communications Corporation. El protocolo de seguridad SSL provee encriptación de datos, autenticación de servidores, integridad de los mensajes y, opcionalmente, la autenticación del cliente, dentro de una conexión TCP/IP (Transmission Control Protocol/Internet Protocol).
Service Center	Afiliado que no alberga módulos de firma de Certificados para la emisión de Certificados de una Clase específica o de un tipo determinado y que, en cambio, descansa en un Processing Center para desarrollar el procesamiento de la emisión, administración, revocación y renovación de tales Certificados.
Servicio de Recupero de Claves	Servicio de DigiCert suministrado por CertiSur, que provee las claves de encriptación necesarias para recuperar el Conjunto de Recupero de Clave (KRB), como parte del uso que un Cliente Corporativo hace del Servicio de Key Manager de Managed PKI, a efectos de recuperar una clave privada de un Suscriptor.
Sistema Confiable	Hardware computacional, software y procedimientos que son razonablemente seguros contra violación por parte de terceros no autorizados o mal uso. Proveen un razonable nivel de disponibilidad, confiabilidad y precisión en la operación. Están razonablemente diseñados para realizar las funciones pretendidas y cumplimentar la política de seguridad aplicable. Un Sistema Confiable no es necesariamente un "sistema confiable" tal como se lo reconoce en la nomenclatura clasificada del gobierno de los Estados Unidos de Norte América.
Solicitante	Individuo u organización legal que requiere la emisión o la renovación de un Certificado por parte de una Autoridad Certificante. Una vez que el Certificado ha sido emitido, el Solicitante pasa a ser el Suscriptor. Para Certificados emitidos a dispositivos, el Solicitante es la entidad que controla u opera el dispositivo nominado en el Certificado, incluso si el propio dispositivo es el que envía la Solicitud de Certificado. En el contexto de una Solicitud de Certificado de Validación Extendida (EV), el Solicitante es la Organización Privada o Entidad Gubernamental que solicita o requiere la renovación de un Certificado de Validación Extendida (EV) nominando a dicha entidad como Sujeto del Certificado.
Solicitante Autorizado	Persona física que es empleado y ha sido autorizado por el Solicitante, o un agente autorizado, que ha expresado su autoridad para representar al Solicitante o un tercero (como un proveedor de servicios de Internet o prestador de servicios de hosteo) que completa y envía una Solicitud de Certificado de Validación Extendida (EV) en representación del Solicitante.
Solicitud de Certificado	Solicitud completada por un Solicitante del Certificado (o su representante autorizado), remitido a una Autoridad Certificante, requiriendo la emisión de un Certificado.
Solicitud de Firma de Certificado (Certificate Signing Request o CSR)	Mensaje que transmite una solicitud para que un Certificado sea emitido.
Subdominio	Porción de la Symantec Trust Network bajo el control de una entidad y todas las entidades subordinadas a ella dentro de la jerarquía de la Symantec Trust Network.
Subsidiaria	Una empresa subsidiaria es una compañía cuyo dueño o accionista mayoritario es el Solicitante, tal como puede verificarse en una Base de Datos Privada Calificada o a través de los correspondientes Estados Contables certificados por un Contador Público Matriculado o equivalente.
Sujeto	Individuo, dispositivo, sistema, unidad o entidad legal identificada en un Certificado como Sujeto del mismo y que es poseedor de una clave privada que se corresponde con una clave pública. El Sujeto es el Suscriptor o un dispositivo bajo el control u operación del Suscriptor. El término "Sujeto" puede referirse, en el caso de Certificados para organizaciones, al equipamiento o dispositivo que almacena la clave privada. A un Sujeto se le asigna un nombre no ambiguo, perfectamente

Término	*Definición*
	definido, que está vinculado con la clave pública contenida en el Certificado de ese Sujeto.
Suscriptor	En el caso de un Certificado para individuos, una persona que es el Sujeto de, y a la cual se la ha emitido un Certificado. En el caso de un Certificado para una organización, la organización dueña del equipamiento o dispositivo que es el Sujeto de, y al cual se le ha emitido un Certificado. Un Suscriptor es capaz de utilizar y está autorizado a emplear la clave privada que se corresponde con la clave pública incluida en el Certificado.
Symantec Trust Network (STN)	Infraestructura de Clave Pública, basada en Certificados, regulada por la Política de Certificación de DigiCert para la Symantec Trust Network.
Tercero Autorizado	Persona física o Entidad Legal que no es una Autoridad Certificante pero que está autorizado por la Autoridad Certificante para asistirla en el Proceso de Administración de Certificados, desarrollando o cumpliendo con alguno de los requerimientos para la Autoridad Certificante establecidos en las presentes Normas.
Token de Solicitud	Valor derivado de un método especificado por una Autoridad Certificante y que vincula la demostración del control de la Solicitud de Certificado. El Token de Solicitud incorpora la clave empleada en la Solicitud del Certificado. También puede incluir otra infomación para asegurar su unicidad. Un Token de Solicitud que incluye un sellado de tiempo es válido por un plazo no mayor a los treinta (30) días desde su generación. Un Token de Solicitud que incluye un sellado de tiempo es considerado inválido si ese sello de tiempo indica una fecha en el futuro. Un Token de Solicitud que no incluye un sellado de tiempo es válido para un uso solamente y DigiCert no reutilizará el mismo para una posterior validación. La vinculación utiliza un algoritmo de firma digital o un algoritmo criptográfico de hash que es, al menos, tan robusto como el utilizado para la firma de la solicitud de Certificado.
Validación Extendida (Extended Validation o EV)	Procedimientos de Validación definidos por los Requerimientos para los Certificados de Validación Extendida (EV) publicados por el Foro conformado por las autoridades certificantes y proveedores de navegadores.
Valor Aleatorio	Valor especificado por una Autoridad Certificante a un Solicitante de Certificado que supone, por lo menos, 112 bits de entropía.

Apéndice B1 - Algoritmos Criptográficos y Tamaño de Claves Mínimos para Certificados de Validación Extendida (EV)

1. Certificados de Autoridad Certificante Raíz

	Fortaleza mínima del algoritmo
Algoritmo de digesto	SHA-1 (*), SHA-256, SHA-384 o SHA-512
RSA	2048 bits
ECC	256 o 384 bits

2. Certificados de Autoridades Certificantes Subordinadas

	Fortaleza mínima del algoritmo
Algoritmo de digesto	SHA-1(*), SHA-256, SHA-384 o SHA-512
RSA	2048 bits
ECC	256 o 384 bits

3. Certificados de Suscriptores

	Fortaleza mínima del algoritmo
Algoritmo de digesto	SHA-1(*), SHA-256, SHA-384 o SHA-512
RSA	2048 bits
ECC	256 o 384 bits

(*) El algoritmo SHA-1 puede ser utilizado con claves RSA de acuerdo con los criterios definidos en la Sección 7.1.3 de los Requerimientos Básicos para la Emisión y Administración de Certificados de Confianza Pública del CA/Browser Forum.

Apéndice B2 - Extensiones de Certificado Requeridas para Certificados de Validación Extendida (EV)

1. Certificado de Autoridad Certificante Raíz

Los Certificados Raíz generados a partir de Octubre de 2006 deben ser Certificados X.509 v3.

(a) Restricciones básicas (*basicConstraints*)

Si el Certificados es v3 y ha sido creado a partir de Octubre de 2006, esta extensión deberá figurar como crítica en todos los Certificados de Autoridad Certificante que contengan Claves Públicas utilizadas para validar firmas digitales en los certificados. El campo Autoridad Certificante debe estar señalado como TRUE. El campo Restricción de Longitud de Cadena (*path.LenConstraint*) no debe estar presente.

(b) Uso de Claves (*keyUsage*)

Si el Certificados es v3 y ha sido creado a partir de Octubre de 2006, esta extensión debe estar presente y figurar como crítica. Las posiciones bit correspondientes a *CertSign* y *cRLSign* deben estar configuradas. Todas las demás posiciones Bit no deben estar configuradas.

(c) Políticas de Certificación (*certificatePolicies*)

Esta extensión no debe estar presente.

(d) Uso de Claves Extendido (*extendedKeyUsage*)

Esta extensión no debe estar presente.

Todos los demás campos y extensiones están configurados de acuerdo con el RFC 5280.

2. Certificado de Autoridad Certificante Subordinada

(a) Políticas de Certificación (*certificatePolicies*)

Esta extensión debe estar presente y no deberá estar marcada como crítica. La configuración de identificadores de política (*policy identifiers*) debe incluir la identificación de la Política de DigiCert para Validación Extendida (EV).

certificatePolicies:policyIdentifier (Requerido)

- El identificador ***anyPolicy***, si se trata de una Autoridad Certificante Subordinada, es controlado por DigiCert.

(b) Punto de Distribución de la Lista de Certificados Revocados (*cRLDistributionPoint*)

Esta extensión está siempre presente y no está marcada como crítica. Contiene la dirección URL del servicio de Lista de Certificados Revocados de DigiCert.

(c) Acceso a la Información de la Autoridad (*authorityInformationAccess*)

Esta extensión está presente y no debe estar marcada como crítica. Debe contener la dirección URL de la Autoridad Certificante Emisora del Respondedor del Servicio OCSP (*accesMethod=1.3.6.1.5.5.7.48.1*). El método de acceso a la URL para el certificado de DigiCert podría estar incluido (*accessMethod=1.3.6.1.5.5.7.48.2*).

(d) Restricciones Básicas (*basicConstraints*)

Esta extensión debe estar presente y debe estar marcada como crítica en todos los Certificados de Autoridad Certificante que contengan Claves Públicas utilizadas para validar firmas digitales en los certificados. El campo Autoridad Certificante debe estar señalado como TRUE. El campo Restricción de Longitud de Cadena (*path.LenConstraint*) puede estar presente.

(e) Uso de Claves (*keyUsage*)

Esta extensión debe estar presente y debe estar marcada como crítica. Las posiciones bit correspondientes a *CertSign* y *cRLSign* deben estar configuradas. Todas las demás posiciones Bit no deben estar configuradas.

Todos los demás campos y extensiones deben estar configurados de acuerdo con el RFC 5280.

3. Certificado de Suscriptor

(a) Políticas de Certificación (*certificatePolicies*)

Esta extensión debe estar presente y no deberá estar marcada como crítica.

certificatePolicies:policyIdentifier (Requerido)
- OID de la política para Validación Extendida.

certificatePolicies:policyQualifiers:policyQualifierId (Requerido)
- Id-qt 2 (RFC5280)

certificatePolicies:policyQualifiers.qualifier (Requerido)
- Dirección URL de las Normas para el Proceso de Certificación (CPS)

(b) Punto de Distribución de la Lista de Certificados Revocados (*cRLDistributionPoint*)

Esta extensión está siempre presente y no está marcada como crítica. Contiene la dirección URL del servicio de Lista de Certificados Revocados de DigiCert.

(c) Acceso a la Información de la Autoridad (*authorityInformationAccess*)

Esta extensión está siempre presente y no está marcada como crítica. Debe contener la dirección URL de la Autoridad Certificante Emisora del Respondedor del Servicio OCSP (*accesMethod=1.3.6.1.5.5.7.48.1*). El método de acceso a la URL para el certificado de DigiCert puede estar incluido (*accessMethod=1.3.6.1.5.5.7.48.2*).

(d) Restricciones Básicas (*basicConstraints*) – Opcional

Si esta extensión está presente, el campo Autoridad Certificante debe estar marcado como FALSE

(e) Uso de Claves (*keyUsage*)

Si esta extensión está presente, las posiciones bit correspondientes a *CertSign* y *cRLSign* no deben estar configuradas

(f) Uso de Claves Extendido (*extendedKeyUsage*)

El valor *id-kp-serverAuth* (RFC 5280) o *id-kp-clientAuth* (RFC 5280) o ambos valores deben estar presentes. Los demás valores no deben estar presentes.

(g) Nombre Alternativo del Sujeto (*subjectAltName*)

Distribuido con arreglo a lo establecido en el RFC 5280 y la criticidad configurada como FALSE.

Todos los demás campos y extensiones están configurados de acuerdo con el RFC 5280.

Apéndice B3 - Requerimientos sobre Nombres de Organizaciones Extranjeras

NOTA: *Este Apéndice es relevante solamente para las Solicitudes de Certificados de Validación Extendida en aquéllos países en donde los registros de los nombres de las organizaciones no cuenten con caracteres latinos. En el futuro, podrá agregarse a este Apéndice información más específica sobre determinados países en particular*.

En caso de que el nombre de una organización del Solicitante de un Certificado de Validación Extendida no esté registrado en caracteres latinos en una Base de Información Gubernamental Calificada y el nombre y registración de dicha organización en otros caracteres hayan sido verificados con una Base de Información Gubernamental Calificada con arreglo a estos Requerimientos, DigiCert podrá incluir en caracteres latinos el nombre de la organización en el Certificado de Validación Extendida. En ese caso, DigiCert procederá con arreglo a lo previsto en este Apéndice.

Nombres Latinizados

A los fines de incluir una transliteración del nombre registrado, la romanización será verificada por DigiCert utilizando un sistema oficialmente reconocido por el Gobierno del país en el que el Solicitante del Certificado se encuentra registrado.

En caso de que DigiCert no pueda confiar en el sistema reconocido oficialmente, deberán confiar en alguna de las opciones citadas a continuación, respetando el orden de preferencia:

- Un sistema reconocido por la Organización de Estándares Internacionales (International Standards Organization o ISO),
- Un sistema reconocido por las Organización de las Naciones Unidas, o
- Una Opinión Legal Profesional confirmando la romanización del nombre registrado.

Nombre en Idioma Inglés

A los fines de incluir en un Certificado de Validación Extendida un nombre en caracteres latinos que no sea una transliteración del nombre registrado, DigiCert verificará que dicho nombre:

- Esté incluido en el Estatuto de Constitución de la organización o documento equivalente, que fue presentado como parte de la documentación de registro o incorporación de dicha organización, o
- Sea reconocido por una Fuente de Información Fiscal Gubernamental Calificada como el nombre del Solicitante, a los efectos de la presentación de las declaraciones impositivas, o
- Pueda ser confirmado con una Fuente de Información Independiente Calificada, como el nombre asociado con el registro o incorporación del Solicitante, o
- Sea confirmado mediante una Carta de Opinión Legal Profesional como el nombre comercial de la organización Solicitante del Certificado.