SERVICIOS DE CONFIANZA DE CERTISUR S.A.

NORMAS PARA EL PROCESO DE CERTIFICACIÓN

Versión 1.0

Vigencia: 30 de Marzo de 2014

Av. Santa Fe 788, 2° Piso (C1059ABO) Buenos Aires, República Argentina

Teléfono (+54 11) 4311 2457

www.certisur.com

Notificación de Derechos de Propiedad Intelectual. Marcas Registradas

CertiSur es marca registrada propiedad de CertiSur S.A. El logotipo de CertiSur es marca registrada 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 CertiSur S.A.

Sin perjuicio de lo mencionado, se otorga el permiso de reproducir y distribuir estas Normas para el Proceso de Certificación para los Servicios de Confianza 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 CertiSur S.A.

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) Ciudad Autónoma de Buenos Aires, Argentina, Teléfono (54 11) 4311 2457, Fax (54 11) 4311 1450, Correo Electrónico: legal@certisur.com.

Tabla de contenido

1 Introducción

Este documento constituye las Normas para el Proceso de Certificación para los Servicios de Confianza de CertiSur S.A. ("CPS").[1] Establece los procedimientos que la Autoridad de Certificación de CertiSur S.A. ("CA") y sus Autoridades de Registro ("RA") emplean para suministrar los servicios de certificación que incluyen, pero no se limitan, a la emisión, administración, revocación y renovación de certificados.

Específicamente, estas Normas para el Proceso de Certificación establecen los procedimientos que CertiSur S.A. emplea dentro de los Servicios de Confianza de CertiSur para:

- administrar de manera segura la infraestructura que soporta la actividad de sus Autoridades Certificantes y de sus Autoridades de Registro y
- emitir, administrar, revocar y renovar los Certificados bajo dichas Autoridades Certificantes

Estas Normas no incluyen otros servicios que CertiSur S.A. puede brindar dentro del territorio de la República Argentina o de otros países de América del Sur, por ejemplo los Servicios de Certificación bajo la Symantec Trust Network, los cuales están regulados por otras Normas. [2]

1.1 Resumen

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

- Autoridades Certificantes de CertiSur S.A. y sus Autoridades de Registro, que emiten Certificados dentro de los Servicios de Confianza de CertiSur.
- Autoridades Certificantes de Infraestructura de CertiSur y Autoridades Certificantes de Administración de CertiSur, en el marco de los Servicios de Confianza de CertiSur S.A.

CertiSur S.A. ofrece dos clases diferentes de Certificados para individuos: a) para generar firmas electrónicas o con propósitos de autenticación, y b) para hacer uso de la infraestructura de la red de confianza de CertiSur. Estas Normas describen de qué forma CertiSur S.A. y las Autoridades de Registro de sus Servicios de Confianza cumple con las normas de validación aplicables y cubren, en un único documento, las normas y procedimientos concernientes a la emisión y administración de los certificados.

---

[1] Las referencias internas a secciones de estas Normas son alusiones a secciones de este mismo documento. Otras referencias pueden vincularse con Normas para el Proceso de Certificación que pueden incluir a este documento o a otras Normas similares, por ejemplo de otras Autoridades Certificantes. *Ver* el Capítulo Definiciones.

[2] En su carácter de Partner de Symantec e integrante de la Symantec Trust Network, CertiSur S.A. brinda servicios de certificación que se hallan regulados por las Normas para el Proceso de Certificación de CertiSur S.A. para los Servicios de Certificación bajo la Symantec Trust Network. Estas Normas pueden consultarse en https://www.certisur.com/repositorio/CPS/ y los servicios allí incluidos no guardan relación alguna con las prestaciones efectuadas bajo los Servicios de Confianza de CertiSur S.A.

(a) Rol de las Normas para el Proceso de Certificación para los Servicios de Confianza de CertiSur S.A. y otros documentos legales.

Estas Normas detallan los aspectos específicos de implementación de los Servicios de Confianza de CertiSur S.A. en relación a la tecnología de Infraestructura de Clave Pública o PKI, como habitualmente se la denomina por sus siglas en idioma inglés ("Public Key Infrastructure"). Más específicamente, las Normas para el Proceso de Certificación describen, entre otras cosas:

- Obligaciones de la Autoridad Certificante, de las Autoridades de Registro, de los Suscriptores y de las Partes Confiadas.
- Asuntos legales que están cubiertos por los Acuerdos del Suscriptor y los Acuerdos del Receptor Confiado.
- Auditorías y revisiones relacionadas con seguridad y normas que deben llevarse a cabo, por parte de CertiSur como de los demás participantes de los Servicios de Confianza de CertiSur S.A.
- Métodos empleados por CertiSur S.A. y sus Autoridades de Registro para confirmar la identidad de los Solicitantes de Certificados.
- Procedimientos operativos llevados a cabo relacionados con el ciclo de vida de los Certificados: solicitud, emisión, aceptación, revocación y renovación.
- Procedimientos operativos de seguridad para llevar registros de auditoría, archivo de documentación y recupero ante desastres empleados por CertiSur S.A.
- Normas en materia de seguridad física, personal, administración de claves y seguridad lógica.
- Contenido de los Certificados y de las Listas de Certificados Revocados, y
- Administración de estas Normas del Proceso de Certificación, incluyendo los métodos para su modificación.

CertiSur S.A. puede publicar políticas de certificación suplementarias a las contenidas en estas Normas para el Proceso de Certificación, como consecuencia de exigencias de estándares de la industria para una aplicación en particular o a efectos de cumplimentar requerimientos específicos.

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 de los Servicios de Confianza de CertiSur S.A. Los demás documentos incluyen:

- Documentos auxiliares relacionados con seguridad y operaciones, que complementan las Normas para el Proceso de Certificación, suministrando mayor grado de detalle en los requerimientos, como por ejemplo:
  - Política de Seguridad de CertiSur S.A., que establece los principios de seguridad que regulan la infraestructura de los Servicios de Confianza.
  - Guía de Requerimientos en materia de Seguridad y Auditoría, que describe detalladamente los requerimientos de CertiSur S.A. concernientes a personal, instalaciones físicas, telecomunicaciones, seguridad lógica y seguridad en la administración de claves criptográficas, y

- Guía de la Ceremonia de Generación de Claves, que describe detalladamente los requerimientos operacionales en materia de administración de claves.

- Acuerdos complementarios establecidos por CertiSur S.A. Estos acuerdos vinculan legalmente a Clientes, Suscriptores y Partes Confiadas de CertiSur S.A. Entre otras cosas, estos acuerdos transmiten los Requerimientos para dichos participantes de estas Normas y, en algunos casos, establecen normas específicas respecto de cómo deben cumplir dichos Requerimientos.

En algunas oportunidades, las Normas para el Proceso de Certificación se refieren a estos documentos para normas específicas y detalles de implementación de los Servicios de Confianza, dado que incluir dichas especificaciones dentro de las Normas podría comprometer la seguridad de dichos Servicios.

La Tabla 1 es una matriz que muestra varios documentos aplicables a los Servicios de Confianza, indicando si los mismos se encuentran disponibles públicamente y, en su caso, su ubicación. La lista de la Tabla 1 no pretende ser exhaustiva. Obsérvese que los documentos en donde se expresan que no están disponibles públicamente son confidenciales a efectos de preservar la seguridad de los servicios brindados.

Documentos	Estado	Ubicación Pública
Normas para el Proceso de Certificación de para los Servicios de Confianza de CertiSur S.A.	Público	Repositorio CertiSur según la Sección 2 de estas Normas. Ver https://www.certisur.com/legal/CPS
Acuerdos complementarios de CertiSur S.A. (Acuerdo del Suscriptor y Acuerdo del Receptor Confiado)	Público	Repositorio CertiSur según la Sección 2 de estas Normas. Ver https://www.certisur.com/legal
Política de Seguridad de CertiSur S.A.	Confidencial	No disponible
Guía de Requerimientos en material de Seguridad y Auditoría	Confidencial	No disponible
Guía de la Ceremonia de Generación de Claves	Confidencial	No disponible

Tabla 1 – Disponibilidad de Documentos legales

(b) Conocimiento respecto de Certificados Digitales de parte de los Participantes de los Servicios de Confianza

Estas Normas asumen que el lector está familiarizado genéricamente con Firmas Digitales, Infraestructuras de Clave Pública (PKI) y tecnologías relacionadas. Si no fuera el caso, CertiSur S.A. recomienda que el lector se capacite en la utilización de criptografía de clave pública e infraestructuras de clave pública, tal como están implementadas por CertiSur S.A. CertiSur S.A. pone a disposición material de lectura general e información de capacitación en **https://www.certisur.com**.

(c) Cumplimiento de los Estándares Aplicables

Los procedimientos establecidos en estas Normas han sido desarrollados para cumplir los requerimientos de los estándares generalmente aceptados y desarrollados por la industria, incluyendo el Programa Web Trust para Autoridades Certificantes de AICPA/CICA, Reseña de Normas y Políticas de una Infraestructura de Clave Pública ANS X9.79:2001 y otros estándares de la industria relacionados con la operación de Autoridades Certificantes.

La estructura de estas Normas se corresponde genéricamente con el documento denominado *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, conocido como RFC 3647 de la Internet Engineering Task Force (IETF), organismo que se ocupa de los estándares de Internet. El documento RFC 3647 se ha transformado en un estándar dentro de la industria de PKI. Estas Normas se ajustan al marco de referencia establecido por el RFC 3647, a efectos de facilitar el análisis de la política, comparaciones, evaluaciones y la interoperabilidad con personas que están utilizando o considerando utilizar los Servicios de Confianza de CertiSur S.A..

CertiSur S.A. ha delineado estas Normas con arreglo a la estructura del RFC 3647, en la medida en que ha resultado posible, aunque pueden observarse pequeñas variaciones en los títulos y detalles. Si bien CertiSur S.A. tiene la intención de mantener la política de adhesión al RFC 3647 en el futuro, se reserva el derecho de apartarse de la estructura del RFC 3647 si resultara necesario, por ejemplo para mejorar la calidad de estas Normas. Incluso, la estructura de las Normas para el Proceso de Certificación puede no corresponderse con futuras versiones del RFC 3647.

1.1.1 Resumen de la Política

CertiSur S.A. emite dos clases diferentes de certificados: para individuos: a) para generar firmas electrónicas o con propósitos de autenticación; y b) para hacer uso de la infraestructura de la red de confianza de CertiSur. Esta diferenciación no implica distinción en el nivel de confianza asignado a cada clase de certificado, como es común observar en otros Servicios de Certificación. Simplemente cada tipo de Certificado suministra una funcionalidad específica para ser empleado en el marco de la aplicación correspondiente.

1.2 Identificación del documento

Este documento constituye las Normas para el Proceso de Certificación para los Servicios de Confianza de CertiSur S.A. 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 de estas Normas.

Las presentes Normas son publicadas en forma electrónica dentro del Repositorio de CertiSur S.A. localizado en **https://www.certisur.com/legal/CPS**. Las Normas están disponibles en formato HTML.

1.3 Participantes de la Infraestructura de Clave Pública

1.3.1 Autoridades Certificantes

El término Autoridad Certificante es un término genérico que se refiere a todas aquellas entidades que emiten Certificados dentro de la infraestructura de los Servicios de Confianza de CertiSur. El término Autoridad Certificante incluye una subcategoría de emisores denominados Autoridades Primarias de Certificación. Las Autoridades Primarias de Certificación actúan como raíces de diferentes dominios, según la estructura de la jerarquía de los Servicios de Confianza de CertiSur. Subordinadas a las Autoridades Primarias de Certificación se encuentran las Autoridades Certificantes que emiten Certificados para Suscriptores usuarios finales u otras Autoridades Certificantes.

Las Autoridades Certificantes de CertiSur S.A. desarrollan todas las funciones de las Autoridades Certificantes, incluyendo en algunos casos las funciones de las Autoridades de Registro.

1.3.2 Autoridades de Registro

Las Autoridades de Registro asisten a las Autoridades Certificantes desarrollando las funciones visibles de confirmación de identidad, aprobación o rechazo de Solicitudes de Certificado, requerimiento de la revocación de Certificados y la aprobación o rechazo de solicitudes de renovación.

CertiSur S.A. autoriza, mediando acuerdo previo por escrito, a las Autoridades de Registro dentro de los Servicios de Confianza y sujeto a las obligaciones impuestas por estas Normas y los documentos complementarios.

1.3.3 Suscriptores

Los Suscriptores son individuos que envían una Solicitud de Certificado a CertiSur o a una Autoridad de Registro autorizada por CertiSur. Antes de solicitar, aceptar o utilizar un Certificado Digital bajo los Servicios de Confianza de CertiSur, el Suscriptor debe leer y aceptar el correspondiente Acuerdo del Suscriptor que lo obliga al cumplimiento de las presentes Normas, en tal carácter.

Los Suscriptores pueden ser individuos que van a utilizar los Certificados Digitales con propósitos de autenticación o para generar firmas electrónicas. Asimismo, en algunos casos, los Suscriptores pueden ser individuos que operen como administradores dentro de la Infraestructura de los Servicios de Confianza de CertiSur, ya sea que hayan sido autorizados por CertiSur S.A. para desarrollar esa tarea o por las Autoridades de Registro debidamente designadas por CertiSur.

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 en estas Normas se aplican solamente a Suscriptores usuarios finales.

1.3.4 Partes Confiadas

Una parte confiada es un individuo que, sin estar vinculado directamente con los Servicios de Confianza de CertiSur, desea confiar en un Certificado Digital o en una firma electrónica generada mediante la clave privada asociada a un Certificado Digital emitido bajo los Servicios de Confianza de CertiSur. Antes de validar un Certificado Digital o una firma electrónica generada por un Certificado Digital emitido bajo los Servicios de Confianza de CertiSur, una Receptor Confiado debe leer y aceptar el Acuerdo del Receptor Confiado que lo obliga al cumplimiento de las presentes Normas, en tal carácter.

Un Receptor Confiado no puede utilizar los Servicios del Protocolo del Estado del Certificado en Línea, consultar la Lista de Certificados Revocados o de cualquier forma acceder o utilizar la base de datos de Certificados de los Servicios de Confianza de CertiSur si no está de acuerdo y no acepta los términos del Acuerdo del Receptor Confiado correspondiente.

1.3.5 Otros Participantes

No aplicable

1.4 Uso de los certificados

Estas Normas se aplican a todos los Participantes de los Servicios de Confianza de CertiSur, incluyendo a CertiSur S.A., Clientes, Revendedores, Suscriptores y Partes Confiadas y describen los procedimientos que regulan la emisión y el uso de los Certificados. Los Certificados resultan apropiados, en términos generales, para su utilización en las aplicaciones descriptas en la Sección 1.1.1 de estas Normas. En caso de que cualquiera de los Participantes de los Servicios de Confianza de CertiSur utilizara los Certificados con otros propósitos, será responsable, de manera exclusiva y excluyente, por cualquier daño o responsabilidad emergente por tal utilización.

1.4.1 Usos permitidos

Tal como se indica en la Sección 1.1.1 de estas Normas, los Certificados emitidos con arreglo a las presentes normas se pueden utilizar: a) para generar firmas electrónicas o con propósitos de autenticación, y b) para hacer uso de la infraestructura de los Servicios de Confianza de CertiSur. Esa enumeración, sin embargo, no pretende ser limitativa. Los Certificados para individuos permiten que las Partes Confiadas verifiquen firmas digitales y/o electrónicas. Los Participantes toman conocimiento y acuerdan, con el alcance permitido por la ley aplicable, que cuando se requiere que una transacción sea formalizada por escrito, un mensaje o cualquier otro registro que cuente con una firma digital verificable con referencia a un Certificado emitido bajo los Servicios de Confianza de CertiSur, es válido, efectivo y vinculante con un alcance no menor al que tiene el mismo mensaje o registro efectuado por escrito y firmado en papel. Sujeto a la legislación que resulte aplicable, una firma electrónica o transacción formalizada con referencia a un Certificado emitido bajo los Servicios de Confianza de CertiSur será válida.

CertiSur S.A. periódicamente reemite las claves de las Autoridades Certificantes Intermedias. Las aplicaciones de terceros o plataformas que tienen Autoridades Certificantes Intermedias embebidas como certificados raíz pueden no operar de la manera prevista después que se haya reemitido el par de claves de una Autoridad Certificante Intermedia determinada. Por lo tanto, CertiSur S.A. no garantiza la utilización de Autoridades Certificantes Intermedias como certificados raíz y recomienda que las mismas no sean embebidas en aplicaciones o plataformas como certificados raíz. CertiSur S.A. recomienda que se utilicen como certificados raíz los correspondientes a las Autoridades Primarias de Certificación.

1.4.2 Usos prohibidos

La utilización de los Certificados emitidos bajo los Servicios de Confianza de CertiSur S.A. no está específicamente restringida a un entorno de negocios en particular, tal como pruebas, servicios financieros, mercados verticales o mercados virtuales. Sin embargo, tal utilización está permitida y los Clientes que usan Certificados para sus propias aplicaciones dentro de su propio ámbito, pueden sufrir restricciones adicionales específicas en el uso de los Certificados dentro de dichos ámbitos. CertiSur S.A. y otros Participantes no son responsables por el control o la implementación de dichas restricciones en esos ámbitos.

Sin perjuicio de lo expresado, algunos Certificados poseen una funcionalidad limitada. Por ejemplo, los Certificados de Autoridad Certificante no pueden ser utilizados para otras funciones que no sean las propias de una Autoridad Certificante. Además, los Certificados en modo cliente están orientados hacia aplicaciones en modo cliente y no pueden ser utilizados como Certificados para organizaciones o Certificados para servidor. Los Certificados de Administrador pueden ser utilizados solamente para desarrollar funciones de Administrador.

Asimismo, con respecto a los Certificados X.509 Versión 3, la extensión de uso de clave (key usage extension) está definida para limitar los objetivos técnicos para los cuales la clave privada que se corresponde con la clave pública incluida en un Certificado puede ser utilizada, según lo establecido en la Sección 7.1.2.5 de estas Normas. Adicionalmente, los Certificados para Suscriptores usuarios finales no pueden ser empleados como Certificados de Autoridad Certificante. Esta restricción se evidencia en la extensión Restricciones Básicas (Basic Constraints extension) del certificado, según lo establecido en la Sección 7.1.2.4 de estas Normas. No obstante, la efectividad de las limitaciones basadas en las extensiones está sujeta a la operación de software desarrollado o controlado por otras entidades, distintas y ajenas a CertiSur S.A.

Más genéricamente, los Certificados sólo pueden ser utilizados con el alcance que resulte consistente con la ley aplicable.

Los Certificados emitidos bajo los Servicios de Confianza de 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.

1.5 Administración de las Regulaciones

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

Las consultas acerca de las presentes Normas deben dirigirse a la dirección de correo electrónico legal@certisur.com o a los siguientes contactos:

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

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

La organización identificada en la Sección 1.5.1 de estas Normas es la responsable de determinar si las mismas y otros documentos de la naturaleza de normas de procedimientos de certificación que complementan o están subordinadas a estas Normas, están en concordancia con la política de Certificación y estas Normas.

1.5.4 Procedimientos de Aprobación de las Normas

Las presentes Normas han sido desarrolladas y aprobadas por CertiSur S.A. Sin una periodicidad previamente establecida, las mismas son actualizadas, con arreglo a los procedimientos establecidos en la Sección 9.10 de las presentes Normas.

1.6 Definiciones y Acrónimos

Tabla de Acrónimos

Acrónimo	Término
AC	Autoridad Certificante.
ANSI	Instituto Americano de Estándares (American National Standards Institute).
APC	Autoridad Primaria de Certificación.
AR	Autoridad de Registro.
CPS	Normas para el Proceso de Certificación (Certification Practice Statement).
CRL	Lista de Certificados Revocados (Certificate Revocation List).
EAL	Nivel de evaluación de seguridad (Evaluation assurance level), con arreglo a lo establecido por la Organización Common Criteria.
FIPS	United State Federal Information Processing Standards.
IEC	International Electrotechnical Commission.
ISO	International Standard Organisation.
OCSP	Protocolo de Estado del Certificado en Línea (Online Certificate Status Protocol).
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).
RFC	Request for comment.
S/MIME	Secure multipurpose Internet mail extensions.
SAS	Normas Estándar de Auditoría (Statement on Auditing Standards) del American Institute of Certified Public Accountants.
SSL	Secure Sockets Layer.

Definiciones

Término	Definición
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	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.

RPA)	
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 Suscriptores.
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 firmó un Acuerdo específico con CertiSur S.A. y desarrolla tareas de validación y otras funciones de Autoridad de Registro.
Auditoría de Cumplimiento	Revisión periódica que realiza un Participante de los Servicios de Confianza de CertiSur para determinar su conformidad con los Requerimientos que le resulten aplicables.
Auditoría Investigativa/ Investigación	Auditoría o investigación llevada a cabo por CertiSur S.A, debido a que tiene razones para suponer que una entidad ha incumplido los Requerimientos o ha ocurrido un incidente o Compromiso relacionado con esa entidad o una amenaza real o potencial para la seguridad de los Servicios de Confianza de CertiSur en virtud del comportamiento de dicha entidad o de terceros.
Autenticación Manual	Procedimiento mediante el cual un Administrador revisa y aprueba, una por una, las Solicitudes de Certificado.
Autoridad Certificante (Certification Authority o CA)	Entidad autorizada para emitir, administrar, revocar y renovar Certificados.
Autoridad Certificante de Infraestructura (Infrastructure CA)	Tipo de Autoridad Certificante que emite Certificados para componentes de la infraestructura de los Servicios de Confianza de CertiSur. Las autoridades Certificantes de Infraestructura no emiten Certificados para Autoridades Certificantes, Autoridades de Registro o para usuarios finales que no sean Administradores.
Autoridad Certificante de la Autoridad de Time-Stamping	Autoridad Certificante que emite un Certificado especial para la Autoridad de Time-Stamping.
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 de Administración de la Política (Policy Management Authority o PMA)	Organización responsable, dentro de la estructura de los Servicios de Confianza de CertiSur S.A., de promulgar y actualizar estas Normas.
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 Time-Stamping	Organización o entidad responsable que firma un Documento Electrónico atestando la existencia de dicho documento en determinada fecha y hora.
Autoridad Primaria de Certificación (Primary Certification Authority o PCA)	Organización responsable que actúa como Autoridad Certificante raíz y emite los Certificados de las Autoridades Certificantes subordinadas a ella.
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.
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 de Administrador	Certificado emitido a un Administrador que puede ser utilizado solamente para desarrollar funciones de Autoridad Certificante o de Autoridad de Registro.
Cliente	Organización que desempeña la función de Autoridad de Registro dentro de los Servicios de Confianza de CertiSur, bajo un acuerdo específico que lo obliga bajo los términos de las presentes Normas.
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.
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.
FALSE	Valor utilizado en las extensiones de los Certificados, tal como está definido en los correspondientes estándares tecnológicos.
Frase de Comprobación	Párrafo secreto elegido por el Solicitante del Certificado, por ejemplo 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 utilizar, revocar o renovar su Certificado.
Guía de la Ceremonia de Generación de	Documento que describe los requerimientos y procedimientos aplicables a la Ceremonia de Generación de Claves.

Claves	
Guía de Requerimientos en materia de Seguridad y Auditoría	Documento que establece los requerimientos y normas en materia de seguridad y auditoría.
Individuo Vinculado	Persona vinculada a una organización determinada (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 S.A., 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 9.4.7 de estas Normas.
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 ha 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 bajo su exclusiva responsabilidad.
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. Los Servicios de Confianza de CertiSur constituyen una Infraestructura de Clave Pública compuesta por sistemas que de manera concurrente proveen e implementan los servicios ofrecidos dentro de un marco de seguridad y confiabilidad.
Lista de Certificados Revocados (Certificate Revocation List o CRL)	Lista emitida periódicamente y también por demanda, firmada digitalmente por una Autoridad Certificante, que identifica a los Certificados que han sido revocados con anterioridad a sus respectivas fechas de vencimiento. 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.
No repudio	Atributo de una comunicación, que provee protección contra una parte que niega falsamente el origen de una comunicación, niega que la misma fuera 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.
Normas para el Proceso de Certificación (Certification Practice Statement o CPS)	Disposiciones vinculantes para las partes acerca de los procedimientos empleados para aprobar o rechazar Solicitudes de Certificados y para emitir, administrar y revocar Certificados. En el contexto de estas Normas, la sigla "CPS" se refiere a este documento.

Objetivos de Control de la Administración de Certificados	Criterio que una Autoridad Certificante o una Autoridad de Registro debe cumplir para satisfacer una Auditoría de Cumplimiento.
Parte Confiada	Individuo u organización que actúa basándose en la confianza en un Certificado y/o en una firma digital o electrónica.
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 de estas Normas.
Participante	Individuo u organización que desempeña una o más funciones de las enumeradas a continuación, dentro de los Servicios de Confianza de CertiSur: CertiSur S.A., un Cliente, un Revendedor, un Suscriptor o una Parte Confiada.
Período de Vigencia	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 los servicios de Confianza de CertiSur, 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 de estas Normas.
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.
Política de Seguridad	Documento de máximo nivel que describe la política en materia de seguridad dentro de los Servicios de Confianza de CertiSur.
Posición de Confianza	Función dentro de una organización participante de los Servicios de Confianza de CertiSur que debe ser ocupada por una Persona Confiable.
Protocolo del Estado del Certificado en Línea (Online Certificate Status Protocol u OCSP)	Registro que suministra a Partes Confiadas la información en tiempo real acerca del estado de un Certificado.
Recibo Digital	Constancia de afirmaciones, firmada electrónicamente, respecto de la existencia, en un momento determinado, de un documento en particular o de una serie de datos, que incluye el hash del documento o de la serie de datos y un sello de tiempo (time-stamp) demostrando que el documento o los datos existían en determinado momento.

Repositorio	Base de datos de Certificados y otros datos relevantes de los Servicios de Confianza de CertiSur que son accesibles en línea.
Requerimientos Estándar	Exigencias en materia legal, técnica y de negocios, para emitir, administrar, revocar, renovar y utilizar Certificados dentro de los Servicios de Confianza de CertiSur.
Revisión Complementaria de Administración del Riesgo	Control de una entidad, por parte de CertiSur S.A., 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.
RSA	Sistema criptográfico de clave pública inventado por Rivest, Shamir y Adleman.
Secreto Particionado	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 Partición de Secreto.
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).
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.
Software del Módulo de Administración Automática	Software provisto por CertiSur S.A. que ejecuta la Administración Automática.
Solicitante del Certificado	Individuo u organización que requiere la emisión de un Certificado por parte de una Autoridad Certificante.
Solicitud de Certificado	Conjunto de datos completados por un Solicitante del Certificado (o su representante autorizado), remitido a una Autoridad Certificante, requiriendo la emisión de un Certificado.
Solicitud de Firma de un Certificado (Certificate Signing Request o CSR)	Mensaje que transmite una solicitud para que un Certificado sea emitido.
Sujeto	Poseedor de una clave privada que se corresponde con una clave pública. A un Sujeto se le asigna un nombre no ambiguo, perfectamente definido, que está vinculado con la clave pública contenida en el Certificado del Sujeto.
Suscriptor	Persona que es el Sujeto de, y a la cual se la 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.
TRUE	Valor utilizado en las extensiones de los Certificados, tal como está definido en los correspondientes estándares tecnológicos

2 Publicación y Repositorio

2.1 Repositorio

CertiSur S.A. es responsable por las funciones del Repositorio para las Autoridades Certificantes de los Servicios de Confianza de CertiSur. CertiSur S.A. publica los Certificados que emite en el repositorio, en un todo de acuerdo con la Sección 2.2 de estas Normas.

Después de la revocación de un Certificado de Suscriptor usuario final, CertiSur S.A. publica la información de dicha revocación en el repositorio. CertiSur S.A. emite Listas de Certificados Revocados (CRL) para sus Autoridades Certificantes, con arreglo a lo establecido en la Sección 4.9.7 de estas Normas. Adicionalmente, para los Clientes que han contratado los servicios de Protocolo del Estado del Certificado en Línea ("Online Certificate Status Protocol u OCSP"), CertiSur S.A. proveerá dichos servicios en un todo de acuerdo con lo establecido en la Sección 4.9.9 de estas Normas.

2.2 Publicación de la Información de los Certificados

CertiSur S.A. es responsable por la función del repositorio con respecto a:

- Autoridades Primarias de Certificación
- Autoridades Certificantes de Infraestructura y Administrativas que soportan los Servicios de Confianza de CertiSur, y
- Autoridades Certificantes CertiSur que emiten Certificados dentro de los Servicios de Confianza de CertiSur.

CertiSur S.A. publica cierta información de Autoridad Certificante en la sección repositorio de su sitio web en **https://www.certisur.com/legal**, tal como se describe más abajo.

CertiSur S.A. publica en la sección repositorio de su sitio web, estas Normas para el Proceso de Certificación, los Acuerdos del Suscriptor y los Acuerdos del Receptor Confiado.

CertiSur S.A. publica Certificados, con arreglo a la Tabla 2 que aparece a continuación:

Tipos de Certificado	*Requerimientos de Publicación*
Certificados de Autoridades Primarias de Certificación, Autoridades Certificantes Raíz o de Autoridad Certificante, emitidos por CertiSur	Disponibles para Partes Confiadas como parte de una Cadena de Certificación que puede ser obtenida con el Certificado del Suscriptor usuario final, a través de las funciones de consulta descriptas más abajo.
Certificados de Respuesta de OCSP	Disponible a través de la consulta en el servidor de directorio LDAP de CertiSur S.A. en https://www.certisur.com/legal, siempre que el Cliente haya contratado dichos servicios con CertiSur S.A..
Certificados de Suscriptores usuarios finales	Disponible para Partes Confiadas a través de las funciones de consulta en el repositorio CertiSur en: https://www.certisur.com/legal

Certificados de Suscriptores usuarios finales, emitidos por pedido de Clientes bajo convenios especiales	Disponible a través de las funciones de consultas mencionadas más arriba, aunque a exclusiva discreción del Cliente, el Certificado puede estar accesible solamente a través del empleo del número de serie del Certificado.

Tabla 2 – Requerimientos de Publicación de Certificados

CertiSur S.A. publica la información respecto del estado de los Certificados de acuerdo con lo establecido en las Secciones 4.9.6 y 4.9.7 de estas Normas.

2.3 Frecuencia de la Publicación

Las actualizaciones de las presentes Normas para el Proceso de Certificación son publicadas de acuerdo con lo establecido en la sección 9.10 de las presentes Normas Las actualizaciones de los Acuerdos del Suscriptor y de los Acuerdos del Receptor Confiado son publicadas cuando resulte necesario. Los Certificados son publicados al emitirlos. La información respecto del estado del Certificado es publicada de acuerdo con lo previsto en las Secciones 4.9.6 y 4.9.7 de estas Normas.

2.4 Controles de Acceso al Repositorio

La información publicada en la sección repositorio del sitio web de CertiSur S.A. es información accesible para el público. La posibilidad de "solo lectura" con respecto a dicha información es irrestricta. CertiSur S.A. requiere que las personas presten su conformidad al Acuerdo del Receptor Confiado, como condición para acceder a información de Certificados, del estado de Certificados o de la Lista de Certificados Revocados. CertiSur S.A. ha implementado medidas de seguridad lógicas y físicas para impedir que personas no autorizadas puedan agregar, borrar o modificar datos del repositorio.

3 Identificación y Autenticación

3.1 Nombres

3.1.1 Tipos de Nombres

Los Certificados de la Autoridad Certificante de CertiSur S.A. contienen Nombres Distintivos (Distinguished Names) X.501 en los campos Emisor (Issuer) y Sujeto (Subject). Los Nombres Distintivos (Distinguished Names) de la Autoridad Certificante de CertiSur S.A. están conformados por los componentes especificados en la Tabla 3 a continuación.

Atributo	*Valor*
País - Country (C) =	"AR" o similar o no utilizado.
Organización - Organization (O) =	CertiSur S.A.
Unidad Organizacional - Organizational Unit (OU) =	Los Certificados de las Autoridades Certificantes de CertiSur S.A. pueden contener múltiples atributos en el campo OU. Dichos atributos pueden contener uno o más de lo siguiente: • Nombre de la Autoridad Certificante • Una declaración con referencia al Acuerdo del Receptor Confiado aplicable y que determina los términos de utilización del Certificado, y • Una notificación de copyright.
Estado o Provincia - State or Province (S) =	No utilizado.
Localidad - Locality (L) =	No utilizado
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 Autoridad Certificante

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

Atributo	*Valor*
País - Country (C) =	"AR" o similar o no utilizado.
Organización -	El atributo Organización ("Organization") es utilizado de la siguiente

Organization (O) =	forma: • "CertiSur S.A." para los Certificados de respuesta del OCSP de CertiSur S.A. y opcionalmente para Certificados para individuos que no estén vinculados a una organización. • Nombre del Suscriptor en el caso de Certificados para individuos que estén vinculados a una organización.
Unidad Organizacional - Organizational Unit (OU) =	Los Certificados para Suscriptores usuarios finales de CertiSur S.A. pueden contener múltiples atributos en el campo OU. Dichos atributos pueden contener uno o más de lo siguiente: • Unidad de negocios del Suscriptor en el caso de Certificados para individuos que estén vinculados a una organización • Una declaración con referencia al Acuerdo del Receptor Confiado aplicable y que determina los términos de utilización del Certificado, y • Una notificación de copyright. • Texto para describir el uso del Certificado.
Estado o Provincia - State or Province (S) =	Si se utiliza, indica el Estado o Provincia del Suscriptor.
Localidad - Locality (L) =	Si se utiliza, indica la Localidad del Suscriptor.
Nombre Común - Common Name (CN) =	Este atributo incluye: • El Nombre del Contestador de OCSP (para los Certificados de respuesta de OCSP) • Nombre (para Certificados para individuos).
Dirección de correo electrónico - E-Mail Address (E) =	Dirección de correo electrónico

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 verificado. El 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.

3.1.2 Necesidad que los Nombres tengan Significado

Los Certificados para Suscriptores usuarios finales contienen nombres con semántica generalmente entendible, que permiten determinar razonablemente la identidad del individuo que es Sujeto del Certificado. Para dichos Certificados, no están permitidos los seudónimos de los Suscriptores usuarios finales (es decir nombres que no sean el verdadero nombre personal del Suscriptor).

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

3.1.3 Uso de Pseudónimos o Anonimato de Suscriptores

No permitido

3.1.4 Reglas para la Interpretación de Variadas Formas de Nombres

No contempladas.

3.1.5 Unicidad de Nombres

CertiSur S.A. asegura 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 S.A., 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 S.A. 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

CertiSur S.A. verifica la posesión, por parte del Solicitante del Certificado, de una clave privada, a través del uso de un requerimiento de firma de certificado según lo establecido en el estándar PKCS #10, cualquier otra demostración criptográficamente equivalente u otro método aprobado por CertiSur S.A.

3.2.2 Autenticación de la Identidad de la Organización

En ciertos casos, el Certificado puede contener el nombre de una organización con la cual el Suscriptor usuario final está relacionado. CertiSur S.A. confirma la identidad de los Suscriptores usuarios finales de Certificados y otra información contenida en la solicitud suministrada por Solicitantes de Certificados (excepto para Información No Verificada del Suscriptor) con arreglo a los procedimientos establecidos en las siguientes secciones. Adicionalmente a los procedimientos descriptos más abajo, CertiSur S.A. o una Autoridad de Registro pueden requerir que el Solicitante del Certificado demuestre que es poseedor legítimo de la clave privada que se corresponde con la clave pública que será incluida en el Certificado, de acuerdo con lo establecido en la Sección 3.2.1 de estas Normas.

Adicionalmente, la organización que figura en el Certificado y con la cual el Suscriptor usuario final está relacionado, puede ser la Autoridad de Registro que intervino en el proceso de emisión de dicho Certificado. En ese caso, la organización suscribió un acuerdo específico con CertiSur, según lo previsto en la Sección 1.3.2 de estas Normas.

CertiSur S.A., en caso que el certificado contenga el nombre de una organización, confirma la identidad de la misma según el siguiente procedimiento:

- Verificación 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 autoridad gubernamental (por ejemplo, la Administración Federal de Ingresos Públicos), que confirme la existencia de la organización, y
- Confirmación con el contacto apropiado de la Organización de manera telefónica, por correo o procedimiento comparable, de cierta información acerca de la misma.

Para tipos específicos de certificados pueden desarrollarse procedimientos adicionales. Por ejemplo, en el caso de los certificados del Administrador que operará en representación de la organización que ha contratado los Servicios de Confianza de CertiSur y/o actuará en carácter de Autoridad de Registro, CertiSur S.A. confirma con el contacto apropiado de manera telefónica, por correo o procedimiento comparable:

- La relación de dependencia del representante que ha remitido la Solicitud de Certificado de Administrador.
- La potestad del representante para actuar en representación de la organización que ha contratado los Servicios de Confianza de CertiSur o actuará como Autoridad de Registro, y
- En forma telefónica, que el Solicitante del Certificado de manera telefónica, por correo o procedimiento comparable que haya remitido la Solicitud de Certificado.

CertiSur S.A. puede subcontratar, parcial o totalmente, los servicios mencionados más arriba, asegurando que el subcontratante cumpla con los requerimientos aquí establecidos, obligaciones en materia de seguridad y otros requisitos impuestos por CertiSur S.A., para el desarrollo de los servicios conforme a las presentes Normas.

3.2.3 Autenticación de la Identidad de un Individuo

CertiSur S.A. en forma directa o a través de una Autoridad de Registro autorizada, confirma que:

- El Solicitante del Certificado es la persona identificada en la Solicitud de Certificado,
- El Solicitante del Certificado es poseedor legítimo o tiene el control sobre la clave privada que se corresponde con la clave pública que será incluida en el Certificado, de acuerdo con lo establecido en la Sección 3.2.1 de estas Normas, y
- La información que será incluida en el Certificado es veraz, excepto la Información No Verificada del Suscriptor.

Para ello, CertiSur S.A. o una Autoridad de Registro autorizada, desarrollan alguno de los procedimientos descriptos en detalle a continuación:

- Utilización de registros de negocios o bases de datos de información comercial para aprobar o rechazar las Solicitudes de Certificado.

- Utilización de información almacenada en una base de datos de un servicio de validación de identidad, aprobado por CertiSur S.A.
- Comparando la información de la solicitud con sus propios registros de negocios o sus bases de datos de información. Por ejemplo, cotejando la información de la solicitud contra los registros de empleados o contratistas contenidos en la base de datos del departamento de recursos humanos.

CertiSur S.A. o una Autoridad de Registro autorizada pueden aprobar manualmente la Solicitud de Certificado, utilizando el Certificado de Administrador emitido a tal efecto, en caso que la información de la solicitud concuerde con los registros o con las bases de datos utilizada para autenticación. Este proceso es conocido como "Autenticación Manual".

El Módulo de Administración Automática de CertiSur S.A. posibilita que CertiSur o una Autoridad de Registro cuenten con la opción de aprobar y rechazar las Solicitudes de Certificado, en forma totalmente automática, directamente desde sistemas administrativos o bases de datos preexistentes, en lugar de requerir la Autenticación Manual de cada Solicitud de Certificado. En estos casos, se autentica previamente la identidad de los individuos que podrán remitir Solicitudes de Certificados antes de incluir su información en la base de datos. Cuando un Solicitante de Certificado remite una Solicitud de Certificado, el Módulo de Administración Automática compara la información de la Solicitud del Certificado con la base de datos y, si concuerdan, aprueba automáticamente la Solicitud de Certificado para su inmediata emisión. Este proceso es denominado "Administración Automática".

Un tercer mecanismo para la aprobación de Solicitudes de Certificado es mediante una Clave única o "Passcode" ("Autenticación mediante Passcode"). Implica la aprobación o rechazo automático de Solicitudes de Certificados, mediante la comparación de los datos de la solicitud del Solicitante del Certificado con datos de autenticación preconfigurados que son previamente cargados en una base de datos de la Autoridad Certificante. Con la Autenticación mediante Passcode, CertiSur S.A. o una Autoridad de Registro autorizada utilizan un proceso fuera de línea para distribuir "passcodes" a los Solicitantes de Certificados potenciales que hayan satisfecho el nivel apropiado de autenticación. El Solicitante del Certificado provee dicho "passcode" cuando remite la Solicitud del Certificado, conjuntamente con otra información de autenticación. El "passcode" y otra información de autenticación adicional son comparados con la base de datos de "passcodes" previamente configurada y, si todos los campos concuerdan, el Certificado es emitido.

3.2.3.1 Certificados de Administrador

Con el propósito de controlar el acceso a los sistemas de la Autoridad Certificante de CertiSur S.A. y para autorizar ciertas acciones dentro de los Servicios de Confianza de CertiSur son utilizados Certificados de Administrador.

CertiSur S.A. autentica las Solicitudes de Certificados de Administrador para las Autoridades de Registro o personal confiable de otras entidades de la siguiente forma:

- CertiSur S.A. autentica la existencia e identidad de la entidad que emplea o contrata al Administrador con arreglo a lo previsto en la Sección 3.2.2 de estas Normas.
- CertiSur S.A. confirma la relación de dependencia y la autorización de la persona nominada como Administrador en la Solicitud de Certificado para actuar en carácter de Administrador.

CertiSur S.A. también aprueba Solicitudes de Certificados para sus propios Administradores. Los Administradores son "Personas Confiables" dentro de sus respectivas organizaciones (ver la Sección 5.2.1 de estas Normas). 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 (ver la Sección 5.2.3 de estas Normas), procedimientos de control de antecedentes (ver la Sección 5.3.2 de estas Normas) y la autorización para actuar en carácter de Administrador.

CertiSur S.A. puede también aprobar Solicitudes de Certificados para sus propios Certificados de Administrador a ser asociados con receptores que no sean personas físicas tales como dispositivos o servicios. CertiSur S.A. autentica las Solicitudes de Certificados de Administrador para receptores que no sean personas físicas de la siguiente forma:

- CertiSur S.A. autentica la existencia e identidad del servicio nominado como Administrador en la Solicitud de Certificado
- CertiSur S.A. autentica que el servicio haya sido implementado de manera segura, en forma consistente con la ejecución de funciones de Administrador, y
- CertiSur S.A: confirma la relación de dependencia y la autorización de la persona que efectuó la solicitud del certificado de Administrador para el servicio nominado como Administrador en la Solicitud de Certificado.

3.2.4 Información no Verificada del Suscriptor

Se considera Información no Verificada del Suscriptor a aquéllos 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 bajo su exclusiva responsabilidad.

3.2.5 Validación de Autoridades Certificantes y de Registro

Las Solicitudes de Certificado para Autoridades Certificantes de CertiSur S.A. son procesadas y aprobadas por personal autorizado de CertiSur S.A., utilizando procedimientos controlados que requieren la participación de múltiples Personas Confiables de CertiSur S.A.

Las Autoridades de Registro suscriben un acuerdo con CertiSur S.A. antes de poder comenzar a ejecutar las funciones para las cuales están autorizadas con arreglo a las presentes Normas. CertiSur S.A. autentica la identidad de una organización que se postula como Autoridad de Registro antes de la aprobación final para desempeñarse como tal, desarrollando los controles requeridos para la confirmación de la identidad de organizaciones especificados en la Sección 3.2.2 de estas Normas. Adicionalmente, CertiSur S.A. confirma que la persona identificada como Administrador de la Autoridad de Registro esté autorizada para actuar en ese rol. Opcionalmente, CertiSur S.A. puede requerir la presencia personal de un representante autorizado de la organización ante el personal autorizado de CertiSur S.A.

CertiSur S.A. autentica la identidad de las entidades que desean convertirse en Autoridades de Registro de acuerdo con lo previsto en la Sección 3.2.2 de estas Normas y, después de la aprobación, emite los Certificados necesarios para desarrollar las funciones correspondientes. CertiSur S.A., antes de firmar un acuerdo con una Autoridad de Registro según lo establecido en la Sección 1.3.2 de estas Normas, confirma su identidad sobre la base de los documentos presentados. La suscripción de dicho contrato implica la

aprobación completa y final de la solicitud por parte de CertiSur S.A. La decisión de aprobar o rechazar una solicitud está sujeta a la total discrecionalidad de CertiSur S.A. Después de dicha aprobación, CertiSur S.A. emite el Certificado para la Autoridad de Registro de acuerdo con lo previsto en la Sección 6.1 de estas Normas.

Para los componentes de la infraestructura de CertiSur S.A. (por ejemplo, el contestador de OCSP), las Solicitudes de Certificado son generadas y aprobadas por personal autorizado de CertiSur S.A., a través de un proceso controlado que requiere la participación de múltiples Personas Confiables.

3.2.6 Criterios para la interoperabilidad

No aplicable.

3.3 Reemisión de Claves

3.3.1 Identificación y Autenticación para Reemisiones Periódicas

Antes de la expiración de un Certificado de Suscriptor vigente, es necesario que el Suscriptor obtenga un nuevo certificado para mantener su continuidad de uso. CertiSur S.A. generalmente requiere 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, CertiSur S.A. puede permitir que los Suscriptores soliciten 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 sea generado o no un nuevo par de claves.

Se pueden emitir nuevos Certificados de Autoridad Certificante con pares de claves de Autoridades Certificantes de CertiSur S.A. existentes. La "renovación" de los Certificados de Autoridad Certificante está permitida en la medida en que la vida útil acumulativa del par de claves de la Autoridad Certificante no exceda el máximo tiempo de vida útil aplicable, especificado en la Sección 6.3.2 de estas Normas. Los pares de claves de las Autoridades Certificantes de CertiSur S.A. pueden ser también "reemitidas", con arreglo a lo previsto en la Sección 4.7 de estas Normas. Por lo tanto, para los Certificados de las Autoridades Certificantes de CertiSur S.A. es tecnológicamente posible tanto la "reemisión de claves" como la "renovación"

Los Certificados de Suscriptor que no han sido revocados, puede ser reemplazados (es decir reemitidas sus claves o renovados), con arreglo a lo previsto en la Tabla 5 que figura a continuación.

Tiempo	Requerimiento
Dentro de los 30 días previos o de los 30 días posteriores al vencimiento del Certificado	CertiSur S.A. o una Autoridad de Registro autorizada autentican a los Suscriptores que intentan renovar o reemitir un Certificado a través del uso de una Frase de Comprobación, Clave de Firma o método equivalente o demostración de la posesión de la clave privada o del control sobre la misma. Como parte del proceso de registración inicial, los Suscriptores pueden elegir una Frase de Comprobación que envían junto con la información de su solicitud. Ante la reemisión o renovación de un Certificado dentro del período especificado, si el Suscriptor envía correctamente la Frase de Comprobación, Clave de Firma o método equivalente conjuntamente con la información de Solicitud del Suscriptor o demuestra la posesión de la clave privada o tener control sobre la misma y la información de la solicitud no ha sufrido cambios, será emitido automáticamente un nuevo Certificado[3]. Después de la reemisión de claves o renovación, de esta manera, y por lo menos en instancias alternadas o subsiguientes reemisiones de claves o renovaciones de allí en adelante, la Autoridad Certificante o la Autoridad de Registro deberá reconfirmar la identidad del Suscriptor con arreglo a los requerimientos especificados en la Sección 3.2.3 de estas Normas para la autenticación de una Solicitud de Certificado original.
Una vez transcurridos 30 días posteriores al vencimiento del Certificado	En este caso, se utilizan los requerimientos especificados en la Sección 3.2.3 de estas Normas para la autenticación de una Solicitud de Certificado original a efectos de renovar o reemitir un Certificado de Suscriptor usuario final.

Tabla 5 – Requerimientos de Reemisión de Claves y Renovación para Certificados de Suscriptores Usuarios Finales

3.3.2 Identificación y Autenticación para Reemisiones Después de la Revocación

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

- La revocación ocurre debido a que el Certificado fue emitido a una persona distinta de la nominada como Sujeto del Certificado,
- El Certificado fue emitido sin la autorización de la persona nominada como el Sujeto de dicho Certificado, o
- La entidad que aprueba la Solicitud de Certificado del Suscriptor descubre o tiene razones para suponer que existe, de hecho, una falsedad en la Solicitud del Certificado.

Sujeto a lo previsto en los párrafos precedentes, los Certificados de Suscriptor que han sido revocados, pueden ser reemplazados (es decir sus claves reemitidas) de acuerdo con la Tabla 6 que figura a continuación.

Tiempo	Requerimiento

[3] Si el Suscriptor no puede utilizar la Frase de Comprobación, Clave de Firma o procedimiento equivalente, CertiSur S.A. o la autoridad de Registro deberán reautenticar la información contenida en la solicitud del suscriptor.

Antes del vencimiento del Certificado	CertiSur S.A. o una Autoridad de Registro verifican que la persona que intenta reemplazar el certificado es, efectivamente, el Suscriptor, a través del uso de una Frase de Comprobación, Clave de Firma o método equivalente, tal como se describe en la Sección 3.2.1 de estas Normas. De no poder emplearse este procedimiento, para reemplazar un Certificado después de la revocación, se utilizan los requerimientos para la validación de una Solicitud de Certificado original según la Sección 3.2.3 de estas Normas. Dichos certificados contienen el mismo nombre distintivo (distinguished name) del Sujeto, tal como figura en el Certificado que será reemplazado.
Después del vencimiento del Certificado	En este caso, a efectos de reemplazar un Certificado de Suscriptor usuario final deben utilizarse los requerimientos especificados en la Sección 3.2.3 de estas Normas para la autenticación de una Solicitud de Certificado original.

Tabla 6 – Requerimientos para el Reemplazo de Certificados después de la Revocación

3.4 Identificación y Autenticación para la Solicitud de Revocación

Antes de la revocación de un Certificado, CertiSur S.A. o una Autoridad de Registro autorizada verifican que la revocación haya sido solicitada por el Suscriptor del Certificado. Los procedimientos aceptables de autenticación de las solicitudes de revocación por parte del Suscriptor incluyen:

- Envío del Suscriptor de la Frase de Comprobación, Clave de Firma o método equivalente y revocación automática del Certificado en caso de que la misma concuerde con la información registrada,
- 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 que la persona 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: telefónica, facsímil, correo electrónico, correo postal o servicio de courier o mensajería.

Los Administradores de CertiSur S.A. o de una Autoridad de Registro están facultados para solicitar la revocación de Certificados de Suscriptores. CertiSur S.A. autentica la identidad de los Administradores mediante controles de acceso seguros, antes de permitirles a los mismos desarrollar las funciones de revocación.

En caso de utilización del Módulo de Administración Automática deben remitirse en bloque a CertiSur S.A. las solicitudes de revocación. Dichas solicitudes son autenticadas mediante un requerimiento firmado digitalmente con la clave privada del dispositivo de hardware de Administración Automática.

Las siguientes entidades pueden solicitar la revocación de un Certificado de Autoridad Certificante, de Autoridad de Registro o de Autoridad Certificante de Infraestructura:

- Únicamente CertiSur S.A. está facultado para solicitar o iniciar el proceso de revocación de los Certificados emitidos para sus propias Autoridades Certificantes, Autoridades de Registro o componentes de su infraestructura.
- CertiSur S.A. puede iniciar el proceso de revocación de cualquier Certificado de Autoridad de Registro, de acuerdo con lo establecido en la Sección 4.9.1.

- Las Autoridades de Registro están facultadas, a través de sus representantes debidamente autorizados, a requerir la revocación de sus Certificados o de los Certificados de sus Administradores.

4 Requerimientos Operativos

4.1 Solicitud de Certificado

4.1.1 Solicitante del Certificado

Todos los Solicitantes usuarios finales de Certificados deben manifestar su conformidad con el Acuerdo de Suscriptor que resulte aplicable y completar un proceso de solicitud, que consiste en:

- Completar una Solicitud de Certificado y suministrar la información requerida,
- Generar o acordar la generación de un par de claves, de acuerdo con lo previsto en la Sección 6.1,
- Enviar su clave pública a CertiSur S.A. o a una Autoridad de Registro, con arreglo a lo establecido en la Sección 6.1.3, salvo las excepciones previstas en la Sección 4.5.
- Demostrar a CertiSur S.A. o a una Autoridad de Registro, en función de lo previsto en la Sección 3.2.1, que el Solicitante del Certificado está en posesión de la clave privada que se corresponde con la clave pública que ha enviado a CertiSur S.A. o tiene control sobre la misma, salvo las excepciones previstas en la Sección 4.5.

Las Autoridades Primarias Certificantes emiten certificados solamente para sus Autoridades Certificantes subordinadas. Para Autoridades Certificantes de CertiSur S.A., que son Suscriptores de Certificados de Autoridades Certificantes, las solicitudes de certificados son generadas y aprobadas por personal autorizado de CertiSur S.A., a través de un proceso controlado que requiere la participación de múltiples Personas Confiables.

CertiSur S.A. también opera Autoridades Certificantes de Infraestructura que emiten Certificados para los componentes de la infraestructura de los Servicios de Confianza de CertiSur (por ejemplo, para el Contestador de OCSP que suministra información acerca del estado de los Certificados).

Las Solicitudes de Certificados son remitidas tanto a CertiSur S.A. como a una Autoridad de Registro para su procesamiento, para su aprobación o rechazo. La entidad que procesa la Solicitud de Certificado y la entidad que emite el Certificado con arreglo a lo previsto en la Sección 4.2 pueden ser dos entidades diferentes.

CertiSur S.A. opera Autoridades Certificantes de Administración, que emiten certificados para los Administradores de las Autoridades de Registro, incluyendo:

- Personal de CertiSur S.A. (Administradores de la Autoridad de Registro de CertiSur S.A) que procesan las Solicitudes de Certificado en nombre de las Autoridades Certificantes de CertiSur S.A.,
- Personal de las Autoridades de Registro (Administradores) que procesan las Solicitudes de Certificado que reciben o que solicitan, y
- Servidores de Administración Automática o de Infraestructura, que procesan Solicitudes de Certificado o que desempeñan otras funciones automatizadas dentro de la Infraestructura de Servicios de Confianza de CertiSur.

Para todas las Autoridades de Registro se cumplimentan los requerimientos establecidos en la Sección 4.1 para los Certificados de Administradores.

4.1.2 Llenado de la Solicitud. Responsabilidades

El Solicitante del Certificado es responsable de completar la Solicitud de Certificado, aportando información precisa y veraz, con arreglo a las obligaciones impuestas por las presentes Normas. En ciertos casos, la Solicitud de Certificado puede ser realizada, en su nombre y representación, por una Autoridad de Registro. En todos los casos, el Suscriptor deberá leer y aceptar el Acuerdo del Suscriptor aplicable antes de solicitar, aceptar o utilizar un Certificado emitido bajo los Servicios de Confianza de CertiSur.

4.2 Procesamiento de la Solicitud de Certificado

4.2.1 Funciones de Identificación y Autenticación

Las Funciones de Identificación y Autenticación son desarrolladas por Personal Confiable, según lo previsto en las Secciones 5.2.1 y 5.2.2 de estas Normas. Dicho personal es especialmente seleccionado y entrenado por CertiSur S.A. Las Funciones de Identificación y Autenticación también pueden ser realizadas por Personal Confiable de una Autoridad de Registro dentro de los Servicios de Confianza de CertiSur, con arreglo a lo previsto en la Sección 1.3.2 de estas Normas.

4.2.2 Aprobación o Rechazo de las Solicitudes de Certificado

Después que un Solicitante de Certificado remite la Solicitud de Certificado, según lo previsto en la Sección 4.1, un Administrador de CertiSur S.A. o de una Autoridad de Registro confirma la información contenida en la Solicitud de Certificado (con excepción de la Información No Verificada del Suscriptor) con arreglo a lo previsto en la Sección 3.2. Después de desarrollar en forma satisfactoria todos los procedimientos de autenticación requeridos, un Administrador de CertiSur S.A. o de una Autoridad de Registro aprueba la Solicitud de Certificado. Si la autenticación no es satisfactoria, un Administrador de CertiSur S.A. o de una Autoridad de Registro rechaza la Solicitud de Certificado.

4.2.3 Plazo para el Procesamiento de las Solicitudes

CertiSur S.A. procesa y emite los Certificados, luego de aprobadas las Solicitudes de Certificado, en plazos que se consideran comercialmente razonables.

4.3 Emisión de Certificados

4.3.1 Tareas de la Autoridad Certificante durante la Emisión de los Certificados

Un Certificado es generado y emitido 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. CertiSur S.A. 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. Cuando una Autoridad de Registro aprueba una Solicitud de Certificado y comunica dicha aprobación a CertiSur S.A., CertiSur S.A. genera un Certificado y se lo emite al Solicitante del Certificado. Los procedimientos detallados en esta sección también son empleados para la emisión de Certificados relacionados con una solicitud para reemplazar (es decir renovar o reemitir las claves) un Certificado.

4.3.2 Notificación al Suscriptor de la Emisión del Certificado

Después de la generación del Certificado, CertiSur S.A. comunica a los Suscriptores que sus Certificados están disponibles y los notifica respecto de los medios para obtener y/o utilizar dichos Certificados. En algunos casos, esta notificación puede ser enviada por la Autoridad de Registro.

4.4 Aceptación del Certificado

4.4.1 Conducta que Constituye la Aceptación del Certificado

Después de la emisión, los Certificados están disponibles para los Suscriptores usuarios finales ya sea permitiéndoles que ejecuten la descarga del mismo desde un sitio web, a través de un mensaje enviado al Suscriptor conteniendo el Certificado o directamente para ser utilizados mediante el empleo de una Clave de Firma. Por ejemplo, CertiSur S.A. puede enviarle al Suscriptor un Número de Identificación Personal (PIN), que el Suscriptor deberá copiar en una página web de solicitud para poder obtener el Certificado. El Certificado también puede ser enviado al Suscriptor a través de un mensaje de correo electrónico. Realizar la descarga de un Certificado, instalar el Certificado recibido a través de un mensaje o emplear la Clave de Firma enviada para activar la clave privada asociada a la clave pública contenida en el Certificado, constituyen la aceptación del Certificado por parte del Suscriptor.

4.4.2 Publicación del Certificado

Los Certificados de Suscriptores usuarios finales podrán estar disponibles para las Partes Confiadas a través de las funciones de consulta en el repositorio de CertiSur en **https://www.certisur.com/legal**. En algunos casos, por pedido de Clientes bajo convenios especiales, la información de los Certificados de Suscriptores usuarios finales emitidos está disponible a través de las funciones de consulta del repositorio, aunque a exclusiva discreción del Cliente, el Certificado puede estar accesible solamente a través del empleo del número de serie.

4.4.3 Notificación de la Emisión del Certificado a Otras Entidades

CertiSur S.A. podrá informar la emisión de un Certificado a un tercero cuando dicho trámite esté previsto en un acuerdo especial suscripto con el Cliente que solicitó el Certificado o el procedimiento forme parte de requisitos impuestos por una autoridad para posibilitar el uso del mismo. Las características de esta comunicación se ajustarán a los requerimientos de la autoridad correspondiente.

4.5 Par de Claves y Utilización del Certificado

4.5.1 Clave Privada del Suscriptor y Utilización del Certificado

La generación del par de claves de un Suscriptor usuario final es generalmente desarrollada por el Suscriptor. Para ello, el Suscriptor utiliza normalmente un módulo criptográfico certificado, según estándares FIPS 140-1 nivel 1, provisto con su software de navegación (browser) o aplicativo especialmente diseñado para este fin.

El par de claves de un Suscriptor usuario final también puede ser generado en dispositivos externos, tales como tokens o tarjetas smartcards. Bajo acuerdos específicos, esta tarea puede ser realizada por CertiSur S.A. o por una Autoridad de Registro. En estos casos, los

dispositivos son luego 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.

De idéntica forma, bajo Acuerdos específicos, CertiSur puede generar bajo un procedimiento seguro el par de claves en dispositivos protegidos criptográficamente y poner a disposición del Suscriptor usuario final la clave privada para su utilización de manera exclusiva. Para ello, le enviará al Suscriptor usuario final una "Clave de Firma" utilizando un procedimiento exclusivo, que le permitirá acceder a su clave privada solamente cuando requiera la utilización de la misma para generar una firma electrónica.

4.5.2 Clave Pública, Receptor Confiado y Utilización del Certificado

Los Suscriptores usuarios finales y las Autoridades de Registro remiten sus claves públicas a CertiSur S.A. 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 electrónicamente, en una sesión segura por la utilización del protocolo SSL.

Según lo previsto en la Sección 4.5.1, bajo Acuerdos específicos CertiSur S.A. puede generar la Clave Pública e incluirla en un Certificado para un Suscriptor usuario final.

El Receptor Confiado deberá utilizar el software y/o hardware que resulten apropiados para desarrollar la verificación de firmas electrónicas u otras operaciones criptográficas que desee llevar a cabo, como condición para confiar en un Certificado relacionado con cada una de dichas operaciones. Dichas operaciones incluyen la identificación de una Cadena de Certificación y la verificación de las firmas digitales o electrónicas incluidas en todos los Certificados que forman parte de la Cadena de Certificación. El Receptor Confiado solamente podrá confiar en un Certificado cuando dichos procedimientos de verificación acrediten su validez y vigencia.

4.6 Renovación del Certificado

4.6.1 Circunstancias para la Renovación

Tal como se indica en la Sección 3.3.1, antes de la expiración de un Certificado de Suscriptor vigente, es necesario que el Suscriptor obtenga un nuevo certificado para mantener su continuidad de uso.

4.6.2 Solicitante de la Renovación

Todos los Solicitantes usuarios finales de Certificados que deseen renovar un Certificado deberán ratificar su conformidad con el Acuerdo de Suscriptor que resulte aplicable y completar un proceso de renovación, que consiste en:

- Completar una Solicitud de Certificado y suministrar la información requerida,
- Generar o acordar la generación de un par de claves, de acuerdo con lo previsto en la Sección 6.1,
- Enviar su clave pública a CertiSur S.A. o a una Autoridad de Registro, con arreglo a lo establecido en la Sección 6.1.3, salvo las excepciones previstas en la Sección 4.5.

- Demostrar a CertiSur S.A. o a una Autoridad de Registro, en función de lo previsto en la Sección 3.2.1 de estas Normas, que el Solicitante del Certificado está en posesión de la clave privada que se corresponde con la clave pública que ha enviado a CertiSur S.A., salvo las excepciones previstas en la Sección 4.5.

Bajo Acuerdos específicos, CertiSur S.A. podrá renovar automáticamente los Certificados de Suscriptores usuarios finales, antes de la finalización del plazo de vigencia de sus Certificados. También podrá renovar los Certificados de Suscriptores usuarios finales por pedido de la Autoridad de Registro que corresponda.

4.6.3 Procesamiento de las Solicitudes de Renovación

Según lo previsto en la Sección 3.3.1, CertiSur S.A. o una Autoridad de Registro autorizada autentican a los Suscriptores que intentan renovar o reemitir un Certificado a través del uso de una Frase de Comprobación, Clave de Firma o método equivalente o demostración de la posesión de la clave privada o control sobre la misma.

Una vez transcurridos 30 días posteriores al vencimiento del Certificado, CertiSur S.A. o una Autoridad de Registro cumplirán con los requerimientos especificados en la Sección 3.2.3 para la autenticación de una Solicitud de Certificado original, a efectos de renovar un Certificado de Suscriptor usuario final

4.6.4 Notificación al Suscriptor de la Emisión del nuevo Certificado

Después de la generación del nuevo Certificado, CertiSur S.A. comunica a los Suscriptores que sus Certificados han sido renovados y que están disponibles y los notifica respecto de los medios para obtener y/o utilizar dichos Certificados. En algunos casos, esta notificación puede ser enviada por la Autoridad de Registro.

4.6.5 Conducta que Constituye la Aceptación del Certificado Renovado

Realizar la descarga de un Certificado, instalar el Certificado recibido a través de un mensaje o emplear la Clave de Firma enviada para activar la clave privada asociada a la clave pública contenida en el Certificado renovado, constituyen la aceptación del Certificado por parte del Suscriptor.

4.6.6 Publicación del Certificado Renovado

Los Certificados de Suscriptores usuarios finales que hayan sido renovados podrán estar disponibles para las Partes Confiadas a través de las funciones de consulta en el repositorio de CertiSur en **https://www.certisur.com/legal**. En algunos casos, por pedido de Clientes bajo convenios especiales, la información de los Certificados de Suscriptores usuarios finales renovados está disponible a través de las funciones de consulta del repositorio, aunque a exclusiva discreción del Cliente, el Certificado puede estar accesible solamente a través del empleo del número de serie.

4.6.7 Notificación de la Emisión del Certificado Renovado a Otras Entidades

CertiSur S.A. podrá informar la renovación de un Certificado a un tercero cuando dicho trámite esté previsto en un acuerdo especial suscripto con el Cliente que solicitó el Certificado o el procedimiento forme parte de requisitos impuestos por una autoridad para posibilitar el uso del mismo. Las características de esta comunicación se ajustarán a los requerimientos de la autoridad correspondiente.

4.7 Reemisión de Claves de los Certificados

Antes de la expiración de un Certificado de Suscriptor vigente, es necesario que el Suscriptor obtenga un nuevo certificado para mantener su continuidad de uso. CertiSur S.A. generalmente requiere 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, CertiSur S.A. puede permitir que los Suscriptores soliciten 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 sea generado o no un nuevo par de claves. Por lo tanto, a los efectos previstos en esta Sección para los Certificados de Suscriptores usuarios finales resulta de aplicación lo normado en la Sección 4.6

En el caso de los pares de Claves de las Autoridades Certificantes, deben tomarse en cuenta las limitaciones impuestas por la Sección 5.6.

4.8 Modificación de Certificados

No está contemplada la modificación de Certificados dentro de los Servicios de Confianza de CertiSur.

4.9 Revocación y Suspensión de Certificados

4.9.1 Circunstancias para la Revocación

Un Certificado de Suscriptor usuario final es revocado si:

- CertiSur S.A., una Autoridad de Registro o un Suscriptor tienen motivos para creer o fuertes sospechas de que ha existido un Compromiso de la clave privada del Suscriptor,
- CertiSur S.A. o una Autoridad de Registro tienen motivos para creer que el Suscriptor ha violado materialmente una obligación, declaración o garantía establecidas por el Acuerdo del Suscriptor aplicable,
- El Acuerdo del Suscriptor con el Suscriptor ha expirado,
- La vinculación del Suscriptor con un Cliente de CertiSur que ha acordado la emisión de los certificados de Suscriptores usuarios finales para un uso específico ha terminado o finalizado de cualquier forma,
- CertiSur S.A. o una Autoridad de Registro 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 ha sido emitido a una persona diferente de la nominada como Sujeto del Certificado o el Certificado ha sido emitido sin la autorización de la persona nominada como Sujeto de dicho Certificado,
- CertiSur S.A. o una Autoridad de Registro tienen razones para suponer que una información relevante incluida en la Solicitud de Certificado es falsa,

- CertiSur S.A. o una Autoridad de Registro determinan que un prerrequisito para la Emisión del Certificado nunca fue satisfecho ni exceptuado su cumplimiento,
- En el caso de que los Certificados para Suscriptores usuarios finales incluyan el nombre de una organización con la cual los Suscriptores estén vinculados, ese nombre haya cambiado o la organización haya dejado de existir,
- La información contenida en el Certificado, distinta de la Información No Verificada del Suscriptor, es incorrecta o ha cambiado,
- El Suscriptor solicita la revocación del Certificado con arreglo a lo previsto en la Sección 3.4 de estas Normas,
- La continuidad en el uso de dicho Certificado es perjudicial para los Servicios de Confianza de CertiSur, o
- Acontece algún otro de los supuestos previstos en la legislación aplicable.

CertiSur S.A. también puede revocar un Certificado de Administrador si la autoridad del Administrador para actuar como tal ha terminado o ha concluido de cualquier otra forma.

Los Acuerdos del Suscriptor para los Servicios de Confianza de CertiSur requieren que los Suscriptores usuarios finales notifiquen inmediatamente a CertiSur S.A. si conocen o sospechan que su clave privada ha sufrido un Compromiso, según los procedimientos establecidos en la Sección 4.9.3.

4.9.2 Solicitante de la Revocación

Las siguientes entidades pueden solicitar la revocación de un Certificado de un Suscriptor usuario final:

- CertiSur S.A. o la Autoridad de Registro que aprobó la Solicitud de Certificado del Suscriptor pueden solicitar la revocación de cualquier Certificado de Suscriptor usuario final o Certificado de Administrador de acuerdo con la Sección 4.9.1 de estas Normas.
- Los individuos Suscriptores pueden solicitar la revocación de sus propios Certificados.
- Un representante debidamente autorizado de CertiSur S.A. o de una Autoridad de Registro cuyo Administrador recibió un Certificado de Administrador están facultados para solicitar la revocación de un Certificado de Administrador.
- En el caso de que, bajo un Acuerdo específico, el Certificado de un Suscriptor usuario final incluya el nombre de una organización con la cual dicho Suscriptor está vinculado, un representante debidamente autorizado de dicha organización puede solicitar la revocación de dicho Certificado.

4.9.3 Procedimiento para Solicitar la Revocación

Un Suscriptor usuario final que solicite la revocación debe notificar dicho requerimiento a CertiSur S.A. o a la autoridad de Registro que aprobó la Solicitud del Certificado del Suscriptor, quienes en cada caso iniciarán el proceso de revocación inmediatamente. La comunicación de dicha solicitud de revocación debe ser efectuada con arreglo a lo establecido en la Sección 3.4.

Cuando el que inicie el proceso de revocación sea una Autoridad de Registro o un Cliente de CertiSur, deberán instruir a CertiSur S.A. para que revoque el Certificado.

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

4.9.4 Período de Gracia de 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 Lapso para el Procesamiento de la Solicitud de Revocación

CertiSur procederá a revocar un Certificado tan pronto como resulte posible, dentro de plazos que resulten comercialmente razonables.

4.9.6 Requerimientos de Control de la Revocación para 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.

- Para Autoridades Certificantes bajo los Servicios de Confianza de CertiSur, las Listas de Certificados Revocados están publicadas en el Repositorio en **https://www.certisur.com/legal**.
- Para Certificados de Suscriptores usuarios finales, las Listas de Certificados Revocados están publicadas en **https://www.certisur.com/legal**.

4.9.7 Frecuencia de la Emisión de las Listas de Certificados Revocados

CertiSur S.A. publica Listas de Certificados Revocados mostrando la revocación de los Certificados de sus Servicios de Confianza y ofrece bajo acuerdos específicos servicios adicionales para controlar el estado de los Certificados. Las Listas de Certificados Revocados para las Autoridades Certificantes que emiten Certificados para Suscriptores usuarios finales son publicadas diariamente. Las Listas de Certificados Revocados para Autoridades Certificantes que solamente emiten Certificados de Autoridad Certificante son publicadas trimestralmente 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 su fecha de vencimiento.

4.9.8 Plazo de Vigencia de las Listas de Certificados Revocados

Las Listas de Certificados Revocados contienen la información respecto del plazo de vigencia de las mismas.

4.9.9 Disponibilidad del Control en Línea del Estado de un Certificado

Adicionalmente a la publicación de Listas de Certificados Revocados, CertiSur S.A. puede suministrar información respecto del estado de un Certificado, a través de funciones de consulta en el repositorio de CertiSur S.A., mediando un acuerdo específico.

La información del estado del Certificado está disponible a través de funciones de consulta basadas en web, accesibles a través del Repositorio de CertiSur S.A. en **https://www.certisur.com/legal**.

CertiSur S.A. también puede proveer información del estado del Certificado a través del Protocolo del Estado del Certificado en Línea (OCSP) a un Cliente específico que haya acordado la prestación de dichos servicios para un grupo determinado de Certificados de Suscriptores usuarios finales. Los Clientes que contraten los Servicios de OCSP pueden controlar el estado del Certificado a través del uso de dicho Protocolo. La dirección URL para el Contestador de OCSP que resulte apropiado es notificada a dicho Cliente.

4.9.10 Requerimientos para el Control en Línea de la Revocación

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 utilizando uno de los métodos aplicables especificados en la Sección 4.9.9 de estas Normas.

4.9.11 Disponibilidad de Otras Formas de Publicación de la Revocación

No especificado.

4.9.12 Requerimientos Especiales con Relación a Compromisos de Claves

Adicionalmente a los procedimientos descriptos en la Sección 4.9.9, CertiSur S.A. emplea todos los esfuerzos que comercialmente resulten razonables para notificar a potenciales Partes Confiadas si CertiSur S.A. descubre o tiene razones para suponer que ha existido un Compromiso de la clave privada de alguna Autoridad Certificante bajo los Servicios de Confianza de CertiSur.

4.9.13 Circunstancias para la Suspensión

Los Servicios de Confianza de CertiSur no contemplan la suspensión de Certificados de Autoridades Certificantes o de Suscriptores usuarios finales.

5 Infraestructura Física, Administración y Controles Operativos

5.1 Controles Físicos

CertiSur S.A. ha implementado la Política de Seguridad Física de CertiSur S.A. que contiene los requerimientos en materia de seguridad de las presentes Normas para el Proceso de Certificación.

5.1.1 Ubicación y Construcción del Centro de Procesamiento

Las operaciones de las Autoridades Certificantes de los Servicios de Confianza de CertiSur se llevan a cabo dentro del Centro de Procesamiento de CertiSur S.A. ubicado en la Ciudad Autónoma de Buenos Aires, República Argentina, el cual cumple con las exigencias establecidas en los Requerimientos en materia de Seguridad y Auditoría. Todas las operaciones de las Autoridades Certificantes y Autoridades de Registro de los Servicios de Confianza de CertiSur son desarrolladas dentro de un entorno físicamente protegido, diseñado para evitar, prevenir y detectar intrusiones abiertas o encubiertas.

CertiSur S.A. cuenta 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

Los sistemas de las Autoridades Certificantes dentro de los Servicios de Confianza de CertiSur están protegidos por al menos cuatro niveles de seguridad física, que requieren que se acceda a un nivel inferior antes de poder acceder al nivel inmediatamente superior.

Los controles de acceso físico para cada nivel son progresivamente más restrictivos. 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. El acceso a cada nivel requiere la utilización de una tarjeta de proximidad identificatoria, para los empleados. El acceso físico es automáticamente registrado y grabado en video. Los niveles adicionales requieren controles de acceso individual a través del uso de dos factores de autenticación, incluyendo métodos biométricos. 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 de seguridad física incluyen niveles adicionales para la seguridad de la administración de claves que protegen los dispositivos criptográficos firmantes y material relacionado con claves, tanto si están siendo utilizados en línea como si están almacenados fuera de línea. Las áreas utilizadas para crear y almacenar material criptográfico exigen controles de acceso doble, cada uno de ellos a su vez con 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/o 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 CertiSur S.A. La apertura y cierre de los gabinetes o contenedores en estos niveles de seguridad es registrado, con propósitos de auditoría.

5.1.3 Suministro Eléctrico y Aire Acondicionado

El centro de procesamiento de CertiSur S.A. está equipado con:

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

5.1.4 Exposición al Agua

CertiSur S.A. 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 Incendios

CertiSur S.A. 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 por CertiSur S.A. 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 del centro de procesamiento de CertiSur S.A. 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 CertiSur S.A.

5.1.8 Copias de Resguardo fuera del Centro de Procesamiento

CertiSur S.A. efectúa copias de resguardo en forma rutinaria sobre los datos de los sistemas críticos, los registros de auditoría y otra información igualmente sensitiva.

5.2 Procedimiento 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.

CertiSur S.A. considera 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 la Sección 5.3 de estas Normas.

5.2.2 Cantidad de Personas Requeridas por Tarea

CertiSur S.A. mantiene 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.

Las operaciones manuales, tales como la validación y emisión manual de Certificados 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.

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 personal gerencial 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.

CertiSur S.A. asegura 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 los Servicios de Confianza de CertiSur.

5.3 Controles sobre el Personal

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. El control de los antecedentes se repetirá, como mínimo, cada 5 años para todo el personal que ocupe Posiciones de Confianza.

5.3.2 Procedimientos de Control de Antecedentes

CertiSur S.A. realiza 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,
- control de los antecedentes crediticios y financieros, y
- búsqueda de registros de aportes a los sistemas de Seguridad Social.

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, CertiSur S.A. utilizará una técnica 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, 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 Empleados Confiables.

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

5.3.3 Requerimientos de Capacitación

CertiSur S.A. provee 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. CertiSur S.A. mantiene registros de dichas

actividades de capacitación. CertiSur S.A. revisa y mejora en forma periódica sus programas de capacitación internos, tal como resulte necesario.

Los programas de capacitación internos de CertiSur S.A. 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 de CertiSur S.A.,
- 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.

5.3.4 Frecuencias y Requerimientos en Materia de Capacitación

CertiSur S.A. provee 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. En forma periódica y continua se dictan cursos de concientización en materia de seguridad.

5.3.5 Frecuencia y Secuencia de Rotación de Tareas

No contempladas.

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 CertiSur S.A., 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 ejecutadas.

5.3.7 Requerimientos para el Personal Contratado

En circunstancias limitadas, se puede utilizar personal contratado o consultores para desempeñar Posiciones de Confianza. Para cualquiera de dichos contratados o consultores resulta aplicable el mismo criterio funcional y de seguridad que para los empleados de CertiSur S.A. 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 CertiSur S.A., solamente si están permanentemente acompañados y directamente supervisados por Personas Confiables.

5.3.8 Documentación Suministrada al Personal

CertiSur S.A. le suministra al personal la documentación de capacitación u otra que fuera necesaria para que desarrollen las responsabilidades que su tarea exige, en forma competente y satisfactoria.

5.4 Procedimientos de Registros de Auditoría

5.4.1 Tipos de Eventos Registrados

CertiSur S.A., en forma manual o automática, registra los siguientes eventos significativos:

- Eventos de administración del ciclo de vida de los Certificados de Autoridad Certificante, de Administrador y de Suscriptor, que incluyen:
  - Solicitudes de Certificado, renovación, reemisión de claves y revocación
  - Procesamiento de solicitudes, aprobadas o rechazadas
  - Generación y emisión de Certificados y Listas de Certificados Revocados.
- Eventos relacionados con seguridad, que incluyen:
  - Intentos de acceso a los sistemas de PKI, exitosos o no
  - Acciones sobre el sistema de PKI y su seguridad desarrolladas por personal de CertiSur S.A.
  - Lectura, escritura o borrado 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 al Centro de Procesamiento.

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 persona que efectúa el ingreso periódico
- Tipo de ingreso.

La información de los registros de las Solicitudes de Certificados para las Autoridades de Registro y Administradores incluye:

- 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.

5.4.2 Frecuencia del Procesamiento de los Registros

Los registros de auditoría son revisados por lo menos semanalmente, en relación con eventos de seguridad u operativos de significación. Adicionalmente, CertiSur S.A. revisa sus registros de auditoría en relación con actividades inusuales o sospechosas, en respuesta a alertas generadas sobre la base de irregularidades o incidentes ocurridos dentro de los sistemas de las Autoridades Certificantes y de las Autoridades de Registro dentro de los Servicios de Confianza de CertiSur.

El procesamiento de los registros de auditoría consiste en una revisión de los registros de auditoría y documentación para todos aquellos eventos significativos incluidos en el resumen de los registros de auditoría. La revisión de los registros de auditoría incluye una verificación de que los mismos no hayan sido adulterados, una revisión de todos los datos ingresados en el registro 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 Guarda de los Registros 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 de estas Normas.

5.4.4 Protección de los Registros 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 para la Copia 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

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 CertiSur S.A.

5.4.7 Notificación de Eventos

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 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 o anualmente, de acuerdo con las exigencias de la Guía de Requerimientos en materia de Seguridad y Auditoría. 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

Adicionalmente a los registros de auditoría especificados en la Sección 5.4, CertiSur S.A. mantiene registros que incluyen documentación acerca de:

- Cumplimiento por parte de CertiSur S.A. de las Normas para el Proceso de Certificación y otras obligaciones bajo sus acuerdos con los Suscriptores, y
- Acciones e información que resultan materiales con relación a cada Solicitud de Certificado y a la creación, emisión, uso, revocación, expiración y reemisión de claves o renovación de todos los Certificados emitidos.

Los registros de CertiSur S.A. de los eventos vinculados con el ciclo de vida del Certificado incluyen:

- La identidad del Suscriptor nominado en cada Certificado,
- La identidad de las personas que solicitan la revocación de Certificados,
- Otra información presente en el Certificado,
- Registro de tiempo, y
- Ciertos hechos materialmente previsibles relacionados con la emisión de certificados incluyendo pero no limitándose a información relevante para cumplimentar satisfactoriamente una Auditoría de Cumplimiento, según lo establecido en el Capítulo 8 de estas Normas.

Los registros pueden ser mantenidos en forma electrónica o en papel, asegurando que dichos registros están adecuada y completamente indexados, almacenados, preservados y reproducidos.

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 Suscriptores usuarios finales, Administradores y Autoridades de Registro,
- Diez (10) años para Autoridades Certificantes.

Si resultara necesario, CertiSur S.A. puede implementar plazos de almacenamiento más largos, a efectos de cumplimentar leyes que resulten de aplicación.

5.5.3 Protección del Archivo

CertiSur S.A. protege sus registros archivados compilados según lo establecido en la Sección 5.4.1 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 la implementación de controles de acceso apropiados, tanto físicos como lógicos. 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 la Sección 5.4.3 de estas Normas.

5.5.4 Procedimientos de Resguardo del Archivo

CertiSur S.A. efectúa resguardos de sus archivos electrónicos con información sobre los Certificados emitidos, incrementalmente en forma diaria y ejecuta un resguardo total y completo una vez por semana. Las copias de los registros en papel compilados según lo previsto en la Sección 5.4.1 son almacenadas en una instalación de recupero ante desastres, fuera del sitio de procesamiento, de acuerdo con lo previsto en la Sección 5.7 de estas Normas.

5.5.5 Requerimientos de Registros de Tiempo

Los Certificados, Listas de Certificados Revocados y otros datos ingresados en la base de datos de revocación contienen información sobre fecha y hora, no generada criptográficamente.

5.5.6 Procedimientos para Obtener y Verificar Información Archivada

Referirse a la Sección 5.5.3 de estas Normas.

5.6 Cambio de Claves

Las claves de las Autoridades Certificantes de CertiSur S.A. deben ser reemitidas periódicamente, de acuerdo con lo establecido en la Sección 6.3.2 de estas Normas.

Los Certificados de las Autoridades Certificantes dentro de los Servicios de Confianza de CertiSur pueden ser renovados dentro de los parámetros especificados en la Sección 6.3.2. Por ejemplo, si un certificado inicial de una Autoridad Certificante fue emitido con una vida útil de 10 años, los certificados de renovación pueden emitirse para extender el período de validez del par de claves de la Autoridad Certificante por un plazo máximo de 20 años, de modo tal de alcanzar el período máximo permitido de validez de 30 años. La renovación del Certificado de una Autoridad Certificante no es posible, una vez que finalizó su Período de Vigencia.

Las solicitudes de renovación de los Certificados de las Autoridades Certificantes dentro de los Servicios de Confianza de CertiSur son generadas y aprobadas por personal autorizado, a través de un proceso controlado que requiere la participación de múltiples Personas Confiables.

Para los Certificados de Autoridades de Registro CertiSur S.A. desarrolla los procedimientos apropiados para verificar que el Solicitante sea el mismo que en la solicitud original, con arreglo a lo previsto en la Sección 3.4 de estas Normas.

Los pares de claves de las Autoridades Certificantes dentro de los Servicios de Confianza de CertiSur son retirados de servicio al finalizar el plazo máximo de sus respectivas vidas útiles tal como está definido en la Sección 6.3.2. Los Certificados de Autoridades Certificantes dentro de los Servicios de Confianza de CertiSur pueden ser renovados en la medida en que el plazo 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 firmante de dicho certificado. 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, de acuerdo con lo previsto en la Sección 6.1 de estas Normas.

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 dentro de los Servicios de Confianza de CertiSur 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 Compromisos de Claves o Desastres

CertiSur S.A. revocará Certificados de Autoridad Certificante, de Autoridad de Registro o de Autoridad Certificante de Infraestructura si:

- CertiSur S.A. descubre o tiene razones para suponer que ha existido un Compromiso de la clave privada de la Autoridad Certificante, de la Autoridad de Registro o de la Autoridad Certificante de Infraestructura,
- El acuerdo entre la Autoridad Certificante o la Autoridad de Registro y CertiSur S.A. ha finalizado,
- CertiSur S.A. descubre o tiene razones para suponer que el Certificado ha sido emitido de una manera que, materialmente, no cumple con los procedimientos requeridos por las presentes Normas para el Proceso de Certificación, el Certificado ha sido emitido a una entidad distinta de la nominada como Sujeto del Certificado o el Certificado ha sido emitido sin la autorización de la entidad nominada como Sujeto de dicho Certificado,
- CertiSur S.A. determina que un prerrequisito para la emisión del Certificado nunca fue satisfecho ni exceptuado su cumplimiento,
- La Autoridad Certificante o la Autoridad de Registro solicitan la revocación del Certificado,
- La continuidad en el uso de dicho Certificado es perjudicial para los Servicios de Confianza de CertiSur, o
- Acontece algún otro supuesto previstos en la legislación aplicable que imponga la obligación de revocar el Certificado.

CertiSur S.A. requiere que las Autoridades de Registro o los Clientes con los cuales ha suscripto un acuerdo específico notifiquen a CertiSur S.A. cuando una revocación es exigida con arreglo a los procedimientos establecidos en la Sección 4.9.3 de estas Normas.

5.7.1 Procedimientos para el Manejo de Incidentes o Compromisos de Claves

CertiSur S.A. ha implementado una robusta combinación de controles físicos, lógicos y de procedimientos, a efectos de minimizar el riesgo y el potencial impacto de un compromiso de claves o de un desastre. Adicionalmente, CertiSur S.A. ha implementado procedimientos de recuperación ante desastres, tal como se describe en la Sección 5.7.4 y procedimientos de respuesta ante compromiso de claves, según se detalla en la Sección 5.7.3 de estas Normas. Los procedimientos de CertiSur S.A. relacionados con compromiso de claves y recupero ante desastres han sido desarrollados para minimizar el potencial impacto de una ocurrencia de ese tipo y restaurar las operaciones de los Servicios de Confianza de CertiSur dentro de un período razonable en función de la materia.

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 CertiSur S.A. 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 CertiSur S.A. relacionados con Compromiso de claves y recupero ante desastres.

5.7.3 Procedimientos en caso de Compromiso de la Clave Privada

En caso de sospecharse o conocerse el Compromiso de una clave privada de una Autoridad Certificante, Autoridad Certificante de Infraestructura o Autoridad de Registro, resultan de aplicación en forma inmediata los procedimientos de Respuesta ante Compromisos de Claves por parte del Grupo Especial de Respuesta ante Incidentes de Seguridad. Este grupo, que incluye personal de Seguridad, Operaciones Criptográficas, Servicios de Producción y otros representantes del personal gerencial de CertiSur S.A., evalúa la situación, desarrolla un plan de acción e implementa el mismo con la aprobación de la gerencia ejecutiva de CertiSur S.A.

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 CertiSur S.A., de acuerdo con lo establecido en la Sección 4.9.7 de estas Normas,
- Se realizan todos los esfuerzos que resulten razonables comercialmente para suministrar notificación adicional de la revocación a las Partes Confiadas 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 de estas Normas.

5.7.4 Capacidad de Continuidad en la Operación ante Desastres

CertiSur S.A., ha diseñado y probado un Plan de Recupero ante Desastres que permite 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.

CertiSur S.A. realiza copias de seguridad de sus sistemas y su información, las cuales son mantenidas en instalaciones de alta seguridad, externas a los centros operativos. CertiSur S.A. tiene la capacidad de recuperar operativamente las siguientes operaciones en un plazo menor a 24 horas:

- Revocación de Certificados
- Publicación de la información sobre revocación
- Suspensión de Servicios a Clientes bajo acuerdos específicos

El Plan de Recupero ante Desastres de CertiSur S.A. ha sido diseñado para que puedan ser recuperadas todas las demás funciones operativas en un plazo inferior a un mes posterior al evento acontecido.

CertiSur S.A. mantiene fuera de línea copias de seguridad de la información relevante sobre las Autoridades Certificantes, las Autoridades de Registro y los Administradores 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 validados, registros de acceso a las aplicaciones y registros de auditoría.

5.8 Finalización de una Autoridad Certificante o una Autoridad de Registro

En caso de que resultara necesario el cese de operaciones de una Autoridad Certificante o de una Autoridad de Registro dentro de los Servicios de Confianza de CertiSur, se realizarán 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 o de una Autoridad de Registro, se desarrollará 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 CertiSur S.A.,
- La preservación de los archivos y registros de la Autoridad Certificante, durante los plazos establecidos en la Sección 5.5.2 de estas 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, hasta que finalice el plazo de vigencia de todos los Certificados

emitidos por esa Autoridad Certificante o con intervención de esa Autoridad de Registro.

- 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.

6 Controles de Seguridad Técnicos

6.1 Generación del par de claves e instalación

6.1.1 Generación del 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 nivel 3. Para otras Autoridades Certificantes, los módulos criptográficos empleados cumplen, como mínimo, con los requerimientos de los estándares FIPS 140-1 nivel 2.

Todos los pares de claves de Autoridades Certificantes son generados en Ceremonias de Generación de Claves, de acuerdo con los requerimientos de la Guía de la Ceremonia de Generación de Claves y la Guía de Requerimientos en Materia de Seguridad y Auditoría. 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 establecido en las presentes Normas.

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 140-1 nivel 1, provistos con su software de navegación (browser).

6.1.2 Clave Privada del Suscriptor

El par de claves de un Suscriptor usuario final es normalmente generado por el Suscriptor usuario final.

El par de claves de un Suscriptor usuario final también puede ser pregenerado por CertiSur o por una Autoridad de Registro en dispositivos externos, tales como tokens o tarjetas smart cards. En estos casos, los 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 a la Autoridad de Registro o al Suscriptor usuario final utilizando un procedimiento totalmente separado del anterior.

Bajo Acuerdos específicos, CertiSur puede generar bajo un procedimiento seguro el par de claves en dispositivos protegidos criptográficamente y poner a disposición del Suscriptor usuario final la clave privada para su utilización de manera exclusiva. Para ello, le enviará al Suscriptor usuario final una "Clave de Firma" utilizando un procedimiento seguro, que le permitirá acceder a la clave privada solamente cuando requiera la utilización de la misma para generar una firma electrónica.

6.1.3 Entrega de la Clave Pública al Emisor del Certificado

En caso que los Suscriptores usuarios finales y las Autoridades de Registro remitan sus claves públicas a CertiSur S.A. para su certificación electrónica, esta entrega se efectuará 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

o de una Autoridad de Registro sea generado por CertiSur S.A., este requerimiento no resulta de aplicación.

6.1.4 Diseminación de la Clave Pública de la Autoridad Certificante a Receptores Confiados

CertiSur S.A. generalmente provee 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. Los Certificados de las Autoridades Certificantes dentro de los Servicios de Confianza de CertiSur están disponibles ser descargadas desde el Repositorio en **https://www.certisur.com/legal**.

6.1.5 Tamaño de Claves

Los pares de claves de las Autoridades Certificantes dentro de los Servicios de Confianza de CertiSur tienen una longitud mínima de 2048 bits RSA. CertiSur S.A. requiere que las Autoridades de Registro y los Suscriptores usuarios finales generen pares de claves de 2048 bits RSA de longitud como mínimo.

6.1.6 Parámetros de Generación y Controles de Calidad de Claves Públicas

No aplicable.

6.1.7 Propósitos de Uso de Claves

Para los Certificados X.509 Versión 3, se completa la extensión Uso de Claves (KeyUsage) de los Certificados de acuerdo con el RFC 5280[4]: Internet X.509 Public Key Infrastructure Certificate and CRL Profile con arreglo a la Tabla 7 a continuación.

		Autoridades Certificantes	*Suscriptores usuarios finales*
Criticidad (Criticality)		FALSE	FALSE
0	digitalSignature	En Blanco (Clear)	Marcado (Set)
1	nonRepudiation	En Blanco (Clear)	Marcado (Set)
2	keyEncipherment	En Blanco (Clear)	En Blanco (Clear)
3	dataEncipherment	En Blanco (Clear)	En Blanco (Clear)
4	keyAgreement	En Blanco (Clear)	En Blanco (Clear)
5	keyCertSign	Marcado (Set)	En Blanco (Clear)
6	CRLSign	Marcado (Set)	En Blanco (Clear)
7	encipherOnly	En Blanco (Clear)	En Blanco (Clear)
8	decipherOnly	En Blanco (Clear)	En Blanco (Clear)

[4]La RFC 5280 reemplazó a la RFC 3280

Tabla 7 – Variables para la Extensión Uso de Claves (KeyUsage)

6.2 Protección de la Clave Privada y Controles de Ingeniería de los Módulos Criptográficos

CertiSur S.A. ha implementado una combinación de controles físicos, lógicos y de procedimiento para reforzar la seguridad de las claves privadas de las Autoridades Certificantes dentro de los Servicios de Confianza de CertiSur. Los controles lógicos y de procedimientos están descriptos en esta Sección 6.2 en tanto que los controles de acceso físico están descriptos en la Sección 5.1 de estas Normas. A los Suscriptores se les exige, por contrato, que tomen las necesarias precauciones para prevenir la pérdida, revelación a terceros, modificación o uso no autorizado de las claves privadas o de las claves de firma que permiten su utilización.

6.2.1 Estándares y Controles de los Módulos Criptográficos

Los pares de claves de las Autoridades Certificantes dentro de los Servicios de Confianza de CertiSur S.A. son generados en módulos de hardware criptográfico apropiados, según se indica más abajo. Los pares de claves de Autoridades de Registro o de Suscriptores usuarios finales pueden ser generados tanto en módulos de hardware como de software.

Para la generación y guarda de las claves privadas de las Autoridades Primarias de Certificación y las Autoridades Certificantes Raíz Emisoras, se utilizan módulos de hardware criptográfico que están certificados o que cumplen materialmente los requerimientos de los estándares FIPS 140-1 Nivel 3. Para otras Autoridades Certificantes, se utilizan módulos de hardware criptográfico que están certificados, como mínimo, para los estándares FIPS 140-1 Nivel 2.

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

CertiSur S.A. ha implementado mecanismos técnicos y de procedimientos que requieren la participación de múltiples individuos confiables para desarrollar operaciones criptográficas sensibles de una Autoridad Certificante. Para ello, utiliza "Partición de Secreto" para dividir los datos de activación necesarios para hacer uso de la clave privada de una Autoridad Certificante entre distintas partes, denominados "Secretos Particionados", que son mantenidos por individuos entrenados y confiables, denominados "Depositarios". Una cantidad mínima de "Secretos Particionados" (m), sobre el número total de "Secretos Particionados", 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 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 Particionados son protegidos con arreglo a lo previsto en la Sección 6.4.2 de estas Normas.

6.2.3 Archivo de Claves Privadas de Suscriptores usuarios finales

Bajo un acuerdo específico, CertiSur S.A. puede resguardar claves privadas de Suscriptores usuarios finales. En estos casos, las mismas son almacenadas en formato PKCS #12, protegidas por una Clave de Firma que es generada en el proceso de creación del par de claves y enviada por medio seguro al Suscriptor usuario final.

6.2.4 Copia de Seguridad de Claves Privadas

CertiSur S.A. genera copias de resguardo encriptadas 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 por la Sección 6.2.1. Las claves privadas de Autoridades Certificantes son copiadas en módulos criptográficos de resguardo que cumplen con lo establecido en la Sección 6.2.5 de estas Normas.

Los módulos que contienen las copias de resguardo encriptadas de las claves privadas de Autoridades Certificantes están sujetos a los requerimientos establecidos por la Sección 6.2.1 de estas 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 la Sección 5.7 de estas Normas.

CertiSur S.A. no almacena copia de las claves privadas de Autoridades de Registro. Para copias de resguardo encriptadas de las claves privadas de Suscriptores usuarios finales, ver la Sección 6.2.3 más arriba.

6.2.5 Archivo de Claves Privadas de Autoridades Certificantes

Cuando los pares de claves de las Autoridades Certificantes dentro de los Servicios de Confianza de CertiSur alcanzan el final del período de vida útil, dichas claves privadas son archivadas de manera encriptada por un período de, como mínimo, cinco (5) años. Los pares de claves de Autoridades Certificantes archivados serán almacenados de manera segura utilizando módulos de hardware criptográfico que cumplen con los requerimientos establecidos por la Sección 6.2.1 de estas Normas. Procedimientos de control previenen que los pares de claves archivados sean nuevamente empleados en producción. Después de la finalización del período de archivo, las claves privadas archivadas de Autoridades Certificantes son destruidas de manera segura, con arreglo a lo establecido por la Sección 6.2.9 de estas Normas.

6.2.6 Transferencia de Claves Privadas de o hacia Dispositivos 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 incorporan copias de resguardo de pares de claves de Autoridades Certificantes en otro módulo de hardware criptográfico, dichos pares de claves son transportados entre los módulos en forma encriptada.

6.2.7 Métodos de Activación de Claves Privadas

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

6.2.7.1 Claves Privadas de Suscriptores Usuarios Finales

Esta sección regula los procedimientos de protección de los datos de activación de las claves privadas de los Suscriptores usuarios finales dentro de los Servicios de Confianza

de CertiSur. Adicionalmente, los Suscriptores tienen la opción de utilizar los mecanismos de mayor protección de claves privadas disponibles, incluyendo el uso de tarjetas smartcards, dispositivos biométricos de acceso y otros dispositivos de hardware para el almacenamiento de claves privadas. Se recomienda enfáticamente la utilización de mecanismos de autenticación que empleen dos factores (por ejemplo, hardware y contraseña, hardware y dispositivo biométrico o contraseña y dispositivo biométrico).

En caso de que el Suscriptor usuario final almacene la clave privada que se corresponde con la clave pública de su Certificado en una estación de trabajo, deberá como mínimo utilizar las siguientes medidas de protección:

- Utilizar una contraseña con arreglo a lo previsto en la Sección 6.4.1 o medidas de seguridad de fortaleza equivalente, para autenticarse 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 o usuario y contraseña de acceso a la red, y
- Tomar las medidas que resulten razonables para la protección física de su estación de trabajo, a efectos de prevenir el uso de dicha estación de trabajo y su clave privada archivada en la misma sin su autorización.

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

6.2.7.2 Claves Privadas de Administradores

6.2.7.2.1 Administradores de Servicios de Infraestructura

Los Administradores de Servicios de Infraestructura dentro de los Servicios de Confianza de CertiSur deberán como mínimo utilizar las siguientes medidas de protección de las claves privadas de sus Certificados de Administrador:

- Utilizar una tarjeta smart card, dispositivo biométrico de acceso o 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
- Tomar las medidas que resulten razonables para la protección física de su estación de trabajo, para prevenir el uso de la misma y su clave privada asociada, sin su autorización.

Se recomienda enfáticamente 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 para autenticar al Administrador antes de la activación de la clave privada.

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

6.2.7.2.2 Otros Administradores

En caso de que el Administrador almacene la clave privada que se corresponde con la clave pública de su Certificado en una estación de trabajo, deberá como mínimo utilizar las siguientes medidas de protección:

- Utilizar una contraseña con arreglo a lo previsto en la Sección 6.4.1 o medidas de seguridad de fortaleza equivalente, para autenticarse 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 o usuario y contraseña de acceso a la red, y
- Tomar las medidas que resulten razonables para la protección física de su estación de trabajo, a efectos de prevenir el uso de dicha estación de trabajo y su clave privada archivada en la misma sin su autorización.

Sin perjuicio de lo indicado, se recomienda enfáticamente la utilización de mecanismos de autenticación que empleen dos factores (por ejemplo, hardware y contraseña, hardware y dispositivo biométrico o contraseña y dispositivo biométrico).

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

6.2.7.3 Claves Privadas en Posesión de CertiSur

Las claves privadas de las Autoridades Certificantes dentro de los Servicios de Confianza de CertiSur son activadas por un número mínimo de Depositarios que suministran sus datos de activación (almacenados en dispositivos seguros) de acuerdo con lo establecido en la Sección 6.2.2 de estas Normas. Para las Autoridades Certificantes fuera de línea, la clave privada de la Autoridad Certificante es activada para una sesión (por ejemplo la certificación de una Autoridad Certificante Subordinada o en la instancia en donde una Autoridad Primaria de Certificación firma una Lista de Certificados Revocados) después de lo cual la misma es desactivada y el módulo es regresado a su lugar de almacenamiento seguro. Para las Autoridades Certificantes que operan en línea, la clave privada de la Autoridad Certificante es activada por un período de tiempo indefinido y el módulo permanece en línea en el centro de procesamiento de producción, hasta que la Autoridad Certificante sea sacada de línea (por ejemplo, por tareas de mantenimiento de sistemas). Los Depositarios de las particiones están obligados a resguardar de manera segura sus Secretos Particionados y firman un acuerdo reconociendo sus responsabilidades como Depositarios.

6.2.8 Métodos de Desactivación de Claves Privadas

Las claves privadas de las Autoridades Certificantes dentro de los Servicios de Confianza de CertiSur son desactivadas en caso de ser removidas del dispositivo de lectura. Las claves privadas de las Autoridades de Registro dentro de los Servicios de Confianza de CertiSur (utilizadas para la autenticación de la solicitud de la Autoridad 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 Administradores, Autoridades de Registro y Suscriptores usuarios finales deben ser desactivadas después de cada operación, al 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 regulado en la Sección 6.4.1 de estas Normas.

6.2.9 Métodos de Destrucción de Claves Privadas

Al finalizar el término operacional de vida útil de las Autoridades Certificantes, una o más copias de la clave privada de la Autoridad Certificante son archivadas con arreglo a lo establecido en la Sección 6.2.5 de estas Normas. Las copias restantes de la clave privada de la Autoridad Certificante son destruidas de manera segura. Adicionalmente, las claves privadas archivadas de Autoridades Certificante son destruidas, de manera segura, al término de sus períodos de archivo. Las actividades de destrucción de la clave de la Autoridad Certificante requieren la participación de múltiples individuos confiables.

Cuando es necesario, se destruyen 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. Para ello, se utilizan las funciones 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 registradas.

6.3 Otros Aspectos de la Administración de Claves

6.3.1 Archivo de Claves Públicas

Los Certificados de las Autoridades Certificantes, de las Autoridades de Registro y de los Suscriptores usuarios finales dentro de los Servicios de Confianza de CertiSur S.A tienen copias de resguardo y son archivados, como parte de los procedimientos de resguardo rutinarios.

6.3.2 Períodos de Vigencia de Certificados y de Uso de 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 están establecidos en la Tabla 8 más abajo.

Además, las Autoridades Certificantes dejan de emitir nuevos Certificados a partir de una fecha que resulte apropiada, con antelación al vencimiento del Certificado de la Autoridad Certificante, de modo tal de 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 para:	*Vigencia Certificado*	*Vigencia de Clave*
Autoridad Primaria de Certificación auto firmada (offline)	Hasta 30 años	Hasta 30 años
Autoridad Primaria de Certificación a una Autoridad Certificante	Hasta 10 años	Hasta 10 años
Autoridad Certificante a una Autoridad Certificante Subordinada	Hasta 5 años	Hasta 10 años

Autoridad Certificante a un Suscriptor usuario final	Hasta 2 años	Hasta 5 años

Tabla 8 – Períodos de Vigencia de los Certificados

Con las excepciones consideradas en esta sección, los Participantes de los Servicios de Confianza de 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 dos (2) años y hasta cinco (5) años, si se cumplimentan los siguientes requerimientos:

- Los Certificados son Certificados para individuos,
- Los pares de claves de los Suscriptores residen en dispositivos de hardware, tales como tarjetas smartcard,
- Se les exige a los Suscriptores que anualmente cumplan con los requerimientos de autenticación establecidos en la Sección 3.2.3 de estas Normas,
- Los Suscriptores deben demostrar, anualmente, que están en posesión y/o controlan la clave privada o la clave de firma que se corresponde con la clave pública contenida en el Certificado,
- Si un Suscriptor no puede completar satisfactoriamente los procedimientos de autenticación establecidos en la Sección 3.2.3 o no puede demostrar satisfactoriamente que está en posesión de la clave privada o la clave de firma según el requerimiento mencionado anteriormente, la Autoridad Certificante debe automáticamente revocar el Certificado del Suscriptor.

6.4 Datos de Activación

6.4.1 Generación e Instalación de los Datos de Activación

Los datos de activación (Secretos Particionados) utilizados para proteger los dispositivos que contienen las claves privadas de las Autoridades Certificantes 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 Particionados son registradas.

Las Autoridades de Registro dentro de los Servicios de Confianza de CertiSur deben seleccionar contraseñas fuertes para proteger sus claves privadas. Los lineamientos de CertiSur S.A. para la selección de contraseñas requieren que las mismas:

- sean generadas por el usuario;
- estén compuestas como mínimo de ocho (8) caracteres;
- contengan como mínimo un caracter alfabético y un caracter numérico;
- contengan como mínimo un caracter 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.

CertiSur S.A. recomienda enfáticamente que los Administradores, las Autoridades de Registro y los Suscriptores usuarios finales seleccionen contraseñas que cumplan con los mismos requerimientos. Recomienda además 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 particiones están obligados a proteger sus Secretos Particionados 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".

CertiSur S.A. recomienda enfáticamente que los Administradores, 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).

6.5 Controles de Seguridad Computacionales

CertiSur S.A. desarrolla todas las funciones de Autoridad Certificante y de Autoridad de Registro empleando Sistemas Confiables que cumplen con los requerimientos de la Guía de Requerimientos en materia de Seguridad y Auditoría.

6.5.1 Requerimientos Técnicos Específicos de Seguridad Computacional

CertiSur S.A. 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, CertiSur S.A. limita los accesos a los servidores de producción a aquellos individuos que resulten necesarios 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 CertiSur S.A. está segmentada de manera lógica de otros componentes. Esta segmentación impide el acceso a la red, excepto a través de procesos aplicativos definidos. CertiSur S.A. utiliza firewalls para proteger la red de producción de intrusiones internas y externas y limita la naturaleza y origen de las actividades de la red que puedan acceder a los sistemas de producción.

CertiSur exige la utilización de contraseñas que cuenten con un número mínimo de caracteres y una combinación de caracteres especiales y alfanuméricos y que dichas contraseñas sean cambiadas periódicamente.

El acceso directo a las bases de datos que soportan el Repositorio 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.

6.5.2 Calificaciones de Seguridad Computacional

Los servidores y el software que conforman los Servicios de Confianza de CertiSur S.A. se encuentran alojados en una instalación de seguridad con acceso restringido por medidas de seguridad lógicas y físicas, incluyendo pero no limitadas a tokens criptográficos, lectores de acceso biométricos con contraseñas y lectores de tarjetas de proximidad, cámaras de seguridad, barreras físicas y similares.

La instalación de seguridad implementa niveles escalonados de seguridad, donde cada nivel sucesivo proporciona un acceso más restringido y una mayor seguridad física contra la intrusión o el acceso no autorizado. Cada nivel cumple con requisitos específicos de seguridad mediante el uso de la combinación apropiada de los mecanismos de control de acceso (tales como una tarjeta de proximidad y biométrico).

Asimismo, se cuenta con un sistema de control para administrar el acceso físico de personas a áreas específicas dentro de la instalación de seguridad. Este sistema permite cumplir con los niveles de seguridad escalonados, regulando y gestionando la entrada y salida de las áreas o zonas específicas dentro de la instalación de seguridad.

El material criptográfico utilizado por los Servicios de Confianza de CertiSur S.A es almacenado en dispositivos criptográficos HSM (Hardware Security Modules) que cuentan con certificación FIPS 140-2 Nivel 3.

6.6 Controles Técnicos del Ciclo de Vida

6.6.1 Controles de Desarrollo de Sistemas

Las aplicaciones son desarrolladas e implementadas por CertiSur S.A., con arreglo a sus estándares de desarrollo de sistemas y administración de cambios. CertiSur S.A. también puede suministrar software a las Autoridades de Registro o a sus Clientes para desarrollar las funciones de Autoridad de Registro y otras tareas dentro de los Sistemas de Confianza de CertiSur. En estos casos, el software es desarrollado de acuerdo con los estándares de desarrollo de sistemas de CertiSur S.A.

6.6.2 Controles de Administración de Seguridad

CertiSur S.A. cuenta con mecanismos o políticas en vigencia para controlar y monitorear la configuración de sus sistemas de Autoridad Certificante. Además, 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 periódica a partir de allí, CertiSur S.A. 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

CertiSur S.A. desarrolla todas las funciones de las Autoridades Certificantes dentro de los Servicios de Confianza de CertiSur utilizando redes seguras, de acuerdo con las exigencias de la Guía de Requerimientos en materia de Seguridad y Auditoría, para prevenir accesos no autorizados u otras actividades maliciosas. Además, protege las comunicaciones de información sensible a través de la utilización de encriptación y firmas digitales.

7 Configuración de Certificados y Lista de Certificados Revocados

7.1 Configuración de los Certificados

Esta sección define los requerimientos para la configuración y el contenido de Certificados emitidos bajo los Servicios de Confianza de CertiSur.

Los Certificados emitidos bajo los Servicios de Confianza de CertiSur cumplimentan básicamente: (a) la Recomendación X.509 de ITU-T (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, Junio de 1997 y (b) RFC 5280[5]: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, Mayo de 2008 ("RFC 5280"). No todos los servicios de certificación permiten la utilización de la codificación UTF8String del DirectoryString.

Como mínimo, los Certificados X.509 contienen los campos básicos de X.509 Versión 3 y los valores prescriptos indicados o los valores restrictivos (value constraints) tal como se muestra en la Tabla 9 a continuación:

Campo	*Valor o Valor restrictivo (Value constraint)*
Versión	Ver la Sección 7.1.1.
Número de Serie	Valor único por Nombre Distintivo (Distinguished Name) del Emisor
Algoritmo de Firma	Nombre del algoritmo 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. El período de validez estará especificado de acuerdo con las restricciones contenidas en la Sección 6.3.2.
Nombre Distintivo (Distinguished Name) del Sujeto	Ver la sección 7.1.4
Clave Pública del Sujeto	Codificado con arreglo al RFC 5280 utilizando los algoritmos especificados en la Sección 7.1.3 y las longitudes de clave especificadas en la Sección 6.1.5.

[5] El RFC 5280 reemplazó al RFC 3280

Firma	Generada y codificada con arreglo al RFC 5280

Tabla 9 – Campos Básicos de la Configuración de Certificados

7.1.1 Número de Versión

Los Certificados de Autoridades Certificantes y de Suscriptores usuarios finales son Certificados X.509 Versión 3.

7.1.2 Extensiones de los Certificados

CertiSur S.A. completa los Certificados con las extensiones requeridas por esta Sección, según se detalla a continuación.

7.1.2.1 Extensión Uso de Claves (Key Usage)

CertiSur S.A. completa la extensión Uso de Claves (KeyUsage) con arreglo a lo establecido en la Sección 6.1.7. El campo criticidad (criticality) de esta extensión está marcado generalmente como TRUE.

7.1.2.2 Extensión Políticas de Certificación (Certificate Policies)

Los Certificados para Suscriptor usuarios finales utilizan la extensión Políticas de Certificación (Certificate Policies). La extensión Políticas de Certificación (CertificatePolicies) está completada con el identificador de objeto apropiado 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.

7.1.2.3 Extensión Nombres Alternativos del Sujeto (Subject Alternative Names)

Los Certificados de Autoridad Certificante contienen en la Extensión Nombres Alternativos del Sujeto (Subject Alternative Name) un campo Nombre de Directorio (directoryName) con un Nombre Distintivo (Distinguished Name) que identifica el rótulo identificador de la clave privada de la Autoridad Certificante.

7.1.2.4 Extensión Restricciones Básicas (Basic Constraints)

CertiSur S.A. completa los Certificados de Autoridades Certificantes con una extensión Restricciones Básicas (BasicConstraints) con el Tipo de Sujeto (Subject Type) marcado como Autoridad Certificante (CA). Los Certificados de Suscriptores usuarios finales son también completados con una extensión Restricciones Básicas (BasicConstraints) con el tipo de Sujeto (Subject Type) igual a Entidad Final (End Entity). La criticidad (criticality) de la extensión Restricciones Básicas (Basic Constraints) está generalmente marcada como TRUE.

Los Certificados de Autoridades Certificantes 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 en línea 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.

7.1.2.5 Extensión Uso de Claves Extendido (Extended Key Usage)

CertiSur S.A. hace uso de la extensión Uso de Claves Extendido (ExtendedKeyUsage) para todos los Certificados, con excepción de los Certificados Raíz.

CertiSur S.A. completa la extensión Uso de Claves Extendido (ExtendedKeyUsage) con arreglo a la Tabla 10 a continuación.

	Autoridad Certificante Raíz	*Autoridad Certificante Intermedia*	*Autoridad Certificante para Individuos*	*Certificados para Individuos*
Criticidad (Criticality)	FALSE	FALSE	FALSE	FALSE
ServerAuth	En Blanco (Clear)	En Blanco (Clear)	En Blanco (Clear	En Blanco (Clear
ClientAuth	En Blanco (Clear)	Marcado (Set)	Marcado (Set)	Marcado (Set)
CodeSigning	En Blanco (Clear)	En Blanco (Clear)	En Blanco (Clear)	En Blanco (Clear)
EmailProtection	En Blanco (Clear)	Marcado (Set)	Marcado (Set)	Marcado (Set)
TimeStamping	En Blanco (Clear)	En Blanco (Clear)	En Blanco (Clear)	En Blanco (Clear)

Tabla 10 – Variables para la Extensión Uso de Claves Extendido (ExtendedKeyUsage)

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

Los Certificados emitidos bajo los Servicios de Confianza de CertiSur 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.

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

Los Certificados emitidos bajo los Servicios de Confianza de CertiSur incluyen la extensión Identificador de Clave de la Autoridad (Authority 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. El campo criticidad (criticality) de esta extensión está marcado como FALSE.

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

El Identificador de clave (keyIdentifier) es generado en base a la clave pública del Sujeto del Certificado. El campo criticidad (criticality) de esta extensión está marcado como FALSE.

7.1.2.9 Extensión Acceso a Información de la Autoridad (Authority Information Access)

Los Certificados para Suscriptores usuarios finales y para Autoridades Certificantes Intermedias incluyen la extensión Acceso a la Información de la Autoridad (Authority Information Access), conteniendo la dirección URL en donde las Partes Confiadas pueden obtener el Certificado de la Autoridad Certificante Emisora de un Certificado.

El campo criticidad (criticality) de esta extensión está marcado como FALSE.

7.1.3 Identificadores de Objeto Algoritmo

Los Certificados están firmados con sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5), de acuerdo con el RFC 3279 o sha2WithRSAEncryption (OID: 1.2.840.113549.1.1.11) de acuerdo con el RFC 4055.

7.1.4 Formas de Nombres

Los Certificados de los Servicios de Confianza de CertiSur incluyen un Nombre Distintivo (Distinguished Name) del Emisor y del Sujeto con arreglo a lo establecido en la Sección 3.1.1 de estas Normas.

7.1.5 Restricciones de Nombres

Sin especificación.

7.1.6 Identificador de Objeto Política de Certificación

Cuando la extensión Políticas de Certificación (Certificate Policies) es utilizada, los Certificados contienen un Identificador de Objeto de la Política de Certificación (Certificate Policy Object Identifier), tal como está establecido en la Sección 1.2 de estas Normas.

Los valores utilizados para identificar la Política de Certificación de los Certificados emitidos en el marco de los Servicios de Confianza de CertiSur son los que figuran en la Tabla 11 a continuación:

Campo	*Valor*
Certificate Policy ID	1.3.6.1.4.1.12456.1.1.1
User Notice Text	CPS de CertiSur S.A. Responsabilidad Limitada (c) 2014.
CPS URL	https://www.certisur.com/legal/CPS

Tabla 11 – Valores utilizados para identificar la Política de Certificación

7.1.7 Uso de la Extensión Restricciones de Política

Sin especificación.

7.1.8 Sintaxis y Semántica de los Calificadores de Política

Los Certificados de los Servicios de Confianza de CertiSur incluyen un calificador de política (policy qualifier) dentro de la extensión Políticas de Certificación (CertificatePolicies) que apunta a la dirección URL en donde se pueden consultar estas Normas.

7.1.9 Procesamiento de la Semántica para la Extensión Políticas de Certificación Críticas

Sin especificación.

7.2 Configuración de las Listas de Certificados Revocados

Los Servicios de Confianza de CertiSur emiten Listas de Certificados Revocados que cumplen con el RFC 5280[6]. Como mínimo, las Listas de Certificados Revocados contienen los campos básicos y los contenidos especificados en la Tabla 12 a continuación:

Campo	*Valor o Valor restrictivo*
Versión	Ver la Sección 7.2.1.
Algoritmo de firma	Algoritmo empleado para firmar la Lista de Certificados Revocados (CRL). Las Listas de Certificados Revocados (CRL) están firmadas utilizando sha1WithRSAEncryption (OID 1.2.840.113549.1.1.5), en un todo de acuerdo con RFC 3279 o sha2WithRSAEncryption (OID: 1.2.840.113549.1.1.11), de acuerdo con el RFC 4055.
Emisor	Entidad que ha firmado y emitido la Lista de Certificados Revocados (CRL). El Nombre del Emisor de la Lista de Certificados Revocados (CRL Issuer Name) está de acuerdo con los requerimientos para el Nombre Distintivo del Emisor (Issuer Distinguished Name) especificados en la Sección 7.1.4.
Día y Hora de Vigencia	Día y hora de la emisión de la Lista de Certificados Revocados (CRL). Las Listas de Certificados Revocados 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 12 – Campos Básicos de la Configuración de la Lista de Certificados Revocados (CRL)

[6] El RFC 5280 reemplazó al RFC 3280

7.2.1 Número de Versión

CertiSur S.A. emite actualmente Listas de Certificados Revocados X.509 Versión 2.

7.2.2 Extensiones Lista de Certificados Revocados y Entrada a la Lista de Certificados Revocados

CertiSur S.A. completa las Listas de Certificados Revocados con las Extensiones que se indican en los puntos 7.2.2.1 y 7.2.2.2, tal como se indica a continuación.

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

Las Listas de Certificados Revocados emitidas bajo los Servicios de Confianza de CertiSur incluyen la extensión Identificador de Clave de la Autoridad (Authority 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 la Lista de Certificados Revocados.

7.2.2.2 Extensión Número de Lista de Certificados Revocados (CRL Number)

La extensión Número de Lista de Certificados Revocados (CRL Number) se completa con un número que indica la secuencia progresiva para un alcance determinado de esa Lista y para un emisor específico de dicha Lista.

8 Revisiones y Auditorias de cumplimiento

Anualmente, se desarrolla una auditoría para Autoridades Certificantes sobre el Centro de Procesamiento de Datos de CertiSur y las operaciones de administración de claves que soportan los Servicios de Confianza de CertiSur. CertiSur S.A. está facultado para requerir que las Autoridades de Registro y Clientes bajo acuerdos específicos lleven a cabo una Auditoría de Cumplimiento y/o programas de auditoría con arreglo a esta sección.

Además de las Auditorías de Cumplimiento, CertiSur S.A. está facultado para desarrollar otras revisiones e investigaciones para asegurar la confiabilidad de los Servicios de Confianza de CertiSur, que incluyen, pero no están limitadas a:

- CertiSur S.A. o su representante autorizado están facultados, a su sola y exclusiva discreción, para efectuar en cualquier momento una Auditoría Investigativa sobre una Autoridad de Registro o un Cliente, en caso de que CertiSur S.A. o su representante autorizado tengan razones para suponer que la entidad auditada ha fallado en el cumplimiento de los Requerimientos establecidos en las presentes Normas, ha sufrido un incidente o Compromiso de seguridad o ha actuado o dejado de actuar de modo tal que dicha falla, incidente o Compromiso o la actuación o falta de ella signifique una amenaza real o potencial a la seguridad o integridad de los Servicios de Confianza de CertiSur.
- CertiSur S.A. o su representante autorizado están facultados para efectuar Revisiones Complementarias de Administración del Riesgo sobre una Autoridad de Registro o un Cliente, luego de detectar cuestiones incompletas 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.

CertiSur S.A. o su representante autorizado 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 CertiSur S.A. y al personal responsable de la ejecución de la auditoría, revisión o investigación.

8.1 Frecuencias o Circunstancias para Efectuar Evaluaciones

Las Auditorías de Cumplimiento son desarrolladas anualmente.

8.2 Identidad y Calificaciones Profesionales del evaluador

Las Auditorías de Cumplimiento de las Autoridades Certificantes son desarrolladas por un auditor profesional matriculado que:

- Demuestre acabado conocimiento en tecnología de infraestructura de clave pública, técnicas y herramientas de seguridad de información, auditoría de seguridad y funciones de certificación hacia terceros, y
- Los profesionales a cargo de la tarea estén inscriptos en el Consejo Profesional de Ciencias Económicas de la Ciudad Autónoma de Buenos Aires o entidad similar y estén 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 y capacitación continua.

8.3 Relación entre el Auditor y la Entidad Auditada

Las Auditorías de Cumplimiento de las operaciones de los Servicios de Confianza de CertiSur son desarrolladas por un profesional que es independiente de CertiSur S.A.

8.4 Puntos a Cubrir durante la Evaluación

El alcance de la auditoría anual para Autoridades Certificantes 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.

8.5 Acciones a Tomar como Consecuencia de Deficiencias

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

8.6 Comunicación de los Resultados

Anualmente, se publicará en el Repositorio el dictamen de la Auditoría Anual de Cumplimiento realizada.

No obstante lo puntualizado, los informes del auditor con los resultados de la Auditoría de Cumplimiento de las operaciones de los Servicios de Confianza de CertiSur serán tratados por el personal gerencial de CertiSur S.A. bajo reglas estrictas de confidencialidad, a fin de no afectar la seguridad de dichas operaciones.

9 Asuntos Legales y otros temas

9.1 Precios

9.1.1 Precios de Emisión y Renovación de Certificados

CertiSur S.A., las Autoridades de Registro y los Clientes bajo acuerdos específicos están facultados para cobrar aranceles a los Suscriptores usuarios finales, en concepto de emisión, administración y renovación de Certificados.

9.1.2 Precios por Acceso a Certificados

CertiSur S.A., las Autoridades de Registro y los Clientes no cobran arancel alguno como condición para que los Certificados estén disponibles en un repositorio para Partes Confiadas.

9.1.3 Precios por Revocación o Información sobre el Estado

CertiSur S.A. no cobra arancel alguno como condición para que las Listas de Certificados Revocados requeridas con arreglo a lo previsto en la Sección 4.9.7 estén disponibles, en un repositorio o de otra forma, para Partes Confiadas. No obstante ello, CertiSur S.A. podrá percibir 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.

CertiSur S.A. no permite el acceso a la información sobre la revocación, información respecto del estado de Certificados o de sello de tiempo en su repositorio, a efectos de que terceros suministren productos o servicios que utilizan dicha información respecto del estado del Certificado, sin su previo consentimiento expreso y por escrito.

9.1.4 Precios por Otros Servicios

CertiSur S.A. no percibe arancel alguno para acceder al texto de 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 CertiSur S.A., quién es titular de los derechos de propiedad intelectual del presente documento.

9.1.5 Política de Reembolso

CertiSur S.A. y las Autoridades de Registro dentro de los Servicios de Confianza de 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 S.A y/o la correspondiente Autoridad de Registro le revoque el certificado dentro de los quince (15) días corridos posteriores a su emisión y le reembolse el costo del mismo. Después de finalizado este período, un suscriptor puede solicitar que CertiSur S.A. y/o la Autoridad de Registro correspondiente le revoquen el certificado y le reembolsen el costo del mismo, sólo si alguno de ellos ha incumplido con una obligación material bajo estas Normas, relacionada con el suscriptor o con su certificado. Después que CertiSur S.A. 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. Para solicitar un reembolso, el suscriptor deberá comunicarse al departamento de Atención al Cliente. Esta política de reembolso no constituye una indemnización, por no resultar procedente indemnización alguna en los presentes casos.

9.2 Responsabilidad Patrimonial – Cobertura de Seguros

CertiSur S.A. mantiene vigente una cobertura de seguro por errores y omisiones

9.3 Confidencialidad de la Información del Negocio – Alcance de la Información Confidencial

Los documentos de seguridad considerados confidenciales por CertiSur S.A. no están disponibles públicamente. Los documentos de seguridad confidenciales incluyen los documentos identificados como tales en la Tabla 1, Sección 1.1(a).

9.4 Privacidad de Datos Personales

La privacidad es un aspecto de gran preocupación para la mayoría de los usuarios de Internet y constituye un aspecto sumamente crítico para que la experiencia de los mismos como tales resulte satisfactoria y gratificante. CertiSur S.A. es consciente y sensible a las inquietudes con respecto a este tema, de los suscriptores de los servicios y de los restantes visitantes de su sitio, en relación a los servicios que se brindan.

Tanto CertiSur S.A. como las Autoridades de Registro solicitan información personal de parte de los Suscriptores usuarios finales, con el propósito de autenticar la identidad de los mismos y, por lo tanto, asegurar confianza e integridad como parte de los servicios de certificación que desarrollan.

9.4.1 Relación con Otras Entidades

El sitio Web de CertiSur puede contener vínculos a otros sitios. CertiSur S.A. no asume ningún tipo de responsabilidad con respecto a las prácticas relativas a la privacidad, ni formula ningún tipo de declaración sobre el tema, respecto de los titulares de esas otras páginas.

9.4.2 Información Solicitada a los Visitantes del Sitio Web

CertiSur S.A. no recoge ningún tipo de información personal de parte de los visitantes a su sitio, sin que la misma sea explícitamente solicitada y provista voluntariamente por los mismos. Si un visitante simplemente consulta nuestra página, no se recolecta información personal alguna. Existen solamente dos formas mediante las cuales un visitante puede explícitamente proveer y consentir voluntariamente que CertiSur S.A. recolecte información personal:

> **Correo electrónico**: CertiSur puede utilizar vínculos a través de su sitio que suministran al visitante la posibilidad de contactarse por medio de correo electrónico, a fin de realizar preguntas o proveer comentarios y sugerencias. Adicionalmente, CertiSur puede ofrecer al visitante la oportunidad de que un representante se contacte personalmente, para suministrar información adicional respecto de algún producto o servicio. Para ello, CertiSur puede requerir algún tipo

de información personal adicional, que resulta relevante o necesaria exclusivamente para satisfacer dicho requerimiento.

Solicitudes: Durante el proceso de llenado de una solicitud de los Certificados dentro de los Servicios de Confianza de CertiSur, se requiere del solicitante cierta información, como por ejemplo nombre y apellido, dirección, número de teléfono, dirección de correo electrónico, número de tarjeta de crédito, número de documento de identidad, número de Clave única de identificación tributaria (CUIT) o situación frente al Impuesto al Valor Agregado (IVA).

9.4.3 Utilización de la Información Recolectada

CertiSur S.A. responde todos los correos electrónicos y otras consultas que recibe. Por ello, puede almacenar esa correspondencia, con el objetivo de mejorar sus productos, servicios y sus páginas Web.

CertiSur S.A. puede comparar la información suministrada en la Solicitud de un Certificado con los datos contenidos en una base de datos de propiedad de un tercero. Esta comparación se realiza a fin de autenticar la identidad y otros atributos del solicitante. Todos los terceros cuyas bases de datos son utilizadas, han suscripto acuerdos de confidencialidad que prohíben la difusión o utilización futura de la información suministrada, en la medida en que ésta no sea de carácter público.

Tanto las presentes Normas como las páginas de solicitud de un Certificado indican explícitamente qué información aparecerá en el Certificado emitido. Normalmente esta información se limita a nombre y dirección de correo electrónico, aunque en algunos casos se podrá incorporar información adicional (número de identificación ante el empleador, nombre de la organización con la cual el Suscriptor está vinculado, etc.).

Asimismo, un solicitante de un certificado, puede voluntariamente escoger que se incluya una determinada parte de la información contenida en la solicitud (tal como se expresa y explica en la correspondiente página de solicitud) en su Certificado digital. Esta información es denominada normalmente "información de personalización". Esta prestación opcional puede ser ofrecida para permitir que algunos sitios puedan leer y utilizar la información de personalización, a fin de suministrarle al solicitante del certificado un servicio específico o para permitir una registración más rápida y apropiada en los mismos.

9.4.4 Publicación de Certificados Digitales en el Repositorio

La publicación de Certificados en un archivo que resulte accesible (un repositorio) es un aspecto inherente a la posibilidad de su utilización. Esta publicación es una práctica mundialmente reconocida y habitual. Estas Normas exigen que se publiquen todos los certificados dentro de sus Servicios de Confianza de CertiSur. Consecuentemente, un suscriptor no debe esperar ningún tipo de privacidad respecto del contenido de su certificado digital. CertiSur S.A. no revela, comercializa o pone a disposición de terceros, de otra manera, ningún tipo de información personal que no se encuentre explicitada en el certificado digital.

9.4.5 Posibilidad de ser Eliminado de la Lista de Contactos

Frecuentemente, CertiSur S.A. se contacta con los suscriptores para brindar información respecto de los servicios ofrecidos. Si un Suscriptor desea ser eliminado de la lista de receptores de dicha información, contáctese con:

CertiSur S.A.
Atención al Cliente
Av. Santa Fe 788 – 2º Piso
(1059) Buenos Aires

No obstante lo expuesto, CertiSur S.A. se reserva el derecho de notificar a sus suscriptores cualquier información que pueda afectar la seguridad de los Servicios de Confianza de CertiSur S.A.

9.4.6 Política con Respecto a la Actualización o Corrección de Datos

CertiSur S.A. no puede corregir o actualizar la información contenida en un Certificado sin destruir su integridad, dado que cada Certificado es firmado digitalmente como parte imprescindible del proceso de emisión del mismo. Si posteriormente se modificara o eliminara información contenida en un Certificado, la firma digital de la Autoridad Certificante emisora no podría verificar el nuevo contenido del mismo. Más aún, si posteriormente el Suscriptor firmara digitalmente un mensaje con su clave privada, el receptor no estaría en condiciones de verificar dicha firma (creada utilizando su clave privada), debido a que el Certificado habría sido alterado después de la creación del correspondiente par de claves. Por lo tanto, no está prevista la modificación de los Certificados, según lo previsto en la Sección 4.8 de estas Normas.

9.4.7 Información Considerada de Carácter Privado

Los siguientes registros de los Suscriptores son mantenidos en forma confidencial y privada, sujeto a lo dispuesto por la Sección 9.4.8 a continuación:

- Registros de solicitudes de Autoridad Certificante, independientemente de que hayan sido aprobadas o rechazadas,
- Registro de Solicitudes de Certificado,
- Registros de transacciones (los registros de las transacciones como así también los registros de auditoría de dichas transacciones),
- Registros de auditoría,
- Planes de contingencia y de recupero ante desastres, y
- Medidas de seguridad para el control de las operaciones del hardware y software y la administración del servicio de Certificados y servicios de solicitudes especificados.

9.4.8 Información no Considerada de Carácter Privado

Los Participantes de los Servicios de Confianza de CertiSur reconocen que los Certificados y la información de la revocación o estado de los Certificados, el Repositorio y la información contenida en el mismo 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 9.4.7 no será considerada como confidencial ni como privada, sujeto a las leyes que resulten de aplicación en materia de privacidad.

9.4.9 Revelación Debido a Procesos Administrativos o Judiciales

CertiSur S.A. está facultado para revelar Información Confidencial o Privada si la misma le es requerida judicialmente o por organismos administrativos, en el marco de procesos judiciales, administrativos u otros procesos legales, durante una acción civil o administrativa, tales como citaciones, interrogatorios, solicitud de pruebas, etc., sujeto a las leyes que resulten de aplicación en materia de privacidad.

9.4.10 Circunstancias para la Revelación de Otra Información

No contempladas.

9.5 Derechos de Propiedad Intelectual

Los temas concernientes a los Derechos de Propiedad Intelectual entre CertiSur S.A. y terceros, con excepción de los Suscriptores usuarios finales y las Partes Confiadas, se rige por los acuerdos que resulten de aplicación entre los mismos. Por lo tanto, las estipulaciones que se indican a continuación son aplicables a los Derechos de Propiedad Intelectual en relación con Suscriptores usuarios finales 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, considerados en sí mismos, y de la información de revocación de los mismos. Se permite 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. También está permitida 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

CertiSur S.A. mantiene en forma exclusiva todos los Derechos de Propiedad Intelectual con respecto a las presentes Normas.

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 a 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, 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 y los Certificados raíz que las contienen, incluyendo todas las claves públicas de las Autoridades Certificantes son propiedad de CertiSur S.A. Finalmente y sin limitar la generalidad de lo mencionado

anteriormente, la clave privada de una Autoridad Certificante es propiedad de la Autoridad Certificante y dicha Autoridad Certificante mantiene en forma exclusiva todos los Derechos de Propiedad Intelectual relacionados con dicha clave privada.

9.6 Declaraciones y Garantías

9.6.1 Declaraciones y Garantías de la Autoridad Certificante

Las Autoridades Certificantes desarrollan las obligaciones específicas incluidas a lo largo de las presentes Normas.

Adicionalmente, CertiSur S.A. efectúa los esfuerzos que comercialmente resultan razonables para asegurar que los Acuerdos del Suscriptor y los Acuerdos del Receptor Confiado obliguen a los Suscriptores y a las Partes Confiadas dentro de los Servicios de Confianza de CertiSur. Ejemplos de estos esfuerzos incluyen, pero no se limitan a, requerir la aceptación del Acuerdo del Suscriptor como condición para solicitar un Certificado, o requerir la aceptación del Acuerdo del Receptor Confiado como condición para recibir información respecto del estado de un Certificado. Del mismo modo, las Autoridades de Registro y los Clientes bajo acuerdos específicos (cuando esté requerido contractualmente) deben utilizar los Acuerdos del Suscriptor y los Acuerdos del Receptor Confiado, con arreglo a los requerimientos impuestos por CertiSur S.A..

Los Clientes de CertiSur S.A. bajo acuerdos específicos pueden utilizar Acuerdos del Suscriptor especiales, sin que ello resulte obligatorio.

El otorgamiento de garantías y los límites de responsabilidad entre CertiSur S.A., sus Autoridades de Registro y Clientes bajo acuerdos específicos están establecidos y se rigen por los acuerdos entre ellos. Esta sección se refiere solamente a las garantías que las Autoridades Certificantes dentro de los Servicios de Confianza de CertiSur deben otorgar a Suscriptores usuarios finales que reciben los Certificados de ellas y a las Partes Confiadas, a los rechazos de garantías que ellas deben efectuar con respecto a dichos Suscriptores y Partes Confiadas y las limitaciones de responsabilidad respecto de dichos Suscriptores y Partes Confiadas.

9.6.1.1 Garantías de la Autoridad Certificante a Suscriptores y Partes Confiadas

Los Acuerdos del Suscriptor deben incluir una garantía hacia los suscriptores respecto de:

- 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, y
- Los servicios de revocación y el uso de un repositorio se efectúan de acuerdo con las presentes Normas en todos sus aspectos relevantes.

Los Acuerdos del Receptor Confiado contienen una garantía hacia las Partes Confiadas que razonablemente confían en un certificado, respecto de:

- La veracidad de toda la información contenida en el Certificado o incorporada por referencia al mismo, con excepción de la Información No Verificada del Suscriptor.
- En el caso de los Certificados publicados en el Repositorio, los Certificados han sido emitidos para el individuo o la organización nominada en el Certificado como Suscriptor y el Suscriptor ha aceptado el Certificado con arreglo a lo previsto en la Sección 4.4 de estas Normas, y
- Las entidades que aprueban la Solicitud de Certificado y emiten el Certificado han cumplido sustancialmente con estas Normas cuando emiten el Certificado.

9.6.2 Declaraciones y Garantías de las Autoridades de Registro

Las Autoridades de Registro asisten a las Autoridades Certificantes desarrollando funciones de validación, aprobando o rechazando Solicitudes de Certificado, requiriendo la revocación de Certificados y aprobando las solicitudes de renovación.

Las Autoridades de Registro deberán realizar los esfuerzos que resulten razonables para que los Acuerdos del Suscriptor y los Acuerdos del Receptor Confiado, vinculen y obliguen a los Suscriptores y a las Partes Confiadas, en un todo de acuerdo con lo previsto en las Secciones 9.6.3 y 98.6.4 de estas Normas.

Las garantías, rechazos de garantías y limitaciones de responsabilidad entre una Autoridad de Registro y la Autoridad Certificante a la que está asistiendo en el proceso de emisión de los Certificados, o al Cliente bajo un acuerdo específico, si resultara aplicable, están establecidos y se rigen por los acuerdos entre ellos.

CertiSur S.A., en nombre de todas las Autoridades Certificantes de los Servicios de Confianza de CertiSur, incluye dentro de los Acuerdos del Suscriptor y los Acuerdos del Receptor Confiado las garantías, rechazos de garantías, limitaciones de responsabilidad y cláusulas contemplando fuerza mayor, establecidas en las presentes Normas y que se detallan en las Secciones a continuación.

9.6.3 Declaraciones y Garantías de los Suscriptores

Las obligaciones de un Suscriptor usuario final resultan de aplicación a través de estas Normas, en función de su aceptación del Acuerdo del Suscriptor vigente, publicado en: **https://www.certisur.com/legal**.

El Acuerdo del Suscriptor exige que los Solicitantes de Certificados suministren información completa y veraz en sus Solicitudes de Certificado y manifiesten su conformidad con el Acuerdo del Suscriptor que resulte aplicable, como condición para obtener un Certificado.

El Acuerdo del Suscriptor recepta las obligaciones específicas contenidas en estas Normas y exigen que los Suscriptores utilicen sus Certificados con arreglo a lo establecido por la Sección 1.4 de estas Normas. También exige que los Suscriptores protejan sus claves privadas de acuerdo con lo previsto en el Capítulo 6 de estas Normas. Con arreglo a lo determinado en el Acuerdo del Suscriptor, si un suscriptor descubre o tiene razones para suponer que ha existido Compromiso de su Clave Privada del Suscriptor o del dato de activación que la protege, o la información contenida en el Certificado es incorrecta o se ha modificado, el Suscriptor debe inmediatamente:

- Notificar a la entidad que aprobó su Solicitud de Certificado, ya sea que se trate de una Autoridad Certificante o una Autoridad de Registro, de acuerdo con lo previsto en la Sección 4.9.1 y solicitar la revocación del Certificado, con arreglo a lo establecido por la Sección 4.9.3 de estas Normas, y

- Notificar a cualquier persona que el Suscriptor estime razonablemente que pueda confiar o proveer servicios en función de su Certificado o en una firma digital verificable con referencia al mismo.

El Acuerdo del Suscriptor exige asimismo que los Suscriptores cesen en la utilización de sus claves privadas al finalizar el período de utilización de sus claves, según lo previsto en la Sección 6.3.2 de estas Normas.

El Acuerdos del Suscriptor establece que los Suscriptores no pueden monitorear, interferir o alterar la implementación técnica de los Servicios de Confianza de CertiSur y no pueden, de ninguna manera, comprometer intencionalmente la seguridad de los mismos.

9.6.3.1 Garantías del Suscriptor

El Acuerdo del Suscriptor requiere que los Suscriptores garanticen que:

- Cada firma electrónica creada utilizando la clave privada que se corresponde con la clave pública contenida en el Certificado o empleando la clave de firma es la firma electrónica del Suscriptor y el Certificado ha sido aceptado y está vigente (es decir no ha vencido ni ha sido revocado) en el momento en que dicha firma es creada,
- Ninguna persona no autorizada ha tenido acceso jamás a la clave privada o a la clave de firma del Suscriptor,
- Todas las declaraciones efectuadas por el Suscriptor al completar la Solicitud del Certificado que ha enviado son verdaderas,
- Toda la información suministrada por el Suscriptor y contenida en el Certificado es verdadera,
- El Certificado es utilizado exclusivamente para propósitos autorizados y legales, de conformidad con la legislación aplicable y con estas Normas, y
- El Suscriptor es un Suscriptor usuario final y no una Autoridad Certificante y no utiliza la clave privada que se corresponde con cualquier clave pública contenida en el Certificado con el propósito de firmar electrónicamente cualquier Certificado (o cualquier otro formato de clave pública certificada), o una Lista de Certificados Revocados como Autoridad Certificante o en cualquier otro carácter.

9.6.3.2 Compromiso de una Clave Privada

Estas Normas establecen los requerimientos dentro de los Servicios de Confianza de CertiSur para la protección de las claves privadas de los Suscriptores, que están incluidas en función de lo establecido en la Sección 6.2.7 y en el Acuerdo del Suscriptor. Dicho Acuerdo establece que los Suscriptores que no cumplen con dichos requerimientos son los únicos responsables por cualquier pérdida o daño que resulte de dicho incumplimiento.

9.6.4 Declaraciones y Garantías de las Partes Confiadas

Las obligaciones de una Parte Confiada resultan de aplicación a las Partes Confiadas a través de estas Normas, en función del Acuerdo del Receptor Confiado vigente, que se encuentra publicado en: **https://www.certisur.com/legal/rpa**.

El Acuerdo del Receptor Confiado establece que 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. Dicho Acuerdo

establece que CertiSur S.A., las Autoridades Certificantes y las Autoridades de Registro no son responsables por la evaluación de la procedencia o no del uso de un Certificado. El Acuerdo del Receptor Confiado específicamente establece que las Partes Confiadas no pueden utilizar Certificados más allá de las limitaciones establecidas en la Sección 1.4.1 y para propósitos prohibidos, según lo previsto en la Sección 1.4.2 de estas Normas.

El Acuerdo del Receptor Confiado también establece que 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. Con arreglo a este Acuerdo, las Partes Confiadas podrán confiar en un Certificado cuando dichos procedimientos de verificación arrojen resultados satisfactorios.

El Acuerdo del Receptor Confiado también exige que las Partes Confiadas verifiquen el estado de un Certificado en el cual ellos desean confiar, como así también el estado de todos los Certificados en su Cadena de Certificación, de acuerdo con lo establecido por la Sección 4.9.6 y concordantes. Si cualquiera de los Certificados de la Cadena de Certificación ha sido revocado, la Parte Confiada no debe confiar en el Certificado del Suscriptor usuario final ni en ninguno de los otros Certificados revocados en la Cadena de Certificación.

Finalmente, el Acuerdo del Receptor Confiado establece que el consentimiento de sus términos es la condición esencial para utilizar o confiar de cualquier otra forma en los Certificados emitidos dentro de los Servicios de Confianza de CertiSur. Los Receptores Confiados que también son Suscriptores acuerdan estar obligados por los términos del Acuerdo del Receptor Confiado bajo esta sección, la renuncia a otorgar garantías y las limitaciones de responsabilidad, cuando ellos prestan conformidad a un Acuerdo del Suscriptor.

El Acuerdo del Receptor Confiado establece que si todas las verificaciones descriptas más arriba arrojan resultado satisfactorio, la Parte Confiada está en condiciones de confiar en el Certificado, en la medida en que la confianza en dicho Certificado resulte razonable bajo las circunstancias del caso. Si las circunstancias indican la necesidad de seguridades adicionales, la Parte Confiada debe obtener las seguridades que estime razonable, para poder contar con dicha confianza.

El Acuerdo del Receptor Confiado establece que las Partes Confiadas no pueden monitorear, interferir o alterar la implementación técnica de los Servicios de Confianza de CertiSur y no pueden, de ninguna manera, comprometer intencionalmente la seguridad de los mismos.

Los Acuerdos del Suscriptor y del Receptor Confiado requieren que las Partes Confiadas reconozcan que han tenido la suficiente información para tomar una decisión apropiada, compatible con el grado de confianza que ellos elijan asignar a la información contenida en el Certificado, que ellos son los únicos responsables respecto de la decisión de confiar o no en dicha información y que ellos asumen las consecuencias legales en el caso de fallar en el cumplimiento de las obligaciones que asumen, según las presentes Normas, al hacer uso de los Servicios de Confianza de CertiSur.

9.7 Descargo de Responsabilidad y Rechazo de Garantías

Con el alcance permitido por la ley aplicable, el Acuerdo del Suscriptor y el Acuerdo del Receptor Confiado cualquier posible garantía de CertiSur S.A., incluida cualquier garantía de comerciabilidad o aplicabilidad para un propósito en particular.

9.8 Limitaciones de Responsabilidad

Con el alcance permitido por la ley aplicable, el Acuerdo del Suscriptor y el Acuerdo del Receptor Confiado limitan la responsabilidad de CertiSur S.A. Las limitaciones de responsabilidad suponen la exclusión de responsabilidad por daños y perjuicios fortuitos o imprevistos, directos o indirectos. Dichos Acuerdos también incluyen el tope máximo de Diez Mil Pesos ($ 10.000,00) respecto de la responsabilidad de CertiSur S.A. por daños y perjuicios, concernientes a un Certificado específico:

9.9 Indemnizaciones

9.9.1 Indemnización por parte de Suscriptores

Con el alcance permitido por la ley aplicable, el Acuerdo del Suscriptor requiere que los Suscriptores indemnicen a CertiSur S.A. y a cualquier otra Autoridad Certificante o Autoridad de Registro distinta de CertiSur S.A. por:

- Falsedad o tergiversación de hecho por parte del Suscriptor en la Solicitud de su Certificado,
- Omisión por parte del Suscriptor de revelar un hecho relevante en su 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 su clave privada, o
- El uso de parte del Suscriptor de un nombre (incluyendo sin limitación alguna al nombre común, el nombre de dominio o una dirección de correo electrónico) que infrinja los Derechos de Propiedad Intelectual de terceros.

9.9.2 Indemnización por parte de Partes Confiadas

El Acuerdo del Suscriptor y el Acuerdo del Receptor Confiado requieren que las Partes Confiadas indemnicen a CertiSur S.A. y a cualquier otra Autoridad de Registro distinta de CertiSur S.A. 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.

9.10 Enmiendas

9.10.1 Procedimientos para Enmiendas

Las modificaciones a las presentes Normas son efectuadas por CertiSur S.A. Las modificaciones pueden ser presentadas en la forma de un documento conteniendo las enmiendas a las Normas vigentes o bien como una actualización de las mismas. Las versiones corregidas o actualizadas están publicadas en el Repositorio en **https://www.certisur.com/legal/actualizaciones**. Las actualizaciones suplantan cualquier especificación aludida o conflictiva de la versión referenciada de las Normas.

9.10.2 Ítems que Pueden Cambiar sin Notificación

CertiSur S.A. 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 S.A. de calificar a una modificación como material o no está sujeta a la exclusiva discrecionalidad de CertiSur S.A.

9.10.3 Ítems que Pueden Cambiar mediando Notificación

CertiSur S.A. puede efectuar cambios a las Normas para el Proceso de Certificación que considere sustanciales, con arreglo a lo previsto en la Sección 9.10.4 de estas Normas.

9.10.4 Mecanismo de Notificación y Plazos

9.10.4.1 Mecanismo de Notificación

CertiSur S.A. colocará las enmiendas propuestas a estas Normas en la sección Actualizaciones y Notificaciones del Repositorio localizada en: **https://www.certisur.com/legal/actualizaciones**. CertiSur S.A. podrá solicitar que otros Participantes también presenten propuestas de enmienda. Si CertiSur S.A. considera que dicha enmienda es conveniente y propone la implementación de la misma, efectuará la notificación correspondiente con arreglo a lo establecido en esta sección.

Sin perjuicio que cualquier disposición de las presentes Normas estipulen lo contrario, si CertiSur S.A. considera que resulta necesario efectuar modificaciones materiales a las mismas para detener o prevenir una falla de seguridad de los Servicios de Confianza de CertiSur, estará facultado para efectuar dichas modificaciones, mediante su publicación en el Repositorio, las cuales entrarán en vigencia en forma inmediata.

9.10.4.2 Período para Comentarios

Con excepción de lo establecido en el segundo párrafo de la Sección 9.10.4.1, el período para comentarios para cualquier enmienda material a las presentes Normas será de quince (15) días, que comenzarán en la fecha en que la modificación sea incluida en el Repositorio. Cualquier Participante estará facultado para enviar comentarios a CertiSur S.A. hasta la finalización del período para comentarios.

9.10.4.3 Mecanismo para el Tratamiento de Comentarios

CertiSur S.A. considerará cualquier comentario respecto de las modificaciones propuestas y 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, según lo establecido en la Sección 9.10.2, o (c) descartar las modificaciones propuestas. CertiSur S.A. está facultado para descartar cualquier modificación propuesta, mediante notificación en la sección Actualizaciones y Notificaciones del Repositorio de CertiSur S.A. Salvo que las enmiendas propuestas sean modificadas o rechazadas, se transformarán en efectivas al finalizar el período para comentarios establecido en la Sección 9.10.4.2.

9.11 Mecanismos de Resolución de Disputas

9.11.1.1 Disputas entre CertiSur S.A. y Clientes

Las disputas entre CertiSur S.A. y cualquiera de sus Clientes deberán ser resueltas con arreglo a las disposiciones del acuerdo aplicable entre las partes.

9.11.1.2 Disputas con Suscriptores Usuarios Finales o Partes Confiadas

Con el alcance permitido por la ley aplicable, el Acuerdo del Suscriptor y el Acuerdo del Receptor Confiado incluyen una cláusula de resolución de disputas.

9.12 Ley y Jurisdicción Aplicables

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, 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, 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. 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.

9.13 Misceláneos

9.13.1 Acuerdo Íntegro

Con el alcance permitido por la ley aplicable, el Acuerdo del Suscriptor y el Acuerdo del Receptor Confiado contienen cláusulas relacionadas con la divisibilidad, continuidad, acuerdo completo y notificaciones. Una cláusula de divisibilidad en un acuerdo previene que cualquier determinación de invalidez o inejecutabilidad de una cláusula en dicho acuerdo, afecte la validez del resto del mismo. Una cláusula de continuidad determina cuáles de las disposiciones de un acuerdo continuarán en vigencia, independientemente de la rescisión o finalización del mismo. Una cláusula de acuerdo completo establece que todos los entendimientos relacionados con el asunto que es sujeto del acuerdo están incorporados en dicho acuerdo. Una cláusula de notificaciones en un acuerdo establece la forma en que las partes efectuarán las notificaciones a la otra parte.

9.13.2 Fuerza Mayor

Con el alcance permitido por la ley aplicable, el Acuerdo del Suscriptor y el Acuerdo del Receptor Confiado incluyen una cláusula que protege a CertiSur S.A. y a las Autoridades Certificantes y Autoridades de Registro dentro de los Servicios de Confianza de CertiSur en caso de fuerza mayor.

9.13.3 Varios

Queda establecido y los Acuerdos del Suscriptor y del Receptor Confiado así lo deben manifestar, que resulta inexistente cualquier otra relación jurídica diferente de la que surge de los mismos entre CertiSur S.A. o una Autoridad de Registro diferente de CertiSur S.A., por un lado, y un Suscriptor o una Parte Confiada, por el otro.
