DECLARACIÓN DE PRACTICAS DE CERTIFICACIÓN

V1.0

ALPHASIDE.COM

Gabriel Araujo E6-136 y José María Batodano. Quito, Ecuador
(593 2) 2814291 / 3281146 / 2811 516

contacto@alphaside.com

Contenido

1. INFORMACION GENERAL

1.1. Control de Versiones

Fecha	Versión	Descripción	Realizado por	Aprobado por
1-jul-2023	1	Creación del documento	Steven Chiriboga	Mónica Maldonado

1.2. Marco Legal

- Ley de Comercio Electrónico, Firmas y Mensajes de Datos, vigente.
- Reglamento a la Ley de Comercio Electrónico, vigente.
- Resolución No. ARCOTEL-CTHB-CTDS-2022-0225 con la que la Agencia de Regulación y Control de las Telecomunicaciones con la que acredita ante el Estado Ecuatoriano a Alpha Technologies.

2. INTRODUCCION

Alpha Technologies es una Entidad de Certificación de Información y Servicios Relacionados inscrita en el Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y Terceros Vinculados a cargo de la Agencia de Regulación y Control de las Telecomunicaciones con el fin de complementar el servicio de Seguridad Digital para sus Clientes.

Los Servicios de Certificación de Información y Servicios Electrónicos Relacionados ofrecidos por Alpha Technologies están dirigidos a Personas Naturales y Jurídicas.

La presente Declaración de Prácticas de Certificación especifica las condiciones, políticas y procedimientos aplicables a la solicitud, emisión, uso, suspensión y revocación de los certificados de firma electrónica así como para la prestación de servicios relacionados y contiene:

1. Datos de identificación de la Entidad de Certificación de Información y Servicios Relacionados Acreditada.
2. Condiciones de manejo de la información suministrada por los usuarios.
3. Límites de responsabilidad en la prestación de servicios de certificación de información y servicios relacionados con la firma electrónica.
4. Obligaciones de la Entidad de Certificación de Información y Servicios Relacionados Acreditada en la prestación de servicios de certificación de información y servicios relacionados con la firma electrónica.
5. Obligaciones de los usuarios y precauciones que deben observar en el manejo, uso y custodia de certificados y claves.

6. Políticas de manejo de los certificados de firma electrónica.
7. Políticas y condiciones de manejo de servicios relacionados con la firma electrónica.
8. Garantías en el cumplimiento de las obligaciones que se deriven de sus actividades.
9. Costos y tarifas de los servicios de certificación de información y servicios relacionados con la firma electrónica.

Esta Declaración de Prácticas de Certificación está tomada de las normas que se emplean dentro de la Entidad de Certificación de Información y Servicios Relacionados vinculadas al ciclo de vida de los certificados digitales y los controles para garantizar el servicio.

1.1 NOMBRE DEL DOCUMENTO E IDENTIFICACION

Este documento es la Declaración de Practicas de Certificación de Alpha Technologies.

Versión: 1.0
Identificador OID: 1.3.6.1.4.1.56105.1
Fecha Emisión: 1-julio-2023
Publicación: www.alphaside.com
Publicación certificado raíz: www.alphaside.com

1.2 Identificadores de Certificados

OID	Tipo de Certificado
1.3.6.1.4.1.56105.2.4	Persona Natural
1.3.6.1.4.1.56105.2.2	Representante Legal

1.3 Participantes de la PKI

1.3.1 Autoridad de certificación (CA)

La CA realiza tareas relacionadas con la gestión del ciclo de vida, emisión, renovación, distribución y revocación de los certificados de firma electrónica. La CA proporciona el estado de los certificados de firma electrónica por medio de la lista de revocación de certificados (CRL) y por el protocolo de estado de certificados en línea (OCSP). Garantiza la disponibilidad de todos los servicios relacionados con la gestión de los certificados de firma electrónica.

1.3.2 Proveedor de Servicios de Certificación Digital (GlobalSign)

Los proveedores de servicios de certificación digital son terceros que prestan su infraestructura PKI y servicios tecnológicos a la Entidad de Certificación de Información y Servicios Relacionados Alpha Technologies, garantizando la continuidad del servicio a los suscriptores, a través de un Acuerdo de Servicios e Infraestructura (ASI).

1.3.3 Autoridad de registro (AR)

Cualquier Entidad Jurídica delegada por la Autoridad Certificadora. Es responsable de la identificación y autenticación de los solicitantes de certificados de firma electrónica. La AR puede iniciar los procesos de renovación, reemisión y revocación de los certificados de firma electrónica.

Alpha Technologies podrá actuar como Autoridad de Registro de los Certificados que expida.

La AR será responsable de:

- Aceptar, evaluar, aprobar o rechazar el registro de solicitudes de Certificado;
- Registro de Suscriptores para los servicios de certificación;
- Proporcionar sistemas para facilitar la identificación de los Suscriptores (según el tipo de Certificado solicitado);
- Usar documentos o fuentes de información notariados oficialmente o autorizados de otro modo para evaluar y autenticar la solicitud de un Solicitante;
- Solicitar la emisión de un Certificado a través de un proceso de autenticación de múltiples factores luego de la aprobación de una solicitud;
- Hacer entrega del certificado al suscriptor o de los medios para su generación;
- Custodiar la documentación relativa a la identificación y registro de los firmantes y/o suscriptores y gestión del ciclo de vida de los certificados;

Los terceros que establezcan una relación contractual con Alpha Technologies podrán operar su propia RA y autorizar la emisión de Certificados. Los terceros deben cumplir con todos los requisitos de esta DPC y los términos de su contrato.

1.3.4 Usuarios (Suscriptores)

Los usuarios son personas naturales o jurídicas que solicitan y reciben con éxito los certificados de firma electrónica. Los usuarios solicitan su certificado de firma electrónica a la autoridad de registro y entregan la documentación necesaria para realizar el proceso de autenticación.

1.3.5 Solicitantes

Los solicitantes son personas naturales o jurídicas, que a nombre propio o en presentación de un tercero, solicita los servicios de certificación y previa identificación solicitan la emisión de un certificado de firma electrónica a la CA.

1.3.6 Terceros que Confían

Terceros que confían son todas aquellas personas naturales o jurídicas que deciden aceptar y confiar en forma libre y voluntaria en los certificados emitidos por la CA a un titular. La CA no asume ningún tipo responsabilidad ante terceros que no hayan verificado la vigencia de los certificados y las limitaciones de uso.

1.4 Uso de certificados

Un Certificado permite a una entidad que participa en una transacción electrónica demostrar su identidad a otros participantes en dicha transacción.

1.4.1 Uso apropiado del Certificado

Los certificados se utilizan en entornos comerciales como un equivalente digital de una tarjeta de identificación, no tienen una limitante técnica, administrativa, financiera, tramites tributarios, tramites de importaciones o exportaciones, etc. para su uso.

Los certificados de Alpha Technologies se pueden utilizar para transacciones de dominio público que requieran:

- **Compromiso de no repudio/contenido**. Una parte no puede negar haber realizado la transacción o haber enviado el mensaje electrónico.
- **Autenticación.** La garantía para una entidad de que otra entidad es quien dice ser.
- **Integridad** La garantía para una entidad de que los datos no han sido alterados (intencionalmente o no) del remitente al destinatario y desde el momento de la transmisión hasta el momento de la recepción.

El suscriptor podrá hacer uso del certificado según lo establecido a continuación:

- Autenticación
- Firma electrónica de documentos
- Correos electrónicos
- Cifrado de transacciones y archivos
- Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

1.4.2 Uso prohibido del Certificado

Los certificados sólo podrán ser empleados para los usos para los que hayan sido emitidos y especificados en esta DPC.

Los certificados no garantizan que el sujeto sea confiable, que opere en una empresa de buena reputación o que el equipo en el que se haya instalado el certificado no esté libre de defectos, malware o virus.

Los certificados emitidos bajo este DPC no se pueden utilizar:

- Para cualquier aplicación o mecanismo donde los problemas con el certificado puedan causar un riesgo de seguridad (por ejemplo, riesgo humano o ambiental)
- Donde esté prohibido por la ley
- El certificado de firma electrónica emitido por Alpha Technologies, deberá ser utilizado tal y como es suministrado. Queda prohibida cualquier alteración del certificado por parte del usuario.

1.5 Administración de la Política

1.5.1 Organización que administra el documento

Nombre: Alpha Technologies Cia. Ltda.
Dirección: Gabriel Araujo E6-136 y José María Batodano
Ciudad: Quito
Teléfono: 593 2 2814291
Correo electrónico: contacto@alphaside.com
Página web: www.alphaside.com

1.5.2 Persona de Contacto

Nombre: Alpha Technologies Cia. Ltda.
Dirección: Gabriel Araujo E6-136 y José María Batodano
Ciudad: Quito
Teléfono: 593 2 2814291
Correo electrónico: contacto@alphaside.com
Página web: www.alphaside.com

1.5.3 Persona que determina la idoneidad de la DPC

La persona que determina la idoneidad de la DPC es el Responsable de la Entidad de Certificación de Alpha Technologies.

1.5.4 Procedimiento de aprobación de la DPC

El Responsable de la CA de Alpha Technologies revisa y aprueba cualquier cambio en la DPC. Tras la aprobación de una actualización de la DPC por parte de la CA, se controlan las versiones del documento y se publica en la página de Alpha Technologies en www.alphaside.com.

La versión actualizada es vinculante para todos los Suscriptores, incluido los Suscriptores y las partes que confían en los Certificados que se han emitido en virtud de una versión anterior de la DPC.

2 PUBLICACION DE INFORMACION Y RESPONSABILIDAD DE REPOSITORIO

2.1 Repositorio

Alpha Technologies publica la lista de los certificados emitidos, el estatus de los certificados, DPC y la información relativa a los servicios de certificación.
La CA garantiza que los datos del servicio estén disponibles a través de dicho repositorio las 24 horas del día, los 7 días de la semana.

2.2 Publicación de Información del Certificado

La información de los certificados estará disponible en https://www.alphaside.com

2.3 Frecuencia de Publicación

Los Certificados de la CA se publican en un Repositorio a través de páginas de soporte tan pronto como sea posible después de la emisión.

2.4 Controles de acceso a los repositorios

La CA pone los repositorios a disposición del público en modo de solo lectura.

Se implementan medidas de seguridad lógica y física para evitar que personas no autorizadas agreguen, eliminen o modifiquen entradas del repositorio.

3 IDENTIFICACION Y AUTENTICACION

Alpha Technologies actúa como AR, verifica y autentica la identidad y otros atributos de un Solicitante antes de la inclusión de esos atributos en un Certificado.

Esta sección describe los procedimientos específicos y criterios aplicados por las Autoridades de Registro (AR) en el momento de autenticar la identidad del solicitante y aprobar la emisión de un certificado.

3.1 Nombres

3.1.1 Tipos de Nombres

Los certificados se emiten con DN de asunto (Distinguished Names) que cumplen los requisitos de denominación X.500, denominación RFC-822 y denominación X.400. Los DN respetan la unicidad del espacio de nombres y no son engañosos.

3.1.2 Necesidad de que los nombres sean significativos

Los campos del DN referentes al nombre y apellidos corresponderán con los datos registrados legalmente del suscriptor, comprensibles en lenguaje natural.

En los casos en que el certificado permite el uso de un rol y donde se incluye el campo de OU en el DN, se pueden agregar elementos únicos adicionales al DN dentro del campo de OU para permitir que las Partes de Confianza diferencien entre los certificados con los Elementos comunes DN.

3.1.3 Anónimos o seudónimos de los Suscriptores

Alpha Technologies no admite anónimos ni seudónimos para identificar el nombre de una persona natural o jurídica, o para vincular o identificar los datos de un certificado con una persona natural.

3.1.4 Reglas para interpretar varias formas de nombres

Los nombres distinguidos en los Certificados se interpretan utilizando los estándares X.500 y la sintaxis ASN.1.

3.1.5 Unicidad de los nombres

El nombre distintivo de los certificados será único para cada suscriptor y está relacionado con el Número de Identificación o equivalente.

Un suscriptor puede pedir más de un certificado siempre que la combinación de los siguientes valores existentes en la solicitud fuera diferente de un certificado válido:

- Número de Identificación Fiscal (RUC) u otro identificador legalmente válido de la persona natural.
- Número de Identificación u otro identificador legalmente válido de la persona natural.
- Tipo de certificado (OID de identificador de política de certificación).
- Soporte del certificado (software o en dispositivo seguro de creación de firma)

3.1.6 Reconocimiento, autenticación y función de las marcas registradas

Los Suscriptores no podrán solicitar Certificados con cualquier contenido que infrinja los derechos de propiedad intelectual de un tercero. Alpha Technologies no exige que se verifique el derecho del Solicitante a utilizar una marca comercial. Alpha Technologies se reserva el derecho de rechazar una solicitud de certificado o revocar cualquier certificado que esté involucrado en una disputa. Alpha Technologies no asume responsabilidad en la emisión de certificados que hagan uso de una marca registrada.

3.2 Validación Inicial de Identidad

Alpha Technologies a través de su AR, hará uso de mecanismos apropiados para validar la identidad del suscriptor, cuya identidad resulta fijada en el momento de la firma del contrato entre Alpha Technologies y el suscriptor.

3.2.1 Prueba de Posesión de la Clave Privada

Las claves son generadas por el propio suscriptor del certificado sin intervención de terceros. La posesión de la clave privada se demuestra en virtud del procedimiento fiable de entrega y aceptación del certificado por el suscriptor.

Cuando se expide un certificado en un dispositivo hardware, la clave privada se crea en el instante previo a la generación del certificado, mediante un procedimiento que garantiza su confidencialidad y su vinculación con la identidad del solicitante.

Cada Tercero Vinculado es responsable de garantizar la entrega del dispositivo al solicitante de forma segura.

3.2.2 Autenticación de la Identidad de una Persona Jurídica – Representante Legal

La AR verificara los siguientes datos para poder autenticar la identidad de la organización:

- RUC, en donde se encuentran los datos relativos a la denominación o razón social de la organización.
- Documento de Constitución de la empresa o similar.
- Nombramiento del Representante legal. En caso de no estar registrado en la Superintendencia de Compañías, se solicita adicionalmente un documento notariado indicando que los estatutos de la empresa no han cambiado.
- Cedula de Identidad de la Persona Natural, pasaporte u otro medio idóneo reconocido en derecho para la identificación del representante.

La validación de la Persona Jurídica se hará mediante el siguiente procedimiento:

1. El solicitante deberá acreditar su identidad por uno de los siguientes métodos:

   1.1. De forma presencial, identificándose ante el operador de la AR, mostrando la documentación solicitada.

   1.2. De forma remota, identificándose electrónicamente a través del sistema de video en línea mediante:
   - Mostrar su documento de identidad.
   - Previo a la sesión por video, deberá enviar la documentación solicitada.

2. El solicitante proporcionara la información como sigue:
   - Documento. RUC, en donde se encuentran los datos relativos a la denominación o razón social de la organización.
   - Documento de Constitución de la empresa o similar.
   - Documento. Nombramiento del Representante legal. En caso de no estar registrado en la Superintendencia de Compañías, se solicita adicionalmente un documento notariado indicando que los estatutos de la empresa no han cambiado.
   - Documento. Cedula de Identidad de la Persona Natural, pasaporte u otro medio idóneo reconocido en derecho para la identificación del representante.

3. El operador de la AR comprobara la identidad del solicitante del siguiente modo:

   3.1. Cuando la identificación se realice de forma presencial, a través de la revisión de:
   - Cedula de Identidad.
   - Documentación que acredite su denominación como representante legal.

   3.2. Cuando la identificación se realice de forma remota, a través de la revisión de:
   - Preguntas de los datos de identidad del solicitante.
   - El solicitante se exhibirá en la videollamada junto con su cedula de identidad. El operador captará el video como evidencia para registrarlo.
   - Previo a la sesión por video, revisara la información entregada por el solicitante.

La AR deberá guardar la documentación acreditativa de la validez de aquellos datos solicitados al subscriptor.

Alpha Technologies se reserva el derecho de no emitir el certificado si considera que la documentación aportada no es suficiente o adecuada para la comprobación de los datos anteriormente citados.

3.2.3 Autenticación de la Identidad de una Persona Natural

La AR verificara los siguientes datos para poder autenticar la identidad de la persona natural:

- Cedula de Identidad de la Persona Natural, pasaporte u otro medio idóneo reconocido en derecho para la identificación del representante.

La validación de la Persona Natural se hará mediante el siguiente procedimiento:

1. El solicitante deberá acreditar su identidad por uno de los siguientes métodos:

1.1. De forma presencial, identificándose ante el operador de la AR, mostrando la documentación solicitada.

1.2. De forma remota, identificándose electrónicamente a través del sistema de video en línea mediante:
- Mostrar su documento de identidad.

2. El solicitante proporcionara la información como sigue:
- Documento. Cedula de Identidad de la Persona Natural, pasaporte u otro medio idóneo reconocido en derecho para la identificación del representante.

3. El operador de la AR comprobara la identidad del solicitante del siguiente modo:

3.3. Cuando la identificación se realice de forma presencial, a través de la revisión de:
- Cedula de Identidad.

3.4. Cuando la identificación se realice de forma remota, a través de la revisión de:
- Preguntas de los datos de identidad del solicitante.
- El solicitante se exhibirá en la videollamada junto con su cedula de identidad. El operador captará el video como evidencia para registrarlo.

La AR deberá guardar la documentación acreditativa de la validez de aquellos datos solicitados al subscriptor.

Alpha Technologies se reserva el derecho de no emitir el certificado si considera que la documentación aportada no es suficiente o adecuada para la comprobación de los datos anteriormente citados.

3.2.4 Información de solicitante no verificada

Alpha Technologies no incluye información de suscriptor no verificada en los certificados emitidos.

En la solicitud del certificado el solicitante debe proporcionar documentos y datos personales que lo identifican absolutamente, toda la información solicitada es verificada aún si no hace parte de la información incluida en el certificado digital.

3.2.5 Validación de Autoridad de Registro

Para la constitución de una Autoridad de Registro Alpha Technologies realiza las verificaciones necesarias para confirmar la existencia de la organización mediante sus propias fuentes de información.

Se inician actividades por medio de un contrato entre las partes firmado por un representante autorizado, en donde se estipulan las responsabilidades entre las cuales están:

- Verificar y validar la identidad de los nuevos operadores de la AR. La AR deberá enviar a Alpha Technologies la documentación correspondiente al nuevo operador, así como su autorización para que actúe como operador.
- Asegurar que los operadores de la AR hayan recibido formación suficiente para el desempeño de sus funciones.

Para la prestación de servicios Alpha Technologies se asegura de que los operadores de la AR accedan al sistema de forma segura.

4 Requisitos operativos del ciclo de vida del certificado

4.1 Solicitud de Certificado

4.1.1 Quién puede presentar una solicitud de certificado

La solicitud de un certificado se admite para cualquier persona natural mayor de edad legalmente capaz para contratar y obligarse de cumplir con las responsabilidades inherentes al uso de dicho certificado.

4.1.2 Proceso de inscripción y responsabilidades

Alpha Technologies mantiene sistemas y procesos que autentican suficientemente la identidad del Solicitante para todos los tipos de Certificados que presentan la identidad a las Partes que Confían.

Los solicitantes deben enviar información suficiente para permitir que Alpha Technologies y cualquier AR de Alpha Technologies realicen con éxito la verificación requerida.

Alpha Technologies y los AR protegerán las comunicaciones y almacenarán de forma segura la información presentada por el Solicitante durante el proceso de solicitud.

Alpha Technologies deslinda toda responsabilidad concerniente a solicitudes de certificados y registros de suscriptores realizados con suplantación de identidad o datos fraudulentos.

El proceso de solicitud de un certificado digital tiene generalmente los siguientes pasos:

- Llenar el correspondiente formulario con toda la información requerida. No toda la información requerida en el proceso de registro aparecerá en el certificado y será conservada de manera confidencial por la AR.
- Suscribir el correspondiente contrato de prestación de servicios. La firma de esos documentos contractuales presupone la aceptación del certificado electrónico y todas las obligaciones y responsabilidades descritas en esta DPC.
- Pagar cualquier tarifa aplicable.

Se deberá acompañar a la solicitud, la documentación justificativa, de acuerdo con lo establecido en la sección 3.2.3.

4.2 Procesamiento de solicitudes de certificados

4.2.1 Realización de funciones de identificación y autenticación

La verificación de identidad es realizada por el equipo de validación de Alpha Technologies como se establece en la Sección 3.2 o por las AR bajo contrato.

Antes de procesar las solicitudes, la AR se asegura de que las solicitudes del certificado sean completas, precisas y estén debidamente suscritas. Para estos efectos el solicitante autoriza y faculta expresamente a Alpha Technologies y a su AR, verificar la información entregada con otras bases de datos públicas o privadas.

La AR comprobara y validara la información y los documentos que son requeridos para solicitar los certificados digitales.

La AR mantendrá un archivo con la información que respalde cada solicitud realizada para la emisión de los certificados por el plazo de cinco 5 años.

Los clientes pueden solicitar un certificado de reemplazo ("reemisión"), que sigue el proceso de un nuevo certificado. Cuando corresponda, la información del Certificado puede reutilizarse.

Si en algún momento la información del nombre del Sujeto incorporada en un Certificado cambia de alguna manera, se deben volver a realizar los procedimientos descritos en este documento.

4.2.2 Aprobación o Rechazo de Solicitudes de Certificado

Alpha Technologies rechazará las solicitudes de Certificados cuando no se pueda completar con éxito la validación de todos los elementos.

Suponiendo que todos los pasos de validación se puedan completar con éxito siguiendo los procedimientos de esta DPC, Alpha Technologies generalmente aprobará la solicitud de certificado.

Alpha Technologies puede rechazar solicitudes incluso por los siguientes motivos:

- Basándose en un posible daño a la marca de Alpha Technologies, al Proveedor de Servicios, a las AR o a los suscriptores al aceptar la solicitud.
- Puede rechazar solicitudes de Certificados de Solicitantes que hayan sido rechazados anteriormente o que hayan violado previamente una disposición de su Acuerdo de Suscriptor.

Alpha Technologies no tiene la obligación de proporcionar un motivo a un Solicitante por el rechazo de una Solicitud de certificado.

Alpha Technologies notifica al solicitante la aprobación o denegación de la solicitud.

4.2.3 Tiempo para procesar las solicitudes de certificados

Alpha Technologies se asegurará de que se utilicen todos los métodos razonables para evaluar y procesar las solicitudes de Certificados, de acuerdo a un orden de llegada. Cuando ocurran problemas fuera del control de Alpha Technologies, Alpha Technologies se esforzará por mantener al Solicitante debidamente informado.

Las solicitudes se mantienen activas hasta su aprobación o rechazo.

Una vez validada la información proporcionada por el suscriptor, si el resultado de la validación es positivo, la AR enviará a la AC la autorización de la emisión del certificado de manera inmediata.

4.3 Emisión de certificados

4.3.1 Acciones de la CA durante la Emisión de Certificados

Una vez aprobada la solicitud de certificación la CA a través de la AR procederá a la emisión del certificado digital, que será entregado de forma segura al suscriptor.

La CA se asegurara que la AR sea capaz de generar la emisión de Certificados mediante a autenticación de múltiples factores.

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

Alpha Technologies notificará al Suscriptor la emisión de un Certificado a la dirección de correo electrónico que le haya proporcionado el Suscriptor durante el proceso de registro o por cualquier otro medio equivalente. El correo electrónico puede contener el Certificado en sí o un enlace para descargar el Certificado solicitado.

4.4 Aceptación del Certificado

4.4.1 Conducta que constituye la aceptación del certificado

La aceptación del certificado digital se da el momento en que los titulares de los certificados expresan la aceptación de los términos y condiciones contenidos en el contrato de aceptación de condiciones de los servicios de certificación.

La CA informará al Suscriptor que no podrá utilizar el Certificado hasta que el Suscriptor haya revisado y verificado la exactitud de los datos incorporados en el Certificado. A menos que el Suscriptor notifique a la AR dentro de los siete (7) días posteriores a la recepción, el Certificado se considerará aceptado.

Un suscriptor puede enviar un mensaje de no aceptación del certificado en el que el mensaje incluye el motivo del rechazo y se identifican los motivos, o de ser el caso los campos en el certificado que son incorrectos o incompletos.

4.4.2 Publicación del Certificado por la AC

La AC publica el Certificado entregándolo al Suscriptor y también puede publicarlo en uno o más Registros de transparencia de certificados. Además, la AC puede publicar el Certificado en un directorio como LDAP.

4.4.3 Notificación de Emisión de Certificados por parte de la CA a Otras Entidades

Las RA, Alpha Technologies y otras entidades pueden ser informadas de la emisión si participaron en la inscripción inicial.

4.5 Uso de pares de claves y certificados

4.5.1 Uso del certificado y la clave privada del suscriptor

Los Suscriptores deben proteger su Clave Privada teniendo cuidado de evitar la divulgación a terceros. El Contrato del Suscriptor identifica las obligaciones del Suscriptor con respecto a la protección de la clave privada. Las claves privadas solo se deben usar como se especifica en los campos de uso de clave apropiado.

Cuando sea posible hacer una copia de seguridad de una Clave privada, los Suscriptores deben usar el mismo nivel de cuidado y protección atribuido a la Clave privada en vivo. Al final de la vida útil de una Clave privada, los Suscriptores deben eliminar de forma segura la Clave privada y cualquier fragmento en que se haya dividido con fines de copia de seguridad.

4.5.2 Uso del certificado y la clave pública de la parte que confía

Dentro de esta DPC, la AC proporciona las condiciones bajo las cuales las Partes que confían pueden confiar en los Certificados, incluidos los servicios de Certificado apropiados disponibles para verificar la validez del Certificado, como CRL y/u OCSP.

Es responsabilidad de los terceros verificar el estado del certificado mediante los servicios ofrecidos por Alpha Technologies concretamente para ello y especificados en el presente documento.

4.6 Renovación del Certificado

Renovación de Certificado significa la emisión de un Certificado con un nuevo período de validez que finaliza después del período de validez del Certificado anterior, pero sin cambiar la Clave Pública del Suscriptor o de otro participante o cualquier otra información en el Certificado.

Las solicitudes de renovación de Certificado se procesan como nuevas solicitudes de Certificado cuando la Clave Pública del Suscriptor o de otro participante o cualquier otra información en el Certificado es diferente.

4.6.1 Circunstancias para la Renovación del Certificado

La renovación del certificado se produce cuando éste va a expirar y el suscriptor desea continuar usando un certificado. Para esto el suscriptor deberá presentar una solicitud de renovación y realizar el mismo proceso utilizado para solicitar un certificado.

La renovación del Certificado se puede realizar a pedido del Suscriptor o un representante autorizado del Suscriptor.

La renovación del Certificado solo se puede realizar si el Certificado original no ha sido revocado ni suspendido.

4.6.2 Quién puede solicitar la renovación

Las solicitudes de renovación deben ser presentadas por el Suscriptor del Certificado o su representante autorizado.

4.6.3 Tramitación de Solicitudes de Renovación de Certificados

Para procesar una solicitud de renovación, la AC debe verificar la solicitud con el Suscriptor o su representante autorizado.

Una solicitud de renovación de certificado se procesa de igual manera que la solicitud inicial de un certificado.

4.6.4 Notificación de Emisión de Nuevo Certificado al Suscriptor

Según 4.3.2

4.6.5 Conducta que Constituye Aceptación de un Certificado de Renovación

Según 4.4.1

4.6.6 Publicación del Certificado de Renovación por parte de la AC

Según 4.4.2

4.6.7 Notificación de Emisión de Certificados por parte de la AC a Otras Entidades

Según 4.4.3

4.7 Renovación de clave de certificado

Renovación de clave de Certificado significa la emisión de un nuevo Certificado con una Clave Pública diferente, pero sin cambiar el período de validez o cualquier otra información en el Certificado.

Las solicitudes de cambio de clave de certificado se procesan como nuevas solicitudes de certificado cuando se cambia el período de validez o cualquier otra información en el certificado es diferente.

4.7.1 Circunstancias para la renovación de claves del certificado

El cambio de clave del certificado se puede realizar a pedido del Suscriptor o por un representante autorizado del Suscriptor.

Se puede solicitar la renovación de la clave del certificado en caso de compromiso de la clave privada del certificado.

La renovación de la clave del certificado solo se puede realizar si el Certificado original no ha sido revocado ni suspendido.

4.7.2 Quién puede solicitar la certificación de una nueva clave pública

Las solicitudes de renovación de clave deben ser presentadas por el Suscriptor del Certificado o su representante autorizado.

4.7.3 Procesamiento de solicitudes de cambio de clave de certificado

Para procesar una solicitud de cambio de clave, Alpha Technologies verifica la solicitud con el Suscriptor o su representante autorizado. Las solicitudes de renovación de clave de certificado se procesan como nuevas solicitudes de certificado.

4.7.4 Notificación de Emisión de Nuevo Certificado al Suscriptor

Según 4.3.2

4.7.5 Conducta que Constituye Aceptación de un Certificado de nueva clave

Según 4.4.1

4.7.6 Publicación del Certificado de Nueva Clave por parte de la AC

Según 4.4.2

4.7.7 Notificación de Emisión de Certificados por parte de la AC a Otras Entidades

Según 4.4.3

4.8 Modificación del Certificado

La modificación del Certificado significa la emisión de un nuevo Certificado debido a cambios en la información del Certificado distinta de la Clave Pública del Suscriptor.

Las solicitudes de modificación de Certificado se procesan como nuevas solicitudes de Certificado cuando se cambia el período de validez o la Clave Pública del Suscriptor es diferente.

4.8.1 Circunstancias para la Modificación del Certificado

La modificación del certificado se puede realizar a pedido del Suscriptor o un representante autorizado del Suscriptor.

4.8.2 Quién puede solicitar la modificación del certificado

Las solicitudes de modificación deberán ser presentadas por el Suscriptor del Certificado o su representante autorizado.

4.8.3 Procesamiento de Solicitudes de Modificación de Certificados

Para procesar una solicitud de modificación, Alpha Technologies verifica la solicitud con el Suscriptor o su representante autorizado.

Las solicitudes de modificación de certificados se procesan como nuevas solicitudes de certificados.

4.8.4 Notificación de Emisión de Nuevo Certificado al Suscriptor

Según 4.3.2

4.8.5 Conducta que constituye la aceptación del certificado modificado

Según 4.4.1

4.8.6 Publicación del Certificado Modificado por la AC

Según 4.4.2

4.8.7 Notificación de Emisión de Certificados por parte de la AC a Otras Entidades

Según 4.4.3

4.9 Revocación y Suspensión de Certificados

La revocación de un certificado supone la pérdida de validez definitiva del mismo, y es irreversible.

La suspensión (o revocación temporal) de un certificado supone la pérdida de validez temporal del mismo, y es reversible.

La reactivación de un certificado supone su paso de estado suspendido a estado activo.

4.9.1 Circunstancias para la revocación

Antes de realizar una revocación, la AR verificará la autenticidad de la solicitud de revocación.

La revocación de un Certificado de Suscriptor se realiza dentro de las veinticuatro (24) horas en las siguientes circunstancias:

1. El Suscriptor o el administrador de la organización solicita la revocación del Certificado a través de una solicitud autenticada al equipo de soporte de Alpha Technologies o a la AR.
2. El Certificado fue mal utilizado.
3. El Suscriptor violó cualquiera de sus obligaciones materiales en virtud del Contrato.
4. Por algún cambio sustancial en la información contenida en el Certificado.
5. Descubrimiento de que el Certificado no se emitió de conformidad con los Requisitos básicos de Alpha Technologies.
6. Descubrimiento de que alguno de los datos contenidos en el certificado es incorrecto.
7. La Clave Privada del Suscriptor correspondiente a la Clave Pública del Certificado sufrió un Compromiso de Clave.
8. Si hay evidencia clara de que el método específico utilizado para generar la clave privada fue defectuoso.
9. Finalización de la relación jurídica de prestación de servicios entre Alpha Technologies y el suscriptor.
10. Alpha Technologies considerará, entre otras cosas, la naturaleza y el número de quejas recibidas, la identidad de los denunciantes, la legislación pertinente vigente y las respuestas al supuesto uso nocivo por parte del Suscriptor.
11. Fallecimiento de un Suscriptor.
12. Alpha Technologies cesa sus operaciones por cualquier motivo y no ha hecho arreglos para que otra CA brinde soporte de revocación para el Certificado.

4.9.2 Circunstancias para la Suspensión

La suspensión de certificados se puede utilizar cuando un administrador deshabilita temporalmente los certificados de los clientes. Dichas situaciones pueden incluir:

- Cuando así sea solicitado por el suscriptor o la persona natural identificada en el certificado por:
  - La pérdida temporal de certificados.
  - La salida temporal de los usuarios de la organización, etc.
  - Si se sospecha el compromiso de una clave, hasta que este hecho sea confirmado o desmentido.

- Si no disponen de toda la información necesaria para determinar la revocación de un certificado.
- Si el suscriptor ha incurrido en falta de pago de su certificado.
- Sea dispuesto por el ARCOTEL, de conformidad en lo previsto en la ley de Comercio electrónico, firmas electrónicas y mensajes de datos

A diferencia de la revocación de certificados que desactiva un certificado de forma permanente, un administrador puede levantar el estado de suspensión del certificado para reactivar el certificado a solicitud del suscriptor.

4.9.3 Quién puede solicitar la revocación y suspensión de certificados

Alpha Technologies y las AR aceptarán solicitudes de revocación autenticadas. La autorización de revocación se aceptará si la solicitud de revocación se recibe del Suscriptor o de una organización afiliada nombrada en el Certificado. Los Suscriptores, las Partes que confían, los Proveedores de software de aplicación y otros terceros pueden enviar Informes de problemas de certificados para notificar a Alpha Technologies de una sospecha de causa razonable para revocar el Certificado.

4.9.4 Procedimiento para Solicitud de Revocación o Suspensión

Alpha Technologies y sus AR registrarán cada solicitud de revocación y autenticarán la fuente, tomando las medidas apropiadas para revocar el Certificado si la solicitud es auténtica y aprobada.

La solicitud se receptara, en forma presencial, vía telefónica o correo electrónico y deberá incorporar la siguiente información:

- Fecha de solicitud
- Identidad del suscriptor.
- Nombre y título de la persona que pide solicita.
- Información de contacto de la persona que solicita.
- Razón detallada para la petición de revocación.

Si se asiste personalmente el suscriptor o firmante quedará autenticada mediante su cédula de identidad o pasaporte y se podrá proceder a la revocación inmediata del certificado, posterior al llenado de la solicitud de revocación.

Si lo hace vía telefónica, la AR autentica las peticiones comprobando que provienen de una persona autorizada. Puede ser por medio de una carta pidiendo la revocación del certificado firmada electrónicamente.

Si lo hace vía correo electrónico, la AR autentica las peticiones comprobando que provienen de una persona autorizada. Puede ser por medio de una carta pidiendo la revocación del certificado firmada electrónicamente.

Una vez que la solicitud ha sido aprobada la AR realiza las siguientes acciones:

- Comunica a la CA su aprobación para la revocación del certificado mediante el sistema web con control de acceso y la protección de un canal SSL, y se informara al suscriptor.
- Una copia de dicha solicitud firmada será enviada a la CA y almacenada en la AR.

Las revocaciones y suspensiones tienen efecto desde el momento en que aparecen publicadas en las CRL.

En caso que no se acepte la revocación, se dejará constancia de los hechos que motivaron dicha denegatoria.

4.9.5 Plazo dentro del cual la CA debe procesar la solicitud de revocación o suspensión

Una vez la identidad del suscriptor haya sido autenticada según lo expuesto anteriormente, y la revocación debidamente tramitada por AR, la revocación se hará efectiva inmediatamente.

Si la solicitud se realiza dentro del horario ordinario de operación se procesara inmediatamente.

Si la solicitud se realiza fuera del horario ordinario de operación será procesada el siguiente día hábil.

4.9.6 Requisitos de verificación de revocación para las partes que confían

Antes de confiar en un Certificado, las Partes que confían deben validar la idoneidad del Certificado para el propósito previsto y asegurarse de que el Certificado sea válido; de lo contrario, todas las garantías quedarán anuladas.

Las partes que confían deberán consultar la información de CRL o OCSP para cada certificado en la cadena, así como también validar que la cadena de certificados en sí esté completa.

Las partes que confían deben tener en cuenta que debido a que las CRL se emiten en plazos establecidos, puede haber un período directamente después de la revocación y antes de la próxima generación de CRL en el que OCSP y CRL no devuelvan el mismo estado. En los

casos en que se produzcan diferencias entre CRL y OCSP, se debe suponer que OCSP es el más preciso.

Alpha Technologies incluye URL aplicables dentro del Certificado para ayudar a las Partes que confían en realizar el proceso de verificación de revocación.

4.9.7 Frecuencia de emisión de CRL

La CA actualiza las CRL dentro de las 24 horas posteriores a la revocación o suspensión de un certificado.

4.9.8 Latencia máxima para CRL

Las CRL se publican en el repositorio dentro de un tiempo comercialmente razonable después de su generación.

4.9.9 Disponibilidad del Sistema en Línea de Verificación del Estado de los Certificados

La información relativa al estado de los certificados estará disponible en línea las 24 horas del día, los 7 días de la semana.

En caso de fallo del sistema, o cualquier otro factor que no esté bajo el control de la AC, ésta realizará los mayores esfuerzos para asegurar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo de 24 horas.

Cuando la CA admite respuestas OCSP además de CRL, los tiempos de respuesta OCSP generalmente no superan los 10 segundos en condiciones normales de funcionamiento de la red. Las respuestas de OCSP cumplen con RFC6960 y/o RFC5019.

4.9.10 Requisitos de verificación de revocación en línea

Los respondedores OCSP operados por la AC DEBERÁN admitir el método HTTP GET, como se describe en RFC 6960 y/o RFC 5019.

La AC deberá actualizar la información proporcionada a través de un Respondedor OCSP dentro de las 24 horas posteriores a la revocación de un Certificado de AC.

Los Respondedores OCSP que reciban una solicitud de estado de un Certificado que no ha sido emitido, no responderán con un estado "good" para dichos Certificados. Los Respondedores OCSP para las AC que no están técnicamente restringidas, no responderán con un estado "good" para dichos Certificados.

La CA requerirá que las solicitudes OCSP contengan los siguientes datos:

- Versión del protocolo
- Petición de servicio

- Identificador de certificado de destino

4.9.11 Otras formas de anuncios de revocación disponibles

Sin estipulación.

4.9.12 Requisitos especiales relacionados con compromiso de clave

La AC y cualquiera de sus AR utilizarán métodos comercialmente razonables para informar a los Suscriptores que su Clave privada puede haber sido comprometida. Esto incluye casos en los que se han descubierto nuevas vulnerabilidades o en los que la AC, a su propia discreción, decide que la evidencia sugiere que se ha producido un posible compromiso de clave.

4.10 Servicios de estado de certificados

4.10.1 Características operativas

La AC proporciona un servicio de estado de certificados, ya sea en forma de un punto de distribución de CRL o un respondedor OCSP o ambos en los certificados. Las entradas de revocación pueden eliminarse después del vencimiento del Certificado para promover una administración más eficiente del tamaño del archivo CRL.

La AC envía una notificación por correo electrónico a los suscriptores en el mes (generalmente 30 días y 7 días) antes del vencimiento, informando a los suscriptores sobre el próximo vencimiento de sus certificados.

4.10.2 Disponibilidad del servicio

La AC opera y mantiene su capacidad de CRL y OCSP con recursos suficientes para proporcionar un tiempo de respuesta de diez segundos o menos en condiciones normales de funcionamiento. La AC mantiene un Repositorio en línea las 24 horas del día, los 7 días de la semana que el software de la aplicación puede usar para verificar automáticamente el estado actual de todos los Certificados no vencidos emitidos por la AC.

La AC mantiene una capacidad continua las 24 horas del día, los 7 días de la semana para responder internamente a un Informe de problema de certificado de alta prioridad y, cuando corresponda, reenviar dicha queja a las autoridades encargadas de hacer cumplir la ley y/o revocar un Certificado que sea objeto de dicha queja.

En caso de falla del sistema, servicio u otros factores que no están bajo el control de la AC, La AC tiene como objetivo garantizar que este servicio de información no esté disponible durante más de 48 horas.

4.10.3 Características operativas

Sin estipulación

4.11 Fin de la Suscripción

Los Suscriptores pueden finalizar su suscripción a los servicios de Certificado mediante la revocación de su Certificado o, naturalmente, dejando que caduque.

4.12 Custodia y recuperación de claves

4.12.1 Política y prácticas de custodia y recuperación de claves

Las claves privadas de AC nunca se custodian. La AC no ofrece servicios de custodia de claves a los Suscriptores.

4.12.2 Política y prácticas de encapsulación y recuperación de claves de sesión

Sin estipulación.

5 Controles de las instalaciones, la gestión y las operaciones

5.1 Controles físicos

La CA a través del acuerdo de Servicios e Infraestructura (ASI) mantiene políticas de seguridad física y ambiental para los sistemas utilizados para la emisión y gestión de certificados que cubren el control de acceso físico, la protección contra desastres naturales, factores de seguridad contra incendios, fallas en los servicios públicos de apoyo (por ejemplo, energía, telecomunicaciones), colapso de estructuras, fugas de plomería, protección contra robo, allanamiento de morada y recuperación ante desastres. Controles son implementados para evitar la pérdida, el daño o el compromiso de los activos y la interrupción de las actividades empresariales y el robo de información y de las instalaciones de procesamiento de la información.

5.1.1 Ubicación y construcción del sitio

La CA se encuentra dentro de un centro de datos seguro. El centro de datos es una instalación especialmente diseñada hecha de hormigón y acero.

5.1.2 Acceso físico

La CA se opera dentro de un centro de datos seguro que brinda seguridad en las instalaciones con escáneres biométricos y sistemas de acceso con tarjeta. Se proporciona un sistema de monitoreo de TV de circuito cerrado (CCTV) las 24 horas, los 7 días de la semana, así como grabación digital. Guardias de seguridad calificados aseguran las instalaciones físicas y solo el personal autorizado y con autorización de seguridad puede ingresar a las instalaciones.

5.1.3 Energía y Aire Acondicionado

La CA funciona dentro de un centro de datos seguro que está equipado con un sistema de alimentación y refrigeración redundante. El UPS y la conmutación por error al generador de energía están en su lugar en el improbable caso de un corte de energía.

5.1.4 Exposiciones al agua

La CA está protegida contra el agua. Se encuentra sobre rasante y en una planta superior con suelo técnico. Además, existe un sistema de alarma de detección de agua y el personal de operaciones del centro de datos en el sitio está listo para responder a cualquier exposición al agua poco probable.

5.1.5 Prevención y protección contra incendios

La CA opera dentro de un centro de datos seguro que está equipado con un sistema de detección y supresión de incendios.

5.1.6 Almacenamiento de medios

El almacenamiento de los medios de copia de seguridad está fuera del sitio, físicamente asegurado y protegido contra incendios y daños por agua.

5.1.7 Eliminación de desechos

La CA garantiza que todos los medios utilizados para el almacenamiento de información se desclasifiquen o destruyan de una manera generalmente aceptada antes de liberarlos para su eliminación.

5.1.8 Copia de seguridad fuera del sitio

Según lo estipulado en el apartado 5.4.

5.2 Controles de procedimiento

5.2.1 Roles de confianza

La CA garantiza que todos los operadores y administradores, incluidos los especialistas en validación, actúen en calidad de roles de confianza. Los roles de confianza son tales que no es posible ningún conflicto de intereses, y los roles se distribuyen de manera que ninguna persona pueda eludir la seguridad del sistema de CA.

Los roles de confianza incluyen, entre otros, los siguientes:

- Desarrollador: Responsable del desarrollo de sistemas CA.
- Oficial de seguridad/Jefe de seguridad de la información: responsabilidad general de administrar la implementación de las prácticas de seguridad de la CA.
- Especialistas en Validación: Responsables de validar la autenticidad e integridad de los datos a ser incluidos dentro de los Certificados a través de un sistema RA adecuado y aprobar la generación/revocación/suspensión de Certificados.
- Ingeniero de sistemas de infraestructura: autorizado para instalar, configurar y mantener los sistemas de CA utilizados para la gestión del ciclo de vida de los certificados.
- Operador de Infraestructura: Responsable de operar los sistemas de CA en el día a día. Autorizado para realizar copias de seguridad/recuperación del sistema, visualización/mantenimiento de archivos del sistema CA y registros de auditoría.
- Auditor: Autorizado para ver archivos y registros de auditoría.
- Titular de los datos de activación de la CA: Persona autorizada que posee los datos de activación de la CA que son necesarios para el funcionamiento del módulo de seguridad del hardware de la CA.

5.2.2 Número de Personas Requeridas por Tarea

Las claves privadas de CA son respaldadas, almacenadas y recuperadas solo por personal en roles de confianza utilizando, al menos, control dual en un entorno físicamente seguro.

5.2.3 Identificación y autenticación para cada rol

Antes de designar a una persona para un puesto de confianza, Alpha Technologies realiza una verificación de antecedentes. Cada función descrita anteriormente se identifica y autentica de manera que se garantice que la persona adecuada tiene la función correcta para respaldar a la CA. El acceso a recursos se realiza dependiendo del activo mediante usuario/contraseña, certificado electrónico, tarjeta de acceso físico y/o llaves.

5.2.4 Roles que requieren separación de funciones

La CA impone la separación de roles ya sea por el equipo de CA o por procedimientos o una combinación de ambos medios. El personal individual de CA se asigna específicamente a las funciones definidas en la Sección 5.2.1 anterior.
Los roles que requieren una separación de funciones incluyen:

- Los que realizan la aprobación de la generación, revocación y suspensión de certificados. (Especialistas en Validación)
- Quienes realicen la instalación, configuración y mantenimiento de los sistemas de CA. (Ingeniero de sistemas de infraestructura)
- Quienes tienen la responsabilidad general de administrar la implementación de las prácticas de seguridad de la CA. (Oficial de seguridad)
- Aquellos que realizan tareas relacionadas con la gestión del ciclo de vida de la clave criptográfica (p. ej., custodios de componentes clave). (titulares de datos de activación de CA)
- Aquellos que realizan el desarrollo de sistemas de CA. (Desarrolladores)
- Quienes realizan auditorías de sistemas de CA (Operador de Infraestructura, Auditor)

5.3 Procedimientos de registro de auditoría

5.3.1 Tipos de eventos registrados

Se generarán archivos de registro de auditoría para todos los eventos relacionados con la seguridad y los servicios de la CA. Siempre que sea posible, los registros de auditoría de seguridad se generarán automáticamente. Cuando esto no sea posible, se utilizará un libro de registro, un formulario en papel u otro mecanismo físico. Todos los registros de auditoría de seguridad, tanto electrónicos como no electrónicos, se conservarán y estarán disponibles durante las auditorías de cumplimiento.

Alpha Technologies garantiza que todos los eventos relacionados con el ciclo de vida de los Certificados se registren de manera que garanticen la trazabilidad a una persona en un rol de confianza para cualquier acción requerida para los servicios de CA. Como mínimo, cada registro de auditoría incluye los siguientes elementos (ya sea registrados de forma automática o manual):

- El tipo de evento.
- La fecha y hora en que ocurrió el evento.
- Éxito o fracaso en su caso.
- La identidad de la entidad y/u operador que originó el evento.
- La identidad a la que se dirigió el evento; y
- La causa del evento.

Alpha Technologies registra los detalles de las acciones realizadas para procesar una solicitud de certificado y emitir un Certificado, incluida toda la información generada y la documentación recibida en relación con la solicitud de certificado; la hora y la fecha; y el personal involucrado. Alpha Technologies pone estos registros a disposición de su auditor calificado como prueba del cumplimiento de la CA con el esquema de auditoría de CA asociado estipulado en la introducción.

Alpha Technologies registra al menos los siguientes eventos:

- Certificado de CA y eventos clave del ciclo de vida, incluidos:
  - Generación, copia de seguridad, almacenamiento, recuperación, archivo y destrucción de claves.
  - Solicitudes de certificados, solicitudes de renovación y renovación de claves y revocación.
  - Aprobación y rechazo de solicitudes de Certificado.
  - Eventos de gestión del ciclo de vida del dispositivo criptográfico.
  - Generación de Listas de Revocación de Certificados y entradas OCSP; e
  - Introducción de nuevos perfiles de certificados y retiro de los perfiles de certificados existentes.

- Eventos de gestión del ciclo de vida del certificado del suscriptor, que incluyen:
  - Solicitudes de certificados, solicitudes de renovación y renovación de claves, suspensión y revocación.
  - Todas las actividades de verificación estipuladas en esta DPC.
  - Aprobación y rechazo de Solicitudes de Certificados.
  - Emisión de Certificados;
  - Generación de Listas de Revocación de Certificados, y
  - Firma de Respuestas OCSP

- Eventos de seguridad, incluyendo:
  - Intentos de acceso al sistema PKI, exitosos y fallidos.
  - Acciones de PKI y sistema de seguridad realizadas.
  - Cambios en el perfil de seguridad.
  - Instalación, actualización y eliminación de software en un sistema de certificados.
  - Caídas del sistema, fallas de hardware y otras anomalías.
  - Actividades de cortafuegos y enrutadores; y
  - Entradas y salidas de las instalaciones de CA.

5.3.2 Frecuencia del registro de procesamiento

Los registros de auditoría se revisan periódicamente para detectar cualquier evidencia de actividad maliciosa y luego de cada operación importante.

5.3.3 Período de retención para el registro de auditoría

Alpha Technologies conserva los registros de auditoría generados durante al menos diez años. Alpha Technologies pone estos registros de auditoría a disposición del Auditor Cualificado que lo solicite.

5.3.4 Protección del registro de auditoría

Los eventos se registran de manera que no se pueden eliminar ni destruir (excepto para la transferencia a medios a largo plazo) durante cualquier período de tiempo que se conserven.

Los registros de eventos están protegidos para evitar alteraciones y detectar manipulaciones y para garantizar que solo las personas con acceso de confianza autorizado puedan realizar cualquier operación sin modificar la integridad, autenticidad y confidencialidad de los datos.

5.3.5 Procedimientos de copia de seguridad del registro de auditoría

Los registros de auditoría y los resúmenes de auditoría se respaldan en una ubicación segura (por ejemplo, una caja fuerte a prueba de incendios), bajo el control de un rol de confianza autorizado y separados de la generación de origen de sus componentes. La copia de seguridad del registro de auditoría está protegida en la misma medida que los originales.

5.3.6 Sistema de recopilación de auditorías

Los procesos de auditoría se inician al iniciar el sistema y finalizan solo al apagar el sistema. El sistema de recopilación de auditoría garantiza la integridad y disponibilidad de los datos recopilados. Si es necesario, el sistema de recopilación de auditorías protege la confidencialidad de los datos. En caso de que se produzca un problema durante el proceso de cobro de la auditoría, la CA determina si suspende las operaciones hasta que se resuelva el problema, informando debidamente a los propietarios de los activos afectados.

5.3.7 Notificación al Sujeto Causante del Evento

Sin estipulación.

5.3.8 Evaluaciones de vulnerabilidad

La AC realiza evaluaciones de riesgo anuales que:

1. Identifica amenazas internas y externas previsibles que podrían resultar en el acceso no autorizado, la divulgación, el uso indebido, la alteración o la destrucción de cualquier Dato de certificado o Proceso de gestión de certificados.
2. Evalúa la probabilidad y el daño potencial de estas amenazas, teniendo en cuenta la sensibilidad de los Datos de Certificado y los Procesos de Gestión de Certificados; y
3. Evalúa la suficiencia de las políticas, los procedimientos, los sistemas de información, la tecnología y otros arreglos que tiene Alpha Technologies para contrarrestar tales amenazas.

La AC también realiza evaluaciones periódicas de vulnerabilidades y pruebas de penetración que cubren todos los activos relacionados con la emisión de certificados, productos y servicios. Las evaluaciones se centran en las amenazas internas y externas que podrían resultar en el acceso no autorizado, la manipulación, la modificación, la alteración o la destrucción del proceso de emisión del Certificado.

5.4 Archivo de registros

5.4.1 Tipos de registros archivados

La CA y RAs archivan registros con suficiente detalle para establecer la validez de una firma y el correcto funcionamiento y seguridad del sistema CA.

5.4.2 Período de retención para el archivo

La CA conserva toda la documentación relacionada con las solicitudes de certificados y la verificación de los mismos, y todos los Certificados y revocaciones de los mismos, así como toda la documentación relacionada con la seguridad del sistema CA durante al menos el período de retención definido por WebTrust.

El período de retención es de 10 años o el periodo que establezca la legislación vigente.

5.4.3 Protección de Archivo

Los archivos se crean de tal manera que no se pueden borrar ni destruir (excepto para la transferencia a medios de larga duración) dentro del período de tiempo durante el cual deben conservarse. Las protecciones de archivos garantizan que solo el acceso de confianza autorizado pueda realizar operaciones sin modificar la integridad, la autenticidad y la confidencialidad de los datos. Si los medios originales no pueden retener los datos durante el período requerido, el sitio de archivo definirá un mecanismo para transferir periódicamente los datos archivados a nuevos medios.

5.4.4 Procedimientos de copia de seguridad de archivos

Se realizan copias de seguridad de archivos que son del sistema en línea o del sistema fuera de línea. Las copias de seguridad en línea se duplican semanalmente y cada copia de seguridad se almacena en una ubicación diferente del sistema en línea original. Una copia de seguridad se almacena en una caja fuerte resistente al fuego. Se realiza una copia de seguridad fuera de línea al final de cualquier ceremonia clave (con la excepción de cualquier material encriptado que se almacena por separado de acuerdo con los procedimientos de la ceremonia clave) y se almacena en una ubicación externa dentro de los 30 días posteriores a la ceremonia.

5.4.5 Requisitos para el sellado de tiempo de los registros

Si se utiliza un servicio de sellado de tiempo para fechar los registros, entonces debe cumplir con los requisitos definidos en la Sección 6.8. Independientemente de los métodos de sellado de tiempo, todos los registros deben tener datos que indiquen la hora en que ocurrió el evento.

5.4.6 Sistema de colección de archivos (interno o externo)

Se dispone de un sistema centralizado de recogida de información de la actividad de los equipos implicados en el servicio de gestión de certificados.

5.4.7 Procedimientos para obtener y verificar información de archivo

El almacenamiento de medios de la información de archivo de la CA se comprueba en el momento de la creación. Periódicamente, se prueban muestras estadísticas de información archivada para verificar la integridad y legibilidad continuas de la información.

Solo el equipo autorizado de la CA, el rol de confianza y otras personas autorizadas pueden acceder al archivo. Las solicitudes para obtener y verificar la información del archivo son coordinadas por operadores en roles de confianza (auditor interno, el gerente a cargo del proceso y el oficial de seguridad).

5.5 Cambio de clave

La CA puede cambiar periódicamente el material clave de acuerdo con la Sección 6.3.2. La información del sujeto del certificado también puede modificarse y los perfiles de certificado pueden modificarse para cumplir con las mejores prácticas. Las claves privadas utilizadas para firmar los Certificados de suscriptor anteriores se mantienen hasta que caduquen todos los Certificados de suscriptor.

5.6 Compromiso y recuperación ante desastres

5.6.1 Procedimientos de manejo de incidentes y compromisos

La CA tiene un Plan de Respuesta a Incidentes y un Plan de Recuperación de Desastres. La CA documenta la continuidad del negocio y los procedimientos de recuperación ante desastres diseñados para notificar y proteger razonablemente a los proveedores de software de aplicaciones, suscriptores y partes de confianza en caso de desastre, compromiso de seguridad o falla comercial.

La CA no divulga los planes de continuidad comercial a los Suscriptores, las Partes que confían o los Proveedores de software de aplicaciones, pero proporcionará un plan de continuidad comercial y planes de seguridad a los auditores de CA a pedido.

5.6.2 Los recursos informáticos, el software o los datos están dañados

Si algún equipo se daña o deja de funcionar pero las claves privadas no se destruyen, la operación debe restablecerse lo más rápido posible, dando prioridad a la capacidad de generar información sobre el estado del certificado de acuerdo con el plan de recuperación de desastres.

5.6.3 Procedimientos de compromiso de la clave privada de la entidad

En caso de que una clave privada de CA se comprometa, se pierda, se destruya o se sospeche que está comprometida:

- Luego de investigar el problema, decidirá si el Certificado de la CA debe ser revocado. Si es así, entonces:
  - Todos los Suscriptores a los que se haya emitido un Certificado serán notificados a la mayor brevedad posible, al igual que a la entidad de control; y
  - Se generará un nuevo Par de Claves, o se utilizará una jerarquía de CA existente alternativa para crear nuevos Certificados de Suscriptor.

5.6.4 Capacidades de continuidad del negocio después de un desastre

El plan de recuperación ante desastres se ocupa de la continuidad del negocio como se describe en la Sección 5.6.1. Los sistemas de información del estado de los certificados deben implementarse para proporcionar disponibilidad las 24 horas del día, los 365 días del año.

5.7 Terminación de CA o RA

Cuando sea necesario terminar las actividades de una CA o RA, el impacto de la terminación se minimizará tanto como sea posible a la luz de las circunstancias predominantes.

Antes de su finalización, la AC informará a los suscriptores, titulares y terceros que confían sobre el cese de sus operaciones con por lo menos treinta (30) días calendario de anticipación. Mientras que, al Arcotel, se le informará con por lo menos sesenta (60) días calendario de anticipación.

Todas las solicitudes y contratos de suscriptores y titulares serán transferidos al Arcotel o a otro Prestador de Servicios de Certificación designado por éste.

Se advertirá a todos los suscriptores, titulares y terceros que confían, respecto a los cambios y todo tipo de condición asociada a la continuidad del uso de los certificados emitidos por la AC finaliza o transfiere sus operaciones, mediante un comunicado publicado en la siguiente dirección: www.alphaside.com

6 Controles técnicos de seguridad

6.1 Generación e instalación de pares de claves

6.1.1 Generación de pares de claves

6.1.1.1 Generación de pares de claves de CA

Para los pares de claves de CA, la CA realiza los siguientes controles:

1. Genera las claves en un entorno físicamente seguro como se describe en la Sección 5.1 y 5.2.2. de esta Declaración de Prácticas de Certificación.
2. Genera las claves de CA utilizando personal en roles de confianza bajo los principios de control de múltiples personas y conocimiento dividido.
3. Genera las claves de la CA dentro de los módulos criptográficos que cumplan con los requisitos técnicos y comerciales aplicables.
4. Registrar sus actividades de generación de claves de CA; y
5. Mantener controles efectivos para brindar una seguridad razonable de que la Clave Privada fue generada y protegida de conformidad con los procedimientos descritos en Declaración de Prácticas de Certificación.

6.1.1.2 Generación de pares de claves de suscriptor

Para las claves de Suscriptor generadas por la AC, la generación de Claves se realiza en un dispositivo criptográfico seguro que cumple con FIPS 140-2 (o equivalente) utilizando el algoritmo de generación de claves y el tamaño de clave como se especifica en las Secciones 6.1.5 y 6.1.6.

6.1.2 Entrega de clave privada al suscriptor

La AC garantiza la integridad de cualquier clave pública/privada y la aleatoriedad del material de la clave a través de un RNG o PRNG adecuado. Si la AC detecta o sospecha que la Clave privada se ha comunicado a una persona no autorizada o a una organización no afiliada al Suscriptor, la AC revoca todos los Certificados que incluyen la Clave pública correspondiente a la Clave privada comunicada.

6.1.3 Entrega de clave pública al emisor del certificado

La CA solo acepta Claves Públicas de RA que hayan sido protegidas durante el tránsito y cuya autenticidad e integridad de origen de la RA se haya verificado adecuadamente.

6.1.4 Entrega de la clave pública de la CA a las partes que confían

La CA se asegura de que sus claves públicas se entreguen a las partes que confían de tal manera que se eviten los ataques de sustitución. Se alienta a los operadores de plataformas

y navegadores web comerciales a incorporar claves públicas de certificados raíz en sus almacenes raíz y sistemas operativos. Las Claves Públicas de CA son entregadas por el Suscriptor en forma de una cadena de Certificados o a través de un Repositorio operado por la CA y referenciado dentro del perfil del Certificado emitido a través de AIA (Acceso a la información de autoridad).

6.1.5 Tamaños de clave

La CA sigue la publicación especial NIST 800-133 Revisión 2 (2020) - Recomendación para la generación de claves criptográficas - para los plazos recomendados y las mejores prácticas en la elección de pares de claves los certificados de entidad final entregados a los suscriptores.

Los certificados deben cumplir los siguientes requisitos de tipo de algoritmo y tamaño de clave.

Algoritmo de Resumen	SHA-17, SHA-256, SHA-384 o SHA-512
Tamaño mínimo del módulo RSA (bits)	2048
Curva ECC	NIST P-256, P-384 o P-521
RSASSA-PSS[8]	

6.1.6 Generación de parámetros de clave pública y control de calidad

La CA genera pares de claves de acuerdo con FIPS 186 y utiliza técnicas razonables para validar la idoneidad de las claves públicas presentadas por los suscriptores. Las claves débiles conocidas se prueban y rechazan en el momento del envío.

6.1.7 Propósitos de uso de claves (según el campo de uso de claves X.509 v3)

La CA establece el uso de claves de los Certificados en función de su campo de aplicación propuesto a través del Campo de uso de claves v3 para X.509 v3.

Las Claves Privadas correspondientes a Certificados Raíz no se utilizan para firmar Certificados excepto en los siguientes casos:

1. Certificados autofirmados para representar a la propia CA Raíz.
2. Certificados para verificación de Respuesta OCSP.

6.2 Protección de clave privada y controles de ingeniería del módulo criptográfico

La CA implementa medidas de seguridad físicas y lógicas para evitar la emisión de certificados no autorizados. La protección de la clave privada de CA fuera del sistema o dispositivo validado especificado anteriormente debe consistir en seguridad física, cifrado o una combinación de ambos, implementados de manera que impida la divulgación de la clave privada de CA. La CA encripta su clave privada con un algoritmo y una longitud de clave que, de acuerdo con el estado de la técnica, son capaces de soportar ataques criptoanalíticos durante la vida residual de la clave encriptada o parte de la clave.

6.2.1 Estándares y controles del módulo criptográfico

La CA garantiza que todos los sistemas que firman Certificados y CRL o generan respuestas OCSP utilizan FIPS 140-2 nivel 3 como nivel mínimo de protección criptográfica. Las CA que requieren que los Suscriptores utilicen sistemas FIPS 140-2 de nivel 2 o superior para la protección de la clave privada deben obligar contractualmente al Suscriptor a utilizar dicho sistema o proporcionar un mecanismo adecuado para garantizar la protección. Un mecanismo adecuado utilizado por la CA es la limitación a un CSP (proveedor de servicios criptográficos) adecuado vinculado a una plataforma de hardware compatible con FIPS conocida como parte del proceso de inscripción.

6.2.2 Control multipersona (n de m) de la Clave privada

La CA activa claves privadas para operaciones criptográficas con control de varias personas (utilizando datos de activación de CA) que realizan tareas asociadas con sus funciones de confianza. Los roles de confianza autorizados para participar en los controles de varias personas de esta clave privada están fuertemente autenticados (es decir, token con código PIN).

6.2.3 Custodia de la clave privada

La CA no custodia las claves privadas por ningún motivo.

6.2.4 Copia de seguridad de clave privada

Si es necesario para la continuidad del negocio, la CA realiza una copia de seguridad de las claves privadas raíz y subordinadas bajo el mismo control de varias personas que la clave privada original. La CA no respalda las claves privadas del suscriptor.

6.2.5 Archivo de clave privada

La CA no archiva las claves privadas del suscriptor y garantiza que se elimine cualquier ubicación temporal en la que pueda haber existido una clave privada en cualquier ubicación de la memoria durante el proceso de generación.

6.2.6 Transferencia de clave privada hacia o desde un módulo criptográfico

Las claves privadas de la CA se generan, activan y almacenan en módulos de seguridad de hardware. Cuando las claves privadas están fuera de un módulo de seguridad de hardware (ya sea para almacenamiento o transferencia), se cifran. Las claves privadas nunca existen en texto sin formato fuera de un módulo criptográfico. Si la CA se entera de que la clave privada se ha comunicado a una persona no autorizada o a una organización no afiliada a la CA, la CA revocará todos los certificados que incluyan la clave pública correspondiente a la clave privada comunicada.

6.2.7 Almacenamiento de claves privadas en el módulo criptográfico

La CA almacena claves privadas en al menos un dispositivo FIPS 140-2 de nivel 3.

6.2.8 Método de activación de clave privada

La CA es responsable de activar la Clave Privada de acuerdo con las instrucciones y documentación proporcionada por el fabricante del módulo de seguridad del hardware. Los Suscriptores son responsables de proteger las Claves Privadas de acuerdo con las obligaciones que se presentan en forma de Contrato de Suscriptor o Términos de Uso.

6.2.9 Método de desactivación de clave privada

La CA garantiza que los Módulos de seguridad de hardware que se han activado no se dejen desatendidos o estén disponibles para el acceso no autorizado. Durante el tiempo que el Módulo de seguridad de hardware de la CA está en línea y operativo, solo se utiliza para firmar certificados y CRL/OCSP. Cuando una CA ya no está operativa, las claves privadas se eliminan del módulo de seguridad de hardware.

6.2.10 Método de destrucción de claves privadas

Las Claves Privadas de la CA se destruyen cuando ya no son necesarias o cuando los Certificados a los que corresponden han caducado o han sido revocados. La destrucción de claves privadas significa que la CA destruye todos los datos de activación secretos de CA asociados en el HSM de tal manera que no se puede utilizar ninguna información para deducir ninguna parte de la clave privada.

Las claves privadas de suscriptor generadas por la AC en GCC se almacenan en formato PKCS#12 y, transcurridos 30 días desde la generación de la clave, el par de claves de suscriptor se elimina automáticamente de GCC.

6.2.11 Clasificación de Módulos Criptográficos

Véase sección 6.2.1

6.3 Otros aspectos de la gestión de pares de claves

6.3.1 Archivo de clave pública

La CA archiva las claves públicas de los certificados.

6.3.2 Periodos de utilización de las claves pública y privada

Los periodos de utilización de las claves están determinados por la duración del certificado, una vez finalizado el mismo no podrá usarse.

6.4 Datos de activación

6.4.1 Generación e instalación de datos de activación

La generación y el uso de los datos de activación de la CA utilizados para activar las claves privadas de CA de la CA se realizan durante una ceremonia de entrega de claves (consulte la Sección 6.1.1). Los datos de activación son generados automáticamente por el HSM apropiado o de tal manera que satisfagan las mismas necesidades. Luego se entrega a un titular de una parte de la clave que es una persona en un rol de confianza. El método de entrega mantiene la confidencialidad y la integridad de los datos de activación.

6.4.2 Protección de datos de activación

La emisión de datos de activación de CA está protegida contra la divulgación a través de una combinación de mecanismos de control de acceso físico y criptográfico. Los datos de activación de la CA se almacenan en tarjetas inteligentes.

6.4.3 Otros aspectos de los datos de activación

Los datos de activación de la CA solo pueden ser conservados por el personal de la CA en funciones de confianza.

6.5 Controles de seguridad informática

6.5.1 Requisitos Técnicos Específicos de Seguridad Informática

Las siguientes funciones de seguridad informática son proporcionadas por el sistema operativo o mediante una combinación de sistema operativo, software y medidas de seguridad físicas. Los componentes de la PKI deben incluir las siguientes funciones:

- Requerir inicios de sesión autenticados para el rol de confianza.
- Proporcionar control de acceso discrecional con privilegios mínimos.
- Proporcionar capacidad de auditoría de seguridad (protegido en integridad).

- Prohibir la reutilización de objetos.
- Requerir el uso de una política de contraseña segura.
- Requerir el uso de criptografía para la comunicación de sesiones.
- Requerir ruta confiable para identificación y autenticación.
- Proporcionar medios para la protección de códigos maliciosos.
- Proporcionar medios para mantener la integridad del software y el firmware
- Proporcionar aislamiento de dominio y partición para diferentes sistemas y procesos; y
- Proporcionar autoprotección para el sistema operativo.

6.6 Controles técnicos del ciclo de vida

6.6.1 Controles de desarrollo del sistema

Usar software que haya sido diseñado y desarrollado bajo una metodología de desarrollo formal y documentada.

6.6.2 Controles de gestión de la seguridad

La administración de la CA documenta y controla la configuración de los sistemas, así como cualquier modificación y actualización.

La CA desarrolla las actividades precisas para la formación y concienciación de los empleados en materia de seguridad.

La CA exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de certificación.

6.6.3 Controles de seguridad del ciclo de vida

La CA mantiene un esquema de mantenimiento para garantizar el nivel de confianza del software y el hardware que se evalúan y certifican.

6.7 Controles de seguridad de la red

Los componentes de PKI de la CA implementan medidas de seguridad adecuadas para garantizar que estén protegidos contra ataques de intrusión y denegación de servicio. Tales medidas incluyen el uso de guardias de seguridad, cortafuegos y enrutadores de filtrado. Los puertos y servicios de red no utilizados están desactivados. Cualquier dispositivo de control de límites utilizado para proteger la red en la que se aloja el equipo PKI niega todos los servicios excepto los necesarios al equipo PKI, incluso si esos servicios están habilitados para otros dispositivos en la red.

6.8 Sellado de tiempo

Todos los componentes de la CA se sincronizan periódicamente con un servicio de tiempo fiable. La CA utiliza una fuente de GPS y tres relojes de fuente NTP no autenticados para establecer la hora correcta para:

- Tiempo de validez inicial de un Certificado de CA.
- Revocación de un Certificado de CA.
- Publicación de actualizaciones de CRL; y
- Emisión de Certificados de entidad final de Suscriptor.

Se pueden usar procedimientos electrónicos o manuales para mantener la hora del sistema. Los ajustes del reloj son eventos auditables.

7 Perfiles de certificado, CRL y OCSP

7.1 Perfil de certificado

7.1.1 Número(s) de versión

La CA emite Certificados de conformidad con X.509 Versión 3.

7.1.2 Extensiones de certificado

La CS emite Certificados de conformidad con RFC 5280 y las mejores prácticas aplicables, incluido el cumplimiento de los requisitos básicos actuales, sección 7.1.2.1 a 7.1.2.5, excepto donde se mencione en este documento. La criticidad también sigue las mejores prácticas para evitar riesgos innecesarios para las partes que confían cuando se aplica a restricciones de nombre. Los certificados de CA y de entidad final incluyen una extensión de uso extendido de clave que contiene KeyPurposeId(s) que describen el(los) uso(s) previsto(s) del certificado. El KeyPurposeId anyExtendedKeyUsage no se incluye en los certificados de entidad final de confianza pública.

7.2 Perfil de CRL

7.2.1 Número(s) de versión

La CA emite CRL de la versión 2 de conformidad con RFC 5280. Las CRL tienen los siguientes campos:

• Emisor	El DN del Sujeto de la CA
• Fecha de vigencia	Fecha y hora
• Próxima actualización	Fecha y hora
• Algoritmo de firma	sha256RSA, etc.

• Número(s) serial	Lista de números de serie revocados
• Fecha de revocación	Fecha de revocación

7.2.2 CRL y extensiones de entrada de CRL

Las CRL tienen las siguientes extensiones:

• Número de CRL.-Número de serie que aumenta monótonamente para cada CRL
• Identificador de clave de autoridad.- (AKI) de la CA para los requisitos de encadenamiento/validación

Se admiten las siguientes extensiones:

• ReasonCode(Codigo de Razón) Identifica el motivo de la revocación del Certificado.

La extensión está presente para una entrada de CRL para un certificado de CA raíz o CA subordinada, incluidos los certificados cruzados. Los valores admitidos son keyCompromise (1), affiliationChanged (3), superseded (4), cessationOfOperation (5), privilegeWithdrawn(9).

La extensión puede estar presente para una entrada de CRL para un Certificado de entidad final de Suscriptor. Los valores admitidos son keyCompromise (1), affiliationChanged (3), superseded (4), cessationOfOperation (5), CertificateHold (6), privilegeWithdrawn (9).

7.3 Perfil OCSP

La CA opera un respondedor de perfil de estado de certificado en línea (OCSP) de conformidad con RFC 6960 y RFC 5019 y destaca esto dentro de la extensión AIA a través de una URL de respondedor OCSP.

7.3.1 Número(s) de versión

La CA emite respuestas OCSP de la versión 1 con los siguientes campos:

- Responder ID Hash SHA-1 de la clave pública del respondedor
- Tiempo producido La hora en que se firmó esta respuesta
- Estado del certificado Estado del certificado al que se hace referencia (bueno/revocado/desconocido)
- ThisUpdate/NextUpdate Intervalo de validez recomendado para la respuesta
- Algoritmo de firma SHA256 RSA
- Firma Valor de firma generado por el respondedor
- Certificados El Certificado del Respondedor OCSP

Una solicitud OCSP debe contener los siguientes datos:

- Versión del protocolo

- Petición de servicio
- Identificador de certificado de destino

Se admiten los siguientes campos:

- revocationReason Identifica el motivo de la revocación del Certificado.

Este campo está presente para las respuestas OCSP para un certificado de CA raíz o CA subordinada, incluidos los certificados cruzados, y puede estar presente para un certificado de entidad final del suscriptor, si se revoca el certificado. El CRLReason indicado contiene un valor permitido para las CRL, tal como se especifica en la Sección 7.2.2.

7.3.2 Extensiones OCSP

Sin estipulación.

8 Auditoría de cumplimiento y otras evaluaciones

Los procedimientos dentro de esta CPS están diseñados para cumplir con los requisitos enumerados en la Sección 1.0 y abarcan todas las partes relevantes de los estándares PKI actualmente aplicables para las diversas industrias verticales de PKI en las que opera la CA.

Alpha Technologies se encuentra sometida a las revisiones de control de ARCOTEL a la que se ha comunicado del inicio de actividades como Entidad de Certificación.

8.1 Frecuencia y circunstancias de las auditorias

La CA mantiene su cumplimiento con los estándares de WebTrust/eIDAS/UK eIDAS a través de un auditor calificado de forma anual (WebTrust), semestral (eIDAS/UK eIDAS) y contigua.

8.2 Identidad/Calificaciones del Auditor

Con respecto a las auditorias de la CA, son realizadas por Ernst & Young como un "auditor calificado" que posee las siguientes calificaciones y habilidades:

- Independencia del sujeto de la auditoría.
- La capacidad de realizar una auditoría que aborde los criterios especificados en una Auditoría Elegible según lo estipulado en la sección 8.0 de este documento.
- Emplea a personas que tienen competencia en el examen de tecnología de infraestructura de clave pública, herramientas y técnicas de seguridad de la información, tecnología de la información y auditoría de seguridad, y la función de certificación de terceros.
- Certificado, acreditado, licenciado o evaluado de otro modo que cumple con los requisitos de calificación de los auditores bajo el esquema de auditoría.

8.3 Relación del Auditor con la Entidad Auditada

La CA ha seleccionado un auditor/asesor que es completamente independiente.

8.4 Temas cubiertos por la evaluación

La auditoría cumple con los requisitos de los esquemas de auditoría destacados en la Sección 1.0 bajo los cuales se realiza la evaluación. Estos requisitos pueden variar a medida que se actualicen los esquemas de auditoría. Se aplica un esquema de auditoría a la CA en el año siguiente a la adopción del esquema actualizado.

8.5 Acciones tomadas como resultado de la deficiencia

La CA sigue el proceso adecuado si los auditores presentan un incumplimiento y crea un plan de acción correctivo adecuado para eliminar la deficiencia.

8.6 Comunicaciones de Resultados

Los resultados de la auditoría se informan a la Autoridad de políticas para el análisis y la resolución de cualquier deficiencia a través de un plan de acción correctivo posterior. Los resultados también podrían ponerse a disposición de cualquier otra entidad apropiada que pueda tener derecho a una copia de los resultados por ley, reglamento o acuerdo.

9 Otros Asuntos Comerciales y Legales

9.1 Tarifas

9.1.1 Tarifas de emisión o renovación de certificados

La CA cobra tarifas por la emisión y renovación de Certificados. La CA no cobra por la reemisión. Las tarifas y los términos y condiciones asociados se aclaran a los Solicitantes tanto en el proceso de inscripción a través de una interfaz web como en los materiales de ventas y marketing en los sitios web específicos.

9.1.2 Tarifas de acceso a certificados

Alpha Technologies no ha establecido tarifas de acceso a certificados emitidos.

9.1.3 Tarifas de acceso a la información de estado o revocación

Alpha Technologies puede cobrar tarifas adicionales a los Suscriptores que tienen una gran comunidad de Usuarios dependientes y optan por no utilizar el engrapado OCSP u otras

técnicas similares para reducir la carga en la infraestructura de estado del Certificado de la CA.

9.1.4 Tarifas por Otros Servicios

Alpha Technologies puede cobrar por otros servicios adicionales, como el sellado de tiempo.

9.1.5 Política de reembolso

Para los clientes que tienen una relación directa con la CA y los Certificados pedidos directamente a la CA, si un Suscriptor no está completamente satisfecho con el Certificado emitido, el Suscriptor puede solicitar un reembolso dentro de los 7 días posteriores a la emisión del Certificado. Cualquier reembolso será neto de cualquier cargo incurrido por la CA.

9.2 Responsabilidad Financiera

9.2.1 Cobertura de Seguro

Alpha Technologies mantiene una garantía de responsabilidad civil, de conformidad con lo dispuesto en el apartado h) del artículo 30 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, las Entidades de Certificación de Información y, Servicios Relacionados Acreditadas deberán contar con una garantía de responsabilidad para asegurar a los usuarios el pago de los daños y perjuicios ocasionados por el incumplimiento de las obligaciones.

9.2.2 Otros Activos

Sin estipulación

9.3 Información Confidencial de los negocios

9.3.1 Alcance de la información confidencial

Los siguientes elementos se clasifican como información confidencial y, por lo tanto, están sujetos al cuidado y la atención razonables por parte del personal de Alpha Technologies, incluidos los especialistas en validación y los administradores:

- Toda información personal obtenida para la expedición como se detalla en la Sección 9.4.
- Los registros de solicitudes de certificados, aprobadas o denegadas
- Los registros de transacciones (registros completos y registros de auditoria de dichas transacciones).
- Registros de auditoría creados o mantenidos por la CA y RA.
- Claves privadas generadas y/o almacenadas por el proveedor de servicios de certificación.
- Documentación interna de los procesos comerciales, incluidos los Planes de seguridad, y los Planes de continuidad de negocios (BCP); y

- Documentación de operaciones, archivo, monitorización y otros semejantes.
- Toda información clasificada como “Confidencial”.

9.3.2 Información no confidencial

Se considerará información pública:

- Cualquier información no definida como confidencial dentro de esta DPC.
- La información sobre el estado del certificado y los propios certificados se consideran públicos.
- La contenida en la Declaración de Prácticas de Certificación y en la Declaración de Políticas de Seguridad vigentes.
- La información contenida en los Certificados de firma electrónica que la CA emita.
- La Lista de Certificados Revocados (CRL).
- Toda otra información clasificada como pública.

9.3.3 Responsabilidad de proteger la información confidencial

La CA protege la información confidencial mediante la capacitación y el cumplimiento con empleados, y contratistas.

9.4 Privacidad de la información personal

9.4.1 Información tratada como privada

Los datos de los usuarios serán usados única y exclusivamente para los fines indicados en el presente documento. No se procederá a la divulgación o cesión de los datos personales salvo en los casos previstos en esta DPC.

La información confidencial se protege mediante medidas de seguridad que garantizan su protección frente a alteración, pérdida, destrucción, daño, falsificación o procesamiento ilícito, de acuerdo a lo dispuesto en el presente documento y en la normativa de referencia aplicable.

Alpha Technologies trata toda la información recibida tanto a los Solicitantes que obtienen un Certificado como a aquellos que no lo logran y son rechazados. Alpha Technologies capacita periódicamente a todo el personal de RA, así como a cualquier persona que tenga acceso a la información sobre el debido cuidado y atención que se debe aplicar.

9.4.2 Información no considerada privada

La información del estado del certificado y cualquier contenido del certificado no se consideran privados.

9.4.3 Responsabilidad de Proteger la Información Privada

La CA es responsable de almacenar de forma segura la información privada y puede almacenar la información recibida en formato digital. Cualquier copia de seguridad de información privada debe cifrarse cuando se transfiere a un medio de copia de seguridad adecuado.

9.4.4 Aviso y consentimiento para usar información privada

La información personal obtenida de los Solicitantes durante el proceso de solicitud e inscripción se considera privada y se requiere el permiso del Solicitante para permitir el uso de dicha información. Alpha Technologies incluye cualquier consentimiento requerido en el Acuerdo de Suscriptor, incluido cualquier permiso requerido para obtener información adicional de terceros que pueda ser aplicable al proceso de validación del producto o servicio ofrecido por Alpha Technologies.

9.4.5 Divulgación conforme a un proceso judicial o administrativo

Alpha Technologies puede divulgar información privada sin previo aviso a los Solicitantes o Suscriptores cuando así lo exija la ley o la normativa.

9.4.6 Otras circunstancias de divulgación de información

Sin estipulación.

9.5 Derechos de propiedad intelectual

La CA no viola deliberadamente los derechos de propiedad intelectual de terceros. Las Claves Públicas y Privadas siguen siendo propiedad de los Suscriptores que las poseen legítimamente. La CA conserva la propiedad de los Certificados; sin embargo, otorga permiso para reproducir y distribuir Certificados de forma no exclusiva y libre de regalías, siempre que se reproduzcan y distribuyan en su totalidad.

9.6 Obligaciones y Garantías

1.1.1 Obligaciones y Garantías de CA

La CA utiliza esta DPC y los contratos de suscriptor aplicables para transmitir las condiciones legales de uso de los Certificados emitidos a los Suscriptores y Partes que confían. Todas las partes, incluidos la CA, los AR y los Suscriptores, garantizan la integridad de sus respectivas Claves privadas. Si alguna de esas partes sospecha que una clave privada se ha visto comprometida, lo notificará de inmediato a la AR correspondiente.

Alpha Technologies declara y garantiza a los Beneficiarios del Certificado que, durante el período de validez del Certificado, Alpha Technologies ha cumplido con su Declaración de prácticas de certificación al emitir y gestionar el Certificado.

Alpha Technologies está obligada a:

- Respetar lo dispuesto en la normatividad vigente y en esta DPC.
- Publicar esta DPC en la página web de Alpha Technologies en su última versión.
- Informar al ARCOTEL sobre las modificaciones de esta DPC.
- Proteger y custodiar de manera segura y responsable la clave privada de la EC.
- Emitir certificados consistentes con la información suministrada por el solicitante y libre de errores de entrada de datos.
- Garantizar la confidencialidad en el proceso de generación de datos de emisión del certificado de firma y su entrega al suscriptor por un procedimiento seguro.
- Garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor.
- Utilizar sistemas fiables para almacenar los certificados e impedir que personas no autorizadas modifiquen los datos.
- Publicar de manera oportuna en la página web los certificados que se encuentran vigentes y las CRL.
- Informar a los suscriptores la proximidad del vencimiento de su certificado enviando un correo electrónico antes del vencimiento.
- Aprobar o denegar las solicitudes de emisión de certificados enviadas por la Autoridad de Registro.
- No mantener copia de la clave privada del solicitante o titular.
- Notificar al Solicitante o Titular la revocación del certificado digital dentro de las 24 horas siguientes a la revocación del certificado de conformidad con esta DPC.

1.1.2 Obligaciones y Garantías de AR

Las AR se encuentran obligadas a:

- Conocer y dar cumplimiento a lo dispuesto en la presente DPC.
- Comprobar la identidad de los Solicitantes y Titulares de certificados digitales, verificando la exactitud, suficiencia y autenticidad de la información suministrada por el Solicitante.
- Validar y enviar de forma segura y con la debida celeridad a la CA las solicitudes que reciba para la emisión del certificado.
- Archivar y custodiar de manera segura la documentación suministrada por el solicitante o titular, durante el tiempo establecido por la legislación vigente.
- Respetar lo dispuesto en los contratos firmados entre la CA y el titular
- Garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor.
- Formalizar con el suscriptor los contratos de emisión de certificados en los términos y condiciones que establezca la CA.
- Garantizar que todos los trámites realizados sean firmados electrónicamente por los operadores que los realizan, asumiendo de esta forma su plena responsabilidad en el proceso.

1.1.3 Obligaciones y Garantías del Suscriptor

Los Suscriptores y/o Solicitantes garantizan que:

- Precisión de la información: el Suscriptor proporcionará información precisa y completa en todo momento, tanto en la Solicitud de certificado como en cualquier otra forma solicitada en relación con la emisión de un Certificado.
- Protección de la clave privada: el solicitante deberá tomar todas las medidas razonables para mantener el control exclusivo, mantener la confidencialidad y proteger adecuadamente en todo momento la clave privada que se incluirá en los certificados solicitados y cualquier dispositivo o dato de activación asociado, por ejemplo, contraseña o token.
- Aceptación del Certificado: el Suscriptor deberá revisar y verificar la precisión del contenido del Certificado.
- Uso del Certificado: el Suscriptor usará el Certificado únicamente de conformidad con todas las leyes aplicables, únicamente de acuerdo con el Contrato del Suscriptor y esta DPC.
- Informes y revocación: el Suscriptor deberá (a) solicitar de inmediato la revocación del certificado, dejar de utilizarlo y su Clave privada asociada, si existe algún uso indebido real o sospechado o compromiso de la Clave privada del Suscriptor asociada con la Clave pública incluida en el Certificado; y (b) solicitar de inmediato la revocación del Certificado y dejar de usarlo, si alguna información en el Certificado es o se vuelve incorrecta o inexacta.
- Terminación del uso del Certificado: el Suscriptor cesará de inmediato el uso de la Clave privada asociada con la Clave pública en el Certificado al momento de la revocación de dicho Certificado; y Capacidad de respuesta: el Suscriptor deberá responder a las instrucciones de la CA relativas a Compromiso o uso indebido del Certificado en un plazo de cuarenta y ocho (48) horas.
- Reconocimiento y aceptación: el Solicitante reconoce y acepta que la CA tiene derecho a revocar el Certificado inmediatamente si el Solicitante viola los términos del contrato de suscripción o si la CA descubre que el Certificado se está utilizando para permitir actividades.
- Informar durante la vigencia del certificado digital cualquier cambio en los datos suministrados inicialmente para la emisión del certificado.
- Responder por el uso del Certificado de Firma Electrónica y de las consecuencias que se deriven de su utilización.
- Cumplir con lo estipulado en el artículo 17 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

1.1.4 Obligaciones y Garantías de la parte que confía

Una parte que confía en un Certificado de CA garantiza lo siguiente:

- Tener la capacidad técnica para utilizar los Certificados.
- Validar el Certificado de una CA utilizando la información de estado del Certificado (p. ej., una CRL u OCSP) publicada por la CA de acuerdo con el procedimiento de validación de la ruta del Certificado adecuado.
- Confiar en el Certificado de una CA solo si toda la información incluida en dicho Certificado puede verificarse a través de dicho procedimiento de validación como correcta y actualizada.

- Confiar en el Certificado de una CA, solo en la medida en que sea razonable dadas las circunstancias; y
- Notificar a la AR correspondiente de inmediato, cualquier hecho o situación anómala relativa al certificado y que pueda ser considerada como causa de revocación.

Las obligaciones de la Parte que confía, si va a confiar razonablemente en un Certificado, son:

- Verificar la validez o revocación del Certificado de CA usando la información de estado de revocación actual como se indica a la Parte que Confía.
- Tener en cuenta cualquier limitación en el uso del Certificado ya sea en el Certificado o en esta DPC; y
- Tomar cualquier otra precaución prescrita en el Certificado de la CA, así como cualquier otra política o términos y condiciones que estén disponibles en el contexto de la aplicación en la que se pueda utilizar un Certificado.

Las Partes que confían deben establecer en todo momento que es razonable confiar en un Certificado dadas las circunstancias, teniendo en cuenta circunstancias tales como el contexto de aplicación específico en el que se utiliza un Certificado.

Aceptar que los mensajes o documentos firmados con la clave privada del suscriptor tienen el mismo efecto y validez legal que si se hubiera realizado la firma manuscrita.

Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados digitales en los que confía.

1.2 Renuncias a garantías

EXCEPTO EN LA MEDIDA EN QUE LO PROHÍBA LA LEY O SEGÚN LO DISPUESTO EN EL PRESENTE DOCUMENTO, ALPHA TECHNOLOGIES RECHAZA TODAS LAS GARANTÍAS, INCLUYENDO CUALQUIER GARANTÍA DE COMERCIABILIDAD Y/O IDONEIDAD PARA UN FIN DETERMINADO.

1.3 Limitaciones de responsabilidad

En la medida en que la CA haya emitido y gestionado el certificado de conformidad con los requisitos básicos y esta DPC, Alpha Technologies no será responsable ante el suscriptor, la parte que confía o terceros por cualquier pérdida sufrida como resultado del uso o la confianza en dicho certificado.

Alpha Technologies limita su responsabilidad a la emisión y gestión de certificados y de pares de claves de suscriptores suministrados por la Entidad de Certificación.

Este límite de responsabilidad limita los daños recuperables fuera de este contexto, en ningún caso Alpha Technologies será responsable de cualquier daño indirecto, incidental, especial o consecuente, ni de cualquier pérdida de beneficios, perdida de datos u otros daños indirectos, incidentales o consecuentes que surjan o estén relacionados con el uso, la entrega o la confianza en licencia, cumplimiento o incumplimiento de certificados, firmas digitales o cualquier otra transacción o servicio ofrecido o contemplado por esta DPC.