Datilmedia S.A.

Política de Certificados v1.0

Control de cambios

Fecha	Cambio	Autor
2021-10-13	Se ajustaron parámetros y formato.	E. Raad

Contenido

1. Introducción

1.1. Visión general

La Infraestructura de llave pública de Dátil (“Dátil ILP”), ha sido establecida por Datilmedia S.A. (“Dátil”), para permitir autenticación de identidad de manera confiable y segura de personas naturales y jurídicas en Ecuador, así como para facilitar la confidencialidad e integridad de todo tipo de transacciones electrónicas.

Esta Política de Certificados (PC) es la declaración principal de las políticas que gobiernan las AC en la ILP de Dátil. Establece los requisitos comerciales, legales y técnicos para aprobar, emitir, administrar, usar, revocar y renovar Certificados Dátil y proporcionar servicios de confianza asociados para todos los Participantes. Estos requisitos protegen la seguridad y la integridad de la ILP de Dátil y comprenden un conjunto único de reglas que se aplican de manera coherente a todas las AC incluidas en el mismo, a fin de garantizar la confianza de manera uniforme en la misma.

Esta PC se ajusta a los estándares del documento Certificate Policy and Certification Practices Framework de la organización Internet Engineering Task Force y como está definido en el estándar (IETF) RFC 3647.

1.2. Nombre del documento e identificación

Dátil ha reservado los siguientes Identificadores de Objetos (OIDs) para sus políticas de emisión:

Esta Política de Certificados (PC): 1.3.6.1.4.1.52643.2.5.1

1.2.1. Revisiones

Ver Apéndice A.

1.3. Participantes de la ILP

1.3.1. Autoridades de Certificación

Datilmedia S.A. es la Autoridad de Certificación (AC) autorizada para emitir certificados de llave pública dentro de la ILP de Dátil.

1.3.2. Autoridad de Registro

Con excepción de las Secciones 3.2.2.4 y 3.2.2.5, la AC podrá delegar la ejecución de todas, o cualquier parte, de los requerimientos de la Sección 3.2 a un Tercero Vinculado, dado que el proceso cumpla completamente con los requerimientos de la sección 3.2.

Antes de que Dátil autorice a un Tercero Vinculado a realizar las funciones delegadas, la AC deberá requerir contractualmente al Tercero Vinculado lo siguiente:

1. Cumplir con los requerimientos de calificación de la Sección 5.3.1, cuando aplique a la delegación.
2. Conservar la documentación en concordancia con la Sección 5.5.2.
3. Cumplir con las otras disposiciones de estos Requerimiento que sean aplicables a las funciones delegadas; y
4. Cumplir con (a) la Declaración de Prácticas de Certificación y Política de Certificados de la AC o (b) la Declaración de Prácticas de Certificación del Tercero Vinculado las cuales han sido revisadas por la AC de cumplir con estos Requerimientos.

La AC podrá designar a una AR Empresarial para verificar solicitudes de emisión de certificados de su propia organización. La AC no aceptará solicitudes de certificados de una AR Empresarial a menos que se cumplan los siguientes requerimientos:

1. La AC confirmará que la solicitud de certificado corresponde a un empleado de la organización legal de la AR Empresarial.
2. En el caso de que el nombre del Sujeto del certificado sea diferente al nombre legal de la persona solicitando el certificado, la AC verificará que esta es un delegado o tiene el poder para realizar la solicitud.

La AC impondrá estas limitaciones en la forma de una obligación contractual de la AR Empresarial y monitorea su cumplimiento por parte de la AR Empresarial.

1.3.3. Suscriptores

Un Suscriptor es una persona natural o jurídica que desea solicitar y utilizar un Certificado emitido por la AC.

1.3.4. Terceros que confían

Un Tercero que Confía es una persona natural o jurídica que decide confiar en un Certificado emitido por la AC para verificar una firma electrónica y/o descifrar un documento o mensaje.

Los Terceros que Confían pueden incluir a Dátil y sus afiliados, así como cualquier otra persona natural o jurídica.

1.3.5. Otros participantes

No aplica.

1.4. Uso de los certificados

1.4.1. Uso apropiado de los certificados

El objetivo principal de esta Política es permitir una comunicación electrónica eficiente y segura, abordando las preocupaciones de los Terceros que Confían sobre la confiabilidad de los Certificados.

1.4.2. Usos prohibidos de los certificados

Las operaciones prohibidas por esta DPC con los Certificados emitidos por ACs de Dátil son:

- No se permite a un Suscriptor utilizar un Certificado para firmar otros Certificados o Listas de Revocación.
- No se permite realizar alteraciones a los Certificados.
- Está prohibido el uso de los Certificados para ocasionar daños personales o ambientales.
- Está prohibido el uso de los Certificados para cualquier actividad que viole las leyes y/o regulaciones legales de Ecuador.

1.5. Administración de políticas

1.5.1. Autoridad de Administración de Políticas

Datilmedia S.A.
Victor Emilio Estrada 1021 y Jiguas
Guayaquil, Guayas
Ecuador

1.5.2. Información de contacto

Para consultas de seguridad y demás asuntos relacionados a la Autoridad de Certificación: ayuda@datil.com

1.5.3. Persona que determina la idoneidad de la PC

La Administración de Autoridad de Certificación determina la integridad y aplicabilidad de esta PC conforme a las políticas de Dátil.

1.5.4. Procedimientos de aprobación de la PC

Dátil podrá modificar esta PC según lo crea necesario. Los cambios que de acuerdo al juicio de Dátil no tengan o tengan mínimo impacto en los Participantes de la ILP de Dátil, pueden ser realizados sin notificación. Cambios, que según el juicio de Dátil tengan impacto significativo en los Participantes de la ILP de Dátil, serán realizados con notificación previa a los Participantes.

Los cambios y potenciales notificaciones a esta PC serán publicados en https://datil.com

Una nueva versión de esta PC entrará en vigencia quince (15) días después de su publicación, y sustituirá a todas las versiones anteriores y será vinculante para todos los Participantes en la ILP de Dátil a partir de ese momento.

Los cambios a esta PC son aprobados por la Administración de Autoridad de Certificación de Dátil.

1.6. Definiciones y acrónimos

Ver apéndice A.

1.6.1. Convenciones

Las palabras clave "DEBE", "NO DEBE", "REQUERIDO", "DEBE", "NO DEBE", "DEBE", "NO DEBE", "RECOMENDADO", "PUEDE" y "OPCIONAL" en estos Requisitos deben interpretarse de acuerdo con RFC 2119.

2. Publicación y responsabilidades del repositorio

El AC DEBE desarrollar, implementar, hacer cumplir y actualizar anualmente una Declaración de Prácticas de Certificación que describa en detalle cómo la AC implementa la última versión de estos Requisitos.

2.1. Repositorios

La AC DEBE publicar la información de revocación para los Certificados Subordinados y Certificados de Suscriptor en cumplimiento de esta Política.

2.2. Publicación de información de certificados

La AC DEBERÁ divulgar públicamente su Política de Certificado y / o Declaración de Prácticas de Certificación a través de un medio en línea apropiado y fácilmente accesible que esté disponible las 24 horas del día, los 7 días de la semana. La AC DEBERÁ divulgar públicamente sus prácticas comerciales en la medida requerida por el esquema de auditoría seleccionado por la AC (consulte la Sección 8.1).

La Política de Certificados y la Declaración de Prácticas de Certificación están estructuradas de acuerdo con RFC 3647 e incluye todo el material requerido por RFC 3647.

2.3. Frecuencia de publicación

La AC DEBERÁ desarrollar, implementar, hacer valer y actualizar anualmente la Declaración de Prácticas de Certificación que describa en detalle como la AC implementa la última versión de estos Requerimientos.

2.4. Control de acceso a los repositorios

La AC debe publicar su Repositorio de manera solo lectura.

3. Identificación y autenticación

3.1. Nombres

3.1.1. Tipos de nombres

Los Certificados deben tener un nombre distintivo X.501 en el campo Subject y deben incorporan al menos los siguientes atributos:

- Personas naturales
    - País (C)
    - Organización (O)
    - Unidad Organizacional (OU)
    - Provincia (S)
    - Ciudad (L)
    - Nombre Común (CN)
    - Email (E)

- Persona jurídica
    - País (C)
    - Provincia (S)
    - Ciudad (L)
    - Razón social (O)
    - Nombres del representante legal (CN)
    - Email (E)

3.1.2. Necesidad de que los nombres sean significativos

Los Certificados emitidos por las AC de Dátil deben requerir la plena identificación del Suscriptor y la asignación de un nombre significativo a su certificado, para vincular la clave pública con su identidad.

3.1.3. Anónimos o seudónimos en los nombres

No se debe permitir a los Suscriptores usar anónimos o seudónimos en los nombres.

3.1.4. Reglas para interpretar varias formas de nombres

Los nombres de los Suscriptores se interpretan conforme a la norma ISO/IEC 9594 (X.500).

3.1.5. Unicidad de los nombres

El nombre distintivo de los Certificados será único para cada Suscriptor y está relacionado a la identificación del usuario sea este un dispositivo, persona natural o persona jurídica.

3.1.6. Reconocimiento, autenticación y roles de marcas registradas

Los Solicitantes de Certificados tienen prohibido solicitar certificados con contenido que infrinja la propiedad intelectual y derechos comerciales de terceros. Dátil no determina si los Aplicantes de Certificados son dueños de los derechos de propiedad intelectual en los nombres de los certificados ni se responsabiliza por el uso de los mismos.

3.2. Validación inicial de identidad

3.2.1. Método para probar la posesión de llave privada

No estipulado.

3.2.2. Autenticación de una organización o persona jurídica

La identidad del Solicitante se DEBE verificar usando las siguientes fuentes de información:

- Registros de instituciones públicas en la jurisdicción del Solicitante.
- Documentos enviados por el Solicitante tales como RUC y otros certificados legales vigentes.

Los procedimientos de verificación se describen en la respectiva Declaración de Prácticas de Certificación.

3.2.2.1. Identidad

La AC DEBE verificar que la identidad y dirección de la organización o persona jurídica, incluyendo la identidad de sus representantes y/o apoderados, presentadas en la Solicitud. La AC debe verificar la identidad y dirección del Solicitante usando documentación provista o mediante comunicación con al menos una de las siguientes:

1. Registro de creación o existencia legal provisto por una Entidad Gubernamental en la jurisdicción del Solicitante.
2. Una base de datos provista por terceros que es actualizada periódicamente y es considerada una Fuente de Datos Confiable.
3. Una visita física por parte de la AC o un tercero actuando como agente de la AC, o
4. Escrituras públicas.

3.2.2.2. Nombre comercial

No estipulado

3.2.2.3. Verificación del país

La AC DEBE verificar la dirección del Solicitante conforme a lo estipulado en la Sección 3.2.2.1.

3.2.3. Autenticación de una persona natural

La identidad de Solicitantes personas naturales se DEBE verificar usando las siguientes fuentes de información:

- Registros de instituciones públicas en la jurisdicción del Solicitante.
- Documentos enviados por el Solicitante tales como copia de identificación legal (ej. Cédula de identidad o pasaporte) y/o nombramiento de representante legal.

Los procedimientos de verificación se describen en la respectiva Declaración de Prácticas de Certificación.

3.2.3.1. Identidad

La AC DEBE verificar que la identidad y dirección de la persona natural presentadas en la Solicitud. La AC debe verificar la identidad y dirección del Solicitante usando documentación provista o o mediante comunicación con al menos una de las siguientes:

1. Cédula de identidad o pasaporte.
2. Una base de datos provista por terceros que es actualizada periódicamente y es considerada una Fuente de Datos Confiable.
3. Una visita física por parte de la AC o un tercero actuando como agente de la AC.

3.2.4. Información del solicitante no verificada

Toda la información en la forma de solicitudes y documentos enviada por el Solicitante es verificada para autenticar la identidad del mismo, aún cuando esta no forma parte de la información incluida en el Certificado. Se debe dejar constancia de cualquier información que no haya sido verificada.

3.2.5. Validación de la autoridad

Para validar la pertinencia de las Solicitudes de Certificados por parte del responsable de una entidad o persona jurídica, se debe verificar las facultades que dispone para el uso de un certificado electrónico, conforme a los documentos legales enviados en la Solicitud.

3.2.6. Criterios de interoperabilidad

La AC DEBE publicar todos los Certificados Cruzados que tengan a la AC como el Sujeto, dado que la AC haya aceptado esa relación de confianza.

3.3. Identificación y autenticación para solicitudes de nueva clave

3.3.1. Identificación y autenticación para emisión rutinaria de nueva clave

No estipulado.

3.3.2. Identificación y autenticación para emisión de una nueva llave después de revocación

No estipulado.

3.4. Identificación y autenticación para solicitudes de revocación

No estipulado.

4. Requerimientos operativos del ciclo de vida de certificados

4.1. Solicitud de Certificados

4.1.1. Tipos de certificados

Certificados de persona jurídica (representante legal)

Es un certificado cuyo suscriptor es una persona jurídica (ej. Empresas, fundaciones o instituciones públicas) e identifica al representante legal como firmante.

Certificados de persona jurídica (miembro de empresa)

Es un certificado cuyo suscriptor es una persona jurídica (ej. Empresas, fundaciones o instituciones públicas) e identifica al firmante como empleado de la empresa.

Certificados de persona natural

Es un certificado cuyo suscriptor es una persona natural.

En el Apéndice A se describen los datos de cada tipo de certificado.

4.1.2. Quién puede enviar una solicitud de certificado

Cualquier persona natural o jurídica debe poder solicitar Certificados.

En concordancia con la Sección 5.5.2, la AC DEBERÁ mantener una base de datos interna de todos los Certificados revocados y de las solicitudes de certificado revocadas por sospecha de fraude o cualquier otra preocupación sobre su uso. La AC DEBERÁ usar esta información para identificar solicitudes de certificado sospechosas.

4.1.3. Proceso de registro y responsabilidades

Antes de la emisión de un Certificado, la AC DEBERÁ obtener la siguiente documentación del Solicitante:

1. Una solicitud de certificado, que puede ser electrónica; y
2. Un Acuerdo de Suscriptor o Términos de Uso firmados, que pueden ser electrónicos.

La AC DEBE obtener cualquier documentación adicional que determine necesaria para cumplir con estos Requisitos.

Antes de la emisión de un Certificado, la AC DEBERÁ obtener del Solicitante una solicitud de certificado conforme al formato establecido y que cumpla con estos Requisitos. Una solicitud de certificado PUEDE ser suficiente para que se emitan varios Certificados al mismo Solicitante, sujeto al requisito de antigüedad y actualización en la Sección 4.2.1, siempre que cada Certificado esté respaldado por una solicitud de certificado válida y actual firmada por el Representante del Solicitante correspondiente en nombre de del solicitante. La solicitud de certificado PUEDE hacerse, enviarse y / o firmarse electrónicamente.

La solicitud de certificado DEBE contener una solicitud del Solicitante, o en su nombre, para la emisión de un Certificado, y una certificación del Solicitante, o en su nombre, de que toda la información que contiene es correcta.

4.2. Procesamiento de solicitudes de certificados

4.2.1. Funciones de identificación y autenticación

La solicitud de certificado PUEDE incluir toda la información de identidad sobre el Solicitante que se incluirá en el Certificado, y la información adicional que sea necesaria para que la AC obtenga del Solicitante para cumplir con esta Política y / o la Declaración de Prácticas de Certificación de la AC. En los casos en que la solicitud de certificado no contenga toda la

información necesaria sobre el Solicitante, la AC DEBERÁ obtener la información restante del Solicitante o, habiéndose obtenido de una fuente de datos confiable, independiente y de terceros, confirmar con el Solicitante. La AC DEBERÁ establecer y seguir un procedimiento documentado para verificar todos los datos solicitados por el Solicitante para su inclusión en el Certificado.

La información del solicitante DEBE incluir, entre otros, al menos un número de identificación legal (ej. Cédula, pasaporte o RUC).

La Sección 6.3.2 limita el período de validez de los Certificados de Suscriptor. La AC PUEDE usar los documentos y datos proporcionados en la Sección 3.2 para verificar la información del certificado, o puede reutilizar validaciones anteriores, siempre que la AC haya obtenido los datos o documentos de una fuente especificada en la Sección 3.2 o haya completado la validación en sí no más de 365 días antes de emitir el Certificado.

En ningún caso se puede reutilizar una validación previa si se obtuvieron datos o documentos utilizados en la validación anterior al tiempo máximo permitido para la reutilización de los datos o documentos antes de emitir el Certificado.

La AC DEBE desarrollar, mantener e implementar procedimientos documentados que identifiquen y requieran actividad de verificación adicional para las Solicitudes de Certificado de Alto Riesgo antes de la aprobación del Certificado, según sea razonablemente necesario para garantizar que dichas solicitudes se verifiquen adecuadamente bajo estos Requisitos.
Si un tercero delegado cumple con alguna de las obligaciones de la AC en virtud de esta sección, la AC DEBE verificar que el proceso utilizado por el tercero delegado para identificar y verificar aún más las solicitudes de certificados de alto riesgo proporciona al menos el mismo nivel de seguridad que los propios procesos de la AC.

4.2.2. Aprobación o rechazo de las solicitudes de certificado

Solo se podrán aprobar solicitudes que cumplan con estos requerimientos. Las solicitudes que no cumplan, serán rechazadas y el Solicitante será notificado por medios electrónicos (ej. Correo electrónico)

4.2.3. Tiempo para el procesamiento de solicitudes de certificados

No estipulado.

4.3. Emisión de certificados

4.3.1. Acciones realizadas durante la emisión del certificado

Los Certificados emitidos por la AC Raíz DEBERÁN requerir que un individuo autorizado por la AC (operador del sistema, oficial de operaciones o administrador de la ILP) ejecute un comando directo para que la AC Raíz firme un certificado.

4.3.2. Notificación al suscriptor por parte de la AC de la emisión de un certificado

La AC deberá notificar al Suscriptor por medios electrónicos (ej. email) cumpliendo con tiempos razonables de negocios.

4.4. Aceptación de los certificados

4.4.1. Conducta que constituye la aceptación de un certificado

La AC debe asegurarse de documentar la entrega del Certificado y establecer las políticas necesarias para dar por entregado el Certificado de no tener confirmación del cliente.

4.4.2. Notificación de la emisión del certificado por parte de la AC a otras entidades

No estipulado.

4.5. Uso del certificado y par de llaves

4.5.1. Uso del certificado y llave privada por parte del suscriptor

Ver Sección 9.6.3, provisiones 2 y 4.

4.5.2. Uso del certificado y llave privada por parte de un tercero que confía

No estipulado

4.6. Renovación de certificados

4.6.1. Circunstancias para renovar un certificado

La AC DEBE establecer las circunstancias bajo las cuales se permite renovar un Certificado.

4.6.2. Quién puede solicitar la renovación de un certificado

Ver Sección 4.4.1.

4.6.3. Procesamiento de renovación de certificados

Ver Sección 4.2.

4.6.4. Notificación de la emisión de un nuevo certificado al suscriptor

Ver Sección 4.3.2.

4.6.5. Conducta que constituye la aceptación de la renovación de un certificado

Ver Sección 4.4.1.

4.6.6. Publicación de la renovación de un certificado por parte de la AC

No estipulado.

4.6.7. Notificación de la emisión de un certificado por parte de la AC a otras entidades

No estipulado.

4.7. Cambio de llaves del certificado

4.7.1. Circunstancias para el cambio de llaves de un certificado

No estipulado.

4.7.2. Quién puede solicitar el cambio de llaves de un certificado

No estipulado.

4.7.3. Procesamiento de solicitudes de cambio de llaves de certificados

No estipulado.

4.7.4. Notificación de la emisión de un nuevo certificado al suscriptor

No estipulado.

4.7.5. Conducta que constituye la aceptación de un certificado con cambio de llaves

No estipulado.

4.7.6. Publicación de un certificado con cambio de llaves por parte de la AC

No estipulado.

4.7.7. Notificación de la emisión de un certificado por parte de la AC a terceros

No estipulado.

4.8. Modificación de un certificado

4.8.1. Circunstancias para la modificación de un certificado

No estipulado.

4.8.2. Quién puede solicitar la modificación de un certificado

No estipulado.

4.8.3. Procesamiento de solicitudes de modificación de certificados

No estipulado.

4.8.4. Notificación de la emisión de un nuevo certificado modificado al suscriptor

No estipulado.

4.8.5. Conducta que constituye la aceptación de un certificado modificado

No estipulado.

4.8.6. Publicación de un certificado modificado por parte de la AC

No estipulado.

4.8.7. Notificación de la emisión de un certificado modificado por parte de la AC a terceros

No estipulado.

4.9. Revocación y suspensión de certificados

4.9.1. Circunstancias para la revocación

4.9.1.1. Razones para revocar el Certificado de un Suscriptor

La AC DEBERÁ revocar un Certificado dentro del plazo de 24 horas si uno o más de los siguientes eventos ocurren:

- El Suscriptor solicita por escrito a la AC la revocación de un Certificado;
- El Suscriptor notifica a la AC que la solicitud de certificado original no fue autorizada y no otorga retroactivamente tal autorización;
- La AC obtiene evidencia de que la Llave Privada del Suscriptor correspondiente a la Llave Pública del Certificado ha sido comprometida y/o divulgada; o
- La AC obtiene evidencia de que alguno de los documentos presentados en la solicitud no son auténticos o no están actualizados.

La AC PODRÁ revocar un certificado dentro del plazo de 5 días si uno o más de los siguientes eventos ocurren:

- La AC ya no cumple con los requerimientos de las Secciones 6.1.5 y 6.1.6;
- La AC obtiene evidencia de que el Certificado ha sido mal utilizado;
- La AC se entera de que el Suscriptor ha violado una o más obligaciones del Acuerdo de Suscriptor o los Términos de Uso;
- La AC se entera de alguna circunstancia indicando que la información del Sujeto del certificado ya no corresponde a la identidad legal presentada en la solicitud de certificados;
- La AC se entera que se han hecho cambios materiales en la información contenida en el Certificado;
- La AC se entera que el Certificado no está siendo usado conforme a estos Requerimientos, la Política de Certificados o la Declaración de Prácticas de Certificación de la AC;
- La AC se entera que el Certificado está siendo usado para actividades fraudulentas.
- La AC se entera que el Certificado no fue emitido en concordancia con estos Requerimientos, la Política de Certificados o la Declaración de Prácticas de Certificación de la AC;

- La AC determina o se entera que cualquier información incluida en el Certificado no es exacta.
- La AC ya no puede emitir Certificados por cualquier circunstancia, a menos que la AC haya hecho arreglos para mantener continuamente los Repositorios CRL/OCSP.
- La revocación sea requerida por parte de la Política de Certificados de la AC o su Declaración de Prácticas de Certificación;
- La CA tiene conocimiento de un método demostrado o probado que expone que la Llave Privada del Suscriptor haya sido comprometida, que se hayan desarrollado métodos que puedan calcularla fácilmente en función de la Llave Pública (ej. http://wiki.debian.org/SSLkeys) o si existe evidencia clara que el método específico utilizado para generar la Llave Privada fue defectuoso.

4.9.1.2. Razones para revocar el Certificado de una AC Subordinada

La AC Emisora DEBERÁ revocar el Certificado de una AC Subordinada en un plazo de 7 días si ocurre uno o más de los siguientes eventos:

- La AC Subordinada solicita la revocación por escrito;
- La AC Subordinada notifica a la AC Emisora que la solicitud de certificado original no fue autorizada y no otorga retroactivamente tal autorización;
- La AC Emisora obtiene evidencia que la Llave Privada de la AC Subordinada correspondiente a la Llave Pública en el Certificado ha sido comprometida o divulgada y ya no cumple con los requerimientos de las Secciones 6.1.5 y 6.1.6;
- La AC Emisora obtiene evidencia que el Certificado ha sido mal utilizado;
- La AC Emisora se entera que el Certificado no fue emitido en concordancia o que la AC Subordinada no ha cumplido con este documento o la Política de Certificados y/o Declaración de Prácticas de Certificación respectiva.
- La AC Emisora determina que la información que aparece en el Certificado no es exacta o es engañosa.
- La AC Emisora o la AC Subordinada cesa operaciones por cualquier motivo y no ha hecho los arreglos con otra AC para proveer soporte de revocación para el Certificado.
- La AC Emisora o AC Subordinada pierde sus derechos de emitir Certificados conforme a estos requerimientos, a menos que la AC haya hecho arreglos para mantener continuamente los Repositorios CRL/OCSP; y
- La revocación es requerida por la Política de Certificados o Declaración de Prácticas de Certificación de la AC Emisora.

4.9.2. Quién puede solicitar revocación

El Suscriptor, la AR o AC Emisora pueden iniciar una revocación. Adicionalmente, los Suscriptores, Terceros que Confían, Proveedores de Aplicaciones de Software o cualquier otra parte pueden enviar Informes de Problemas de Certificados informando a la AC Emisora sobre causas razonables para revocar el Certificado.

4.9.3. Procedimiento para solicitar una revocación

La AC DEBERÁ proporcionar un proceso para que los Suscriptores soliciten la revocación de sus propios Certificados. El proceso DEBE describirse en la Política de Certificados o la Declaración de Prácticas de Certificación de la AC.

La AC DEBERÁ mantener una capacidad continua 24x7 para aceptar y responder a solicitudes de revocación e Informes de Problemas de Certificados.

La AC DEBERÁ proporcionar a los suscriptores, terceros de confianza, proveedores de software de aplicación y otros terceros instrucciones claras para informar sobre sospechas de compromisos de Llaves Privadas, uso indebido de certificados u otros tipos de fraude, compromiso, uso indebido, conducta inapropiada o cualquier otro asunto relacionado a los certificados. El AC DEBE divulgar públicamente las instrucciones a través de un medio en línea de fácil acceso y en la sección 1.5.2 de su DPC.

4.9.4. Período de gracia de solicitud de revocación

No estipulado.

4.9.5. Tiempo dentro del cual la AC debe procesar una solicitud de revocación

Dentro de las 24 horas posteriores a la recepción de un Informe de Problemas de Certificado, la AC DEBE investigar los hechos y circunstancias relacionados con el Informe de Problemas de Certificado y proporcionar un informe preliminar sobre sus hallazgos tanto al Suscriptor como a la entidad que presentó el Informe de Problemas de Certificado.

Después de revisar los hechos y circunstancias, la AC DEBE trabajar con el Suscriptor y cualquier entidad que envíe el Informe del Problemas del Certificado u otro aviso relacionado con la revocación para determinar si el certificado será revocado o no, y de ser así, una fecha en la que la AC realizará la revocación el certificado.

El período desde la recepción del Informe del Problemas de Certificado o el aviso relacionado con la revocación hasta la revocación publicada NO DEBE exceder el plazo establecido en la Sección 4.9.1.1. La fecha seleccionada por el AC DEBE considerar los siguientes criterios:

1. La naturaleza del supuesto problema (alcance, contexto, gravedad, magnitud, riesgo de daño);
2. Las consecuencias de la revocación (impactos directos y colaterales para los Suscriptores y Terceros que Confían);

3. La cantidad de Informes de Problemas de Certificados recibidos sobre un certificado o sub-certificado en particular;
4. La entidad que presenta la queja; y
5. Legislación relevante.

4.9.6. Requerimientos de chequeo de revocación de los Terceros que Confían

Luego de la emisión de un certificado, este puede ser revocado en cualquier momento de acuerdo a la sección 4.9.1. Por este motivo, los terceros que confían deben chequear el estatus de revocación de todos los certificados que contengan una referencia a un servicio OCSP y/o DPC.

4.9.7. Frecuencia de emisión de la LRC

Para el estatus de Certificados de Suscriptores:

Si la AC publica su LRC, entonces la AC DEBERÁ actualizar y re-emitir las LRCs al menos cada siete días y el valor del campo nextUpdate NO DEBERÁ ser mayor que diez más allá del campo thisUpdate.

Para el estatus de Certificados de ACs Subordinadas:

La AC DEBERÁ actualizar y re-emitir las LRC al menos (i) una vez cada doce meses (ii) dentro de 24 horas de haber revocado el Certificado de una AC Subordinada, y el valor del campo nextUpdate NO DEBE ser menor de doce meses más allá del campo thisUpdate.

4.9.8. Latencia máxima para las CRL

No estipulado.

4.9.9. Disponibilidad de chequeo en línea de revocación/status

Las respuestas OCSP DEBEN cumplir con RFC6960 y / o RFC5019. Las respuestas de OCSP DEBEN:

1. Estar firmadas por la AC que emitió los Certificados cuyo estado de revocación se está verificando, o
2. Estar firmado por un servidor de OCSP cuyo Certificado está firmado por la AC que emitió el Certificado cuyo estado de revocación se está verificando.

En el último caso, el Certificado de firma OCSP DEBE contener una extensión de tipo id-pkix-ocsp-nocheck, tal como se define en RFC6960.

4.9.10. Requerimientos de chequeo en línea de revocación

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

Para el estado de Certificados de Suscriptores:

- La AC DEBERÁ actualizar la información a través de OCSP al menos cada cuatro días. Las respuestas de OCSP de este servicio DEBEN tener un tiempo de vencimiento máximo de diez días.

Para el estado de los Certificados de AC Subordinadas:

- La AC DEBERÁ actualizar la información vía OCSP (i) al menos cada doce meses; y (ii) dentro de las 24 horas posteriores a la revocación de un Certificado de AC Subordinada.

Si el servidor OCSP recibe una solicitud para el estado de un número de serie del certificado que está "sin usar", entonces el respondedor NO DEBE responder con un estado "ok". Si el servidor OCSP es para una AC que no está técnicamente restringida de acuerdo con la Sección 7.1.5, el respondedor NO DEBE responder con un estado "ok" para tales solicitudes.

La AC DEBE monitorear al servidor OCSP para solicitudes de números de serie "no utilizados" como parte de sus procedimientos de respuesta de seguridad.

El servidor OCSP PUEDE proporcionar respuestas definitivas sobre números de serie de certificados "reservados", en el caso que hubiera un Certificado correspondiente que coincida con el Precertificado [RFC6962].

Un número de serie del certificado dentro de una solicitud OCSP es una de las siguientes tres opciones:

1. “asignado” si la AC Emisora ha emitido un Certificado con ese número de serie, utilizando cualquier clave actual o anterior asociada con esa firma de AC; o
2. "reservado" si (a) la AC Emisora ha emitido un Precertificado [RFC6962] con ese número de serie; o (b) un Certificado de Firma de Precertificado [RFC6962] asociado con la AC Emisora; o
3. "no utilizado" si no se cumple ninguna de las condiciones anteriores.

4.9.11. Otras formas disponibles de publicación de revocaciones

No estipulado.

4.9.12. Requerimientos especiales relacionados a compromiso de llaves

Ver Sección 4.9.1.

4.9.13. Circunstancias para la suspensión

El Repositorio NO DEBE incluir registros que indiquen que un Certificado está suspendido.

4.9.14. Quién puede solicitar la suspensión

No aplica.

4.9.15. Procedimiento para la solicitud de suspensión

No aplica.

4.9.16. Límites para el período de suspensión

No aplica

4.10. Servicios de estatus de certificados

4.10.1. Características operacionales

Los registros de revocación en las LRC y respuestas OCSP NO DEBEN ser removidas hasta después de la Fecha de Expiración del Certificado revocado.

4.10.2. Disponibilidad del servicio

El AC DEBE operar y mantener su capacidad LRC y OCSP con recursos suficientes para proporcionar un tiempo de respuesta de diez segundos o menos en condiciones normales de operación.

La AC DEBERÁ mantener un repositorio en línea 24x7 con el software necesario para verificar automáticamente el estado actual de todos los certificados no vencidos emitidos por la AC.
El AC DEBERÁ mantener una capacidad continua las 24 horas del día, los 7 días de la semana, para responder internamente a Informes de Problemas de Certificados de alta prioridad y, cuando corresponda, remitir dicha queja a las autoridades policiales y / o revocar un Certificado que sea objeto de dicha queja.

4.10.3. Características opcionales

No estipulado.

4.11. Fin de la suscripción

No estipulado.

4.12. Recuperación de llaves

4.12.1. Política y prácticas custodia y recuperación de llaves

No estipulado.

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

No estipulado.

5. Controles de seguridad física, administración y operación

La AC DEBE desarrollar, implementar y mantener un Programa de Seguridad Integral diseñado para:

1. Proteger la confidencialidad, integridad y disponibilidad de los Datos del Certificado y los Procesos de Gestión del Certificado;
2. Proteger contra amenazas o peligros anticipados a la confidencialidad, integridad y disponibilidad de los Datos del Certificado y los Procesos de Gestión del Certificado;
3. Proteger contra el acceso, uso, divulgación, alteración o destrucción no autorizados o ilegales de los Datos del Certificado o los Procesos de Gestión del Certificado;
4. Proteger contra la pérdida accidental o destrucción o daño de los Datos del Certificado o los Procesos de Gestión del Certificado; y
5. Cumplir con todos los demás requisitos de seguridad aplicables a la AC por ley.

El Proceso de Gestión de Certificados DEBE incluir:

1. Seguridad física y controles ambientales;
2. Controles de integridad del sistema, incluida la gestión de la configuración, el mantenimiento de la integridad de código confiable y detección / prevención de malware;
3. seguridad de red y gestión de firewall, incluidas restricciones de puerto y filtro de dirección IP;
4. gestión de usuarios, asignaciones separadas de roles confiables, educación, concientización y capacitación; y

5. controles de acceso lógico, registro de actividades y registros de inactividad para proporcionar respaldo individual de cada acceso.

El Programa de Seguridad de la AC DEBE incluir una evaluación de riesgos anual que:

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

Con base en la Evaluación de Riesgos, la AC DEBE desarrollar, implementar y mantener un Plan de Seguridad que consista en procedimientos, medidas y productos de seguridad diseñados para lograr los objetivos establecidos anteriormente y para administrar y controlar los riesgos identificados durante la Evaluación de Riesgos, conmensurado con la sensibilidad de los Datos del Certificado y los Procesos de Gestión del Certificado. El plan de seguridad DEBE incluir salvaguardas administrativas, organizativas, técnicas y físicas adecuadas a la sensibilidad de los Datos del Certificado y los Procesos de Gestión del Certificado. El plan de seguridad también DEBE tener en cuenta la tecnología disponible en ese momento y el costo de implementar las medidas específicas, y DEBE implementar un nivel razonable de seguridad apropiado al daño que pueda resultar de una violación de la seguridad y la naturaleza de los datos a proteger.

5.1. Controles físicos

La infraestructura de la AC deberá estar localizada y operada desde instalaciones seguras de Dátil. Se DEBEN establecer procedimientos que prohiban el acceso no autorizado y la entrada a las áreas de las instalaciones donde operen los sistemas de la AC.

5.1.1. Localización del sitio y construcción

No estipulado.

5.1.2. Acceso físico

La AC DEBE tener controles de seguridad física apropiados para restringir el acceso a todo el hardware y software utilizado para proporcionar los Servicios de AC. El acceso a dicho hardware y software DEBERÁ limitarse al personal que desempeñe roles de confianza y al proveedor de servicios.

5.1.3. Energía y aire acondicionado

No estipulado.

5.1.4. Exposición a agua

No estipulado.

5.1.5. Prevención y protección contra incendios

No estipulado.

5.1.6. Almacenamiento de medios físicos

No estipulado.

5.1.7. Eliminación de residuos

No estipulado.

5.1.8. Copia de seguridad fuera del sitio

No estipulado.

5.2. Controles procedurales

5.2.1. Roles de confianza

No estipulado.

5.2.2. Número de personas requeridas para una tarea

La Llave Privada DEBE respaldarse, almacenarse y recuperarse solo por parte de personas en Roles de Confianza usando, al menos, control dual en un ambiente físicamente seguro.

5.2.3. Identificación y autenticación para cada rol

No estipulado

5.2.4. Roles que requieren separación de deberes

No estipulado.

5.3. Controles de personal

5.3.1. Calificaciones, experiencia y requerimientos de autorización

Antes de la participación de cualquier persona en el proceso de gestión de certificados, ya sea como empleado, agente o contratista independiente de la AC, la AC DEBE verificar la identidad y la confiabilidad de dicha persona.

5.3.2. Chequeo de antecedentes

No estipulado.

5.3.3. Requerimientos de entrenamiento

La AC DEBERÁ proporcionar a todo el personal que realiza tareas de verificación de información, capacitación en habilidades que cubra el conocimiento básico de Infraestructura de Llave Pública, políticas y procedimientos de verificación (incluyendo la Política de Certificados de la AC y/o la Declaración de Prácticas de Certificación), amenazas comunes a la verificación de información (incluyendo phishing y otras tácticas de ingeniería social) y estos Requisitos.

La AC DEBE mantener registros de dicha capacitación y garantizar que el personal encargado de las tareas de Especialista en Validación mantenga un nivel de habilidad que les permita realizar dichas tareas satisfactoriamente.

La AC DEBE documentar que cada Especialista en Validación posee las habilidades requeridas por una tarea antes de permitir que el Especialista en Validación realice esa tarea.

La AC DEBERÁ exigir a todos los Especialistas en Validación que aprueben un examen proporcionado por la AC sobre los requisitos de verificación de información descritos en estos Requisitos.

5.3.4. Frecuencia y requerimientos de re-entrenamiento

Todo el personal en Roles de Confianza DEBERÁ mantener niveles de habilidad consistentes con los programas de capacitación y desempeño de la AC.

5.3.5. Secuencia y frecuencia de rotación de personal

No aplica.

5.3.6. Sanciones por acciones no autorizadas

No estipulado.

5.3.7. Contratistas independientes

El AC DEBE verificar que el personal del tercero delegado involucrado en la emisión de un Certificado cumpla con los requisitos de capacitación y habilidades de la Sección 5.3.3 y los requisitos de retención de documentos y registro de eventos de la Sección 5.4.1.

5.3.8. Documentación provista al personal

No estipulado.

5.4. Procedimientos de registros de auditoría

5.4.1. Tipos de eventos registrados

La AC y cada tercero delegado DEBERÁN registrar detalles de las acciones tomadas para procesar una solicitud de certificado y emitir un Certificado, incluyendo toda la información generada y la documentación recibida en relación con la solicitud de certificado; la hora y fecha; y el personal involucrado. La AC DEBE poner estos registros a disposición de su Auditor calificado como prueba del cumplimiento de la AC con estos Requisitos.

La AC DEBE registrar al menos los siguientes eventos:

1. Eventos de administración del ciclo de vida Llave de la AC, que incluyen:
    a. Generación de claves, respaldo, almacenamiento, recuperación, archivo y destrucción; y
    b. Eventos de gestión del ciclo de vida del dispositivo criptográfico.

2. Eventos de administración del ciclo de vida del certificado de la AC y del Suscriptor, que incluyen:
    a. Solicitudes de certificados, solicitudes de renovación y nueva clave, y revocación;
    b. Todas las actividades de verificación estipuladas en estos Requisitos y la Declaración de Prácticas de Certificación.
    c. Fecha, hora, número de teléfono utilizado, personas con quienes se habló y resultados finales de la verificación mediante llamadas telefónicas;
    d. Aceptación y rechazo de solicitudes de certificados; Frecuencia de procesamiento de registro
    e. Emisión de certificados; y
    f. Generación de listas de revocación de certificados y entradas de OCSP.

3. Eventos de seguridad, que incluyen:
    a. Intentos exitosos y fallidos de acceso al sistema PKI;
    b. Acciones del sistema realizadas;
    c. Cambios en el perfil de seguridad;
    d. Fallos del sistema, fallas de hardware y otras anomalías;
    e. Actividades de firewall y enrutador; y
    f. Entradas y salidas de la instalación de AC.

4. De existir, las entradas de registro DEBEN incluir los siguientes elementos:
    a. Fecha y hora de entrada;
    b. Identidad de la persona que hace la entrada del diario; y
    c. Descripción de la entrada.

5.4.2. Frecuencia de procesamiento de registros

No estipulado

5.4.3. Período de retención de registros de auditoría

L AC DEBE conservar los registros de auditoría generados durante al menos siete años. La AC DEBE poner estos registros de auditoría a disposición de su Auditor calificado, previa solicitud.

5.4.4. Protección de los registros de auditoría

No estipulado.

5.4.5. Procedimientos de respaldo de registros de auditoría

No estipulado.

5.4.6. Sistemas de recolección de registros (internos vs. externos)

No estipulado.

5.4.7. Notificaciones sobre eventos de interés

No estipulado.

5.4.8. Evaluaciones de vulnerabilidad

El programa de seguridad de la AC DEBE incluir una evaluación de riesgos anual que:

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

5.5. Archivo de registros

5.5.1. Tipos de registros archivados

No estipulado

5.5.2. Período de retención del archivo

La AC DEBERÁ conservar toda la documentación relacionada con las solicitudes de certificados y su verificación, y todos los Certificados y la revocación de los mismos, durante al menos siete años después de que cualquier Certificado basado en esa documentación deje de ser válido.

5.5.3. Protección del archivo

No estipulado.

5.5.4. Procedimientos de respaldo de archivos

No estipulado

5.5.5. Requerimientos de sellado de tiempo de los registros

No estipulado

5.5.6. Sistema de recolección de archivos (interno o externo)

No estipulado.

5.5.7. Procedimientos para obtener y verificar un archivo

No estipulado.

5.6. Cambio de llaves

No estipulado.

5.7. Recuperación de desastres

5.7.1. Procedimientos para manejo de incidentes

Las organizaciones de la AC deberán tener un Plan de Respuesta a Incidentes y un Plan de Recuperación ante Desastres.

La AC DEBERÁ documentar un Procedimiento de Recuperación de Desastres y Continuidad del negocio diseñado para notificar y proteger razonablemente a los proveedores, suscriptores y terceros que confían en caso de desastre, compromiso de seguridad o falla comercial.

La AC no está obligada a divulgar públicamente sus planes de continuidad de negocios, pero DEBERÁ poner a disposición de los auditores de la AC su plan de continuidad de negocios y sus planes de seguridad. La AC DEBE probar, revisar y actualizar anualmente estos procedimientos.

El plan de continuidad del negocio DEBE incluir:

1. Las condiciones para activar el plan,
2. Procedimientos de emergencia,
3. Procedimientos de reserva,
4. Procedimientos de reanudación,
5. Un cronograma de mantenimiento para el plan;
6. Requisitos de sensibilización y educación;
7. Las responsabilidades de los individuos;
8. Objetivo del tiempo de recuperación;
9. Pruebas periódicas de planes de contingencia.
10. El plan de la AC para mantener o restaurar las operaciones comerciales de la AC de manera oportuna luego de la interrupción o falla de los procesos comerciales críticos,
11. Requisito de almacenar materiales criptográficos críticos (es decir, dispositivos criptográficos seguros y materiales de activación) en una ubicación alternativa;
12. Definición de qué constituye una interrupción del sistema aceptable y tiempo de recuperación,
13. Con qué frecuencia se toman copias de seguridad de la información comercial esencial y el software;
14. La distancia de las instalaciones de recuperación al sitio principal de la AC; y
15. Procedimientos para asegurar su instalación en la medida de lo posible durante el período de tiempo siguiente a un desastre y antes de restaurar un entorno seguro en el sitio original o remoto.

5.7.2. Procedimientos de recuperación si los recursos de cómputo, software y/o datos están corrompidos

No estipulado.

5.7.3. Procedimientos de recuperación después de la divulgación de una llave

No estipulado.

5.7.4. Capacidades de continuidad de negocios luego de un desastre

No estipulado.

5.8. Terminación de la AC o AR

No estipulado.

6. Controles técnicos de seguridad

6.1. Generación e instalación de un par de llaves

6.1.1. Generación de un par de llaves

6.1.1.1. Generación de un par de llaves de la AC

Para los pares de llaves de la AC Raíz que (i) se utilizan como pares de llaves de la AC Raíz o (ii) pares de claves generados para una AC Subordinada que no sea el operador de la AC raíz o un afiliado de la AC Raíz, la AC DEBERÁ:

1. preparar y seguir una secuencia de comandos de generación llave,
2. Hacer que un auditor calificado sea testigo del proceso de generación del par de llaves de la AC o grabe un video de todo el proceso de generación del par de llaves de la AC, y
3. haga que un auditor calificado emita un informe en el que opine que la AC siguió su ceremonia de llaves durante su proceso de generación de llaves y certificados y que se aplicaron los controles utilizados para garantizar la integridad y confidencialidad del par de llaves.

Para otros pares de llaves de la AC que son para el operador de la AC Raíz o un afiliado de la AC raíz, la AC DEBE:

1. preparar y seguir un guión de generación de llaves y
2. hacer que un auditor calificado sea testigo del proceso de generación del par de llaves de la AC o grabar un video de todo el proceso de generación del par de llaves de la AC.

En todos los casos, la AC DEBERÁ:

1. generar las llaves en un entorno físicamente seguro como se describe en la Declaración de Práctica de Certificación de la AC;
2. generar las llaves de la AC utilizando personal en Roles de Confianza, bajo los principios de control de múltiples personas y división de conocimiento;
3. generar las llaves de la AC dentro de los módulos criptográficos que cumplan con los requisitos técnicos y comerciales aplicables como se establecen en la Declaración de Prácticas de Certificación de la AC;
4. registrar sus actividades de generación de llaves de la AC; y
5. Mantener controles efectivos para proporcionar una seguridad razonable de que la llave privada fue generada de acuerdo con los procedimientos descritos en la Declaración de Práctica de Certificación y (si corresponde) su guión de generación de llaves.

6.1.1.2. Generación de un par de llaves de una AR

No estipulado

6.1.1.3. Generación de un par de llaves del Suscriptor

La AC DEBE rechazar una solicitud de certificados si la Llave Pública enviada no cumple con los requerimientos establecidos en las Secciones 6.1.5 y 6.1.6 o si se conoce que utilizan una Llave Privada débil.

6.1.2. Envío de la llave privada al suscriptor

Las partes que no sean el suscriptor NO DEBERÁN archivar la llave privada del Suscriptor sin la autorización del Suscriptor. Si la AC o cualquiera de sus AR designadas generó la llave privada en nombre del suscriptor, entonces la AC cifrará la llave privada para su envío al Suscriptor.

Si la AC o cualquiera de sus AC designadas se dan cuenta de que la llave privada del suscriptor se ha comunicado a una persona no autorizada o una organización no afiliada con el suscriptor, la AC revocará todos los certificados que incluyan la llave pública correspondiente a la llave privada comunicada.

6.1.3. Envío de la clave pública al emisor del certificado

No estipulado

6.1.4. Envío de la clave pública a terceros relacionados

No estipulado.

6.1.5. Tipos de algoritmo y tamaños de llaves

Los Certificados DEBEN cumplir los siguientes requerimientos de tipos de algoritmos y tamaños de llaves.

Los Certificados de la AC Raíz, AC Subordinada y de Suscriptores, siguen los mismos requerimientos:

Tipos	**Valores permitidos**
Algoritmo de Digest	SHA-256, SHA-384 o SHA-512
Tamaño mínimo de módulo RSA (bits	2048
Curva ECC	NIST P-256, P-384, o P521
Tamaño mínimo de módulo DSA y divisor	L=2048 N=225 o L=2048 N=256

L y N (las longitudes de bits del módulo p y el divisor q, respectivamente) se describen en FIPS 186-4.

6.1.6. Generación de parámetros de clave pública y control de calidad

RSA: La AC DEBE confirmar que el valor del exponente público es un número impar igual a 3 o más. Además, el exponente público DEBE estar en el rango entre 216 + 1 y 2256-1. El módulo también DEBE tener las siguientes características: un número impar, no la potencia de un primo, y no tener factores menores que 752. [Fuente: Sección 5.3.3, NIST SP 800-89]

ECC: La AC DEBE confirmar la validez de todas las llaves utilizando la Rutina de validación de clave pública completa de ECC o la Rutina de validación de clave pública parcial de ECC. [Fuente: Secciones 5.6.2.5 y 5.6.2.6, respectivamente, NIST SP 800-56A].

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

Las llaves privadas correspondientes a los certificados raíz NO DEBEN utilizarse para firmar certificados, excepto en los siguientes casos:

1. Certificados autofirmados para representar la propia AC raíz;
2. Certificados para AC subordinadas y certificados cruzados;
3. Certificados para fines de infraestructura (certificados de función administrativa, operación interna de la AC); y
4. Certificados para la verificación de respuesta OCSP.

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

La AC DEBERÁ implementar salvaguardas físicas y lógicas para evitar la emisión no autorizada de certificados. La protección de la llave privada fuera del sistema o dispositivo validado especificado anteriormente DEBE consistir en seguridad física, cifrado o una combinación de ambos, implementados de manera que evite la divulgación de la llave privada. La AC DEBE cifrar su llave privada con un algoritmo y una longitud de clave que, de acuerdo con el estado de la técnica, son capaces de resistir ataques criptoanalíticos durante la vida residual de la llave cifrada o parte de la llave.

6.2.1. Estándares y controles del módulo criptográfico

No estipulado.

6.2.2. Control multipersona de la llave privada (n de m)

No estipulado.

6.2.3. Custodia de clave privada

No estipulado.

6.2.4. Copia de seguridad de clave privada

Ver Sección 5.2.2.

6.2.5. Archivo de clave privada

Las partes que no sean la AC Subordinada NO DEBERÁN archivar las llaves privadas de la AC Subordinada sin autorización de la AC Subordinada.

6.2.6. Transferencia de clave privada hacia o desde un módulo criptográfico

Si la AC Emisora generó la llave privada en nombre de la AC Subordinada, entonces la AC Emisora DEBE cifrar la llave privada para su transporte a la AC Subordinada. Si la AC Emisora se da cuenta de que la llave privada de una AC Subordinada se ha comunicado a una persona no autorizada o una organización no afiliada a la AC Subordinada, la AC Emisora DEBERÁ revocar todos los certificados que incluyen la llave pública correspondiente a la llave privada comunicada.

6.2.7. Almacenamiento de clave privada en módulo criptográfico

La AC DEBERÁ proteger su llave privada en un sistema o dispositivo que haya sido validado para cumplir al menos FIPS 140 nivel 3 o un perfil de protección de criterios comunes u objetivo de seguridad apropiado, EAL 4 (o superior), que incluya requisitos para proteger la llave privada y otros activos contra amenazas conocidas.

6.2.8. Método de activación de clave privada

No estipulado.

6.2.9. Método de desactivación de clave privada

No estipulado.

6.2.10. Método de destrucción de clave privada

No estipulado.

6.2.11. Clasificación del módulo criptográfico

No estipulado.

6.3. Otros aspectos de la administración de pares de llaves

6.3.1. Archivo de clave pública

No estipulado.

6.3.2. Periodos operativos de certificado y períodos de uso de pares de claves

Los certificados deben ser válidos desde el momento de la firma, a menos que se especifique lo contrario en la estructura de validez del certificado, hasta el final indicado en el tiempo de vencimiento del certificado.

Los Certificados de Suscriptores se emiten por un período de un, dos, tres o cinco años de acuerdo con la Declaración de Prácticas de Certificación respectiva.

6.4. Datos de activación

6.4.1. Generación e instalación de datos de activación

No estipulado.

6.4.2. Protección de datos de activación

No estipulado.

6.4.3. Otros aspectos de los datos de activación.

No estipulado.

6.5. Controles de seguridad informática

6.5.1. Requisitos técnicos específicos de seguridad informática

La AC DEBE forzar el uso de autenticación de doble factor en todas las cuentas que puedan actuar sobre la emisión de certificados.

6.5.2. Calificación de seguridad informática

No estipulado.

6.6. Controles técnicos del ciclo de vida

6.6.1. Controles de sistema de desarrollo

No estipulado.

6.6.2. Controles de gestión de seguridad

No estipulado.

6.6.3. Controles de seguridad de ciclo de vida

No estipulado.

6.6. Controles de seguridad de redes

No estipulado.

6.7. Sellado de tiempo

No estipulado.

7. Perfil de certificados, LRC y OCSP

7.1. Perfil de certificados

El AC DEBE cumplir con los requisitos técnicos establecidos en la Sección 2.2 - Publicación de información, Sección 6.1.5 - Tamaños clave y Sección 6.1.6 - Generación de parámetros de clave pública y verificación de calidad.

Las AC DEBERÁN generar números de serie de certificados no secuenciales mayores que cero (0) que contengan al menos 64 bits de salida de un CSPRNG.

7.1.1. Números de versión

Los Certificados DEBEN ser de tipo X.509 v3.

7.1.2. Contenido del Certificado y Extensiones; Aplicación de RFC 5280

Esta sección especifica los requerimientos adicionales para el contenido de los Certificados y extensiones de Certificados generados por la AC

7.1.2.1. Certificado de AC Raíz

a. basicConstraints

Esta extensión DEBE aparecer como extensión crítica. El campo cA debe ser true. El campo pathLenConstraint NO DEBE ser estar presente.

b. keyUsage

Esta extensión DEBE estar presente y DEBE ser marcada como crítica. Las posiciones de bits para keyCertSign y cRLSign DEBEN estar establecidas. Si la Llave Privada de la AC Raíz es usada para firmar respuestas OCSP, entonces el bit de digitalSignature DEBE establecerse.

c. certificatePolicies

Esta extensión NO DEBE estar presente.

d. extendedKeyUsage

Esta extensión NO DEBE estar presente.

7.1.2.2. Certificado de AC Subordinada

a. certificatePolicies

Esta extensión DEBE estar presente y NO DEBE ser marcada como crítica.
certificatePolicies:policyIdentifier (Requerido)

Los siguientes campos PUEDEN estar presentes si la AC Subordinada no está afiliada a la entidad que controla la AC Raíz.

certificatePolicies:policyQualifiers:policyQualifierId (Opcional) id-qt 1 [RFC 5280]
certificatePolicies:policyQualifiers:policy:qualifier:cPSuri (Opcional)

La URL HTTP para la Política de Certificados, Declaración de Prácticas de Certificación, Acuerdo con Terceros que Confían y cualquier otra información provista por la AC.

b. cRLDistributionPoints

Esta extensión DEBE estar presente y NO DEBE ser marcada como crítica. DEBE contener una URL HTTP al servicio LRC de la AC.

c. authorityInformationAccess

Esta extensión DEBE estar siempre presente. NO DEBE ser marcada como crítica y DEBE incluir la URL HTTP del servidor OCSP de la AC Emisora (accessMethod = 1.3.6.1.5.5.7.48.1). DEBE también incluir la URL HTTP del certificado de la AC Emisora.

d. basicConstraints

Esta extensión DEBE estar presente y DEBE ser marcada como crítica. El campo cA DEBE ser marcado como true. El campo pathLenConstraint PUEDE estar presente.

e. keyUsage

Esta extensión DEBE estar presente y DEBE ser marcada como crítica. Las posiciones de bits para keyCertSign y cRLSign DEBEN ser marcadas como true. Si la Llave Privada de la AC

Subordinada se usa para firmar respuestas OCSP, entonces el bit de digitalSignature debe ser establecido.

7.1.2.3. Certificado de Suscriptor

a. certificatePolicies

Esta extensión DEBE estar presente y NO DEBE ser marcada como crítica.

certificatePolicies: policyIdentifier (Requerido)

Un Identificador de Políticas, según lo defina la AC emisora, que indica una Política de Certificados, declarando la adherencia de la AC emisora y el cumplimiento de esos requerimientos.

Las siguientes extensiones PUEDEN estar presentes:
certificatePolicies:policyQualifiers:policyQualifierId (Recomendado)

Id-qt 1 [RFC 5280]. certificatePolicies: policyQualifiers:qualifiers:cPSuri (Opcional)

La URL HTTP de la Declaración de Prácticas de Certificación, Acuerdo con Terceros que Confían y cualquier otra información provista por la AC.

b. cRLDistributionPoints

Esta extensión DEBE estar presente y NO DEBE ser marcada como crítica. DEBE contener una URL HTTP al servicio LRC de la AC.

c. authorityInformationAccess

Esta extensión DEBE estar siempre presente. NO DEBE ser marcada como crítica y DEBE incluir la URL HTTP del servidor OCSP de la AC Emisora (accessMethod = 1.3.6.1.5.5.7.48.1). DEBE también incluir la URL HTTP del certificado de la AC Emisora.

d. basicConstraints

Esta extensión DEBE estar presente y DEBE ser marcada como crítica. El campo cA DEBE ser marcado como true. El campo pathLenConstraint PUEDE estar presente.

e. keyUsage

Esta extensión DEBE estar presente y DEBE ser marcada como crítica. Las posiciones de bits para keyCertSign y cRLSign DEBEN ser marcadas como true. Si la Llave Privada de la AC Subordinada se usa para firmar respuestas OCSP, entonces el bit de digitalSignature debe ser establecido.

7.1.2.4. Todos los Certificados

Todos los demás campos y extensiones DEBEN establecerse de acuerdo con RFC 5280. La AC NO DEBE emitir un Certificado que contenga un indicador de keyUsage, extendedKeyUsage,

extensiones de Certificado u otros datos no especificados en la Sección 7.1.2.1, 7.1.2.2 o 7.1 .2.3 a menos que la AC tenga conocimiento de una razón para incluir los datos en el Certificado.

Las extensiones privadas de los certificados deben utilizar un OID para el cual el Solicitante demuestra la propiedad, o el solicitante pueda demostrar de otra manera el derecho de hacer valer los datos en un contexto público.

7.1.2.5. Aplicación de RFC 5280

Para fines de aclaración, un Precertificado, como se describe en RFC 6962 - Certificate Transparency, no se considerará un "certificado" sujeto a los requisitos de RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile bajo estos requisitos de referencia.

7.1.3. Identificadores de Objeto de Algoritmos

No estipulado.

7.1.4. Formas de nombres

7.1.4.1. Información del emisor

El contenido del campo Distinguished Name del Emisor del Certificado DEBE coincidir con el campo Subject DN de la AC Emisora con el objetivo de soportar nombres encadenados según lo especificado en RFC 5280, Sección 4.1.2.4.

7.1.4.2. Información del Sujeto - Certificados de Suscriptor

Al emitir el Certificado, la AC declara que siguió el procedimiento establecido en su Política de Certificados y/o Declaración de Prácticas de Certificación para verificar que, a partir de la fecha de emisión del Certificado, toda la Información del Sujeto era exacta.

7.1.4.2.1. Campos de Nombre Distintivo

a. Campo: subject:commonName (OID 2.5.4.3)

Requerido: Si
Contenido: DEBE incluir el nombre completo de la persona natural o representante de la organización.

b. Campo: subject:OrganizationName (OID 2.5.4.10) Opcional

Contenido: Debe incluir el nombre legal de la organización del Solicitante.

7.1.4.2.2. Campos de Extensión de Nombre Alternativo

c. Campo: subject:SubjectAlternativeName (OID 2.5.29.17) Requerido

Contenido: Debe incluir el email de la persona o representante de la organización.

7.1.5. Restricciones de nombres

Para los Certificados de AC Subordinadas que son considerados técnicamente restringidos, el Certificado DEBE incluir una extensión de ExtendedKeyUsage (EKU) especificando todos los usos de llaves que el Certificado de la AC Subordinada está autorizado para incluir como usos en los Certificados que emite. El anyExtendedKeyUsage KeyPurposeId NO DEBE aparecer en esta extensión.

7.1.6. Identificador de Objeto de la Política de Certificados

7.1.6.1. Identificadores reservados para la Política de Certificados

No estipulado.

7.1.6.2. Certificados de AC Raíz

El Certificado de la AC Raíz NO DEBE contener la extensión certificatePolicies.

7.1.6.3. Certificados de AC Subordinadas

No estipulado

7.1.6.4. Certificados de Suscriptor

Un Certificado emitido a un Suscriptor DEBE contener uno o más identificadores de políticas, definidos por la AC Emisora, en la extensión certificatePolicies del Certificado que indique la adherencia y cumplimiento de estos Requerimientos. Las ACs que cumplan con estos Requerimientos PODRÁN también declarar una o más OIDs reservadas en estos Certificados.

Las ACs Emisoras DEBERÁN documentar en estas Políticas de Certificados o Declaración de Práctica de Certificación que los Certificados que emite contienen los identificadores de política especificados son gestionados en concordancia con estos Requerimientos.

7.1.7. Extensión de Restricciones de Políticas de Uso

No estipulado.

7.1.8. Sintaxis de calificadores de políticas y semántica

No estipulado.

7.1.9. Procesamiento de semántica para las extensiones críticas de Política de Certificados

No estipulado.

7.2. Perfil de LRC

7.2.1. Número de versión

No estipulado

7.2.2. Extensiones de LRC y extensiones de LRC

No estipulado.

7.3. Perfil OCSP

7.3.1. Número de versión

No estipulado.

7.3.2. Extensiones OCSP

No estipulado.

8. Auditoría de cumplimiento y otras declaraciones

La AC deberá en todo momento:

1. Emitir Certificados y operar su ILP en concordancia con las leyes aplicables a su negocio y los Certificados que emite en cada jurisdicción en la que opere.
2. Cumplir con estos Requerimientos.
3. Cumplir con los requerimientos de auditoría establecidos en esta sección; y
4. Estar autorizado como una Autoridad de Certificación por la Entidad de Control de la jurisdicción donde opere, en el caso que las leyes de esa jurisdicción lo requiera para la emisión de Certificados.

8.1. Frecuencia o circunstancias de la evaluación

Los Certificados que pueden usarse para emitir nuevos Certificados DEBEN estar restringidos técnicamente de acuerdo con la sección 7.1.5 y auditados de acuerdo con la sección 8.7, o sin

restricciones y totalmente auditados de acuerdo con todos los requisitos restantes de esta sección.

Se considera que un Certificado puede usarse para emitir nuevos certificados si contiene una extensión X.509v3 basicConstraints, con el booleano cA establecido en verdadero y, por lo tanto, es por definición un Certificado de AC Raíz o un Certificado de AC Subordinada.

El período durante el cual la AC emite Certificados DEBERÁ dividirse en una secuencia ininterrumpida de períodos de auditoría. Un período de auditoría NO DEBE exceder un año de duración.

Si la entidad emisora de certificados tiene un informe de auditoría válido actualmente que indique el cumplimiento de un esquema de auditoría enumerado en la Sección 8.1, entonces no es necesaria una evaluación de preparación previa a la emisión.

Si la AC no tiene un Informe de auditoría válido actualmente que indique el cumplimiento de uno de los esquemas de auditoría enumerados en la Sección 8.1, entonces, antes de emitir Certificados de confianza pública, la AC DEBERÁ completar con éxito una evaluación de preparación de un punto en el tiempo realizada de acuerdo con normas aplicables bajo uno de los esquemas de auditoría enumerados en la Sección 8.1. La evaluación de disponibilidad en un momento dado DEBE completarse no antes de doce (12) meses antes de la emisión de Certificados de confianza pública y DEBE seguir una auditoría completa bajo dicho esquema dentro de los noventa (90) días posteriores a la emisión de la primera publicación de un Certificado de confianza pública.

8.2. Identidad/calificaciones del evaluador

La auditoría de la AC DEBE ser realizada por un auditor calificado. Un auditor calificado se refiere a una persona física, entidad jurídica o grupo de personas físicas o entidades jurídicas que poseen colectivamente las siguientes calificaciones y habilidades:

1. Independencia del tema de la auditoría;
2. La capacidad de realizar una auditoría que aborde los criterios especificados en estos Requerimientos.
3. Emplea a personas que tienen competencia para examinar la tecnología de Infraestructura de llave pública, herramientas y técnicas de seguridad de la información, tecnología de la información y auditoría de seguridad.
4. Obligado por la ley, la regulación gubernamental o el código de ética profesional; y

8.3. Relación del evaluador con la entidad evaluada

No estipulado.

8.4. Temas cubiertos en la evaluación

No estipulado.

8.5. Acciones realizadas como resultado de una deficiencia

No estipulado.

8.6. Comunicación de resultados

El Informe de Auditoría DEBERÁ declarar explícitamente que cubre los sistemas y procesos relevantes utilizados en la emisión de todos los Certificados que afirman uno o más de los identificadores de políticas enumerados en la Sección 7.1.6.1. La AC DEBE hacer público el Informe de Auditoría. La AC no está obligada a poner a disposición del público ningún hallazgo general de auditoría que no afecte la opinión general de la auditoría. La CA DEBE poner su Informe de auditoría a disposición del público a más tardar tres meses después del final del período de auditoría. En el caso de un retraso mayor de tres meses, y si así lo solicita un Proveedor de Software de Aplicación, la AC DEBERÁ proporcionar una carta explicativa firmada por el Auditor Calificado.

8.7. Auto-auditorías

Durante el período en que la AC emite Certificados, la AC DEBE monitorear el cumplimiento de su Política de Certificados, Declaración de Prácticas de Certificación y estos Requisitos y controlar estrictamente la calidad de su servicio realizando auto-auditorías al menos trimestralmente contra una muestra seleccionada aleatoriamente de un certificado o al menos el tres por ciento de los Certificados emitidos durante el período que comienza inmediatamente después de que se tomó la muestra de auto-auditoría anterior.

A excepción de los Terceros Delegados que se someten a una auditoría anual que cumpla con los criterios especificados en la Sección 8.1, la AC DEBERÁ controlar estrictamente la calidad del servicio de los Certificados emitidos o que contengan información verificada por un Tercero Delegado al hacer que un Especialista en Validación empleado por la AC realice un trabajo de auditorías continuas trimestrales contra una muestra seleccionada al azar de al menos el mayor de un certificado o el tres por ciento de los certificados verificados por el tercero delegado en el período que comienza inmediatamente después de que se tomó la última muestra. El AC DEBE revisar las prácticas y procedimientos de cada Tercero Delegado para asegurarse de que el Tercero Delegado cumpla con estos Requisitos y la Política de Certificado y/o Declaración de Práctica de Certificación correspondiente.

El AC DEBERÁ auditar internamente el cumplimiento de cada Tercero Delegado con estos Requisitos anualmente.

Durante el período en que una AC Subordinada técnicamente restringida emite certificados, la AC que firmó la AC Subordinada DEBE monitorear el cumplimiento de la Política de Certificados de la AC y la Declaración de Práctica de Certificación de la AC Subordinada. Al menos trimestralmente, contra una muestra seleccionada al azar del mayor de un certificado o al menos el tres por ciento de los Certificados emitidos por la AC subordinada, durante el período que comienza inmediatamente después de que se tomó la muestra de auditoría anterior, la AC DEBERÁ asegurar que se cumple las PC y DPC aplicables.

9. Otros asuntos legales y comerciales

9.1. Tarifas

9.1.1. Tarifas de emisión y renovación de certificados

No estipulado.

9.1.2. Tarifas de acceso a certificados

No estipulado.

9.1.3. Tarifas de revocación o acceso a información de estatus

No estipulado.

9.1.4. Tarifas de otros servicios

No estipulado

9.1.5. Política de reembolsos

No estipulado.

9.2. Responsabilidad financiera

9.2.1. Cobertura de seguros

La AC deberá disponer de una póliza de responsabilidad civil con cobertura razonable.

9.2.2. Otros activos

No estipulado.

9.2.3. Cobertura de seguros o garantía para usuarios finales

No estipulado.

9.3. Confidencialidad de información de negocios

9.3.1. Alcance de la confidencialidad de información

No estipulado.

9.3.2. Información que no está en el alcance de información confidencial

No estipulado.

9.3.3. Responsabilidad de proteger la información confidencial

No estipulado.

9.4. Privacidad de información personal

9.4.1. Plan de privacidad

No estipulado.

9.4.2. Información tratada como privada

No estipulado.

9.4.3. Información que no es tratada como privada

No estipulado.

9.4.4. Responsabilidad de proteger la información privada

No estipulado.

9.4.5. Aviso y consentimiento de uso de información privada

No estipulado.

9.4.6. Divulgación en cumplimiento de un proceso judicial o administrativo

No estipulado.

9.4.7. Otras circunstancias de divulgación de información

No estipulado.

9.5. Derechos de propiedad intelectual

No estipulado.

9.6. Representaciones y garantías

9.6.1. Representaciones y garantías de la AC

Al emitir un Certificado, la AC otorga las siguientes garantías respecto del Certificado a los siguientes Beneficiarios del Certificado:

1. El Suscriptor que es parte del Acuerdo de Suscriptor o Términos de Uso;
2. Todos los Proveedores de Software de Aplicación con los que la AC Raíz ha celebrado un contrato para incluir su Certificado Raíz en el software distribuido por dicho proveedor de software de aplicación; y
3. Todas las partes relacionadas confían razonablemente en un certificado válido.

La AC representa y garantiza a los Beneficiarios del Certificado que, durante el período en que el Certificado es válido, la AC ha cumplido con estos Requisitos y su Política de Certificados y/o Declaración de Práctica de Certificación al emitir y administrar el Certificado.

Las garantías de certificados incluyen específicamente, entre otras, las siguientes:

1. Derecho a usar el nombre legal de la persona natural y/o persona jurídica: que, en el momento de la emisión, la AC (i) implementó un procedimiento para verificar la identidad del Solicitante que aparece en el Sujeto del Certificado y la extensión de subjectAltName; (ii) siguió el procedimiento al emitir el Certificado; y (iii) describió con precisión el procedimiento en el Política de Certificados y/o Declaración de Práctica de Certificación;
2. Autorización para el Certificado: Que, al momento de la emisión, la AC (i) implementó un procedimiento para verificar que el Sujeto autorizó la emisión del Certificado y que el Representante Solicitante está autorizado para solicitar el Certificado en nombre del Sujeto; (ii) siguió el procedimiento al emitir el Certificado; y (iii) describió con precisión el

procedimiento en la Política de Certificados y/o la Declaración de Práctica de Certificación;

3. Precisión de la información: que, en el momento de la emisión, la AC (i) implementó un procedimiento para verificar la exactitud de toda la información contenida en el Certificado (con el excepción del asunto: atributo organizationalUnitName); (ii) siguió el procedimiento al emitir el Certificado; y (iii) describió con precisión el procedimiento en la Política de Certificados y/o la Declaración de Práctica de Certificación;
4. Sin información engañosa: que, en el momento de la emisión, la AC (i) implementó un procedimiento para reducir la probabilidad de que la información contenida en el Sujeto del Certificado: atributo organizationalUnitName sería engañosa; (ii) siguió el procedimiento al emitir el Certificado; y (iii) describió con precisión el procedimiento en la Política de certificación de AC y / o la Declaración de Práctica de Certificación;
5. Identidad del solicitante: que, si el Certificado contiene información de identidad del Sujeto, la AC (i) implementó un procedimiento para verificar la identidad del solicitante de acuerdo con las Secciones 3.2 y 11.2; (ii) siguió el procedimiento al emitir el Certificado; y (iii) describió con precisión el procedimiento en la Política de Certificados y/o la Declaración de Práctica de Certificación;
6. Acuerdo del suscriptor: que, si la AC y el Suscriptor no están afiliados, el Suscriptor y la AC suscribirán un Acuerdo de Suscriptor legalmente válido y exigible que cumpla con estos requisitos, o, si la AC y el Suscriptor están afiliados, el representante solicitante reconoció y aceptó los Términos de Uso;
7. Estado: que la AC mantiene un repositorio de acceso público las 24 horas del día, los 7 días de la semana, con información actualizada sobre el estado (válido o revocado) de todos los certificados no vencidos; y
8. Revocación: que la AC revocará el Certificado por cualquiera de los motivos especificados en estos Requisitos. La AC Raíz DEBERÁ ser responsable del desempeño y las garantías de la AC Subordinada, del cumplimiento de la AC Subordinada con estos Requisitos y de todas las responsabilidades y obligaciones de indemnización de la AC Subordinada bajo estos Requisitos, como si la AC Raíz fuera la AC Subordinada emitiendo los Certificados.

9.6.2. Representaciones y garantías de la AR

No estipulado.

9.6.3. Representaciones y garantías del Suscriptor

La AC DEBERÁ, como parte del Acuerdo de Suscriptor y los Términos de Uso, que el Solicitante asuma los compromisos y garantías en esta sección en beneficio de la AC y los Beneficiarios del Certificado. Antes de la emisión de un Certificado, la AC DEBERÁ, para el beneficio expreso de la AC y los Beneficiarios del Certificado, exigir al Solicitante lo siguiente:

1. El Acuerdo de Suscriptor firmado con la AC, o

2. La aceptación del Solicitante a los Términos de uso

El AC DEBE implementar un proceso para garantizar que cada Acuerdo de Suscriptor y Términos de uso sea legalmente exigible contra el Solicitante. En cualquier caso, el Acuerdo DEBE aplicarse al Certificado que se emitirá de conformidad con la solicitud del certificado. La AC puede usar un dispositivo electrónico, firma facsímil o firma electrónica siempre que la AC haya determinado que dichos acuerdos son legalmente exigibles. Se PUEDE usar un Acuerdo de Suscriptor por separado para cada Solicitud de certificado, o se puede usar un Acuerdo de Suscriptor único para cubrir múltiples solicitudes de certificados futuras y los Certificados resultantes, siempre que cada Acuerdo de Suscriptor o Términos de uso del Certificado cubran claramente cada Certificado que la AC emite al Solicitante.

El Acuerdo de Suscriptor o Términos de Uso DEBE contener disposiciones que impongan al Solicitante las siguientes obligaciones y garantías:

1. Exactitud de la información: Obligación y garantía de proporcionar información precisa y completa en todo momento a la AC, tanto en la Solicitud del Certificado como en cualquier otra forma de información solicitada por la AC en relación con la emisión del Certificado (s) a ser suministrado por la AC;
2. Protección de la clave privada: Obligación y garantía del solicitante de tomar todas las medidas razonables para mantener el control exclusivo, mantener la confidencialidad y proteger adecuadamente en todo momento la Clave Privada que corresponde a la Clave Pública que se incluirá en el certificado solicitado. (s) (y cualquier dispositivo o datos de activación asociados, por ejemplo, contraseña o token);
3. Aceptación del Certificado: Obligación y garantía de que el Suscriptor revisará y verificará la exactitud del contenido del Certificado;
4. Uso del Certificado: Obligación y garantía de usar el Certificado únicamente de conformidad con todas las leyes aplicables y únicamente conforme al Acuerdo de Suscriptor y Términos de Uso;
5. Informes y revocación: Obligación y garantía de dejar de usar rápidamente un Certificado y su Llave Privada asociada, y solicitar de inmediato a la AC que revoque el Certificado, en caso de que: (a) cualquier información contenida en el Certificado sea, o se vuelve, incorrecto o inexacto, o (b) hay un uso o compromiso real o sospechado de la llave privada del suscriptor asociada con la clave pública incluida en el certificado;
6. Terminación del uso del certificado: Obligación y garantía de suspender rápidamente el uso de la llave privada correspondiente a la llave pública incluida en el certificado tras la revocación de dicho certificado por razones de compromiso de la llave.
7. Capacidad de respuesta: una obligación de responder a las instrucciones de la AC con respecto al uso indebido de los Compromisos o certificados clave dentro de un período de tiempo específico.
8. Reconocimiento y aceptación: Un reconocimiento y aceptación de que la AC tiene derecho a revocar el certificado de inmediato si el Solicitante viola los términos del

Acuerdo de Suscriptor o los Términos de Uso o si la AC descubre que el Certificado se está utilizando para realizar delitos como ataques de phishing, fraude o distribución de malware.

9.6.4. Representaciones y garantías de terceros que confían

No estipulado

9.6.5. Representaciones y garantías de otros participantes

No estipulado.

9.7. Renuncia de garantías

No estipulado.

9.8. Limitaciones de responsabilidad

Para las tareas delegadas, la AC y cualquier tercero delegado PUEDEN asignar responsabilidad entre ellos contractualmente según lo determinen, pero la AC DEBERÁ seguir siendo totalmente responsable del desempeño de todas las partes de acuerdo con estos Requisitos, como si las tareas no hubieran tenido sido delegado.

Si la AC ha emitido y administrado el Certificado de conformidad con estos Requisitos y su Política de Certificados y/o Declaración de Práctica de Certificación, la AC puede rechazar la responsabilidad ante los Beneficiarios del Certificado o cualquier otro tercero por cualquier pérdida sufrida como resultado del uso o dependencia en dicho Certificado más allá de los especificados en la Declaración de Práctica de Certificación de la AC. Si la AC no ha emitido o administrado el Certificado de conformidad con los requisitos aplicables y su Declaración de práctica de certificación, la AC puede tratar de limitar su responsabilidad ante el Suscriptor y las Partes que Confían, independientemente de la causa de acción o teoría legal involucrada, por cualquier y todas las reclamaciones, pérdidas o daños sufridos como resultado del uso o dependencia de dicho Certificado por cualquier medio apropiado que la AC desee. Si la AC decide limitar su responsabilidad, entonces la AC DEBE incluir las limitaciones de responsabilidad en su Declaración de Prácticas de Certificación.

9.9. Indemnizaciones

No estipulado

9.10. Plazo y terminación

9.10.1. Plazo

El plazo de los Certificados DEBE ser igual o menor al tiempo de validez y/o vigencia de los documentos de identidad, autorización, poder y/o existencia legal enviados por el Solicitante.

9.10.2. Terminación

No estipulado.

9.10.3. Efectos de la terminación y supervivencia

No estipulado

9.11. Avisos individuales y comunicación con los participantes

No estipulado.

9.12. Enmiendas

No estipulado.

9.12.1. Procedimientos para enmiendas

No estipulado.

9.12.2. Mecanismos de notificación y período

No estipulado.

9.12.3. Circunstancias bajo las cuales se DEBE cambiar un OID

No estipulado.

9.13. Provisiones para resolución de disputas

No estipulado.

9.14. Ley aplicable

La operación de Dátil AC debe cumplir con el siguiente marco legal:

1. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicada en el suplemento del Registro Oficial No. 577 de fecha 17 de abril de 2002. [Ley No. 2002 –67].
2. Reglamento a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (No. 3496) y las Reformas contenidas en los decretos 1356 y 867.

9.15. Cumplimiento de ley aplicable

No estipulado.

9.16. Provisiones varias

9.16.1. Aceptación completa

No estipulado.

9.16.2. Asignación

No estipulado.

9.16.3. Divisibilidad

No estipulado.

9.16.4. Cumplimiento

No estipulado.

9.16.5. Fuerza mayor

No estipulado.

9.17. Otras provisiones

No estipulado.

Apéndice A: Datos de los certificados

Certificados de persona jurídica representante legal

Campo	**Descripción**
Version	Versión del estándar X.509 (v3)
Serial number	Número de serie del certificado
Signature algorithm	Algoritmo de firma (sha256RSA)
Signature hash algorithm	Algoritmo de firma de hash (sha256)
Issuer	Datos del emisor incluyendo OU, DC, O, C, etc.
Valid from	Fecha de emisión del certificado
Valid to	Fecha de caducidad del certificado
Subject	Datos del suscriptor incluyendo CN (nombre completo del suscriptor), OU (unidad organizacional), O (razón social del suscriptor), etc.
Public key	Llave pública
Key usage	Uso de clave aplicable para el certificado
Certificate policy	Enlace a la política de certificados
1.3.6.1.4.1.52643.3.1	Identificación del representante legal
1.3.6.1.4.1.52643.3.2	Nombres del representante legal
1.3.6.1.4.1.52643.3.3	Primer apellido
1.3.6.1.4.1.52643.3.4	Segundo apellido (si no tiene va en blanco)
1.3.6.1.4.1.52643.3.5	Cargo
1.3.6.1.4.1.52643.3.7	Dirección de la empresa
1.3.6.1.4.1.52643.3.8	Teléfono de la empresa
1.3.6.1.4.1.52643.3.9	Ciudad de la empresa

1.3.6.1.4.1.52643.3.10	Razón social de la empresa
1.3.6.1.4.1.52643.3.11	RUC de la empresa
1.3.6.1.4.1.52643.3.12	País de la empresa
1.3.6.1.4.1.52643.3.32	Número de factura de la venta del certificado
1.3.6.1.4.1.52643.3.34	Código postal (si no tiene va en blanco)

Certificados de persona jurídica miembro de empresa

Campo	**Descripción**
Version	Versión del estándar X.509 (v3)
Serial number	Número de serie del certificado
Signature algorithm	Algoritmo de firma (sha256RSA)
Signature hash algorithm	Algoritmo de firma de hash (sha256)
Issuer	Datos del emisor incluyendo OU, DC, O, C, etc.
Valid from	Fecha de emisión del certificado
Valid to	Fecha de caducidad del certificado
Subject	Datos del suscriptor incluyendo CN (nombre completo del suscriptor), OU (unidad organizacional), O (razón social del suscriptor), etc.
Public key	Llave pública
Key usage	Uso de clave aplicable para el certificado
Certificate policy	Enlace a la política de certificados
1.3.6.1.4.1.52643.3.1	Identificación del empleado
1.3.6.1.4.1.52643.3.2	Nombres del empleado
1.3.6.1.4.1.52643.3.3	Primer apellido
1.3.6.1.4.1.52643.3.4	Segundo apellido (si no tiene va en blanco)
1.3.6.1.4.1.52643.3.5	Cargo

1.3.6.1.4.1.52643.3.7	Dirección de la empresa
1.3.6.1.4.1.52643.3.8	Teléfono de la empresa
1.3.6.1.4.1.52643.3.9	Ciudad de la empresa
1.3.6.1.4.1.52643.3.10	Razón social de la empresa
1.3.6.1.4.1.52643.3.11	RUC de la empresa
1.3.6.1.4.1.52643.3.12	País de la empresa
1.3.6.1.4.1.52643.3.32	Número de factura de la venta del certificado
1.3.6.1.4.1.52643.3.34	Código postal (si no tiene va en blanco)

Certificados de persona natural

Campo	**Descripción**
Version	Versión del estándar X.509 (v3)
Serial number	Número de serie del certificado
Signature algorithm	Algoritmo de firma (sha256RSA)
Signature hash algorithm	Algoritmo de firma de hash (sha256)
Issuer	Datos del emisor incluyendo OU, DC, O, C, etc.
Valid from	Fecha de emisión del certificado
Valid to	Fecha de caducidad del certificado
Subject	Datos del suscriptor incluyendo CN (nombre completo del suscriptor), OU (unidad organizacional), O (razón social del suscriptor), etc.
Public key	Llave pública
Key usage	Uso de clave aplicable para el certificado
Certificate policy	Enlace a la política de certificados
1.3.6.1.4.1.52643.3.1	Identificación de la persona
1.3.6.1.4.1.52643.3.2	Nombres de la persona

1.3.6.1.4.1.52643.3.3	Primer apellido
1.3.6.1.4.1.52643.3.4	Segundo apellido (si no tiene va en blanco)
1.3.6.1.4.1.52643.3.7	Dirección
1.3.6.1.4.1.52643.3.8	Teléfono (si no tiene va en blanco)
1.3.6.1.4.1.52643.3.9	Ciudad
1.3.6.1.4.1.52643.3.11	RUC (si no tiene, va en blanco)
1.3.6.1.4.1.52643.3.12	País
1.3.6.1.4.1.52643.3.32	Número de factura de la venta del certificado
1.3.6.1.4.1.52643.3.34	Código postal (si no tiene va en blanco)