Datilmedia S.A.
Declaración de Prácticas de Certificación
v1.0

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.

Este documento es publicado por Dátil para identificar las prácticas y procedimientos que Dátil emplea en la emisión de certificados dentro de Dátil ILP.

1.2. Nombre del documento e identificación

Este documento se llama Declaración de Prácticas de Certificación de Datilmedia S.A. (“DPC”). Ha sido publicada en respuesta a la Política de Certificados de Dátil y establece las prácticas que Dátil ha adoptado para implementar las provisiones realizadas aquí.

1.2.1. Revisiones

Ver Apéndice A.

1.3. Participantes de la ILP

1.3.1. Autoridades de Certificación

El término Autoridad de Certificación (AC) es un término general que se refiere a las entidades que emiten, administran, revocan y renuevan certificados de firma electrónica. También actúan como terceros de confianza entre los demás participantes de la ILP.

Esta DPC cubre todos los certificados emitidos por las ACs descritas a continuación:

Subject: C=EC, L=Guayaquil, O=Datilmedia S.A., OU=Autoridad de Certificacion CN=Datil Autoridad de Certificacion Raiz

Subject: C=EC, L=Guayaquil, O=Datilmedia S.A., OU=Autoridad de Certificacion CN=Datil Autoridad de Certificacion Subordinada

1.3.2. Autoridad de Registro

Las Autoridades de Registro (ARs) son entidades que aprueban y autentican solicitudes para obtener, renovar o revocar Certificados. Las ARs son responsables de identificar y autenticar a los Solicitantes de Certificados, verificando sus documentos y autorizando a una Autoridad de Certificación la emisión, renovación o revocación de un Certificado a una persona natural o jurídica.

Todas las funciones relacionadas a ARs descritas en esta DPC son realizadas por Dátil.

1.3.3. Autoridad de Validación

Las Autoridades de Validación (AVs) proporcionan servicios de validación de Certificados emitidos por una Autoridad de Certificación a través del protocolo OCSP (Online Certificate Status Protocol) y/o una Lista de Revocación de Certificados (LRC).

Todas las funciones relacionadas a AVs descritas en esta DPC son realizadas por Dátil.

1.3.4. Suscriptores

Un Suscriptor es una persona natural o jurídica capaz de utilizar y autorizar el uso de la Llave Privada que corresponda a la Llave Pública listada en un Certificado y que: 1) Su nombre legal aparece en el campo “Subject” del Certificado y, 2) ha acordado los términos del Acuerdo de Suscriptor con Dátil.

Todos los Suscriptores requieren suscribir un acuerdo, respecto de cada Certificado emitido a su nombre, que los obligue a:

- Presentar información auténtica cuando sea solicitada por Dátil, respecto de la identificación y autenticación del Suscriptor y la información que se incluye en el certificado.
- Mantener posesión y control permanente de la Llave Privada que corresponde a la Llave Pública del Certificado.
- Implementar medidas de seguridad apropiadas para proteger la Llave Privada que corresponde a la Llave Pública del Certificado.
- Informar a tiempo a Dátil de cualquier cambio en cualquier tipo de información que haya sido incluida en un Certificado o una Solicitud de Certificado.
- Informar a tiempo a Dátil de cualquier sospecha de divulgación de la Llave Privada.
- Dejar de usar inmediatamente un Certificado cuando haya expirado, haya sido revocado o en el caso de sospechas que la Llave Privada haya sido divulgada.
- Usar los Certificados exclusivamente para propósitos legales y cumpliendo con estas DPC.

1.3.5. Terceros que confían

Un Tercero que Confía es una persona natural o jurídica que decide confiar en un Certificado emitido por Dátil 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.

1.4. Uso de los certificados

1.4.1. Uso apropiado de los certificados

Esta DPC considera apropiado cualquier uso de los Certificados que sea con el propósito de autenticar a una persona natural o jurídica, usando firmas electrónicas, cifrado y/o control de acceso, conforme con las extensiones de uso de llaves del Certificado respectivo y que no incumpla con esta DPC, leyes aplicaciones o cualquier otro acuerdo entre el Suscriptor y Dátil.

Las AC de Dátil emiten Certificados Electrónicos a personas naturales y jurídicas con el propósito de realizar firmas electrónicas y cifrado de datos.

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

La Administración de Autoridad de Certificación de Dátil es responsable de escribir, mantener e interpretar esta Declaración de Prácticas de Certificación.

1.5.2. Información de contacto

Datilmedia S.A.

Administración de Autoridad de Certificación
Victor Emilio Estrada 1021 y Jiguas
Guayaquil, Guayas
Ecuador
ac@datil.co

1.5.3. Persona que determina la idoneidad de la DPC

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

1.5.4. Procedimientos de aprobación de la DPC

Dátil podrá modificar esta DPC 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 DPC serán publicados en https://datil.com

Una nueva versión de esta DPC 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 DPC son aprobados por la Administración de Autoridad de Certificación de Dátil.

1.6. Definiciones y acrónimos

Ver apéndice B.

2. Publicación y responsabilidades del repositorio

Las ACs de Dátil descritas en esta DPC son operadas por:

Datilmedia S.A.
Victor Emilio Estrada 1021 y Jiguas
Guayaquil, Guayas
Ecuador
ca@datil.co

2.1. Repositorios

Dátil mantiene un Repositorio que almacena los certificados de las AC, una lista de las revocaciones recientes a certificados emitidos, esta DPC y otros documentos.

El Repositorio puede ser accedido desde https://datil.com.

2.2. Publicación de información de certificados

Dátil publica una Lista de Revocación de Certificados (LRC) y respuestas OCSP para sus ACs de manera pública, accesibles las 24 horas del día, los 7 días de la semana y están diseñados para maximizar su disponibilidad.

AC	**CRL**
Dátil Autoridad de Certificación Subordinada	https://ac.datil.com/crl/b547a740-dc95-4cee-9572-4686cf3dee1e.crl

2.3. Frecuencia de publicación

Las LRC se actualizan inmediatamente cuando un Certificado es revocado, pero en ningún momento más allá de un día laboral luego de la revocación. Las LRC son actualizadas periódicamente y reemitidas al menos cada treinta (30) días, y su validez está limitada a diez (10) días.

2.4. Control de acceso a los repositorios

El Repositorio está disponible públicamente. Dátil, en conjunto con sus Proveedores de Servicios, operan los controles de seguridad física y lógica para proteger el repositorio de modificación o eliminación no autorizada.

3. Identificación y autenticación

3.1. Nombres

3.1.1. Tipos de nombres

Los Certificados contienen un nombre distintivo X.501 en el campo Subject e incorporan al menos los siguientes atributos:

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

3.1.2. Necesidad de que los nombres sean significativos

Los Certificados emitidos por las AC de Dátil tienen como característica principal 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 permiten Suscriptores con 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

El Solicitante de Certificado debe probar ser el dueño de la llave privada entregando una solicitud de firma de certificado cumpliendo con el estándar PKCS #10 o una prueba criptográfica equivalente.

3.2.2. Autenticación de una organización o persona jurídica

La identidad del Solicitante se verifica 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.

3.2.3. Autenticación de una persona natural

La identidad de Solicitantes personas naturales se verifica 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.

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

Los criterios de interoperabilidad con otras AC es función de la Administración de Autoridad de Certificación de Dátil. La Autoridad de Certificación de Dátil garantiza y permite la autenticación, validación y firma electrónica de los Certificados emitidos por todas las

Entidades de Certificación de Información y Servicios Relacionados debidamente acreditadas en Ecuador.

3.3. Identificación y autenticación para solicitudes de nueva clave

3.3.1. Identificación y autenticación para emisión rutinaria de nueva clave

El proceso para la solicitud de una nueva clave es el mismo requerido para el proceso de solicitud inicial de un certificado y está definido en la respectiva Política de Certificados. También es posible la identificación del Solcitante haciendo uso del Certificado original a renovar, siempre que no haya caducado ni se haya revocado.

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

El procedimiento para solicitar una nueva clave luego de la revocación de un Certificado es el mismo requerido para la solicitud inicial de un Certificado.

3.4. Identificación y autenticación para solicitudes de revocación

Para la revocación de un Certificado se siguen los procedimientos de autenticación e identificación del Solicitante. Si la solicitud de revocación es realizada por el Suscriptor, se realiza la identificación y autenticación conforme a esta sección. Si la solicitud de revocación es originada por un miembro del equipo de seguridad de Dátil, no se requiere de identificación y autenticación.

4. Requerimientos operacionales del ciclo de vida de los certificados

4.1. Solicitud de certificados

4.1.1. Quiénes pueden enviar solicitudes de certificado

Las Solicitudes para obtener un Certificado pueden ser enviadas por una persona natural a título personal o a nombre de una organización o persona jurídica.

Dátil mantiene una lista de todos los Certificados revocados y/o rechazados anteriormente, para verificar que quien esté haciendo la Solicitud, no se encuentre en esas listas.

El Solicitante debe tener conexión a internet, un explorador de Internet y tener credenciales de acceso en Dátil.

4.1.2. Proceso de enrolamiento y responsabilidades

Para solicitar un Certificado, el Solicitante debe enviar a Dátil un formulario de aplicación, incluyendo una solicitud de certificado, los documentos adjuntos requeridos y cualquier otro requisito por parte de Dátil al momento de la solicitud.

La información personal de los Suscriptores es tratada conforme a las políticas de privacidad de Dátil la cual, como mínimo, establece los procedimientos y prácticas para garantizar la confidencialidad y seguridad de la información personal.

Mediante el Acuerdo de Suscriptor, los Suscriptores garantizan que toda la información provista y contenida en el Certificado es correcta y auténtica.

4.2. Procesamiento de las solicitudes

Dátil realiza las validaciones aplicables a los Certificados y verifica que la información provista por el Solicitante esté completa, sea precisa y auténtica, antes de emitir un Certificado. Los procedimientos incluyen:

- Verificar que el Solicitante está permitido a obtener un Certificado bajo las normas de esta DPC.
- Verificar que el Solicitante haya provisto una Solicitud de Certificados (CSR) válida y bien formada, y que contenga una firma electrónica válida.
- Obtener o generar la Llave Pública del Solicitante.
- Verificar que el Solicitante haya aceptado el Acuerdo de Suscriptor.
- Realizar los procedimientos de identificación y autenticación descritos en esta DPC.

4.2.1. Funciones de identificación y autenticación

Dátil realiza las funciones de identificación y autenticación durante el procesamiento de una Solicitud de Certificado y el proceso de generación de nuevas claves.

Las solicitudes no son aprobadas hasta que Dátil haya obtenido y validado toda la información necesaria especificada en esta DPC. Es posible que Dátil requiera información adicional al Solicitante para complementar el proceso.

El Solicitante debe permitir y aceptar que Dátil valide su información en fuentes de datos externas.

Dátil dispone de procedimientos para identificar Solicitudes de Certificados de alto riesgo, que requieren de verificación adicional antes de su aprobación. Esto incluye mantener una base de datos interna de todos los Certificados previamente revocados y Solicitudes de Certificado rechazadas con sospechas de falsificación de información o cualquier otro uso fraudulento. Esta información se utiliza en los procedimientos de identificación y autenticación para identificar solicitudes de certificados sospechosas.

4.2.2. Aprobación o rechazo de solicitudes de certificados

Dátil considera únicamente las solicitudes de Certificado que tengan información completa y que haya sido validada. Todas las demás solicitudes serán rechazadas.

Las solicitudes rechazadas serán notificadas al Solicitante por correo electrónico, detallando la causa del rechazo. El Solicitante podrá enmendar y/o completar la Solicitud para que sea validada nuevamente.

4.2.3. Tiempo de procesamiento de solicitudes de certificado

Las solicitudes de Certificados son procesadas en el menor tiempo posible razonable, a menos que el Solicitante haya suscrito un Acuerdo de Nivel de Servicio con Dátil, para lo cual las solicitudes se atenderán conforme a esos términos.

4.3. Emisión de certificados

4.3.1. Funciones de la AC durante la emisión del certificado

Antes de emitir un Certificado, Dátil procesa la Solicitud de Certificado y realiza los procedimientos de identificación y autenticación conforme a esta DPC. Una vez que se completan estos procesos, el Certificado es generado incluyendo las extensiones de uso de llaves apropiadas.

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

Luego de emitir un Certificado, Dátil le notifica al Solicitante vía correo electrónico o cualquier forma alternativa de comunicación y proveerá al Solicitante las instrucciones de cómo obtener su certificado. La entrega del Certificado se realiza mediante los servicios y aplicaciones de Dátil.

4.4. Aceptación de los certificados

4.4.1. Conducta que constituye la aceptación de un certificado

El Suscriptor expresa la aceptación de un certificado al momento de obtenerlo.

Al aceptar un Certificado, el Suscriptor se adhiere a las responsabilidades, obligaciones y deberes impuestos por el Acuerdo de Suscripción y esta DPC, además declara y garantiza que:

- Sabe que ninguna persona no autorizada tiene acceso a la Llave Privada asociada al Certificado.
- La información provista durante el proceso de registro es auténtica y se refleja de manera correspondiente en el Certificado.
- Mantendrá control y confidencialidad de la Llave Privada correspondiente a la Llave Pública listada en el Certificado.
- Informará inmediatamente a Dátil en caso de cualquier evento que invalide o afecte la integridad del Certificado, como por ejemplo sospechas de pérdida, divulgación o cualquier otra afectación a la Llave Privada asociada.

4.4.2. Publicación del certificado por parte de la AC

Dátil realiza la publicación en el Repositorio de las Llaves Públicas de los certificados emitidos por sus CA.

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

Cuando corresponda, Dátil notificará a terceros sobre la emisión de un certificado, como por ejemplo, la Autoridad de Registro que lo solicitó o entidades de control.

4.5. Uso de llaves y certificados

4.5.1. Uso de la llave privada y certificado por parte del Suscriptor

Ver la sección *Representaciones y garantías del Suscriptor*.

4.5.2. Uso de la llave pública y certificado por parte de terceros de confianza

Los terceros que confíen en los Certificados emitidos por Dátil, deben hacer uso del Certificado de conformidad con lo establecido en el campo de usos permitidos (“keyUsage“) y/o en la presente DPC.

Los terceros que confían deben verificar el estado del Certificado utilizando los mecanismos establecidos en esta DPC.

4.6. Renovación de certificados

4.6.1. Circunstancias para la renovación de un certificado

La renovación de un Certificado es el proceso mediante el cual Dátil emite un nuevo certificado con un período de validez actualizado, para un mismo Par de Llaves.

Para efectos prácticos, Dátil no ofrece renovación de Certificados. En cualquier caso en el que expire un Certificado, el Suscriptor debe generar un nuevo Par de Llaves y solicitar un nuevo Certificado conforme a esta DPC.

4.6.2. Quién puede solicitar la renovación de un certificado

No aplica.

4.6.3. Procesamiento de renovación de certificados

No aplica.

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

No aplica.

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

No aplica.

4.6.6. Publicación de renovación de certificados por parte de la AC

No aplica.

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

No aplica.

4.7. Cambio de llaves del certificado

4.7.1. Circunstancias para el cambio de llaves de un certificado

Dátil trata la solicitud de cambio de llaves de un Certificado como la emisión de un nuevo Certificado.

4.7.2. Quién puede solicitar la certificación de una nueva llave pública

Ver Sección 4.1.1.

4.7.3. Procesamiento de solicitudes de nuevas llaves

Ver Sección 4.2.

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

Ver Sección 4.3.2.

4.7.5. Conducta que constituye la aceptación de la generación de nuevas llaves

Ver Sección 4.4.1.

4.7.6. Publicación por parte de la AC del certificado con las nuevas llaves

Ver Sección 4.4.2.

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

Ver Sección 4.4.3.

4.8. Modificación de certificados

Dátil no permite modificar certificados ya emitidos. Cualquier solicitud de modificación del certificado será tratada como la solicitud de emisión de un nuevo certificado.

4.8.1. Circunstancias para la modificación de un certificado

No aplica.

4.8.2. Quién puede solicitar la modificación de un certificado

Ver Sección 4.1.1.

4.8.3. Procesamiento de solicitudes de modificación de certificados

Ver Sección 4.2.

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

Ver Sección 4.3.2.

4.8.5. Conducta que constituye la aceptación de un certificado modificado

Ver Sección 4.4.1.

4.8.6. Publicación por parte de la AC del certificado modificado

Ver Sección 4.4.2.

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

Ver Sección 4.4.3.

4.9. Revocación y suspensión de certificados

Dátil permite la Revocación de Certificados. No se utiliza la suspensión.

Cuando un Certificado es Revocado, se marca como revocado agregando su número de serie a la LRC para su estado como revocado. Adicionalmente, se genera una respuesta OCSP firmada.

4.9.1. Circunstancias para la revocación

Los certificados que hayan expirado no son revocados.

4.9.1.1. Razones para revocar el Certificado de un Suscriptor

Dátil revoca el Certificado de un Suscriptor en un plazo de 24 horas laborables si ocurre cualquiera de los siguientes eventos:

1. El Suscriptor solicita por escrito a Dátil la revocación del Certificado.
2. El Suscriptor notifica a Dátil que la solicitud de certificado original no fue autorizada y que no permite la emisión del certificado.

3. Dátil obtiene evidencia de que la Llave Privada del Suscriptor, correspondiente a la Llave Pública del Certificado, ha sido comprometida o divulgada sin autorización del Suscriptor.

Dátil revoca un Certificado de un Suscriptor en un plazo de 5 días laborables si ocurre cualquier de los siguientes eventos:

- Traslado o cesación de funciones del Suscriptor.
- Fallecimiento del titular o el Suscriptor.
- Por robo, sustracción, pérdida, modificación o revelación de la llave que permita el uso de la Llave Privada del certificado
- Al tener cualquier tipo de evidencia de que la Llave Privada del certificado ha sido divulgada o pueda ser calculada a partir de la Llave Pública.
- Cambio en los datos del certificado
- Mal uso de las claves o certificados
- Incumplimiento de las normas establecidas en esta DPC y el Acuerdo de Suscriptor
- Emisión de un certificado con datos incorrectos

4.9.1.2. Razones para Revocar el Certificado de una AC Subordinada

Dátil revoca el Certificado de una AC Subordinada cuando tenga cualquier tipo de sospecha de que la Llave Privada que corresponde a la Llave Pública del Certificado utilizado por la AC para la firma de Certificados de Suscriptores, ha sido comprometida o divulgada sin autorización de Dátil.

4.9.2. Quién puede solicitar la revocación

La Revocación de Certificados puede ser solicitada únicamente por el Suscriptor o un representante debidamente autorizado mediante nombramiento o poder legal.

En algunos casos, el departamento de Seguridad de Información de Dátil puede solicitar la Revocación de Certificados cuando lo crea conveniente.

4.9.3. Procedimiento para la solicitud de revocación

Las solicitudes de revocación de Certificados así como reportes relacionados a sospechas sobre mal uso de certificados, fraude, conducta inapropiada o cualquier otro asunto relacionado a los certificados puede ser enviada por email a ac@datil.co.

Dátil tiene la capacidad para recibir solicitudes de revocación de Certificados 24/7.

Las solicitudes de revocación realizadas por el Suscriptor son evaluadas conforme a los criterios de Identificación y Autorización descritos en la Sección 3 de esta DPC. Solicitudes enviadas por otras partes son evaluadas caso por caso, considerando el siguiente criterio:

- La naturaleza del problema reportado por el solicitante;
- La evidencia que soporte la solicitud;
- La urgencia de la solicitud;
- La cantidad de solicitudes recibidas relacionadas a ese Certificado o Suscriptor;
- La entidad o persona haciendo la solicitud; y
- La legislación aplicable.

Si Dátil determina que la revocación procede, se actualiza inmediatamente la información del Certificado conforme a las políticas de revocación. Cuando corresponda, Dátil podrá informar a las autoridades legales competentes.

4.9.4. Períodos de gracia de revocación

Dátil podrá otorgar períodos de gracia para la revocación.

4.9.5. Plazo para procesamiento de solicitudes de revocación por parte de la AC

Dentro de 24 horas laborables luego de recibir la solicitud de revocación o notificación, Dátil validará los hechos y circunstancias relacionados y determinará si procede o no la revocación.

En el caso de que proceda la revocación, notificará al Suscriptor y/o a la entidad que solicitó la revocación y realizará el procedimiento de revocación conforme a esta DPC.

4.9.6. Requerimientos de chequeo de revocaciones para los Terceros que Confían

Los Terceros que Confían deben confirmar la validez de cada Certificado en la cadena de certificados chequeando la LRC o respuesta OCSP respectiva, antes de depositar su confianza en un Certificado emitido por Dátil.

4.9.7. Frecuencia de emisión de LRC

La LRC será actualizada y reemitida al menos una vez cada siete (7) días y el valor del parámetro nextUpdate no será mayor a diez (10) días después del valor del parámetro thisUpdate.

Ver la Sección 2.2. para la ubicación de la LRC.

4.9.8. Latencia máxima de la LRC

Dátil mantiene suficientes recursos para proveer un tiempo de respuesta de LRCs y OCSP de 10 segundos o menos en condiciones normales de operación.

4.9.9. Disponibilidad de chequeo en línea de estatus/revocación

Dátil hace disponible información de estatus OCSP para todos sus certificados. La ubicación del servidor OCSP se incluye en el certificado respectivo.

Las respuestas OCSP se hacen conforme a los estándares RFC6960 y FFC5019. Estas cumplen con al menos una de las siguientes:

1. Está firmada por la AC que emitió los Certificados de los cuales se indica el estatus de revocación, o
2. Está firmada por un Servidor OCSP cuyo Certificado fue firmado por la AC que emitió los Certificados cuyo estatus de revocación se indica. El Certificado de firma del Servidor OCSP contiene una extensión de tipo id-pkix-ocsp-nocheck, de acuerdo a lo definido en RFC9690.

4.9.10. Requerimientos de chequeo on-line de revocación

El Servidor OCSP soportas la recepción de solicitudes OCSP mediante el método GET. No responde una respuesta de estatus “válido” a certificados que no hayan sido emitidos.
Para Certificados de Suscriptores, se actualiza inmediatamente luego de la emisión del certificado. Tiene una validez mínima de un día y una validez máxima de siete días.

4.9.11. Otras formas disponibles de publicación de revocación

No aplica.

4.9.12. Circunstancias para la suspensión

Dátil no suspende certificados.

4.9.13. Quién puede solicitar la suspensión

No aplica.

4.9.14. Procedimiento para solicitud de suspensión

No aplica.

4.9.15. Límite de tiempo para la suspensión

No aplica.

4.10. Servicios de estatus de certificados

4.10.1. Características operacionales

Los registros de revocación en una LRC o Respuesta OCSP no se eliminan hasta después de la Fecha de Expiración del Certificado que fue revocado.

4.10.2. Disponibilidad del servicio

Los Servicios de Status de Certificados están disponibles 24x7, a menos que estén temporalmente no disponibles por mantenimiento o falla en los servicios. Adicionalmente, Dátil mantiene habilidades continuas 24x7 para responder internamente a problemas o reportes de alta prioridad relacionados a Certificados.

4.10.3. Características operacionales

No aplica.

4.11. Fin de la suscripción

La suscripción de un Suscriptor termina cuando su Certificado expira o cuando el Certificado haya sido revocado. Una suscripción también se da por terminada cuando el acuerdo de suscripción respectivo expire o no se renueve.

5. Controles de seguridad física, administración y operación

5.1. Controles de seguridad física

La infraestructura de Dátil AC es operada por instalaciones seguras de Datilmedia S.A., operadas por Amazon Web Services, Inc. El acceso no autorizado a las instalaciones donde opera Dátil AC está prohibido por los procedimientos de seguridad respectivos.

5.1.1. Localización del sitio y construcción

Los sistemas de Dátil AC están instalados en puntos geográficos seleccionados que han sido evaluados por su seguridad física, además de las consideraciones legales que puedan afectar la operación de la AC.

Todos los sistemas de la AC funcionan desde edificios que están construidos sólidamente para evitar el acceso no autorizado.

5.1.2. Acceso físico

Dátil implementa 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 está limitado al personal que desempeña un rol confiable como se describe en la Sección 5.2.1.

El acceso se controla mediante el uso de controles de acceso electrónicos, juegos de cerraduras de combinación mecánica, cerrojos u otros mecanismos de seguridad. Dichos controles de acceso se controlan manual o electrónicamente para detectar intrusiones no autorizadas en todo momento. Solo el personal autorizado podrá acceder, ya sea físico o lógico, a los sistemas desde los cuales opera la AC. El acceso físico está limitado a personal autorizado de Amazon Web Services, Inc, exclusivamente para tareas de mantenimiento, cumpliendo con los más altos estándares de seguridad.

Los servidores de Dátil AC se encuentran dentro de un gabinete cerrado o área de jaula en una sala de servidores cerrada. El acceso a la sala del servidor está controlado por lectores de credenciales. Las claves privadas para las AC se almacenan en módulos de seguridad de hardware que están validados para FIPS 140-2 Nivel 3 o superior y que son físicamente evidentes y resistentes a la manipulación.

5.1.3. Energía y aire acondicionado

Las instalaciones en las cuales opera Dátil AC están conectadas a sistemas de UPS y generadores de energía de emergencia. Están equipados con sistemas de enfriamiento para asegurar la confiabilidad de las operaciones.

5.1.4. Exposición al agua

Todas las instalaciones de Dátil AC están equipadas con controles que protegen a los sistemas de la AC de cualquier tipo de daño resultante de fugas de agua.

5.1.5. Prevención y protección contra incendios

Todas las instalaciones de Dátil AC están equipadas con alarmas con detector de incendios y equipos de protección.

5.1.6. Almacenamiento de medios

No aplica.

5.1.7. Eliminación de residuos

Dátil toma medidas razonables para asegurarse que todos los medios físicos usados para almacenar información como llaves, información de activación o cualquier archivo relacionado, son sanitizados y/o destruidos antes de ser liberados para su depósito como residuo.

5.1.8. Copias de seguridad fuera del sitio

Dátil mantiene instalaciones de respaldo para almacenar copias de los certificados emitidos y demás archivos relacionados.

5.2. Controles de procedimientos

5.2.1. Roles de confianza

El personal que tiene acceso o control sobre las operaciones criptográficas en Dátil AC que afecten la emisión, uso y gestión de Certificados se consideran sirviendo bajo un rol de confianza (“Rol de Confianza”). Este personal incluye, pero no está limitado a, miembros del equipo de Autoridad de Certificación de Dátil.

5.2.2. Número de personas requeridas para una tarea

La Llave Privada puede ser creada o recuperada por personal en un rol de confianza, utilizando, al menos dos controles en un ambiente físicamente seguro.

5.2.3. Identificación y autenticación de cada rol

Dátil mantiene controles que aseguran de manera razonable que:

- Se sigue un procedimiento documentado para embestir personas en un Rol de Confianza y asignar las responsabilidades correspondientes;
- Solo personal que tenga asignado un Rol de Confianza tendrá acceso a Zonas Seguras y Zonas de Alta Seguridad;
- Personas en un Rol de Confianza actúan bajo ese rol únicamente cuando realicen actividades administrativas;
- Empleados y contratistas externos observan el principio del Mínimo Privilegio cuando accedan o configuren accesos a los Sistemas de Certificados;

- Cuando un Rol de Confianza utilice un usuario y contraseña para autenticarse, los controles de acceso están configurados de tal manera que se satisfagan los siguientes requerimientos:

    - Las contraseña tiene al menos doce (12) caracteres para cuentas internas (accesibles solo desde Zonas Seguras o Zonas de Alta Seguridad);

    - Las contraseñas de cuentas accesibles desde fuera de Zonas Seguras o Zonas de Alta Seguridad son configuradas para tener al menos ocho (8) caracteres y una combinación de al menos un número y caracteres alfabéticos, evitando que sea una de las cuatro últimas contraseñas utilizadas; e implementar bloqueo de la cuenta por intentos de acceso fallidos;

- Los Roles de Confianza cierran sesión en su computador cuando no la están usando;

- Las Estaciones de Trabajo están configuradas con detectores de inactividad que cierran la sesión del usuario automáticamente;

- Se revisan todos los sistemas al menos cada 90 días y se desactivan cuentas que ya no sea necesario mantener en operación;

- Revocar el acceso a Sistemas de Certificados a cuentas que superen los cinco (5) intentos de acceso no autorizados;

- Desactivar todos los privilegios de acceso individuales a los Sistemas de Certificados en un plazo máximo de 24 horas luego del fin de la relación laboral de determinado empleado con la AC.

- Aplicar múltiples factores de autenticación para accesos de administrador a los Sistemas de Emisión y Sistemas de Administración de Certificados;

- Restringir el acceso remoto o el acceso a los Sistemas de Emisión, Sistemas de Administración de Certificados o Sistemas de Seguridad excepto cuando:

    - La conexión remota se origine de un dispositivo de propiedad y/o controlado por la AC desde una IP externa pre-aprobada;

    - El acceso remoto se realice mediante un canal seguro y cifrado, de carácter temporal y no persistente que soporta autenticación de dos factores;

    - La conexión remota es realizada a un dispositivo intermedio que cumple con lo siguiente:

- Está localizado en la red de la AC.
- Está asegurado conforme a los requerimientos de esta DPC, y
- Actúa como intermediario para la conexión remota con el Sistema de Emisión.

5.2.4. Roles que requieren separación de deberes

Los auditores de la infraestructura y emisión de certificados es independiente de los operadores que aprueban y emiten certificados usando Dátil AC.

Para verificar la conformancia con las políticas y procedimientos aplicables, Dátil AC realiza auditorías anuales realizadas por auditores independientes.

5.3. Controles de seguridad del personal

5.3.1. Calificaciones, experiencia y requerimientos de autorización

Dátil ha implementado políticas para verificar la identidad e integridad de su personal. Adicionalmente, Dátil evalúa el desempeño del equipo de la AC para asegurarse que desempeñan sus tareas de manera satisfactoria.

Todo el personal de Dátil AC es empleado por Datilmedia S.A. No se involucran a contratistas ni otro tipo de terceros en el Proceso de Administración de Certificados.

5.3.2. Chequeo de antecedentes

Dátil sigue un grupo de procedimientos para seleccionar y evaluar personal que opera Dátil AC o actúa en cualquier otro rol relacionado a seguridad de la información.

5.3.3. Requerimientos de entrenamiento

Todo el personal de Dátil que realiza tareas de verificación de información recibe capacitación en habilidades que cubre el conocimiento básico de Infraestructura de Clave Pública, políticas y procedimientos de autenticación y verificación (incluida esta DPC), amenazas comunes al proceso de verificación de información, incluido el phishing y otras tácticas de ingeniería social.

Los especialistas en validación reciben su capacitación de habilidades antes de comenzar su trabajo y Dátil les exige que aprueben un examen sobre los requisitos de verificación de información aplicables.

Dátil mantiene registros de dicha capacitación y se asegura de que el personal encargado de las tareas de Especialista en Validación mantenga un nivel de habilidad adecuado.

5.3.4. Frecuencia y requerimientos de re-entrenamiento

Dátil requiere al personal en Roles de Confianza el mantener niveles de habilidad consistentes con los programas de capacitación y rendimiento de la AC. Con este fin, Dátil requiere que dicho personal se someta a una nueva capacitación al menos anualmente.

5.3.5. Secuencia y frecuencia de rotación de personal

No aplica.

5.3.6. Sanciones por acciones no autorizadas

Dátil impone sanciones, incluyendo la suspensión y/o despido si es apropiado, a sus empleados en Roles de Confianza si ellos realizan actos no autorizados, abusan de su autoridad; o por cualquier otra razón apropiada, a discreción de la gerencia de la AC.

5.3.7. Contratistas independientes

Los contratistas independientes deben cumplir con los mismos requerimientos que los empleados de Dátil. Los contratistas independientes no serán usados en Roles de Confianza.

5.3.8. Documentación provista al personal

Dátil provee a sus empleados el entrenamiento y documentación necesarios para ejecutar su rol de trabajo de manera completa.

5.4. Procedimientos de registros de auditoría

5.4.1. Tipos de eventos registrados

Dátil registra todos los eventos del sistema y las aplicaciones de la AC y crea registros de gestión de certificados a partir de los datos recopilados de acuerdo con los procedimientos de auditoría interna. Se registran los siguientes eventos:

- Eventos clave de gestión del ciclo de vida de la AC
    - Generación de claves, copia de seguridad, almacenamiento, recuperación, archivo y destrucción;
    - Eventos del ciclo de vida del dispositivo criptográfico.
- Eventos de solicitante y suscriptor
    - Solicitud para crear un certificado;
    - Solicitud de revocación de un certificado.

- Eventos del ciclo de vida del certificado de CA y del suscriptor
    - Actividades de verificación estipuladas en esta DPC;
    - Aceptación y rechazo de solicitudes de certificados, frecuencia de registro de procesamiento;
    - Generación de claves;
    - Notificación de compromiso clave;
    - Creación de un certificado;
    - Entrega de un certificado;
    - Revocación de un certificado;
    - Generación de una lista de revocación de certificados;
    - Generación de una respuesta OCSP;
- Acciones del personal de confianza
    - Eventos de inicio de sesión y uso de mecanismos de identificación y autenticación;
    - Cambios a las políticas de CA;
    - Cambios a las claves de CA;
    - Cambios de configuración a la CA.
- Eventos de seguridad
    - Intentos exitosos y fallidos de acceso al sistema PKI;
    - PKI y acciones del sistema de seguridad realizadas;
    - Cambios de perfil de seguridad;
    - Fallos del sistema, fallas de hardware y otras anomalías;
    - Actividades de firewall y enrutador;
    - Entradas y salidas de la instalación de CA.
- Las entradas de registro incluyen los siguientes elementos:
    - Fecha y hora de entrada;
    - Identidad de la persona que hace la entrada del diario; y
    - Descripción de la entrada.

Dátil recopila información de eventos y crea registros de gestión de certificados mediante procedimientos automatizados. Cuando esto no sea posible, se pueden utilizar los métodos manuales de registro y mantenimiento de eventos.

5.4.2. Frecuencia de procesamiento de registros

Los registros de auditoría son revisados bajo demanda.

5.4.3. Período de retención de registros de auditoría

Dátil retiene cualquier registro de auditoría por al menos siete años o más si es requerido por la ley. Estos registros están disponibles a través de métodos automatizados.

5.4.4. Protección de los registros de auditoría

Se almacenan múltiples copias de los registros de auditoría, almacenados en lugares diferentes y protegidos por los controles de acceso físico y lógico respectivos.

5.4.5. Procedimientos de respaldo de registros de auditoría

Dátil mantiene procedimientos formales para garantizar que los registros de auditoría son respaldados y retenidos para mantenerlos disponibles mientras sean necesarios para el servicio de la AC y como sea dispuestos por los estándares aplicables.

5.4.6. Sistema de recolección de registros de auditoría (interno vs. externo)

No aplica.

5.4.7. Notificaciones sobre eventos de interés

Los eventos que sean considerados potenciales problemas de seguridad relacionados a la infraestructura de la Autoridad de Certificación serán escalados a un equipo de monitoreo permanente de seguridad.

5.4.8. Evaluaciones de vulnerabilidad

El equipo de seguridad de Dátil ejecuta anualmente una Evaluación de Riesgos que:

1. Identifica amenazas previsibles internas y externas que puedan resultar en acceso no autorizado, divulgación, mal uso, alteración o destrucción de cualquier información de Certificados o los Procesos de Administración de Certificados.
2. Evalúa la posibilidad y el daño potencial causados por estas amenazas, tomando en consideración la sensibilidad de los datos de Certificados y los Procesos de Administración de Certificados; y
3. Evalúa la adecuación de las políticas, los procedimientos, los sistemas de información, la tecnología y otros asuntos que la Autoridad de Certificación tiene para contrarrestar tales amenazas.

Dátil sigue un proceso formal documental de corrección de vulnerabilidades que incluye identificación, revisión, respuesta y remediación de vulnerabilidades.

Además, Dátil realiza un Análisis de Vulnerabilidades en las direcciones IP públicas y privadas que pertenecen a los Sistemas de Certificados en los siguientes casos:

- Al menos una vez cada tres meses;
- Después de hacer algún cambio significativo en los sistemas o redes.

Dátil realiza una prueba de penetración en sus Sistemas de Certificados al menos una vez al año y después de cualquier cambio en la infraestructura que crea determine como significativo.

5.5. Archivo de registros

5.5.1. Tipos de registros archivados

Los registros que se archivan son los especificados en la Sección 5.4.1.

5.5.2. Periodo de retención para archivo

Dátil conserva toda la documentación relacionada con las solicitudes de certificados y la verificación de las mismas, 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, o por más tiempo según lo exija la ley.

Se mantiene una copia de seguridad de la información de archivo en una ubicación distinta e independiente con requisitos de seguridad y disponibilidad similares.

5.5.4. Procedimientos de copia de seguridad de archivo

Los procedimientos de copia de seguridad y recuperación existen y pueden utilizarse para que esté disponible un conjunto completo de copias de seguridad en caso de pérdida o destrucción de los archivos primarios.

5.5.5. Requisitos para sellado de tiempo de registros

Todos los registros archivados llevarán una marca de tiempo en las instalaciones de registro normales de la AC. Tal información de tiempo no necesita estar basada en criptografía.

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

No estipulado.

5.5.7. Procedimientos para obtener y verificar información de archivo

No estipulado.

5.6. Cambio de claves

El procedimiento para proporcionar un nuevo certificado de AC a un Sujeto después de la generación de una nueva clave es el mismo que el procedimiento para proporcionar inicialmente el certificado de la AC.

5.7. Recuperación de desastres

5.7.1. Procedimientos de manejo de incidentes y compromisos

Si un desastre hace que una AC de Dátil deje de funcionar, Dátil reiniciará sus operaciones en hardware de reemplazo, en una instalación segura y comparable después de garantizar la integridad y seguridad de los sistemas de la AC.

Dátil mantiene un Plan de Respuesta a Incidentes y un Plan de Recuperación ante Desastres, que establece los procedimientos necesarios para garantizar la continuidad del negocio, para notificar a las partes interesadas afectadas y para proteger razonablemente el Software de aplicación, los Proveedores, los Suscriptores y los Terceros que Confían en caso de un desastre, compromiso de seguridad o fracaso empresarial. Dátil prueba, revisa y actualiza anualmente su plan de continuidad comercial y sus planes de seguridad y los pone a disposición de sus auditores a solicitud.

El plan de continuidad del negocio incluye:

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 de tiempo de recuperación (RTO);
9. Pruebas periódicas de planes de contingencia;
10. Un plan 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. Requisitos sobre cómo almacenar materiales criptográficos críticos (es decir, dispositivos criptográficos seguros y materiales de activación) en una ubicación alternativa;
12. Una definición de interrupción aceptable del sistema y tiempos de recuperación;
13. La frecuencia con la que se realizan copias de seguridad de la información comercial y software esenciales;

14. La distancia de las instalaciones de recuperación al sitio principal de la AC; y
15. Procedimientos para asegurar una instalación afectada después de un desastre y antes de restaurar una instalación segura ya sea en el sitio original o en uno remoto.

5.7.2. Procedimientos de recuperación si los recursos informáticos, el software o los datos están dañados

Dátil mantiene un sitio de respaldo en una ubicación remota que refleja su instalación principal, de modo que si algún software o datos están dañados, se puede restaurar desde el sitio de respaldo a través de una conexión segura.

Las copias de seguridad de todo el software y los datos relevantes se toman de forma regular. Se almacenan fuera del sitio y se pueden recuperar electrónicamente cuando sea necesario.

5.7.3. Procedimientos de recuperación después del compromiso clave

En caso de que la clave privada de una AC de Dátil se vea comprometida, Dátil:

- Deja de usar inmediatamente el material de clave comprometido;
- Revoca todos los certificados firmados con la clave comprometida;
- Toma medidas comercialmente razonables para notificar a todos los suscriptores de la revocación; y
- Toma medidas comercialmente razonables para que todos los suscriptores dejen de usar, para cualquier propósito, cualquiera de estos certificados.

Una vez que el material clave comprometido haya sido reemplazado y se haya establecido una operación segura de la AC en cuestión, la AC puede volver a emitir los certificados revocados siguiendo el procedimiento usado inicialmente para emitir los certificados.

5.7.4. Capacidades de continuidad comercial después de un desastre

Dátil emplea y contrata personal de seguridad que utilizará todos los medios razonables para monitorear las instalaciones de la AC después de un desastre natural u otro tipo de desastre para proteger los materiales sensibles y la información contra pérdidas, daños adicionales y robos.

Para confirmar que posee las capacidades apropiadas de recuperación ante desastres, Dátil realiza pruebas periódicas de sus planes de continuidad del negocio y recuperación ante desastres.

5.8 Terminación de una AC o AR

Cuando sea necesario terminar la operación de una AC de Dátil, el impacto de la terminación se debe minimizar lo más posible dadas las circunstancias. Esto incluye:

- Proporcionar aviso previo factible y razonable a todos los Suscriptores;
- Ayudar con la transferencia ordenada del servicio y los registros operativos a una AC sucesora, de existir alguna;
- Preservar todos los registros por mínimo un (1) año o según lo requiera esta DPC, o lo que sea más largo; y
- Revocar todos los certificados emitidos por la AC, a más tardar en el momento de la terminación.
-

Si es comercialmente razonable, se dará aviso previo de la finalización de una AC de Dátil al menos 3 meses antes de la fecha de finalización.

6. Controles técnicos de seguridad

6.1. Generación de par de llaves e instalación

6.1.1. Generación de par de llaves

Los pares de claves para las AC de Dátil se generan de conformidad con los procedimientos formales de generación de claves y dentro de un Módulo de Seguridad de Hardware certificado FIPS 140-2 Nivel 3 del que no se puede extraer la clave privada en texto sin formato.

Las solicitudes de certificados de suscriptor se rechazan si la clave pública no cumple con los requisitos establecidos en las Secciones 6.1.5 y 6.1.6 o si tiene una clave privada débil conocida.

6.1.2. Entrega de clave privada al suscriptor

Los Certificados son emitidos en formato PKCS#12 y la clave privada se encuentra contenida en un archivo que se enviará email al Suscriptor. La contraseña del archivo es escogida por el Suscriptor o generada por Dátil por solicitud del Suscriptor, cumpliendo con las prácticas de seguridad de esta DPC.

6.1.3. Entrega de clave pública al emisor del certificado

Los Suscriptores proporcionan su llave pública a Dátil para la certificación a través de una Solicitud de firma de certificado PKCS # 10. El método de transferencia preferido para enviar esta información es HTTP sobre Secure Sockets Layer (SSL).

6.1.4. Entrega de clave pública de CA a Terceros que Confían

Las claves públicas de las AC de Dátil están disponibles en el repositorio en línea en https://ac.datil.com.

6.1.5. Tamaños de claves

Para evitar ataques criptoanalíticos, todas las AC de Dátil utilizan tamaños de clave y protocolos criptográficos que se adhieren a las recomendaciones del NIST y a las disposiciones aplicables de los Requisitos de Referencia.

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

Para las claves RSA, Dátil confirma que el valor del exponente público es un número impar igual a 3 o más.

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

No estipulado.

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

6.2.1. Estándares y controles del módulo criptográfico

Todas las claves privadas de la AC utilizadas para firmar certificados, LRC o cualquier información relacionada utilizan módulos de seguridad de hardware que cumplen con el estándar FIPS 140-2 Nivel 3 o superior y las especificaciones de seguridad Common Criteria EAL4 +. La criptografía aplicada para proteger esta información está seleccionada para resistir ataques criptoanalíticos durante la vida útil de la clave cifrada.

Las claves privadas de la AC se guardan en una ubicación físicamente segura y nunca se almacenan sin cifrar fuera de los módulos de seguridad de hardware.

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

Todos los pares de llaves de la Autoridad de Certificación se generan en ceremonias de generación de claves planificadas previamente. Al finalizar la ceremonia, todas las personas involucradas firman la finalización exitosa del guión y describen a fondo cualquier excepción que pueda haberse aplicado en el proceso.

Los registros se mantienen al menos durante la vida útil del par de claves.

6.2.3. Custodia de clave privada

Las claves privadas de las AC de Dátil no están en custodia.

6.2.4. Copia de seguridad de clave privada

Las copias de seguridad de las claves privadas de la AC se almacenan de forma segura de acuerdo con la política de Dátil que sea aplicable.

6.2.5. Archivo de clave privada

Las claves privadas que pertenecen a las AC de Dátil no son archivadas por terceros que no sean Dátil.

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

Todas las transferencias de claves privadas hacia o desde un módulo criptográfico se realizan de acuerdo con los procedimientos especificados por el proveedor del módulo criptográfico.

6.2.7. Almacenamiento de clave privada en módulo criptográfico

Las claves privadas se almacenan de acuerdo con las instrucciones aplicables especificadas por el fabricante del módulo criptográfico.

6.2.8. Método de activación de clave privada

Las claves privadas se activan de acuerdo con las instrucciones aplicables especificadas por el fabricante del módulo criptográfico.

6.2.9. Método de desactivación de clave privada

Las claves privadas se desactivan de acuerdo con las instrucciones aplicables especificadas por el fabricante del módulo criptográfico.

6.2.10. Método de destrucción de clave privada

Las claves privadas se destruyen de acuerdo con las instrucciones aplicables especificadas por el fabricante del módulo criptográfico. Además, se sigue la política de Dátil sobre la destrucción de información altamente confidencial.

6.2.11. Clasificación del módulo criptográfico

Ver Sección 6.2.1.

6.3. Otros aspectos de la gestión de pares de claves

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 son 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.

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

Las claves del Módulo de seguridad de hardware se almacenan en el Módulo de seguridad de hardware y solo pueden ser utilizadas por administradores autorizados de la AC tras la autenticación respectiva. Las contraseñas necesarias para desbloquear las claves se almacenan en forma cifrada.

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 información del sistema de Dátil AC está protegida contra accesos no autorizados a través de una combinación de controles del sistema operativo, físicos y de redes. Los controles de seguridad de redes se especifican en la sección 6.7.

Los sistemas de la AC utilizan autenticación de doble factor para todas las cuentas con capacidad de afectar directamente 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

Dátil utiliza software que ha sido probado formalmente para determinar su idoneidad y aptitud para el propósito que se le da. El hardware y acceso a redes es tercerizado a proveedores líderes en la industria con capacidad de cumplir los estándares operativos y de seguridad exigidos por Dátil.

6.6.2. Controles de gestión de seguridad

Dátil ha establecido una Organización de Seguridad de Información que implementa y opera marcos de trabajo de control interno y abarca medidas de nivel técnico, organizacional y de procedimientos.

6.6.3. Controles de seguridad de ciclo de vida

La gestión de seguridad del sistema se controla a través de los privilegios asignados a las cuentas del sistema operativo de la infraestructura de la AC y mediante los Roles de Confianza descritos en esta DPC.

6.6. Controles de seguridad de redes

Los equipos seguros en los cuales operan las AC de Dátil se encuentran detrás de dispositivos de firewall que restringen el acceso solo a la red interna de Dátil y solo a los puertos utilizados para administrar la AC y emitir Certificados.

6.7. Sellado de tiempo

Todos los registros de auditoría contienen marcas de tiempo sincronizadas.

7. Perfil de certificados, LRC y OCSP

7.1. Perfil de los certificados

Los certificados de Dátil cumplen con el RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*. Las extensiones de certificado y su criticidad, así como los identificadores de objetos del algoritmo criptográfico, se completan de acuerdo con los estándares IETF RFC 5280.

7.1.1. Número de versión

Los Certificados X.509 de Suscriptores emitidos por las AC de Dátil cumplen la versión 3 de X.509.

7.1.2. Extensiones de los certificados.

Los campos y extensiones de los certificados se establecerán de acuerdo con RFC 5280. Las extensiones que se pueden incluir son:

- authorityKeyIdentifier
- subjectKeyIdentifier
- keyUsage
- certificatePolicies
- subjectAltName
- basicConstraints
- extKeyUsage
- cRLDistributionPoints
- authorityInformationAccess

La definición específica para cada tipo de Certificado se establece en la Política de Certificados respectiva.

7.1.3. Identificación de objeto del algoritmo

Se utilizan las siguientes identificaciones de objetos (OIDs):

- OID del algoritmo de firma sha256withRSA Encryption.

- OID del algoritmo de clave pública RSA Encryption.

7.1.4. Formas de los nombres

Al emitir un Certificado, Dátil declara que siguió el procedimiento establecido en esta DPC para verificar que, a partir de la fecha de emisión, la información del campo subject name es correcta, corresponde al nombre distintivo del Suscriptor y cumple con las estipulaciones descritas en la Sección 3.2.

Los campos de subject name o issuer name siempre contienen información que ha sido verificada.

7.1.5. Restricciones de nombres

La única restricción que Dátil aplica es que sean únicos y no ambiguos.

7.1.6. Identificador de objeto de la política de certificados

Los Certificados de Suscriptores podrán incluir los siguientes identificadores de objetos confirmando su cumplimiento con esta DPC y para indicar qué método de validación fue usado para su emisión.

El OID correspondiente a esta DPC es: 1.3.6.1.4.1.52643.2.5.1

Cada política podrá tener asignado un OID a partir de la raíz 52643.

7.1.7. Uso de la extensión de Restricciones de Políticas

No estipulado.

7.1.8. Sintaxis y semántica de calificadores de política

No estipulado.

7.1.9. Semántica de procesamiento para la extensión crítica de Política de Certificados

No estipulado.

7.2. Perfil de la LRC

Las LRC emitidas por las ACs de Dátil cumplen con los estándares de RFC 5280.

7.2.1. Número de versión

No estipulado.

7.2.2. Extensiones de LRC

Sin estipulación.

7.3. Perfil OCSP

Todas las AC de Dátil soportan OCSP y sus servidores correspondientes cumplen con el estándar RFC 6960.

7.3.1. Número de versión

No estipulado.

7.3.2. Extensiones OCSP

Se utilizan las siguientes extensiones conforme al estándar X.509 versión 3:

- keyUsage: crítica
- basicContraints: crítica

8. Auditorías de cumplimiento y otras evaluaciones

8.1. Frecuencia y circunstancia de las auditorías

Dátil realiza auditorías de cumplimiento al menos anualmente.

8.2. Identidad y calificaciones del evaluador

Las auditorías de cumplimiento de las AC de Dátil son realizadas por una firma de contadores públicos que posee las siguientes calificaciones y habilidades:

1. Independencia del tema de la auditoría;
2. Contrata a personas que tienen competencia para examinar 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;
3. Está obligado por la ley, la regulación gubernamental o un código de ética profesional.

8.3. Relación del evaluador con la entidad evaluada

Las auditorías de cumplimiento de las AC de Dátil son realizadas por firmas de contadores públicos independientes del objeto de la auditoría.

8.4. Temas cubiertos en la evaluación

Las evaluaciones anuales de cumplimiento de las AC de Dátil abarcan la validación de controles relevantes con la correcta operación de la AC. En particular, cubren la evaluación del cumplimiento con esta DPC y los estándares relacionados.

8.5. Acciones a tomar como resultado de deficiencias

En caso de encontrarse deficiencias significativas durante una auditoría de cumplimiento, se determinan acciones que deben ser realizadas por los administradores de la AC. Estas decisiones se hacen con la asesoría del auditor e implementadas comercialmente en un tiempo razonable.

8.6. Comunicación de resultados

El informe de auditoría se pone a disposición del público a más tardar tres meses después del final del período de auditoría. Dátil no está obligado a poner a disposición del público ningún hallazgo general de auditoría que no afecte la opinión general de la auditoría. En el caso de un retraso superior a tres meses, y si así lo solicita un proveedor de software de aplicaciones, Dátil proporcionará una carta explicativa firmada por el auditor calificado.

El Informe de Auditoría deberá indicar explícitamente que cubre los sistemas y procesos relevantes utilizados en la emisión de todos los Certificados por parte de las AC de Dátil.

8.7. Autoauditorías

Dátil monitorea su adherencia a estas DPC realizando auto auditorías al menos trimestralmente contra una muestra seleccionada al azar de lo que sea mayor entre un certificado o al menos tres por ciento de los Certificados emitidos por durante el período que comienza inmediatamente después de la toma de muestra de la última autoauditoría.

Dátil requiere que todas sus AC subordinadas, así como todos los terceros delegados, se sometan a una auditoría anual que cumpla con los criterios especificados en la Sección 8.1.

9. Otros asuntos legales y comerciales

9.1. Tarifas

9.1.1. Tarifas de emisión y renovación

Dátil podrá cobrar a sus Suscriptores por la emisión, administración y renovación de Certificados. Dátil nunca cobrará por la revocación de certificados que haya emitido.

9.1.2. Tarifas de acceso a certificados

Dátil podrá cobrar una tarifa razonable por el acceso a su base de datos de Certificados.

9.1.3. Tarifas de acceso a información de revocación y estatus

Dátil no cobra por el acceso a las LRC en cumplimiento con los requerimientos de esta DPC de que siempre estén disponibles en el Repositorio para los Terceros que Confían. Dátil, sin embargo, podrá cobrar una tarifa para proveer LRCs o servicios OCSP personalizados, o cualquier otro servicio de valor agregado relacionado a la información de estado y revocación.

Dátil no permite el acceso a la información de revocación, información de estatus de Certificados o sellados de tiempo en sus Repositorios por parte de terceros que provean productos o servicios que utilicen esa información de estatus de Certificados sin la autorización por escrito de Dátil.

9.1.4. Tarifas para otros servicios

Dátil no cobra por el acceso a esta DPC. Cualquier uso diferente a ver el documento, tal como reproducción, distribución, modificación o creación de trabajo derivativo, estará sujeto a un acuerdo de licenciamiento con Dátil.

9.1.5. Políticas de reembolso

No estipulado.

9.2. Responsabilidad financiera

9.2.1. Cobertura de seguros

Dátil mantiene una póliza general de responsabilidad civil.

Esta póliza no cubre actos relacionados con el incumplimiento de las obligaciones contraidas por el Suscriptor o el uso incorrecto de un Certificado y/o sus llaves privadas.

9.2.2. Otros activos

No estipulado.

9.3. Confidencialidad de información de negocios

9.3.1. Alcance de la confidencialidad de información

La siguiente información relacionada con el Solicitante y el Suscriptor se considera información confidencial.

1. Solicitudes de certificados;
2. Registros presentados por el solicitante en apoyo de las solicitudes de certificado;
3. Claves privadas;
4. Archivos de registro y otros registros de auditoría;
5. Registros de transacciones.

9.3.2. Información no confidencial

Los certificados y los datos de revocación no se consideran información confidencial. Además, la información no se considera confidencial si su divulgación es obligatoria de conformidad con esta DPC.

9.3.3. Responsabilidad para proteger la información confidencial

Dátil, sus contratistas y agentes utilizan medidas razonables de cuidado cuando procesan y al proteger información confidencial.

9.4. Privacidad de información personal

9.4.1. Plan de privacidad

Dátil sigue la Política de Privacidad publicada en: https://datil.com/privacy

9.4.2. Información que se trata como privada

Ver Sección 9.4.1.

9.4.3. Información no privada

Ver Sección 9.4.1.

9.4.4. Responsabilidad para proteger información privada

Ver Sección 9.4.1.

9.4.5. Aviso y consentimiento de uso de información privada

Ver Sección 9.4.1.

9.4.6. Divulgación de conformidad con procesos judiciales o administrativos

Ver Sección 9.4.1.

9.4.7. Otras circunstancias de divulgación de información

Ver Sección 9.4.1.

9.5. Derechos de propiedad intelectual

Dátil, o sus otorgantes de licencias, poseen los derechos de propiedad intelectual de los servicios de Dátil AC, incluidos los Certificados, las marcas comerciales utilizadas para proporcionar servicios de Certificados y esta DPC.

La información del certificado y la revocación son propiedad exclusiva de Dátil. Dátil otorga permiso para reproducir y distribuir certificados de forma no exclusiva y libre de regalías, siempre que se reproduzcan y distribuyan en su totalidad. Dátil no permite trabajos derivados de sus Certificados o productos sin un permiso previo por escrito.

Las claves privadas y públicas siguen siendo propiedad de los suscriptores que las poseen legítimamente. Todos los recursos compartidos secretos (elementos distribuidos) de las claves privadas de Dátil son propiedad de Dátil.

9.6. Representaciones y garantías

9.6.1. Representaciones y garantías de la AC

Dátil ofrece la siguiente garantía limitada a los Beneficiarios del Certificado en el momento de la emisión del Certificado: (a) emitió el Certificado sustancialmente de conformidad con esta DPC; b) la información contenida en el Certificado refleja con precisión la información proporcionada a Dátil por el Solicitante en todos los aspectos materiales; y (c) ha tomado medidas razonables para verificar que la información contenida en el Certificado sea precisa. Los pasos que Dátil da para verificar la información contenida en un Certificado se establecen en esta DPC.

9.6.2. Representaciones y garantías de la AR

No estipulado.

9.6.3. Representaciones y garantías del suscriptor

Dáti requiere, como parte del Acuerdo de Suscriptor o Acuerdo de Términos de Uso, que el Solicitante asuma los compromisos y garantías de esta Sección en beneficio de la AC y los Beneficiarios del Certificado.

Antes de la emisión de un Certificado, Dátil obtiene, para su beneficio expreso y el de los Beneficiarios del Certificado, ya sea:

1. La aceptación por parte del Solicitante del Acuerdo de Suscriptor con la AC, o
2. La aceptación por parte del Solicitante del acuerdo de Términos de Uso.

Dátil implementa un proceso para garantizar que cada Acuerdo de Suscriptor o 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. Dátil puede usar un acuerdo electrónico o de "clic" a condición de que haya determinado que dichos acuerdos son legalmente exigibles. Se puede usar un Acuerdo separado para cada solicitud de certificado, o un solo Acuerdo para cubrir múltiples solicitudes de certificados futuras y los Certificados resultantes, siempre que cada Certificado que la AC emita al Solicitante esté claramente cubierto por eso Suscriptor o Acuerdo de Términos de Uso.

El Acuerdo de Suscriptor o Términos de Uso contiene disposiciones que imponen al Solicitante o su representada las siguientes obligaciones y garantías:

1. Exactitud de la información: Obligación y garantía de proporcionar información precisa y completa en todo momento a Dátil, tanto en la solicitud del certificado como en la solicitud de Dátil en relación con la emisión de los Certificados que se proporcionarán;
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 (y cualquier dispositivo o datos de activación asociados, por ejemplo, contraseña o token);
3. Aceptación del Certificado: Obligación y garantía que el Suscriptor revisará y verificará la exactitud del contenido del Certificado;
4. Uso del Certificado: Obligación y garantía de utilizar el Certificado únicamente de conformidad con todas las leyes aplicables y únicamente de acuerdo con el Acuerdo de Suscriptor y Términos de Uso;

5. Informes y revocación: Obligación y garantía de dejar de usar rápidamente un Certificado y su Clave privada asociada, y solicitar de inmediato a Dátil que revoque el Certificado, en caso de que: (a) cualquier información en el Certificado sea incorrecta o se vuelva incorrecta o inexacto, o (b) hay un uso indebido o divulgación real o sospecha de la que clave privada del suscriptor asociada con la clave pública incluida en el certificado ha sido comprometida;
6. Terminación del uso del certificado: Obligación y garantía de suspender rápidamente el uso de la clave privada correspondiente a la clave pública incluida en el certificado tras la revocación de dicho certificado por razones de compromiso o divulgación de la clave.
7. Capacidad de respuesta: Obligación de responder a las instrucciones de Dátil sobre el uso de la clave del Certificado o el uso indebido del Certificado dentro de un período de tiempo específico.
8. Reconocimiento y aceptación: un reconocimiento y aceptación de que Dátil tiene derecho a revocar el certificado de inmediato si el Solicitante viola los términos del Acuerdo de Suscriptor o el Acuerdo de Términos de Uso o si Dátil descubre que el Certificado se está utilizando para habilitar ilegales.

Los Acuerdos de Suscriptor pueden incluir representaciones y garantías adicionales.

9.6.4. Representaciones y garantías de los terceros que confían

Los Terceros que Confían declaran y garantizan que: (a) han leído, entienden y aceptan esta DPC; (b) han verificado tanto el Certificado de Dátil AC relevante como cualquier otro certificado en la cadena de certificados utilizando la LRC u OCSP pertinente; (c) no utilizarán un Certificado si el Certificado ha expirado o ha sido revocado; (d) tienen información suficiente para tomar una decisión informada sobre el grado en que eligen confiar en la información en un Certificado; (e) han estudiado las limitaciones aplicables en el uso de Certificados y están de acuerdo con las limitaciones de Dátil sobre la responsabilidad relacionada con el uso de Certificados; (f) son los únicos responsables de decidir si confiar o no en la información contenida en un Certificado; y (g) son los únicos responsables de las consecuencias legales y de otro tipo de su incumplimiento de las obligaciones de la Parte Confiable en esta DPC.

Los Terceros que Confían también declaran y garantizan que tomarán todas las medidas razonables para minimizar el riesgo asociado con confiar en una firma digital, incluyendo solo confiar en un Certificado después de considerar:

1. La ley aplicable y los requisitos legales para la identificación de una parte, la protección de la confidencialidad o privacidad de la información y la exigibilidad de la transacción;
2. El uso previsto del Certificado como se indica en el Certificado o en esta DPC;
3. Los datos enumerados en el Certificado;
4. El valor económico de la transacción o comunicación;

5. La pérdida o daño potencial que sería causado por una identificación errónea o una pérdida de confidencialidad o privacidad de la información en la aplicación, transacción o comunicación;
6. La experiencia previa del Tercero que Confía lidiando con el Suscriptor.
7. La opinión y experiencia del Tercero que Confía respecto de los métodos de comercio basados en computadora; y
8. Cualquier otro indicio de confiabilidad o falta de confiabilidad perteneciente al Suscriptor y / o la aplicación, comunicación o transacción.

9.6.5. Representaciones y garantías de otros participantes

No estipulado.

9.7. Exclusión de garantías

Dátil no se hará responsable en las siguientes circunstancias respecto de la emisión y uso de los Certificados emitidos:

- Desastres naturales o cualquier otro caso de fuerza mayor.
- Uso de los certificados fuera del cumplimiento de esta DPC, fuera de su período de vigencia o cuando hayan sido revocados.
- Uso fraudulento de los Certificados, LRC o cualquier otra información relacionada.
- Por daños y/o prejuicios producto de la interpretación errada de esta Declaración de Prácticas de Certificación por parte de los Participantes.
- Por el incumplimiento de las obligaciones del Acuerdo de Suscriptor, Términos de Servicio o la ley vigente.
- Por el contenido de los mensajes, sitios web o documentos firmados y/o cifrados usando los Certificados.
- Por fraudes en la documentación presentada por el Solicitante.

9.8. Limitación de responsabilidad

EN LA MEDIDA PERMITIDA POR LA LEY APLICABLE, DÁTIL NO SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, INCIDENTAL, CONSECUENTE, EJEMPLAR O PUNITIVO, INCLUYENDO PERO NO LIMITADO A DAÑOS POR PÉRDIDA DE DATOS, LUCRO CESANTE O INGRESOS PERDIDOS, COSTOS DE ADQUISICIÓN DE BIENES O SERVICIOS SUSTITUTOS, HAYAN SIDO ESTOS CAUSADOS BAJO CUALQUIER TIPO DE RESPONSABILIDAD O CONTRATO. LA RESPONSABILIDAD AGREGADA DE DÁTIL BAJO ESTA DPC SE LIMITA A USD 500 (QUINIENTOS DÓLARES DE LOS ESTADOS UNIDOS DE AMÉRICA).

9.9. Indemnizaciones

No estipulado.

9.10. Plazo y terminación

9.10.1. Plazo

Esta DPC entra en vigencia al momento de su publicación en el Repositorio. Las enmiendas a esta DPC entran en vigencia al momento de su publicación en el Repositorio.

9.10.2. Terminación

Esta DPC y cualquier enmienda se mantienen vigentes hasta que sean reemplazadas por una nueva versión.

9.10.3. Efectos de la terminación

A la terminación de esta DPC, los participantes están sujetos a sus términos para todos los certificados emitidos por el resto de los períodos de validez de dichos certificados.

9.11. Notificaciones y comunicaciones individuales con los participantes

A menos que se especifique lo contrario por acuerdo entre las partes, los Participantes utilizarán métodos comercialmente razonables para comunicarse entre sí, teniendo en cuenta la importancia crítica y el tema de la comunicación.

9.12. Enmiendas

9.12.1. Procedimiento para enmiendas

Dátil puede cambiar esta DPC en cualquier momento a su exclusivo criterio y sin previo aviso a los Suscriptores o Terceros que Confían. La DPC y sus enmiendas están disponibles en el Repositorio. Cualquier enmienda a esta DPC se evidenciará con un nuevo número de versión y fecha, excepto cuando las enmiendas sean puramente administrativas.

9.12.2. Mecanismos de notificación y período

Dátil puede proporcionar un aviso adicional (en el Repositorio o en un sitio web separado) en caso de que realice cambios importantes en su DPC. Dátil es responsable de determinar qué

constituye un cambio importante de la DPC. Dátil no garantiza ni establece un período de notificación para los Suscriptores

Todas las enmiendas a la DPC serán notificadas a la Entidad de Control respectiva según lo requiera la Ley.

9.12.3. Circunstancias en la cuales deba ser cambiado un OID

No estipulado.

9.13. Provisiones sobre resolución de disputas

No estipulado.

9.14. Ley aplicable

La operación de Dátil AC y esta DPC, así como las Políticas de Certificados están sujetos a la siguiente normativa:

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.

Todos los Participantes se someten exclusivamente a la jurisdicción de los tribunales de Guayaquil, República del Ecuador.

9.15. Cumplimiento de la ley aplicable

Esta DPC está sujeta a las leyes, normas, reglamentos, ordenanzas, decretos y pedidos nacionales, estatales, locales y extranjeros aplicables. Dátil obtiene las licencias para sus AC en cada jurisdicción que opera donde la ley de dicha jurisdicción requiere la licencia para la emisión de Certificados.

9.16. Provisiones varias

9.16.1. Aceptación completa

No estipulado.

9.16.2. Asignación

Los Terceros que Confían y los Suscriptores no pueden asignar sus derechos u obligaciones bajo esta DPC, por ley o de otro modo, sin la aprobación previa por escrito de Dátil. Cualquier intento de asignación será nulo. Sujeto a lo anterior, esta DPC será vinculante y redundará en beneficio de las partes del presente, sus sucesores y cesionarios permitidos.

9.16.3. Divisibilidad

Si alguna disposición de esta DPC se considera inválida, ilegal o inaplicable, la validez, legalidad o exigibilidad del resto de esta DPC no se verá afectada o perjudicada de ninguna manera por el presente.

9.16.4. Cumplimiento

Dátil puede solicitar indemnización y honorarios de abogados de la otra parte por daños, pérdidas y gastos relacionados con la conducta de esa parte. El hecho de que Dátil no haga cumplir una disposición de esta DPC no significa que renuncie al derecho de Dátil de hacer cumplir la misma disposición más adelante o del derecho de hacer cumplir cualquier otra disposición de esta DPC. Para ser efectivos, las exenciones deben ser por escrito y firmadas por Dátil.

9.16.5. Fuerza mayor

Dátil no será responsable de ningún incumplimiento o retraso en el cumplimiento de sus obligaciones en virtud del presente documento en la medida y mientras dicho incumplimiento o retraso sea causado, directa o indirectamente, por fuego, inundación, terremoto, elementos de la naturaleza o actos de Dios, actos de guerra, terrorismo, disturbios, desórdenes civiles, rebeliones o revoluciones en los Estados Unidos de América o la República del Ecuador, huelgas, cierres patronales o dificultades laborales o cualquier otra causa similar más allá del control razonable de Dátil.

9.17. Otras provisiones

No estipulado.

Apéndice A: Revisiones

Versión	**Fecha**	**Autores**	**Descripción**
1.0	2021-10-01	Eduardo Raad	Versión inicial

Apéndice B: Definiciones, acrónimos y referencias

Definiciones

Autoridad de Certificación (AC): Una organización que es responsable de la creación, emisión, revocación y administración de Certificados. El término aplica igual para ACs Raiz y ACs Subordinadas. El términos AC, dependiendo del contexto, también puede referirse a la infraestructura usada por esa organización para proveer Servicios de AC.

AC Emisora: En relación a un Certificado en particular, la AC que emitió el Certificado. Esta podría ser una AC Raíz o AC Subordinada.

AC Subordinada: Una Autoridad de Certificación cuyo Certificado está firmado por una AC Raíz y otra AC Subordinada.

AC Raíz: La Autoridad de Certificación de primer nivel de la cual el Certificado Raíz se usa para emitir Certificados de ACs Subordinadas.

Acuerdo de Suscriptor: El contrato entre Dátil y un Suscriptor mediante el cual el Suscriptor acepta los términos y condiciones requeridos por esta DPC respecto de cada Certificado emitido para el Suscriptor y su nombramiento como Sujeto en cada uno de ellos.

AR: Ver Autoridad de Registro.

Autoridad de Registro (AR): Cualquier Entidad Legal que sea responsable de la identificación y autenticación de sujetos de Certificados, pero no es una AC, de manera que no firma ni emite Certificados. Una AR puede asistir en la aplicación para obtener un Certificado, en su proceso de revocación o ambos. Cuando se usa “AR” como adjetivo para describir una función o rol, no necesariamente implica una entidad separada sino que puede ser parte de la AC.

Beneficiarios de Certificados: Cualquiera de estas partes:

- El Suscriptor que es parte del Acuerdo de Suscripción o Términos de Uso de un Certificado.
- Todos los Proveedores de Software con quienes la AC Raíz ha suscrito un contrato para que sus Certificados Raíz sean incluidos y distribuidos en el software de ese Proveedor de Aplicaciones de Software y
- Todos los Terceros que Confían quienes razonablemente dependan de un Certificado válido.

Certificado: Un documento electrónico que utiliza una firma electrónica para vincular una llave pública con una identidad.

CN: Nombre Común.

Dátil: DATILMEDIA S.A. (sociedad anónima constituida en la República del Ecuador).

Dátil AC: Una AC operada por Dátil en concordancia con esta DPC y que está listada en la Sección 1.2.1 de esta DPC.

Dátil ILP: La Infraestructura de Llave Pública de Dátil, establecida, operada y mantenida por Dátil para certificados públicamente confiables.

Certificado Dátil: Un certificado emitido por una AC de Dátil bajo esta DPC.

Certificado Raíz: Un Certificado auto-firmado emitido por la AC Raíz para identificarse a sí mismo y para facilitar la verificación de Certificados emitidos por por sus AC Subordinadas.

Criptografía de Llave Pública: Un tipo de criptografía, también conocida como criptografía asimétrica, que utiliza un par de llaves únicas de tal manera que la llave privada de ese par de llaves puede descifrar un registro electrónico cifrado con la llave pública, o puede generar una firma digital, y la correspondiente Llave pública, para cifrar ese registro electrónico o verificar esa firma digital.

Datos de Activación: Datos diferentes a las llaves, que son requeridos para acceder u operar módulos criptográficos (ej. Claves secretas o Números de Identificación Principal o “PIN”).

Declaración de Prácticas de Certificación (DPC): Este documento.

Entidad Legal: Una asociación, corporación, alianza, entidad de gobierno o cualquier otra entidad con validez legal en el sistema legal de un país.

Entidad Reguladora: Una entidad legal operada por el gobierno local, seccional o ministerial.

Equipo de Seguridad de Información: Empleados de Dátil que pertenecen a la organización se Seguridad y Privacidad.

Especialista de Validación: Alguien que realiza las tareas y deberes de verificación de información de acuerdo a lo especificado en estos requerimientos.

FIPS: (US Government) Federal Information Processing Standard.

Identificación y Autenticación: El proceso para determinar y confirmar mediante la consulta e investigación apropiadas la identidad y autoridad de una persona o entidad. Ver sección 3.2.

Infraestructura de Llave Pública (ILP): Un conjunto de hardware, software, personas, procedimientos, reglas, políticas y obligaciones que se utilizan para facilitar la creación, emisión, administración y uso confiables de certificados y llaves basadas en criptografía de clave pública.

Lista de Revocación de Certificados (LRC): Una lista con sello de tiempo qye es actualizada regularmente con los Certificados revocados y que es firmada digitalmente por la AC que emitió esos Certificados.

Llave Privada: La llave de un par de llaves que el titular del par de llaves mantiene en secreto y que se utiliza para crear firmas digitales y / o para descifrar registros o archivos electrónicos que se cifraron con la llave pública correspondiente.

Llave Pública: La llave de un par de llaves que puede ser divulgada públicamente por el titular de la llave privada correspondiente y que es utilizada por una parte confiable para verificar las firmas digitales creadas con la llave privada correspondiente del titular y / o para cifrar mensajes para que puedan se descifrara solo con la llave privada correspondiente del titular.

NIST: (Us Government) National Institute of Standards and Technology.

OCSP: Online Certificate Status Protocol.

OID: Object Identifier.

Object Identifier: Un identificador alfanumérico o numérico único registrado bajo el estándar aplicable de la Organización Internacional de Normalización para un objeto específico o clase de objeto.

Online Certificate Status Protocol: Un protocolo en línea para chequeo de Certificados que permite a las aplicaciones de software de los Terceros que Confían determinar el estatus de un Certificado identificable. Ver también Servicio OCSP.

Par de llaves: Dos números matemáticamente relacionados, conocidos como clave pública y su clave privada correspondiente, poseen propiedades tales que: (i) la clave pública puede usarse para verificar una firma digital generada por la clave privada correspondiente; y / o (ii) la Clave pública se puede utilizar para cifrar un registro electrónico que solo se puede descifrar utilizando la Clave privada correspondiente.

Participantes: Las personas autorizadas a participar en Dátil ILP, conforme a como están identificadas en la Sección 1.2.

Política(s) de Certificados: Las Políticas de Certificados de Dátil.

Proceso de Administración de Certificados: Procesos, prácticas y procedimientos asociados con el uso de llaves, software y hardware con los que la AC verifica los Datos de Certificados, emite Certificados, mantiene un Repositorio y revoca Certificados.

Proveedor de Aplicaciones de Software: Es un proveedor de software para firma electrónica o cualquier otro tipo de uso que utiliza y muestra los Certificados e incorpora los Certificados Raíz.

Re-emisión: El proceso de adquirir un nuevo Certificado Dátil y un Par de Llaves asociado para reemplazar a un Certificado Dátil y su Par de Llaves asociado existentes, previo a la expiración del período operacional de un Certificado Dátil y Par de Llaves existentes.

Reporte de Auditoría: Un reporte por un auditor externo con la opinión sobre si los procesos y controles de la entidad cumplen con los requerimientos de esta DPC.

Repositorio: Una base de datos accesible en línea en la Dátil ILP que contenga esta DPC, la LRC de Certificados Dátil revocados y cualquier otra información especificada por Dátil.

Revocado: La designación de estatus de un Certificado que significa que ha sido invalidado permanentemente.

Servicios de AC: Son servicios relacionados a la creación, emisión y administración de Certificados provistos por Dátil bajo esta DPC.

Servicio OCSP: Un servidor en línea operado bajo la autoridad de la AC y conectado a su Repositorio para procesar solicitudes de estado de Certificado. Consulte también, Online Certificate Status Protocol.

Solicitante: Persona natural o jurídica que aplica para (o busca renovar) un Certificado. Una vez que el Certificado es emitido, el Solicitante pasa a llamarse el Suscriptor.

Sujeto: Individuo u organización con un nombre mencionado en el campo “Subject” del Certificado.

Suscriptor: Una persona u organización que se nombra como el Sujeto de un Certificado y que ha aceptado los términos y condiciones del Acuerdo de Suscriptor con Dátil.

Tercero que Confían: Cualquier persona natural o jurídica que confía en un Certificado Válido. Un Proveedor de Aplicaciones de Software no se considera un Tercero que Confía cuando el software distribuido por ese Proveedor sólo despliega o muestra la información relacionada al Certificado.

Acrónimos

AC, Autoridad de Certificación

AAC, Autoridad de Autorización de Certificación

AR, Autoridad de Registro

PC, Política de Certificados

LRC, Lista de Revocación de Certificados

FIPS, (US Government) Federal Information Processing Standard

IANA, Internet Assigned Numbers Authority

ILP, Infraestructura de Llave Pública

ISO, International Organization for Standardization

NIST, (US Government) National Institute of Standards and Technology

OCSP, Online Certificate Status Protocol

OID, Object Identifier

PKI, Public Key Infrastructure

Referencias

ETSI EN 319 403, Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.

ETSI EN 319 411-1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

ETSI TS 102 042, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.

FIPS 140-2, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, May 25, 2001.

ISO 21188:2006, Public key infrastructure for financial services -- Practices and policy framework. Network and Certificate System Security Requirements, v.1.0, 1/1/2013.

RFC2527, Request for Comments: 2527, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, March 1999.

RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.