Declaración de Prácticas de Certificación

TuID

Versión 1.2

20/04/2020

TABLA DE CONTENIDOS

1 INTRODUCCIÓN

1.1 Descripción general

ANTEL brinda a sus clientes un servicio de identidad digital custodiada, que consiste en realizar el registro de los solicitantes, generar la identidad digital en sus sistemas y emitirle factores de identificación para que puedan hacer uso de esta al momento de acceder a servicios, propios de ANTEL y de terceros. Formalmente, Antel es un Prestador de Servicios de Certificación Acreditada (PSCA) y un Prestador de Servicios de Confianza (PSCo) acreditado ante la Unidad de Certificación Electrónica (UCE) y para ello opera una plataforma, llamada TuID, de firma e identificación en custodia centralizada en conformidad con la normativa europea eIDAS y la reglamentación vigente en Uruguay.

Las Identidades Digitales estarán formadas por una serie de datos personales de cada usuario, factores de autenticación y un certificado reconocido. Los usuarios de TuID podrán gestionar su Identidad digital de forma remota a través del portal www.tuid.uy

El presente documento constituye la Declaración de Prácticas de Certificación (Certificate Practice Statement, CPS en adelante) de la Autoridad Certificadora de ANTEL, utilizada para la emisión de certificados de Firma en Custodia Centralizada e Identificación Digital. El alcance de este documento es la definición de las prácticas y procedimientos empleados por ANTEL en la emisión de los certificados que dan soporte al servicio de firma e identificación con custodia centralizada que brinda a sus clientes.

Desde mayo de 2020 Antel se constituyó también en Prestador de Servicios de Sellado de Tiempo, en conformidad con la Política de Sellado de Tiempo de la UCE y legislación vigente. Para dicho servicio Antel cuenta con una Declaración de Prácticas separada, que oficia como extensión de la presente declaración para contemplar lo relativo a los servicios de sellado de tiempo.

A efecto de permitir a los solicitantes y usuarios conocer la reglamentación vigente, este documento, otras declaraciones y las políticas definidas por la UCE estarán disponibles en www.tuid.uy.

1.2 Identificación

Nombre: Declaración de Prácticas de Certificación de la AC de ANTEL.

Versión: 1.2

Fecha de elaboración: 07/02/2019

Fecha de última actualización: 20/04/2020

OID: 2.16.858.10000157.66565.5

Sitio web de publicación: www.tuid.uy/legal/Declaracion_Practicas_Certificacion_TuID.pdf

1.3 Usuario y ámbito de aplicación

1.3.1 Autoridad Certificadora

El rol de Autoridad Certificadora es desempeñado por ANTEL, en conformidad con la Política de firma electrónica avanzada con custodia centralizada de Persona Física de la UCE, y sus funciones están

detalladas en el presente documento. En adelante se referirá a la Autoridad Certificadora de Antel como "ACPA" (Autoridad Certificadora de Prestador Acreditado).

1.3.2 Autoridad de Registro

El rol de Autoridad de Registro para la ACPA de Antel es también desempeñado por Antel a través de sus oficinas comerciales de todo el país o puestos móviles, y sus funciones están estipuladas en el presente documento.

Antel podrá delegar en otras organizaciones este rol a través de un acuerdo específico el cual será enviado a la UCE antes de comenzar la operación. En el portal www.tuid.uy estará disponible el listado y las condiciones para cada autoridad de registro delegada. Estas autoridades también deberán cumplir con lo establecido en el presente documento y se informará a la UCE todos los acuerdos que se realicen.

1.3.3 Suscriptores

Los suscriptores de los certificados emitidos por la ACPA son Personas Físicas, nacionales o extranjeras, mayores de dieciocho (18) años, que utilizan los mismos a través del servicio de custodia centralizada, contrayendo derechos y obligaciones establecidos en la Política de firma electrónica avanzada con custodia centralizada de Persona Física y la Política de firma electrónica avanzada de Persona Física.

1.3.4 Terceros Aceptantes

Personas físicas o jurídicas que confían en los certificados emitidos por la ACPA a los suscriptores según la presente Declaración de Prácticas de Certificación. Los Terceros aceptantes utilizan estos certificados para validar la cadena de confianza de la PKI al momento de validar una firma electrónica avanzada de un documento o realizar una autenticación basada en el certificado que se encuentra en custodia centralizada.

1.3.5 Autoridad de Sellado de Tiempo

Antel también se constituyó ante la UCE como Autoridad de Sellado de Tiempo. Las funciones de Antel para dicho rol exceden el alcance del presente documento y se encuentran estipuladas en la Declaración de Prácticas de la TSA de Antel, que es una extensión del presente documento.

1.4 Usuario y ámbito de aplicación

1.4.1 Usos Permitidos de los Certificados

Al tratarse de un servicio de firma en custodia centralizada, los sujetos hacen uso de los certificados exclusivamente a través del servicio de firma e identificación que Antel dispone. Para tal fin, los usuarios finales se autentican en la plataforma y autorizan explícitamente la realización de una firma o autenticación en su nombre, mediante el ingreso de un PIN que protege la clave de firma en exclusividad.

Los usos habilitados y restricciones para los certificados emitidos bajo la presente Política están definidos en la Política de firma electrónica avanzada con custodia centralizada de Persona Física de UCE.

1.4.2 Restricciones en el Uso de los Certificados

Los certificados no pueden ser utilizados con otro fin a los estipulados en el punto 1.4.1. La utilización de la llave privada asociada al certificado para otro fin es considerada causal de revocación de este.

1.5 Administración de la política de certificación

1.5.1 Restricciones en el Uso de los Certificados

La administración de la presente Declaración de Prácticas de Certificación es responsabilidad de ANTEL.

1.5.2 Persona de Contacto

Por consulta o sugerencias, ANTEL designa al siguiente contacto:

Nombre: Antel

Dirección de correo: tuid@antel.com.uy

Teléfono: 08004343

1.5.3 Persona que determina la idoneidad de la CPS

No estipulado.

1.5.4 Procedimiento de aprobación de la CPS

La presente CPS es elaborada y mantenida por Antel, rigiendo para ello los procedimientos internos de aprobación. Toda versión de la CPS además es enviada a la UCE para su aprobación.

1.6 Definiciones y abreviaturas

Autoridad Certificadora (CA): refiere a la entidad de confianza responsable de emitir o revocar los certificados electrónicos, se utiliza como sinónimo de ACPA (Autoridad Certificadora del Prestador Acreditado).

Autoridad Certificadora Raíz Nacional (ACRN): conjunto de sistemas informáticos, personal, políticas y procedimientos que, en la estructura de PKI Uruguay por herencia, constituyen la raíz de confianza. Permite certificar a otras entidades encargadas de emitir certificados dentro de PKI Uruguay.

Autoridad Certificadora del Prestador Acreditado (ACPA): suscriptor de los certificados emitidos por la ACRN que, durante su operativa, emite certificados a usuarios finales bajo las políticas de certificación que le fueron asignadas.

Certificado Electrónico (CE): documento electrónico firmado electrónicamente que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de la firma electrónica.

Declaración de Prácticas de Certificación (CPS – Certificate Practice Statement): declaración de las prácticas que emplea una entidad certificadora en la gestión de los certificados emitidos por ella (emisión, revocación, renovación, etc.).

Escrow: acuerdo mediante el cual una clave privada puede ser custodiada por una entidad y, bajo ciertas circunstancias, ser devuelta a su legítimo dueño.

FIPS (Federal Information Processing Standard) 140 nivel 3: estándar de seguridad de ordenadores del gobierno de los Estados Unidos para la acreditación de módulos criptográficos. En su nivel 3 asegura que los módulos sean resistentes a la intrusión física.

Firma electrónica avanzada con custodia centralizada: firma electrónica avanzada en la cual la clave privada del firmante se encuentra en custodia de un prestador de servicios de confianza acreditado, que realiza la firma bajo orden expresa del firmante.

Infraestructura de clave pública (PKI – Public Key Infrastructure): es una combinación de hardware, software, y políticas y procedimientos de seguridad, que permiten la ejecución con garantías de operaciones criptográficas, como el cifrado, la firma digital, y el no repudio de transacciones electrónicas.

Lista de Certificados Revocados (CRL – Certificate Revocation List): Es un listado de todos los certificados digitales que han sido revocados.

Medio de identificación electrónica o digital: unidad material o inmaterial, procesable por un sistema informático, con una parte en control del sistema y otra en exclusivo control de la persona, ya sea mediante:

a. su conocimiento;
b. un dispositivo físico o lógico;
c. algún rasgo físico o comportamental.

Módulo de Hardware de Seguridad (HSM – Hardware Security Module): dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas.

Política de Certificación (CP – Certificate Policy): conjunto de políticas que indican la aplicabilidad de un certificado a una comunidad particular y/o clase de solicitud con requerimientos comunes de seguridad, y además definen los requisitos que cualquier prestador debe respetar para trabajar con ese tipo de certificado. En el contexto de PKI Uruguay estas políticas son promovidas, aprobadas y mantenidas por la UCE.

Prestador de Servicios de Certificación Acreditado (PSCA): entidad acreditada ante la UCE y responsable de la operación de una Autoridad de Certificación de PKI Uruguay.

Prestador de Servicios de Confianza (PSCo): entidad acreditada ante la UCE para brindar uno o más servicios de confianza. En el contexto del presente documento, corresponde al prestador del servicio de firma e identificación en custodia centralizada.

Protocolo de comprobación del Estado de Certificados en Línea (OCSP – Online Certificate Status Protocol): Permite validar el estado de un certificado electrónico, comprobando que es correcto y que no está revocado.

Registro de Identificación Digital: proceso de identificar a una persona, verificar sus datos, expedir o asociar uno o más medios de identificación digital a ésta, y almacenar dicha asociación para su posterior utilización.

Servicios de Confianza: servicios electrónicos que permiten brindar seguridad jurídica a los hechos, actos y negocios realizados o registrados por medios electrónicos, entre ellos:

- Servicios de firma electrónica avanzada con custodia centralizada;
- Servicios de identificación digital;
- Servicios de sellado de tiempo;
- Otros servicios establecidos por la Unidad de Certificación Electrónica.

Servicios de Identificación Digital: servicios que realizan registros de autenticación electrónica de personas para su verificación por terceros.

Solicitud de Firma de Certificado (CSR – Certificate Signing Request): es un mensaje emitido por la ACPA bajo el estándar PKCS#10 mediante el que solicita y provee información a la ACRN para la emisión de un certificado firmado por ella.

Terceros Aceptantes: en el contexto de PKI Uruguay, usuarios que validan y confían en certificados emitidos por una Autoridad de Certificación de la PKI, sea la ACRN o una de las ACPA.

VA (Autoridad de Validación): prestador de servicios de certificación que asegura la autenticidad, validez e integridad de los certificados electrónicos.

2 RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIO

2.1 Repositorios

Los repositorios públicos de la ACPA de ANTEL están disponibles durante las veinticuatro (24) horas los siete (7) días de la semana y en caso de error del sistema fuera del control de ANTEL, éste dedicará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en un período establecido en 48 horas.

2.2 Publicación de la información de certificación

ANTEL dispone del siguiente sitio web como repositorio público de información: www.tuid.uy.

2.3 Tiempo o frecuencia de la publicación

Se realizan revisiones anuales al presente documento. De surgir cambios en el mismo, se publicará la nueva versión luego de su aprobación.

2.4 Controles de acceso a los repositorios

ANTEL brinda acceso irrestricto a toda la información contenida en el repositorio público y establece controles adecuados para restringir la posibilidad de escritura y modificación de la información publicada, garantizando su integridad.

3 IDENTIFICACIÓN Y AUTENTICACIÓN

En el contexto de la presente Declaración de Prácticas, la Identificación y Autenticación comprende el proceso que se aplica cuando el suscriptor persona física desea obtener su identidad digital custodiada, para lo cual se presenta en la AR, quien a través de sus funcionarios valida su identidad y habilita la emisión de su certificado.

3.1 Nombres

La Autoridad de Registro de Antel asignará al certificado del suscriptor el nombre que figure en el documento de identidad utilizado para realizar el registro.

Para el nombre del suscriptor se utiliza el campo “Subject” del certificado. El formato para indicar el nombre es es X.500 (Distinguished Name) tal como es especificado en la política de persona física.

3.2 Validación de identidad inicial

3.2.1 Método para probar la posesión de la clave privada

Al tratarse de un PSCo, en todos los casos la clave privada se genera utilizando los HSM de la plataforma, queda siempre en custodia de ésta y es utilizada a través de mecanismos específicamente destinados para tal fin. Es por eso por lo que la posesión de la clave privada es verificada por la propia generación de ésta en el entorno seguro del PSCo.

3.2.2 Registro presencial inicial

El Registro Presencial se realizará frente a una Autoridad de Registro, presentando la CI común, pasaporte o la CI electrónica como mecanismo de identificación. Este proceso permitirá crear la identidad digital del sujeto o renovarla si ya existía.

Existirán dos tipos de registro presencial, dependiendo de si se realiza una verificación biométrica del solicitante (nivel tres) o no (nivel dos). Este nivel de registro podrá ser utilizado posteriormente por las aplicaciones integradas al servicio de TuID para aplicar niveles de seguridad diferenciales.

En caso de presentar CI común o pasaporte, el funcionario de la AR valida la autenticidad del documento, valida visualmente que sea el documento del sujeto que se presenta e ingresa manualmente los datos identificatorios en el sistema para continuar con el proceso, logrando un nivel dos (2) en el registro.

El funcionario de la AR podrá solicitar al solicitante registrar sus datos biométricos, huellas dactilares y biometría de rostro. El dispositivo utilizado para realizar este registro no guardará ningún dato del sujeto. Durante ese registro adicionalmente se realizará la verificación biométrica del solicitante.

- En caso de contar con CI electrónica, se deberá insertar la CI en el lector correspondiente para que el sistema realice una validación de la autenticidad del documento y extraiga los datos de identificación de éste. Adicionalmente, se utiliza un lector de huellas para realizar un Match On Card como verificación biométrica del sujeto, logrando así un nivel tres (3) en el registro.
- En caso de no contar con CI electrónica, el funcionario solicitará la validación biométrica del solicitante utilizando el lector de huellas, a partir del servicio de cotejo de huellas de la Dirección Nacional de Identificación Civil (DNIC). En caso de que el servicio retorne un nivel aceptable de similitud también se logrará un nivel tres (3) de registro.

Se generará una traza con el resultado de la validación biométrica que guardará como datos más relevantes las minucias obtenidas, identificador del solicitante, el método de verificación y el resultado obtenido. Las minucias de las huellas dactilares son guardadas de tal forma que no es posible reconstruir a partir de las mismas las huellas que las originaron y además la información estará cifrada. Los datos biométricos en ningún caso son extraídos ni compartidos a terceros.

Durante el registro presencial el usuario deberá definir una contraseña para asociar el mecanismo *usuario y contraseña* a su Identidad Digital.

Si el usuario es mayor de dieciocho (18) años utilizará su contraseña para ingresar al portal de auto gestión de las Identidades Digitales de TuID con el fin de habilitar la generación de su certificado y PIN de firma, que es independiente de los demás factores de autenticación y es usado en exclusividad para proteger el acceso a la clave privada del certificado electrónico reconocido.

3.2.3 Registro presencial con identidad previa

Este proceso es análogo al anterior, pero aplica para el caso en que el usuario ya posee una identidad digital en el servicio, pero que no necesariamente fue registrada con un nivel elevado de validación (por ejemplo, con auto registro remoto) y por lo tanto tampoco tiene certificado digital de firma y autenticación. Se realiza el registro presencial entonces de la misma forma que en el punto anterior, sólo que se utilizará el perfil de usuario ya creado. Se podrá modificar la información de éste si hubiera diferencias con respecto al documento de identidad presentado. Se asignará a la identidad un nivel de registro dos o tres según sea el caso. Finalmente, el sujeto utilizará su usuario y contraseña o la app de TuID para solicitar la emisión de su certificado asociado a la identidad validada, y podrá definir el PIN de firma correspondiente para protegerlo.

La app de TuID consiste en una aplicación móvil, que se sincroniza con la Identidad del Usuario y luego puede usar para autenticarse en forma sencilla, utilizando los factores de autenticación de su teléfono como ser patrón, pin, huella dactilar o reconocimiento facial. Se trata de un factor de autenticación basado en algo que se tiene, dado que el perfil de la app de TuID se genera con claves únicas para cada usuario e instancia de instalación.

3.2.4 Auto-Registro remoto

El servicio de identidades de Antel contempla la posibilidad de que un usuario se conecte por internet y solicite en forma remota su identidad, utilizando para eso su cédula. El proceso consiste en el ingreso de sus datos y la activación de uno o más factores de autenticación (usuario y contraseña, OTP, app móvil de TuID). Se verificará la consistencia de los datos utilizando el servicio de la DNIC para validar que se trate de un registro único en la plataforma. El nivel de registro asociado en este caso será el nivel uno (1) y el solicitante no podrá en este caso solicitar la generación de un certificado.

3.2.5 Información no verificada del suscriptor

Los certificados emitidos por la ACPA de Antel no contienen ninguna información no verificada del suscriptor, ya que son generados exclusivamente a partir de identidades con nivel de registro dos o tres, las cuales se asignan luego de un proceso de registro presencial por un funcionario o por un sistema de autogestión que extrae los datos de la CI electrónica de Uruguay.

Las identidades generadas mediante auto registro remoto sí contienen información no verificada del suscriptor, pero para ellas no es posible solicitar emisión de certificado, precisamente porque no se tiene un registro de nivel aceptable del suscriptor.

3.3 Identificación y autenticación para las solicitudes de cambio de claves

No se realiza cambio de claves de certificados. En caso de requerirse, se realiza un cambio de clave en el marco de los procesos de renovación o revocación y reemisión de certificados.

3.3.1 Identificación y autenticación para la reasignación de clave rutinaria

No aplica.

3.3.2 Identificación y autenticación para la reasignación de clave luego de la revocación

No aplica.

3.4 Identificación y autenticación para la solicitud de revocación

La Autoridad de Registro valida la identidad del solicitante previo a la solicitud de revocación del certificado emitido previamente de la misma manera que en el registro presencial, sea a través del funcionario de la Autoridad de registro o a través del sistema de auto gestión.

La Revocación de un certificado podrá realizarse a través de diversas vías:

- Presencial: donde la Autoridad de Registro validará la identidad del solicitante previo a la solicitud de revocación del certificado emitido previamente de la misma manera que en el registro presencial
- Remota: donde el usuario deberá autenticarse en el sistema de auto gestión para luego solicitar la revocación de su certificado
- Administrativa: por disposición de la UCE
- Judicial: por orden judicial
- Telefónica: A partir de una mesa de ayuda disponible 24/7, con previa identificación del usuario a través de la solicitud de información personal, los usuarios podrán solicitar el bloqueo de su Identidad Digital durante un período de 48hs.

4 REQUERIMIENTOS OPERATIVOS DEL CICLO DE VIDA DE LOS CERTIFICADOS

En esta sección se declaran los controles que realiza la AC de ANTEL para asegurar una gestión segura del Ciclo de Vida de los Certificados emitidos por ella, y también se especifican controles que los suscriptores de esos certificados deben considerar.

4.1 Solicitud de certificados

4.1.1 Quién puede presentar una solicitud de certificado

Los suscriptores finales de certificados del servicio de firma e identidad custodiada de Antel son personas físicas, nacionales o extranjeras, mayores de dieciocho (18) años.

4.1.2 Proceso de enrolamiento y responsabilidades

El suscriptor solicita inicialmente la creación de su identidad digital en la plataforma, a través de los procedimientos detallados en la sección 3.2. Al inicio de este proceso el suscriptor deberá firmar el *Contrato para la obtención de Certificado electrónico para firma avanzada de TuID* para aceptar los términos y condiciones de su emisión y uso. Luego de creada su identidad digital, si tiene nivel de registro dos o tres, se tienen garantías sobre la identidad de la persona y por lo tanto puede usar esa identidad digital para solicitar su certificado de firma electrónica avanzada. Este proceso lo realiza a través del portal de auto gestión, en forma presencial o remota, y elige en el mismo un PIN para protegerlo.

Es responsabilidad de la Autoridad de Registro la validación correcta de la identidad del sujeto a través de los procedimientos ya detallados, y es responsabilidad del suscriptor la elección de un PIN que sólo él conozca y el no compartirlo. Antel no asume ninguna responsabilidad respecto al mal uso del certificado derivado de un mal uso del PIN de firma.

4.2 Procesamiento de solicitud de certificado

Una vez registrado el usuario en la plataforma de custodia centralizada de firma e identificación, y a través de un proceso de registro presencial, se autentica en el portal de auto gestión de TuID y solicita la emisión del certificado definiendo el PIN que lo protegerá. La plataforma de custodia centralizada realiza entonces la generación del par de llaves en su entorno seguro y utilizando sus HSM, crea el CSR y lo envía a la ACPA para completar la emisión. La ACPA verifica la firma del CSR y que la información contenida en el mismo tenga el formato adecuado; emite el certificado y lo devuelve a la plataforma de TuID para que ésta lo almacene en el perfil del usuario correspondiente.

La plataforma de custodia centralizada está implementada en una infraestructura privada, y con productos que cuentan con certificaciones CC EAL4+ y eIDAS.

4.2.1 Realización de funciones de identificación y autenticación

Las funciones de identificación son realizadas por la Autoridad de Registro al momento de crear la identidad digital custodiada como se describe en la sección 3.2.2. La autenticación del sujeto para solicitar el certificado es realizada por la plataforma de custodia centralizada de firma e identificación a partir del factor de autenticación entregado al usuario en el proceso de registro.

4.2.2 Aprobación o rechazo de las solicitudes de certificado

No se permiten solicitudes de certificados con identidades cuyo nivel de registro no sea presencial. Además, es requisito que el usuario se autentique con algún factor que esté asociado a su Identidad.

4.2.3 Plazo para procesar las solicitudes de certificado

La ACPA opera en forma online, por lo que las solicitudes de certificado son procesadas instantáneamente.

4.3 Emisión de certificado

La emisión del certificado se realiza utilizando los sistemas de la ACPA, en particular los HSM que protegen su clave privada. Dichos sistemas se encuentran en una infraestructura privada y dedicada, bajo los perímetros y controles de seguridad exigidos por WebTrust for Certification Authorities 2.0 y ETSI.

El período de validez del certificado emitido será de un máximo de dos (2) años.

El certificado emitido por la ACPA es devuelto al sistema de custodia centralizada para su almacenamiento como parte de la identidad custodiada. Una copia del certificado es almacenada en el directorio de certificados de la ACPA. Esta copia no es publicada en el repositorio de información pública.

4.3.1 Acciones de la CA durante la emisión del certificado

La CA recibe la solicitud de emisión (CSR) de parte de la plataforma de custodia a través de un canal privado, la cual además es generada en función a una identidad de nivel de registro presencial con previa autenticación, por lo que simplemente procede a validar el formato de la información recibida en el CSR y su autenticidad y realiza la emisión siguiendo el método definido en los puntos 4.1 y 4.2 de este documento.

4.3.2 Notificaciones al suscriptor de la emisión del certificado por parte de la CA

Al cargarse el certificado de firma electrónica avanzada e identificación en el perfil de custodia centralizada del usuario, éste recibe una notificación vía correo electrónico validado.

4.4 Aceptación del certificado

Previo a la emisión del certificado, al usuario le son presentados los términos y condiciones de uso del certificado de firma, los cuales deberá aceptar, brindando así su consentimiento con sus derechos y obligaciones para con el uso del certificado.

Una vez cargado el certificado en su perfil, el usuario tiene 24 horas para rechazar el certificado si éste no cumpliera con algún requisito o formalidad, como ser con su documento de identidad o su nombre completo. De no mediar comunicación por parte del usuario en esas 24 horas, el certificado se considera aceptado. Si hubiese algún reclamo, Antel activará la revocación del certificado anterior, y tomará las medidas necesarias para corregir los datos que se encuentren erróneos y realizar nuevamente la emisión del certificado siguiendo el mismo procedimiento.

4.4.1 Conducta que constituye aceptación del certificado

Pasadas las 24 horas desde la recepción del certificado, el mismo se considera aceptado por parte del usuario. De la misma forma, el uso reiterado del mismo a través del servicio de firma (única vía para su utilización por tratarse de custodia centralizada) también constituye la aceptación implícita del mismo por parte del usuario.

4.4.2 Publicación del certificado por la CA

La CA no publica los certificados emitidos, a menos que se encuentren revocados.

4.4.3 Notificación de la emisión del certificado a otras entidades por parte de la CA

Además de al usuario y a la plataforma de custodia centralizada, no se notifica a ningún otro actor acerca de la emisión del certificado.

4.5 Uso del par de claves y del certificado

Estipulado en la Política de Firma electrónica avanzada con custodia centralizada de Persona Física de la UCE.

4.5.1 Uso de la clave privada y certificado por el suscriptor

Estipulado en la Política de Firma electrónica avanzada con custodia centralizada de Persona Física de la UCE.

4.5.2 Uso de la clave pública y certificado por el tercero aceptante

Estipulado en la Política de Firma electrónica avanzada con custodia centralizada de Persona Física de la UCE.

4.6 Renovación de certificado

La renovación de un certificado consiste en la emisión de un nuevo certificado con la misma información que el anterior.

Para la renovación del certificado, el sujeto debe realizar nuevamente el proceso de registro presencial al igual que el registro inicial. Con ello se actualiza la fecha de vigencia del registro de su identidad custodiada y puede utilizarla nuevamente para solicitar un certificado a través de su portal de auto gestión. El usuario se deberá autenticar en el portal de auto gestión utilizando alguno de los mecanismos disponibles: usuario y contraseña o la app de TuID. La app de TuID consiste en una aplicación móvil, que se sincroniza con la Identidad del Usuario y luego puede usar para autenticarse en forma sencilla, utilizando los factores de autenticación de su teléfono como ser patrón, pin, huella dactilar o reconocimiento facial. Se trata de un factor de autenticación basado en algo que se tiene.

El certificado previo quedará inutilizable.

Otros requisitos para la renovación están estipulados en la Política de Firma electrónica avanzada con custodia centralizada de Persona Física de la UCE.

4.6.1 Circunstancias para la renovación de certificado

La única circunstancia que habilita la solicitud de la renovación del certificado es el vencimiento de éste. Se podrá solicitar la renovación desde tres (3) meses antes del vencimiento hasta tres (3) meses luego de vencido. Pasado ese período, se debe realizar una emisión nueva.

4.6.2 Quién puede solicitar la renovación

El suscriptor final es la única persona habilitada a solicitar la renovación de su certificado.

4.6.3 Procesamiento de solicitudes de renovación de certificado

Tanto la renovación de la vigencia del registro presencial como la solicitud del nuevo certificado se procesan de forma análoga al primer registro y primera emisión.

4.6.4 Notificación al suscriptor de la emisión de un nuevo certificado

Análogo a la primera emisión.

4.6.5 Conducta que constituye aceptación del certificado de renovación

Análogo a la primera emisión.

4.6.6 Publicación del certificado renovado por la CA

Análogo a la primera emisión.

4.6.7 Notificación de la emisión del certificado por parte de la CA a otras entidades

Análogo a la primera emisión.

4.7 Cambio de claves del certificado

No se realizan cambios de clave de Certificados. En caso de ser necesario, se aplican los procedimientos de Revocación y Emisión de Certificado en el orden mencionado, o de Renovación.

4.7.1 Circunstancias para la reasignación de claves del certificado

No aplica.

4.7.2 Quién puede solicitar la certificación de una nueva clave pública

No aplica.

4.7.3 Procesamiento de solicitudes de reasignación de claves del certificado

No aplica.

4.7.4 Notificación al suscriptor de la emisión de un nuevo certificado

No aplica.

4.7.5 Conducta que constituye aceptación del certificado para claves reasignadas

No aplica.

4.7.6 Publicación del certificado de clave reasignada por la CA

No aplica.

4.7.7 Notificación de la emisión del certificado por parte de la CA a otras entidades

No aplica.

4.8 Modificación del certificado

La modificación de un certificado es definida como la creación de un nuevo certificado que contiene la información modificada respecto a un certificado previamente emitido.

Únicamente se atienden solicitudes de modificación cuando éstas se realizan previo a la aceptación formal del certificado, y el procedimiento a realizar es la revocación del certificado anterior y la emisión de uno nuevo.

4.8.1 Circunstancias para la modificación del certificado

Sólo se acepta la modificación del certificado cuando el usuario no lo acepte antes del plazo de 24 horas de la emisión o no haya sido usado activamente, lo cual constituye su aceptación.

4.8.2 Quién puede solicitar modificación del certificado

El suscriptor es la única persona habilitada a solicitar modificación.

4.8.3 Procesamiento de solicitudes de modificación del certificado

Se realiza el procedimiento de renovación del certificado erróneo y de emisión de un nuevo certificado.

4.8.4 Notificación al suscriptor de la emisión de un nuevo certificado

Análogo a la primera emisión.

4.8.5 Conducta que constituye aceptación del certificado modificado

Análogo a la primera emisión.

4.8.6 Publicación del certificado modificado por la CA

Análogo a la primera emisión. El certificado sustituido es revocado, por lo que es publicado en los servicios de estado de revocación de certificados (OCSP y CRL).

4.8.7 Notificación de la emisión del certificado por parte de la CA a otras entidades

Análogo a la primera emisión. En caso de que el certificado modificado haya sido utilizado en algún tercero, hecho del cual la plataforma de custodia centralizada tiene registro, se notificará a éste para que tome las medidas que considere convenientes.

4.9 Revocación y suspensión de certificado

Para la Revocación, se comunica el número de serie del certificado a revocar a la Autoridad de Certificación (AC), junto con la fecha de revocación y la causal de la misma. La AC actualiza su Base de Datos para reflejar esta revocación y lo incluye en la CRL posteriores. La VA es el componente de la ACPA encargado de responder a través del protocolo OCSP sobre el estado de un certificado particular. Una vez que el certificado revocado es comunicado a la VA, esta lo agregará a la base de datos de respuesta del servicio OCSP, efectivizando así su revocación.

Las causales para la revocación del certificado están estipuladas en la Política de Firma Electrónica Avanzada con Custodia Centralizada de Persona Física de la UCE y en la Política de Certificación de la ACRN, pero pueden resumirse como:

- La sola voluntad del suscriptor de no contar más con el certificado
- La sospecha de compromiso de la clave privada por parte del usuario
- La sospecha de compromiso de los factores de autenticación que permiten el acceso a la clave privada en custodia centralizada, como ser el PIN de firma, el usuario y la contraseña o el teléfono móvil por el cual se realiza el OTP
- La pérdida irrecuperable de dichos factores que impidan al suscriptor el acceso a su clave privada
- La utilización del certificado fuera de los usos permitidos del mismo
- La contravención de cualquier otro acuerdo particular entre ANTEL y el suscriptor, como por ejemplo de condiciones comerciales
- La revocación del certificado de la ACPA de ANTEL por cualquier causal.

Antel atiende los pedidos de revocación a través de la Autoridad de Registro.

Adicionalmente, Antel podrá proceder a la revocación de un certificado cuando constate que el suscriptor ha incurrido en alguna de las causales de revocación.

El proceso de revocación del certificado y actualización de los servicios de estado se realiza en un plazo no mayor a un (1) día a partir de la autenticación y aprobación de la solicitud de revocación del suscriptor.

En caso de revocación del certificado de la ACPA se dispondrá de un funcionario de la ACRN para presenciar el proceso de revocación efectiva de todos los certificados emitidos, y también del proceso de destrucción efectiva de la clave privada asociada a la misma.

4.9.1 Circunstancias para la revocación

Se cumple con lo estipulado en las políticas de la UCE y con lo estipulado en el punto anterior.

4.9.2 Quién puede solicitar la revocación

El suscriptor, ANTEL, la UCE, siempre y cuando se configure alguna de las causales anteriormente descriptas o por orden judicial.

4.9.3 Procedimiento para la solicitud de revocación

El suscriptor final podrá solicitar la revocación concurriendo a cualquier local de la Autoridad de Registro y realizando cualquiera de los procedimientos de registro presencial (por un funcionario o auto gestionado).

Si aún poseyera acceso a su identidad digital custodiada, que por tener certificado asociado deberá ser de nivel de registro dos o tres, puede ingresar al portal de auto registro, autenticarse y pedir la revocación del certificado, la cual será efectivizada por la ACPA.

4.9.4 Período de gracia de solicitud de revocación

No estipulado.

4.9.5 Tiempo dentro del cual la CA debe procesar la solicitud de revocación

La solicitud de revocación será procesada en un plazo no mayor a las 24 horas desde su identificación y autenticación ante la Autoridad de Registro.

4.9.6 Requerimientos de comprobación de revocación por terceros aceptantes

Dado que se trata de un servicio de firma e identificación con custodia centralizada, la plataforma no permite la realización de firmas ni autenticaciones basadas en certificados revocados. No obstante, actos firmados previos a la revocación sí pueden dar como resultado un documento firmado con certificado revocado. Es por esto que siempre es responsabilidad de los terceros aceptantes la comprobación del estado de revocación del certificado que realizó la firma o autenticación que están procesando.

4.9.7 Frecuencia de emisión de CRL

De no mediar revocaciones, la CRL es actualizada cada 24 horas. De lo contrario, la nueva CRL es publicada inmediatamente se procesa la revocación.

4.9.8 Latencia máxima de CRL

La latencia máxima de la CRL es de 48 horas.

4.9.9 Disponibilidad de comprobación en línea de revocación/estado

Se cumple con lo estipulado en la Política de la ACRN para los PSCA, y con lo estipulado en la Política de firma con custodia centralizada de Persona Física. La CRL está disponible 24 horas al día, 7 días a la semana, en servicios altamente disponibles y redundantes.

La VA de Antel cuenta con servicio de comprobación online de estado de certificados (OCSP por sus siglas en inglés) y es el mecanismo preferido para la verificación de estado. Dicho servicio también está disponible 24 horas al día, 7 días a la semana, en servicios altamente disponibles y redundantes.

En caso de contar con períodos de indisponibilidad Antel dedicará sus mejores esfuerzos para restablecer el servicio con la mayor brevedad posible.

4.9.10 Requerimientos de comprobación de revocación en línea

La comprobación de revocación en línea alcanza los servicios de estado de revocación de los certificados, es decir, a la CRL y el servicio OCSP.

4.9.11 Otras formas de publicidad de revocación disponibles

Además de la CRL y el servicio OCSP, no hay otras formas de publicación de estado de revocación. Sin perjuicio de lo anterior, y para preservar la salud del ecosistema de firma e identificación digital, Antel se reserva el derecho de realizar publicaciones especiales en su sitio web, en sitios de terceros o en la prensa de certificados que hayan sido revocados pero que hayan estado comprobadamente involucrados en actividades fraudulentas o de alto riesgo para los terceros aceptantes.

4.9.12 Requerimientos especiales en relación con compromiso de claves

Se cumple con lo estipulado en la Política de la ACRN para los PSCA, y con lo estipulado en la Política de firma con custodia centralizada de Persona Física.

4.9.13 Circunstancias para la suspensión

No se realiza suspensión de certificados emitidos por la ACPA de ANTEL

4.9.14 Suspensión de PSCA o ACPA

De ser suspendido ANTEL como PSCo, se cumplirá con lo estipulado en las Políticas y Procedimientos de la UCE y de la ACRN.

4.9.15 Quién puede solicitar la suspensión

No aplica.

4.9.16 Procedimiento para la solicitud de suspensión

No aplica.

4.9.17 Límites del período de suspensión

No aplica.

4.10 Servicios de estado de certificados

Antel publica en su sitio destinado al servicio de custodia centralizada de identidades y firma, la CRL actualizada y el servicio OCSP para acceso al estado de revocación de los certificados.

Antel no se responsabiliza por ningún tipo de incidente que derive de una falta de verificación de la CRL o el OCSP de la ACPA en el momento de validación de un certificado por parte de los Terceros aceptantes.

Este servicio de publicación de información está disponible durante las 24 horas los 7 días de la semana y en caso de error del sistema fuera del control de Antel, éste dedicará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en un período máximo establecido en 48 horas.

El Repositorio se encuentra en www.tuid.uy

La CRL se encuentra en crl.tuid.uy/crls

El endpoint del servicio OCSP se encuentra en ocsp.tuid.uy

4.10.1 Características operacionales

Tanto la CRL como la base de datos del servicio OCSP son mantenidos por la Autoridad de Validación (VA), que es el componente de la ACPA dedicado al servicio de estado de los certificados. La VA mantiene el estado de los certificados en forma online, por lo que cualquier revocación es propagada a los clientes que consulten en forma inmediata.

El modo preferido de consulta de estado de certificados es el consumo del servicio OCSP. La CRL se publica para cumplir con lo estipulado en las Políticas de la UCE, y para dar soporte a la validación de certificados por parte de sistemas legados que no cuenten con soporte para OCSP.

4.10.2 Disponibilidad del servicio

Se cumple con lo estipulado en la Política de la ACRN. El servicio de publicación de información está disponible durante las 24 horas los 7 días de la semana y en caso de error del sistema fuera del control de Antel, éste dedicará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en un periodo establecido en 48 horas.

4.10.3 Características opcionales

No aplica.

4.11 Fin de la suscripción

Para dar cumplimiento a lo estipulado en la Política de Certificación de la ACRN para con las ACPA subordinadas, en la eventualidad de que la ACPA de ANTEL finalice sus servicios:

a) Se publicará la fecha de finalización con sesenta (60) días de antelación en el Sitio Oficial de ANTEL y un vínculo a dicha información en el Diario Oficial durante un (1) día hábil
b) Se notificará a los suscriptores con al menos quince (15) días de antelación
c) La UCE procederá a la suspensión de la ACPA de ANTEL, inhabilitándola a emitir y/o renovar certificados
d) Luego de expirados todos los certificados de suscriptores, ANTEL procederá a la destrucción de la clave privada de la ACPA mediante la destrucción lógica y física de los HSM que alojaban la clave, y la destrucción lógica con borrado seguro de los equipos donde la clave haya podido encontrarse cifrada
e) La UCE publicará en su Sitio Oficial y una referencia en el Diario Oficial, el cese total de actividades de la ACPA de ANTEL
f) El certificado de ANTEL, el directorio de certificados emitidos y la última lista de revocación emitida serán transferidos a la UCE
g) La UCE publicará en su Sitio Oficial y una referencia en el Diario Oficial, el enlace al sitio donde se encuentra la lista de revocación y el certificado de la ACPA que finalizó sus operaciones

Luego de la suspensión de la ACPA de Antel, ésta no emitirá ningún certificado, pero continuará dando soporte a las operaciones de revocación y publicación. Al tratarse de un PSCo, Antel tampoco continuará brindando acceso a la firma utilizando los certificados aún vigentes, por lo que los suscriptores no tendrán acceso a usar los certificados. Antel mantendrá los servicios de revocación de certificados, publicación de CRL y validación OCSP durante ese lapso. Una vez expirados o revocados todos los certificados, Antel notificará a la UCE de este hecho, cesando automáticamente su responsabilidad para con esa ACPA.

Sin perjuicio de lo anterior, Antel se reserva el derecho de realizar un cese de las operaciones de su ACPA, pero continuar brindando servicios de identidad custodiada, sin firma electrónica avanzada ni autenticación de nivel tres que requiere el uso de certificados electrónicos reconocidos.

El procedimiento detallado para el cese de actividades de un PSCA está estipulado en la Política de Certificación de la ACRN.

4.12 Custodia (escrow) y recuperación de claves

No se realiza escrow, respaldo ni recuperación de claves para la ACPA de ANTEL.

4.12.1 Políticas y prácticas de custodia y recuperación de claves

No aplica.

4.12.2 Políticas y prácticas de encapsulamiento y recuperación de claves de sesión

No aplica.

5 GESTIÓN DE LAS INSTALACIONES Y CONTROLES OPERACIONALES

El objetivo de los controles administrativos, operativos y físicos es implementar medidas de protección para la clave privada utilizada por la ACPA de Antel, las claves privadas de los usuarios que son custodiadas en forma centralizada y el ciclo de vida de los certificados emitidos por la ACPA.

Para esto, la plataforma de firma e identificación en custodia centralizada de Antel cuenta con Políticas y Procedimientos para garantizar la seguridad en sus operaciones. Los mismos están alineados a los requerimientos de WebTrust for Certification Authorities y con el código de buenas prácticas ISO 27001, y están enfocados a proteger el material criptográfico involucrado en el ciclo de vida de los certificados de los PSCA.

5.1 Controles físicos

Los sistemas que dan soporte a toda la plataforma de firma e identificación con custodia centralizada se encuentran alojados en un datacenter propio de Antel, que cuenta con certificación Tier III en diseño, lo cual abarca todos los controles físicos requeridos por la UCE para la operación de un PSCo. En particular, el acceso a los equipos más sensibles de la plataforma, es decir, los HSM que custodian las claves de la CA y las claves de los usuarios finales, se encuentran protegidos por cuatro perímetros de seguridad.

5.1.1 Localización del sitio y construcción

El equipamiento dedicado a la gestión de certificados del Prestador Acreditado (la CA misma) se instaló durante la ceremonia de claves, en presencia de una autoridad designada, de forma de certificar su correcta instalación.

5.1.2 Acceso físico

Las condiciones del datacenter donde se alojan los sistemas permiten dar cumplimiento a lo estipulado en las Políticas de la UCE para PSCo.

5.1.3 Energía y aire acondicionado

Las condiciones del datacenter donde se alojan los sistemas permiten dar cumplimiento a lo estipulado en las Políticas de la UCE para PSCo.

5.1.4 Exposición del agua

Las condiciones del datacenter donde se alojan los sistemas permiten dar cumplimiento a lo estipulado en las Políticas de la UCE para PSCo.

5.1.5 Prevención y protección contra incendios

Las condiciones del datacenter donde se alojan los sistemas permiten dar cumplimiento a lo estipulado en las Políticas de la UCE para PSCo.

5.1.6 Almacenamiento de medios

Las condiciones del datacenter donde se alojan los sistemas permiten dar cumplimiento a lo estipulado en las Políticas de la UCE para PSCo.

5.1.7 Eliminación de residuos

Las condiciones del datacenter donde se alojan los sistemas permiten dar cumplimiento a lo estipulado en las Políticas de la UCE para PSCo.

5.1.8 Respaldo fuera de las instalaciones (off-site)

Se cuenta con un cold site de contingencia en otro datacenter de redundancia equivalente y con procedimientos para su activación en caso de ser necesario.

5.2 Controles de procedimiento

Los procesos que permiten el funcionamiento de ANTEL como PSCo se basan en la contraposición de intereses para sus operaciones más críticas, interviniendo varias personas durante la solicitud, aprobación, ejecución y control de las tareas desarrolladas.

Para aquellas tareas críticas como la gestión de la clave privada de la autoridad certificadora, o la gestión de las claves de protección de las claves custodiadas de los usuarios finales, se implementan medidas de división del conocimiento y contraposición de intereses.

Los procedimientos de operación de la plataforma tienen carácter de reservado para preservar su confidencialidad y evitar así revelar a terceros información del funcionamiento interno que pueda viabilizar un ataque al servicio. No obstante, son parte del alcance de las auditorías realizadas periódicamente, para garantizar a los terceros aceptantes y suscriptores el cumplimiento con la normativa vigente en Uruguay y los estándares internacionales de seguridad que aplican para Servicios de Confianza.

5.3 Controles de personal

Antel cumple con controles y procedimientos asociados a la gestión del personal involucrado en su funcionamiento como PSCo. Dichos controles y procedimientos tienen carácter de reservado para preservar su confidencialidad y evitar así revelar a terceros información del funcionamiento interno que pueda viabilizar un ataque al servicio. No obstante, son parte del alcance de las auditorías realizadas periódicamente, para garantizar a los terceros aceptantes y suscriptores el cumplimiento con la normativa vigente en Uruguay y los estándares internacionales de seguridad que aplican para Servicios de Confianza.

Sin perjuicio de lo anterior, Antel declara que dichos controles y procedimientos incluyen requerimientos de calificaciones y experiencia del personal, requerimientos de capacitación continua en seguridad de la información en general y sobre servicios de confianza en forma específica, mecanismos de sanción por acciones no autorizadas o contravenciones a los procedimientos establecidos y requerimientos específicos para la relación con proveedores independientes, entre otros.

5.4 Procedimiento de registro de auditoría

ANTEL tiene definida para sus funciones de PSCo una política de registros de auditoría (*logs*) que define qué opciones se registran y cómo se garantiza la integridad de estos registros.

Se registrarán todas las actividades relativas a la gestión de claves (generación, destrucción, activación, desactivación, etc.) tanto de la CA como de los suscriptores finales, a la gestión de certificados (emisión, revocación, renovación, etc.), a la emisión de CRLs, a la actualización de los estados del servicio OCSP, al registro de usuarios finales y a la entrega de factores de autenticación para que puedan acceder a la plataforma, especialmente las actividades de autenticación y firma, sea cual sea el nivel empleado para la misma.

Todos los registros se almacenan con la fecha en que fueron generados, la opción realizada, los objetos afectados, el resultado de dicha operación y la identificación del/los autores.

Los registros se almacenan de tal forma que se asegura su disponibilidad e integridad, impidiendo la modificación indebida, eliminación y su lectura.

5.5 Archivo de registros

Cada tipo de registro tiene definido el tiempo de retención. Los registros relativos a la generación de claves y emisión/renovación de certificados se almacenan hasta que el certificado expira o es revocado. Los registros relativos a los demás operativos se mantienen por tres (3) años.

Los certificados emitidos por la ACPA son mantenidos en su directorio privado por tiempo indefinido, incluso luego de su expiración y/o revocación, para permitir a terceros validar las firmas que fueron realizadas con ellas.

5.6 Cambio de clave

No se realizan procedimientos de cambio de clave certificados.

5.7 Compromiso y recuperación de desastres

ANTEL en su rol de PSCo tiene definidos planes de continuidad del negocio y recuperación ante desastres, que le permiten continuar con su operativa en la eventualidad de fallas de equipamiento y/o siniestros. Estos planes contienen análisis de riesgos de interrupción del servicio y las estrategias de recuperación propuestas, así como también ventanas máximas de interrupción aceptables.

Los servicios de firma e identificación custodiada, así como los de publicación de CRL y OCSP, están disponibles durante las 24 horas los 7 días de la semana y en caso de error del sistema fuera del control de ANTEL, se dedicarán sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en un período establecido en 48 horas.

Los servicios de registro están sujetos a la disponibilidad de los locales comerciales de ANTEL, puestos móviles y autoridades de registro delegadas en todo el país, que son la vía por la cual se brindan.

Los pedidos de revocación son atendidos en un máximo de 24 horas.

5.7.1 Procedimientos de manejo de incidentes y compromisos

ANTEL cuenta con procedimientos para el manejo de incidentes y compromisos. Dichos procedimientos son de carácter reservado para preservar la confidencialidad de las operaciones sensibles, pero incluyen mecanismos para la detección de incidentes, su análisis de riesgo y evaluación de impacto, la contención y resolución de éstos y la notificación a las autoridades competentes en los casos que corresponda.

5.7.2 Procedimientos ante el compromiso de clave privada de la CA

Es un tipo de incidente contemplado dentro de los procedimientos de manejo de incidentes y compromisos.

5.7.3 Procedimientos ante el compromiso clave privado o factores de autenticación de suscriptor

Es un tipo de incidente contemplado dentro de los procedimientos de manejo de incidentes y compromisos.

5.7.4 Capacidades de continuidad de negocio después de un desastre

Se encuentran contemplados en los planes de continuidad del negocio.

5.8 Terminación de la CA o de la RA

Los procedimientos de terminación de las operaciones se especifican en el punto 4.11.

5.9 Procedimiento para el cambio de certificado de la ACPA

El único escenario de cambio de certificado de la ACPA es ante la eventual emisión del certificado con información errónea por parte de la ACRN y no aceptado el mismo, caso en que aplica el procedimiento de la ACRN destinado a tal fin. En caso de aceptado el certificado y comenzadas las operaciones, no se realiza cambio de certificado de la ACPA.

6 CONTROLES DE SEGURIDAD TÉCNICA

Los controles técnicos descriptos en esta sección tienen el objetivo de proteger el par de llaves de la ACPA durante su ciclo de vida, los pares de llaves de los certificados custodiados por el servicio de confianza y el material sensible asociado a los factores de autenticación de los factores de autenticación de los usuarios. Se especifican además medidas generales para la protección de información que dan soporte a las actividades del servicio de confianza.

6.1 Generación e instalación de pares de claves

6.1.1 Generación de claves

6.1.1.1 Autoridad Certificadores de ANTEL

ANTEL elaboró un guión detallado de las actividades que ejecutó para poner en marcha su ACPA, incluyendo la generación de llaves y realizó la instalación en forma auditada y de acuerdo con dicho guión. Esto cubrió todo el proceso de instalación de la CA.

La generación del par de llaves para la ACPA se realizó en instalaciones de ANTEL, en presencia de un funcionario designado por la ACRN y la UCE y de acuerdo con los requerimientos estipulados por la Política de Certificación de la ACRN.

6.1.1.2 Claves custodiadas de usuarios finales

Al tratarse de un PSCo, ANTEL genera también las claves de los suscriptores en forma centralizada y las custodia durante todo su ciclo de vida. La generación de la clave del suscriptor se realiza bajo su pedido a través del sistema, una vez registrado con un nivel de confianza de dos o superior y autenticado con un factor también. Al recibir el pedido, la plataforma de custodia de claves realiza la generación del par de llaves usando sus HSM, almacena la misma en forma cifrada por claves que viven exclusivamente dentro de sus HSM y la protege adicionalmente con el PIN de firma que el usuario debe ingresar para pedir la emisión. De esta forma la clave queda custodiada por todos los mecanismos de seguridad de la plataforma de confianza, y por el PIN que sólo el usuario final conoce, garantizando así el acceso exclusivo a su clave de firma.

6.1.2 Entrega de la clave privada al suscriptor

La CA de ANTEL genera su propia clave, que nunca abandona el entorno de sus HSM y por lo tanto no le es entregado nunca. De manera similar, los suscriptores de los certificados emitidos por dicha CA tienen la clave custodiada por la plataforma de confianza, y son generadas como fue descripto en el punto anterior, por lo que tampoco son entregadas nunca al usuario final. El PIN de firma es elegido por el suscriptor al momento de solicitar la emisión del certificado y será solicitado cada vez que se utilice, y los factores de autenticación utilizados para controlar el acceso son configurados durante el registro, cada uno con sus reglas definidas para garantizar su efectividad.

6.1.3 Entrega de la clave pública al emisor del certificado

La clave pública de la CA se envió a la ACRN a través del CSR, el cual fue entregado al funcionario de la ACRN que presenció la ceremonia de instalación.

En el caso de los suscriptores, la generación de la clave se hace en el entorno del Servicio de Confianza, y la clave pública se envía en un CSR que viaja por un canal privado y autenticado entre el servicio de custodia y firma y la CA misma.

6.1.4 Entrega de la clave pública de la CA a los terceros aceptantes

Una vez emitido el certificado de la CA, el mismo es publicado por la ACRN y por ANTEL en el sitio destinado a su servicio de confianza.

6.1.5 Tamaños de clave

Se cumple con lo estipulado en la Política de la ACRN. La clave de la ACPA es RSA de 4096 bits. Las claves privadas de los suscriptores son RSA de 2048 bits.

6.1.6 Generación y control de calidad de parámetros de clave pública

Se cumple con lo estipulado en la Política de la ACRN.

6.1.7 Propósitos de uso de la clave (por campo Key Usage de certificado X.509 v3)

Se cumple con lo estipulado en la Política de la ACRN.

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

Se cumple con lo estipulado en la Política de Certificación de la ACRN.

La protección de la clave privada de la CA se realiza en un módulo HSM que cumple con la normativa estipulada en la Política de Certificación de la ACRN.

La llave privada de la ACPA se encuentra siempre protegida por el HSM. El equipamiento de producción y el de contingencia tienen los controles de seguridad físicos y lógicos requeridos por la Política de Certificación de la ACRN y la presente Declaración de Prácticas de Certificación.

El retiro de las llaves privadas de los HSM se realiza únicamente para procedimientos de respaldo de la llave en otros HSM, y para el cambio de HSM, en cuyos casos se retira en forma cifrada. Estos procedimientos son aprobados y controlados por la UCE.

Una vez que el certificado de la ACRN expira, se procede a la destrucción de la clave privada. La destrucción se realiza con un mecanismo que impide su recuperación. Los HSM utilizados proveen funciones para la eliminación segura de la llave privada.

Las claves privadas de suscriptores también generan y protegen en base a módulos HSM y a los PIN de firma elegidos por ellos mismos. Los módulos HSM que protegen estas claves son independientes de los que protegen a la clave de la CA.

6.2.1 Normas y controles para el módulo criptográfico

Se cumple con lo estipulado en la Política de la ACRN.

6.2.2 Control multi-persona (m de un total de n) de clave privada

Para la activación de los HSM se utilizan esquemas M de N.

6.2.3 Custodia de la clave privada

La custodia de las claves privadas siempre es realizada en base a los dispositivos HSM y a sus perfiles de seguridad configurados.

6.2.4 Respaldo de la clave privada

No se realiza respaldo de claves privadas, ni de CA ni de suscriptor, fuera de los HSM de producción o contingencia fría.

6.2.5 Archivo de la clave privada

No se realiza archivo de la clave privada.

6.2.6 Transferencia de la clave privada desde/hacia un módulo criptográfico

La transferencia de claves privadas entre módulos HSM se realiza siguiendo los procedimientos estipulados por los fabricantes específicamente para tal fin y respetando los perfiles de protección, acceso y cifrado configurados para los mismos.

6.2.7 Almacenamiento de la clave privada en el módulo criptográfico

Las claves privadas se almacenan protegidas por módulos HSM.

6.2.8 Método de activación de la clave privada

Dado que se trata de una CA online y un servicio de firma custodiada online, las claves privadas de los HSM se mantienen activadas para su uso por parte de los sistemas autorizados únicamente. Para acceder a la firma de suscriptor es además necesaria la provisión de PIN de firma, que sólo el suscriptor conoce.

6.2.9 Método de desactivación de la clave privada

Las claves privadas sólo se desactivan para operaciones de mantenimiento o respaldo.

6.2.10 Método de destrucción de clave privada

Para la destrucción de las claves se utilizan mecanismos de los HSM definidos específicamente para tal fin y se emplea borrado lógico con shredding en las zonas de almacenamiento de los servidores donde la clave pueda haber estado alojada, aunque lo haya hecho en forma cifrada.

6.2.11 Clasificación del módulo criptográfico

Los HSM cuentan con certificación FIPS 140-2 Nivel 3.

6.3 Otros aspectos de la gestión del par de claves

No estipulado.

6.4 Datos de activación

La activación de la clave de la CA se realiza mediante un esquema M de N, con tokens de seguridad y PIN que son asignados en forma nominada a los operadores autorizados a realizar una activación. El HSM que se utiliza para salvaguardar la clave privada de la PKI de ANTEL, está configurado para que en su activación sean necesarios 1 de 9 operadores.

La activación de la clave de suscriptor se hace autenticando al usuario con sus factores de autenticación en un nivel dos o superior y validando el PIN de firma independiente que el usuario también ingresa. De esa forma se garantiza que sólo puede ser utilizada la clave privada bajo expresa voluntad del usuario final.

6.5 Controles de seguridad computacional

El servicio de confianza de ANTEL implementa políticas, estándares y procedimientos que permiten una operación segura, en forma alineada a las Políticas y procedimientos y siguiendo los estándares internacionales de la industria para tal fin. Dichos controles tienen carácter de reservado, pero son objeto de las auditorías de seguridad a las que periódicamente se somete el servicio de confianza de ANTEL.

6.6 Controles técnicos de ciclo de vida

Existe un inventario actualizado con los sistemas de información y medios de almacenamiento asociados a la operativa del PSCo. Dicho inventario es mantenido por ANTEL en forma privada y revelado sólo a los encargados de la auditoría, es decir, no forma parte de la información a publicar.

6.7 Controles de seguridad de la red

El servicio de confianza opera en una red dedicada, con segmentación de zonas públicas de privadas, aislamiento entre las zonas y control estricto del tráfico permitido entre zonas exclusivamente en base a la necesidad de acceso. En particular, la Autoridad de Registro está separada de la plataforma de firma e identificación y ésta a su vez está separada de la CA y la VA. Los HSM se encuentran en todos los casos en subredes dedicadas, con acceso restringido únicamente a los equipos que necesitan realizar firmas.

6.8 Sellado de tiempo

ANTEL utiliza la fecha y la hora de GMT al firmar los certificados que emite, con margen de error máximo del orden del minuto.

El servicio de firma y autenticación utiliza la hora estándar de Uruguay (UYST).

Durante la Ceremonia de Claves se estableció esta hora y fue verificada por una autoridad designada y por el personal de la ACRN presente. La sincronización horaria es objeto de control de las auditorías periódicas.

Antel cuenta desde Abril de 2020 con un Servicio de Sellado de Tiempo acreditado ante la UCE. El objetivo de dicho servicio es brindar sellado de tiempo a externos y no para la gestión de tiempos dentro de la infraestructura de la CA o la plataforma de custodia centralizada. No obstante, el servicio de sellado forma parte de TuID y su Declaración de Prácticas debe considerarse una extensión del presente documento.

7 PERFILES DE CERTIFICADO Y CRL

El formato de los certificados cumple con lo especificado en el estándar ITU-T X.509 versión 3[2] (Internet X.509 Public Key Infrastructure Certificate and CRL Profile), mientras que la lista de revocación de certificados cumple con el mismo estándar, pero en su versión 2. Ambas están definidas en su versión más reciente en el RFC 52800[3].

7.1 Perfil de certificado de la CA

7.1.1 Número(s) de versión

X.509 Versión 3.

7.1.2 Extensiones del certificado

Se cumple con lo estipulado en la Política de la ACRN.

7.1.3 Identificadores de objeto de algoritmos

Se cumple con lo estipulado en la Política de la ACRN

7.1.4 Formas de nombre

Se cumple con lo estipulado en la Política de la ACRN.

7.1.5 Restricciones de nombres

Se cumple con lo estipulado en la Política de la ACRN.

7.1.6 Identificadores de objeto de política de certificación

Se cumple con lo estipulado en la Política de la ACRN.

7.1.7 Uso de la extensión “Policy Constraints”

Se cumple con lo estipulado en la Política de la ACRN.

7.1.8 Sintaxis y semántica de calificadores de política

Se cumple con lo estipulado en la Política de la ACRN.

7.1.9 Semántica de procesamiento para la extensión critica “Certificate Policies”

Se cumple con lo estipulado en la Política de la ACRN.

7.1.10 Perfil de certificado de los suscriptores

Atributos	*Contenido*
Versión	V3
Número de Serie (Serial Number)	Número asignado por la ACPA emisora
Algoritmo de Firma (Signature Algorithm)	sha256RSA
Nombre Distintivo del Emisor (Issuer DN)	DN de la ACPA emisora tal cual figura en su certificado
Validez (Valid From / Valid To)	0 a 2 Años (en formato desde/hasta)
Nombre Distintivo del Suscriptor (Subscriber DN)	CN = Nombre completo de la Persona Física C = País del Documento de identificación Presentado serialNumber = Código y número de documento givenName = Nombres de la Persona Física. surname = Apellidos de la Persona Física.
Clave Pública del Suscriptor (Subject Public Key)	Clave pública RSA de 2048 bits

Extensiones	
Identificador de la clave del suscriptor (Subject Key Identifier)	Hash de 20 bytes del atributo Subject Public Key
Identificador de la clave de la autoridad (Authority Key Identifier)	Valor de la Extensión Subject Key Identifier del certificado de la ACPA emisora
Uso de Claves (Key Usage)	DigitalSignature = 1 NonRepudiation/contentCommitment = 1 KeyEncipherment = 1 DataEncipherment = 1 KeyAgreement = 0 KeyCertSign = 0 CRLSign = 0 EncipherOnly = 0 DecipherOnly = 0
Uso de Claves Extendido (Extended Key Usage)	clientAuth, emailProtection
Políticas de Certificación (Certificate Policies)	OID: 2.16.858.10000157.66565.12 URI: www.uce.gub.uy/informacion-tecnica/politicas/cp_persona_fisica_centralizada.pdf OID: OID asignado a la CPS del PSCA para la ACPA emisora URI: URL de publicación de la CPS
Restricciones Básicas (Basic Constraints)	CA = FALSE
Puntos de distribución de las CRL (CRL Distribution Points)	URI = URL primaria de publicación de la CRL
QCStatements	Id-etsi-qcs-QcCompliance Id-etsi-qcs-QcSSCD

7.2 Perfil de la CRL

Atributos	*Contenido*
Versión	V2
Algoritmo de Firma (Signature Algorithm)	sha256RSA
Nombre Distintivo del Emisor (Issuer DN)	DN de la ACPA tal cual figura en su certificado
Día y Hora de Emisión (Efective Date)	Día y hora de la emisión de esta CRL
Próxima Actualización (Next Update)	Día y hora de la próxima actualización planificada de la CRL
Certificados Revocados (Revoked Certificates)	Lista de los certificados revocados. Incluye número de serie (Serial Number), fecha de revocación (Revocation Date) y motivo (Reason Code).

7.2.1 Número(s) de versión

Versión 2.

7.2.2 CRL y Extensiones de entradas CRL

Extensiones	
Identificador de la clave de la Autoridad Certificadora (Authority Key Identifier)	Valor de la Extensión Subject Key Identifier del certificado de la ACPA
Número de CRL (CRL Number)	Secuencial que se incrementa con cada CRL emitida

8 AUDITORIA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

8.1 Frecuencia o circunstancias de evaluación

ANTEL se somete a auditorías según la frecuencia que la UCE estipule.

8.2 Identidad/calificaciones del evaluador

El auditor será siempre uno de los auditores acreditados por la UCE para tal fin.

8.3 Relación del evaluador con la entidad evaluada

El auditor guarda independencia absoluta con ANTEL, mediando simplemente un contrato de servicio para el servicio brindado que establece dichas condiciones.

8.4 Tópicos cubiertos por la evaluación

El alcance de la auditoría comprende la seguridad física y lógica de todos los sistemas del Servicio de confianza prestado, los procedimientos de operación, los procedimientos de registro y la alineación de todas esas prácticas con la presente declaración de prácticas y las políticas y regulaciones aplicables. También incluye todos los sistemas del servicio de sellado, y las prácticas y políticas del mismo que deben ser consideradas una extensión de las presentes.

8.5 Acciones para tomar como resultado de la deficiencia

De detectarse apartamientos de la normativa, ANTEL se compromete a dedicar los mejores esfuerzos a solucionarlos en el menor plazo posible.

8.6 Comunicación de los resultados

Los resultados completos de las auditorías son enviados a la UCE para su evaluación y una versión revisada de los mismos para evitar filtraciones de información sensible es publicada en el sitio del Servicio de Confianza de ANTEL con finalidades de transparencia.

9 OTROS ASPECTOS COMERCIALES Y LEGALES

9.1 Tarifas

9.1.1 Tarifas de emisión o revocación de certificados

La emisión y renovación de certificados no tiene costo para los suscriptores.

9.1.2 Tarifas de acceso a los certificados

No se perciben tarifas.

9.1.3 Tarifas de acceso a la información de estado o revocación

No se perciben tarifas.

9.1.4 Tarifas para otros servicios

Los servicios de acceso a la autenticación de usuarios con identidad custodiada, para todos los niveles de confianza, así como la realización de una firma digital de un documento con el certificado custodiado, son operaciones con costo para el tercero que las solicita.

Las tarifas para los servicios de sellado de tiempo se estipulan en la Declaración de Prácticas de la TSA de TuID.

9.1.5 Política de reembolsos

Las políticas de reembolsos son parte de las condiciones comerciales que ANTEL acuerde con los terceros en forma oportuna.

9.2 Responsabilidad financiera

9.2.1 Cobertura de seguros

ANTEL cuenta con cobertura de seguros de responsabilidad civil para sus operaciones de Servicios de Confianza (CA, identidad digital, firma en custodia centralizada y sellado de tiempo), tal como lo estipula la regulación vigente de la UCE.

9.2.2 Otros activos

No estipulado.

9.2.3 Garantía o cobertura de seguro para entidades finales

ANTEL cuenta con cobertura de seguros de responsabilidad civil para sus operaciones de Servicios de Confianza (CA, identidad digital, firma en custodia centralizada y sellado de tiempo), tal como lo estipula la regulación vigente de la UCE.

9.3 Confidencialidad de la información de negocios

9.3.1 Alcance de la información confidencial

A los efectos de la determinación del carácter de confidencial de la información recibida por ANTEL se estará a los recaudos previstos de acuerdo con lo establecido en la Ley N° 18.381, del 17 de octubre de 2008 [4].

La información personal queda regulada por las Leyes Nos. 18.331, de 11 de agosto de 2008[4].

9.3.2 Información fuera del alcance de la información confidencial

No estipulado.

9.3.2.1 Publicación de información sobre los suscriptores

No se publica información de los suscriptores de los certificados, salvo en caso de que el certificado se encuentre revocado.

9.3.2.2 Publicación de información sobre la revocación o suspensión de un certificado

La información referida a la revocación de un certificado no se considera confidencial y se publica por ANTEL a través de su CRL y su servicio OCSP, disponibles en el sitio público del servicio de confianza. Las razones que da lugar a una revocación se consideran públicas, y se incluyen en la presente declaración de prácticas de certificación y en las Políticas de Certificación de Persona Física de la UCE, tanto en la de custodia centralizada como en la tradicional.

9.3.3 Responsabilidad de proteger la información confidencial

ANTEL asume su responsabilidad de protección de toda la información de los suscriptores que le fuese conferida y que no esté alcanzada por las excepciones de información no confidencial.

9.4 Confidencialidad de la información personal

9.4.1 Plan de privacidad

Para el servicio de confianza aplican las mismas políticas y normativas de privacidad que para el resto de los negocios y operaciones de ANTEL.

9.4.2 Información tratada como privada

A los efectos de la determinación del carácter de confidencial de la información recibida por ANTEL se estará a los recaudos previstos de acuerdo con lo establecido en la Ley N° 18.381, del 17 de octubre de 2008 [5].

La información personal queda regulada por las Leyes Nos. 18.331, de 11 de agosto de 2008[4] y 18.381, de 17 de octubre de 2008[5].

9.4.3 Información que no se considera privada

La información relativa al estado de revocación de los certificados no se considera privada

9.4.4 Responsabilidad de proteger información privada

ANTEL asume su responsabilidad de protección de toda la información de los suscriptores que les fuese conferida y que no esté alcanzada por las excepciones de información no confidencial.

9.4.5 Aviso y consentimiento de usar información privada

Excepto en los casos previstos en los apartados anteriores, toda divulgación de información referida a los datos de identificación del suscriptor o de cualquier otra información generada o recibida durante el ciclo de vida del certificado, solo se hará efectiva previa autorización de dicho suscriptor. No será necesario el consentimiento cuando los datos se hayan obtenido de fuentes de acceso público.

9.4.6 Divulgación de conformidad con proceso judicial o administrativo

La condición de información secreta por ley, reservada o confidencial cesa ante la solicitud de juez competente en el marco de un proceso jurisdiccional.

9.4.7 Otras circunstancias de divulgación de información

Excepto por los casos mencionados en los apartados anteriores, no existen otras circunstancias bajo las cuales ANTEL divulgue información.

9.5 Derechos de propiedad intelectual

ANTEL mantiene en forma exclusiva todos los derechos de propiedad intelectual con respecto a la presente documentación, a documentación que la amplía y aplicaciones pertenecientes a ella. Ninguna parte de este documento o sus extensiones se puede reproducir o distribuir sin que la previa notificación de derechos de propiedad intelectual aparezca en forma precisa, completa y sin modificaciones, atribuyendo a su auditoría a ANTEL.

9.6 Declaraciones y garantías

9.6.1 Declaraciones y garantías de la CA

Estipulado en la Política de Certificación de la ACRN, en la Política de Firma electrónica avanzada con custodia centralizada de Persona Física y en la Política de Persona Física.

9.6.2 Declaraciones y garantías de la RA

Estipulado en la Política de Certificación de la ACRN, en la Política de Firma electrónica avanzada con custodia centralizada de Persona Física y en la Política de Persona Física.

9.6.3 Declaraciones y garantías del Servicio de Confianza

Estipulado en la Política de Certificación de la ACRN, en la Política de Firma electrónica avanzada con custodia centralizada de Persona Física y en la Política de Persona Física.

9.6.4 Declaraciones y garantías del Servicio de Sellado de Tiempo

Estipulado en la Política de Sellado de Tiempo de la UCE.

9.6.5 Declaraciones y garantías del suscriptor

Estipulado en la Política de Certificación de la ACRN, en la Política de Firma electrónica avanzada con custodia centralizada de Persona Física y en la Política de Persona Física.

9.6.6 Declaraciones y garantías del tercero aceptante

Estipulado en la Política de Certificación de la ACRN, en la Política de Firma electrónica avanzada con custodia centralizada de Persona Física y en la Política de Persona Física.

9.6.7 Declaraciones y garantías de los demás participantes

Estipulado en la Política de Certificación de la ACRN, en la Política de Firma electrónica avanzada con custodia centralizada de Persona Física y en la Política de Persona Física.

9.7 Renuncia de garantías

No aplica.

9.8 Limitaciones de responsabilidad

Estipulado en la Política de Certificación de la ACRN, en la Política de Firma electrónica avanzada con custodia centralizada de Persona Física, en la Política de Persona Física y en la Política de Sellado de Tiempo.

9.9 Indemnizaciones

Estipulado en la Política de Certificación de la ACRN, en la Política de Firma electrónica avanzada con custodia centralizada de Persona Física, en la Política de Persona Física y en la Política de Sellado de Tiempo.

9.10 Vigencia y término

9.10.1 Vigencia

La presente CPS tendrá vigencia mientras el Servicio de Confianza de ANTEL se encuentre en operación.

9.10.2 Término

La presente CPS terminará su vigencia en la eventualidad que ANTEL descontinúe el Servicio de Confianza y cumpla con todas las etapas de terminación estipuladas en la presente declaración de prácticas.

9.10.3 Efecto de término y sobrevivencia

La presente CPS terminará su vigencia en la eventualidad que ANTEL descontinúe el Servicio de Confianza y cumpla con todas las etapas de terminación y estipuladas en la presente declaración de prácticas.

9.11 Avisos Individuales y comunicaciones con los participantes

Estipulado en la Política de Certificación de la ACRN, en la Política de Firma electrónica avanzada con custodia centralizada de Persona Física, en la Política de Persona Física y en la Política de Sellado de Tiempo.

9.12 Modificaciones

Las modificaciones a la presente declaración de prácticas de certificación y a sus extensiones son responsabilidad de ANTEL, serán comunicadas a la UCE, son sujeto de auditorías y serán publicadas en el sitio oficial del Servicio de Confianza de ANTEL.

9.12.1 Procedimiento para cambio de especificaciones

ANTEL cuenta con procedimientos internos para la administración de los cambios sobre la presente Declaración de Prácticas de Certificación y sus extensiones.

9.12.2 Procedimiento de enmiendas

Las modificaciones a la presente declaración de prácticas de certificación y sus extensiones son responsabilidad de ANTEL, serán comunicadas a la UCE, son sujeto de auditorías y serán publicadas en el sitio oficial del Servicio de Confianza de ANTEL.

9.12.3 Mecanismo y período de notificación

Las nuevas versiones de la presente declaración de prácticas y sus extensiones serán publicadas en forma inmediatamente posterior a su aprobación.

9.12.4 Circunstancias en las que el OID debe ser cambiado

Los OID de la presente CPS y de sus extensiones sólo serán cambiados cuando la naturaleza misma del Servicio de Confianza u otro Servicio objeto de la declaración se modifique, o sea transferida la operación a otro actor fuera de Antel.

9.13 Disposiciones de resolución de disputas

Estipulado en la Política de Certificación de la ACRN, en la Política de Firma electrónica avanzada con custodia centralizada de Persona Física, en la Política de Persona Física y en la Política de Sellado de Tiempo.

9.14 Ley aplicable

Aplica en este contexto toda la legislación vigente de la República Oriental del Uruguay.

9.15 Conformidad con la ley aplicable

Estipulado en la Política de Certificación de la ACRN, en la Política de Firma electrónica avanzada con custodia centralizada de Persona Física, en la Política de Persona Física y en la Política de Sellado de Tiempo.

9.16 Provisiones varias

9.16.1 Acuerdo completo

Estipulado en la Política de Certificación de la ACRN, en la Política de Firma electrónica avanzada con custodia centralizada de Persona Física, en la Política de Persona Física y en la Política de Sellado de Tiempo.

9.16.2 Asignación

Estipulado en la Política de Certificación de la ACRN, en la Política de Firma electrónica avanzada con custodia centralizada de Persona Física, en la Política de Persona Física y en la Política de Sellado de Tiempo.

9.16.3 Divisibilidad

Estipulado en la Política de Certificación de la ACRN, en la Política de Firma electrónica avanzada con custodia centralizada de Persona Física, en la Política de Persona Física y en la Política de Sellado de Tiempo.

9.16.4 Cumplimiento (honorarios de abogado y renuncia de derechos)

Estipulado en la Política de Certificación de la ACRN, en la Política de Firma electrónica avanzada con custodia centralizada de Persona Física, en la Política de Persona Física y en la Política de Sellado de Tiempo.

9.16.5 Fuerza mayor

Estipulado en la Política de Certificación de la ACRN, en la Política de Firma electrónica avanzada con custodia centralizada de Persona Física, en la Política de Persona Física y en la Política de Sellado de Tiempo.

9.17 Otras disposiciones

9.17.1 Forma de interpretación y aplicación

Estipulado en la Política de Certificación de la ACRN, en la Política de Firma electrónica avanzada con custodia centralizada de Persona Física, en la Política de Persona Física y en la Política de Sellado de Tiempo.

9.17.2 Obligaciones

Estipulado en la Política de Certificación de la ACRN, en la Política de Firma electrónica avanzada con custodia centralizada de Persona Física, en la Política de Persona Física y en la Política de Sellado de Tiempo.