Box CUSTODIA Y GESTIÓN DIGITAL

POLÍTICA ÚNICA DE CERTIFICACIÓN

CERTIFICADOR LICENCIADO
BOX CUSTODIA DE ARCHIVOS S.A.

Versión 2.3

www.boxcustodia.com

Sede Córdoba:
Ruta 19 Km 3 y 1/2
+54 (0351) 496 1518

Sede Buenos Aires:
Perú 227 piso 4°
+54 (011) 5032 2355

Sede Rosario:
Bv. Oroño 6190
+54 (0341) 462 4567

ÍNDICE

1- INTRODUCCIÓN.

1.1- Descripción general.

El presente documento establece las políticas que se aplican a la relación entre el Certificador Licenciado Box Custodia de Archivos S.A. en el marco de la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA (Ley Nº 25.506 y sus modificatoria) y los solicitantes, suscriptores y terceros usuarios de los certificados que éste emita. Un certificado vincula los datos de verificación de Firma Digital de una persona humana o jurídica o con una aplicación a un conjunto de datos que permiten identificar a dicha entidad, conocida como suscriptor del certificado.

La Autoridad de Aplicación de la Infraestructura de Firma Digital antes mencionada es la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS.

1.2.· Nombre e Identificación del Documento.

a) Nombre: Política Única de Certificación de BOX CUSTODIA DE ARCHIVOS S.A.

b) Versión: 2.2

c) Fecha de aplicación: A partir de su aprobación por el Ente Licenciante

d) OID de la Política de Certificación: 2.16.32.1.1.6

e) Lugar o sitio de publicación: se publica en el sitio web de la AC - BOX CUSTODIA FIRMA DIGITAL https://pki.boxcustodia.com/

1.3.- Participantes y aplicabilidad.

Integran la infraestructura del certificador las siguientes entidades:

1.3.1.- Certificador.

BOX CUSTODIA DE ARCHIVOS S.A.

Domicilio: Perú Nº 277, piso 4, oficina 1. CIUDAD AUTÓNOMA DE BUENOS AIRES.

Teléfono: +54 11 5032 2355

Correo electrónico: info@pki.boxcustodia.com

CUIT: 30-70458237-0

1.3.2.- Autoridad de Registro.

Los datos de la Autoridad de Registro Central y Delegadas, junto con sus respectivos Responsables, se publicarán en el sitio web https://pki.boxcustodia.com/web/identidaddigital/autoridades-de-registro seleccionando la opción Autoridades de Registro.

1.3.3.- Suscriptores de certificados.

Podrán ser suscriptores de los certificados emitidos por la Autoridad Certificante **AC – BOX CUSTODIA FIRMA DIGITAL** las personas humanas o jurídicas sean éstas públicas o privadas y aquellos que presten otros servicios relacionados con la firma digital.

La **AC - BOX CUSTODIA FIRMA DIGITAL** será además, suscriptora de un certificado para ser utilizado en relación con el servicio **On Line Certificate Status Protocol** (en adelante, OCSP) de consulta sobre el estado de los certificados digitales.

1.3.4.- Terceros Usuarios.

Son Terceros Usuarios de los certificados emitidos bajo la presente Política Única de Certificación toda persona humana o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente, de acuerdo a la normativa vigente aplicable a la Firma Digital.

1.4.- Uso de los certificados.

Las claves correspondientes a los certificados digitales que se emitan bajo la presente Política Única ele Certificación podrán ser utilizadas en forma interoperable en los procesos de firma digital de cualquier documento o transacción y para la autenticación o el cifrado.

1.5.- Administración de la Política.

1.5.1.- Responsable del Documento.

La Política Única de Certificación es administrada por BOX CUSTODIA DE ARCHIVOS S.A.

Domicilio: Perú Nº 277, piso 4, oficina 1. CIUDAD AUTÓNOMA DE BUENOS AIRES.

Correo electrónico: info@pki.boxcustodia.com

Teléfono: +54 11 5032 2355

Sitio web: https://pki.boxcustodia.com/

1.5.2.- Contacto.

BOX CUSTODIA DE ARCHIVOS S.A. es el responsable del registro, mantenimiento e interpretación ele la Política Única ele Certificación.

Contacto: El responsable de la Autoridad de Registro Central de la AC - BOX CUSTODIA

FIRMA DIGITAL.

Domicilio: Perú Nº 277, piso 4, oficina 1. CIUDAD AUTÓNOMA DE BUENOS AIRES.

Correo electrónico: info@pki.boxcustodia.com

Teléfono: +54 11 5032 2355

Sitio web: https://pki.boxcustodia.com

1.5.3.-Procedirniento de aprobación de la Política Única de Certificación.

La Política Única de Certificación del Certificador Licenciado BOX CUSTODIA DE ARCHIVOS S.A. fue presentada ante el Ente Licenciante durante el proceso de licenciamiento, el que fue aprobado por la Resolución de la SECRETARÍA DE GABINETE de la JEFATURA DE GABINETE DE MINISTROS Nº 43 del 15 de mayo de 2015.

1.6. - Definiciones y Acrónimos.

1.6.1. - Definiciones.

Se incluirán las definiciones de los conceptos relevantes utilizados en la Política de Certificación, incluyendo los siguientes:

- **Autoridad de Aplicación:** Es quien tiene por función el dictado de las normas reglamentarias de aplicación de la Ley N° 25.506 y lo establecido en la normativa regulatoria de Firma Digital de la REPÚBLICA ARGENTINA.
- **Autoridad de Registro:** es la entidad que tiene a su cargo las funciones de:
    a) Recepción de las solicitudes de emisión de certificados.
    b) Validación de la identidad y autenticación de los datos de los titulares de certificados.
    c) Validación de otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue el Certificador Licenciado BOX CUSTODIA DE ARCHIVOS S.A.
    d) Remisión de las solicitudes aprobadas al Certificador Licenciado BOX CUSTODIA DE ARCHIVOS S.A. con la que se encuentre operativamente vinculada.
    e) Recepción y validación de las solicitudes de revocación de certificados; y su direccionamiento al Certificador Licenciado BOX CUSTODIA DE ARCHIVOS S.A. con el que se vinculen.
    f) Identificación y autenticación de los solicitantes de revocación de certificados.
    g) Archivo y la conservación de toda la documentación respaldatoria del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por el certificador licenciado.
    h) Cumplimiento de las normas y recaudos establecidos para la protección de datos personales.
    i) Cumplimiento de las disposiciones que establezca la Política Única de Certificación y el Manual de Procedimientos del Certificador Licenciado con el que se encuentre vinculada, en la parte que resulte aplicable.
- **Autoridad de Sello de Tiempo:** Entidad que acredita la fecha y hora cierta, asignada a un documento o registro electrónico por una tercera parte confiable y firmada digitalmente por ella.
- **Autoridad de Sello de Competencia:** Entidad que acredita competencias, roles, funciones o relaciones laborales del titular de un certificado de firma digital.

- **Certificado Digital:** Se entiende por certificado digital al documento digital firmado digitalmente por un Certificador Licenciado, que vincula los datos de verificación de firma a su titular.
- **Certificador Licenciado:** Se entiende por Certificador Licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el Ente Licenciante.
- **Certificación digital de fecha y hora:** Indicación de la fecha y hora cierta, asignada a un documento o registro electrónico por una tercera parte confiable y firmada digitalmente por ella.
- **Ente licenciante:** Es el encargado de aprobar las Políticas Únicas de Certificación, el Manual de Procedimiento, el Plan de Seguridad, el Plan de Cese de Actividades y el Plan de Contingencia, presentados por los Certificadores solicitantes de la licencia o licenciados en el marco de la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA..
- **Lista de certificados revocados** : Lista de certificados que han sido dejados sin efecto en forma permanente por el Certificador Licenciado, la cual ha sido firmada digitalmente y publicada por el mismo. En inglés: Certificate Revocation List (CRL).
- **Manual de Procedimientos** Conjunto de prácticas utilizadas por el Certificador Licenciado en la emisión y administración de los certificados. En inglés: Certification Practice Statement (CPS)
- **Plan de Cese de Actividades:** conjunto de actividades a desarrollar por el certificador licenciado en caso de finalizar la prestación de sus servicios.
- **Plan de Contingencia:** Conjunto de procedimientos a seguir por el Certificador Licenciado ante situaciones de ocurrencia no previstas que comprometan la continuidad de sus operaciones.
- **Plan de Seguridad:** Conjunto de políticas, prácticas y procedimientos destinados a la protección de los recursos del certificador licenciado.
- **Política de Privacidad:** conjunto de declaraciones que el Certificador Licenciado se compromete a cumplir de manera de resguardar los datos de los solicitantes y suscriptores de certificados digitales por él emitidos.
- **Servicio OCSP (Protocolo en línea del estado de un certificado - "Online**

Certificate Status Protocol"): servicio de verificación en línea del estado de los certificados. El OCSP es un método para determinar el estado de revocación de un certificado digital usando otros medios que no sean el uso de Listas de Revocación de Certificados (CRL).

- **Suscriptor o Titular de Certificado Digital:** Persona, jurisdicción o entidad a cuyo nombre se emite un certificado y que posee una clave privada que se corresponde con la clave pública contenida en el mismo.
- **Tercero Usuario:** persona humana o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente.

1.6.2. - Acrónimos.

CRL - Lista de Certificados Revocados ("Certificate Revocation List")
CUIT - Clave Única de Identificación Tributaria
IEC - lnternational Electrotechnical Commission
IETF - Internet Engineering Task Force
OCSP - Protocolo en línea del estado de un certificado ("On line Certificate Status Protocol")
OID - Identificador de Objeto ("Object ldentifier")
ONTI - Oficina Nacional de Tecnologías de Información
RFC - Request For Comments

2. RESPONSABILIDADES VINCULADAS A LA PUBLICACIÓN Y A LOS REPOSITORIOS.

Se detallan a continuación las responsabilidades del certificador y de todo otro participante respecto al mantenimiento de repositorios, publicación de certificados y de información sobre sus políticas y procedimientos.

2.1. - Repositorios.

Los repositorios de información y la publicación de la Lista de Certificados Revocados son administrados en forma directa por BOX CUSTODIA DE ARCHIVOS S.A., el servicio es propio y no es provisto por terceros.

2.2. - Publicación de Información del Certificador.

El Certificador garantizará el acceso a la información actualizada y vigente publicada en el repositorio que mantiene en línea y de acceso público, de la siguiente documentación:

a) Política Única de Certificación en sus versiones vigentes y anteriores
b) Acuerdo con Suscriptores.
c) Los Términos y Condiciones con Terceros Usuarios ("relying parties")
d) Política de Privacidad.
e) Manual de Procedimientos en sus aspectos de carácter público, versiones vigentes y anteriores.
f) Información relevante de los informes de su última auditoría.
g) Repositorio de certificados revocados.
h) Certificados del Certificador licenciado y acceso al de la Autoridad Certificante Raíz.
i) Consulta de certificados emitidos (indicando su estado).

2.3. Listado de Autoridades de Registro - Frecuencia de publicación

Se garantiza la actualización inmediata del repositorio cada vez que cualquiera de los documentos publicados sea modificado.

El servicio de repositorio se encuentra disponible para uso público durante las VEINTICUATRO (24) horas los SIETE (7) días de la semana, sujeto a un razonable calendario de mantenimiento.

La información antedicha se encuentra disponible durante las VEINTICUATRO (24) horas los SIETE (7) días de la semana en el sitio web del Certificador https://pki.boxcustodia.com

2.4. - Controles de acceso a la información.

Se garantizan los controles de los accesos al certificado del certificador, a la Lista de Certificados Revocados y a las versiones anteriores y actualizadas de la Política de Certificación y a su Manual de Procedimientos (excepto en sus aspectos confidenciales). Solo se revelará información confidencial o privada, si es requerida judicialmente o en el marco de procedimientos administrativos.

En virtud de la Ley de Protección de Datos Personales Nº 25.326 y lo dispuesto por el inciso h) del artículo 21 de la Ley Nº 25.506, el solicitante o titular de un certificado digital podrá solicitar el acceso a toda la información relativa a las tramitaciones realizadas.

BOX CUSTODIA DE ARCHIVOS S.A. garantiza el acceso permanente, eficiente y gratuito de los titulares y terceros a la información publicada en su repositorio incluyendo la lista de certificados revocados y a disponer y dedicar los recursos necesarios para garantizar la seguridad de los datos almacenados, desde el punto de vista técnico y jurídico.

3.· IDENTIFICACIÓN Y AUTENTICACIÓN.

En esta sección se describen los procedimientos empleados para autenticar la identidad de los solicitantes de certificados digitales y utilizados por las Autoridades Certificantes o sus Autoridades de Registro como prerrequisito para su emisión. También se describen los pasos para la autenticación de los solicitantes de renovación y revocación de certificados.

La **AC - BOX CUSTODIA FIRMA DIGITAL** únicamente emite certificados digitales a aquellos suscriptores que cumplan con los requisitos para ostentar tal carácter establecidos en la presente Política, efectuándose a esos efectos una validación personal de la identidad del solicitante.

Para llevarse a cabo tal validación es requisito inescindible la presencia física del solicitante ante una Autoridad de Registro, sea ésta central o delegada.

El solicitante debe probar ante la Autoridad de Registro, mediante la documentación que corresponda, su carácter de tal.

A fin de efectuar la validación mencionada, se deben cumplir los siguientes procedimientos:

El solicitante efectúa el requerimiento de certificado ingresando al siguiente sitio web: https://pki.boxcustodia.com

b) Completa el requerimiento de certificado con sus datos personales y lo remite vía web a la AC - BOX CUSTODIA FIRMA DIGITAL.

c) Acepta el Acuerdo con Suscriptores en el que se hace referencia a la Política de Certificación que respalda la emisión del certificado.

d) Envía su solicitud a la **AC - BOX CUSTODIA FIRMA DIGITAL**.

e) Se presenta ante la Autoridad de Registro que corresponda con la documentación requerida para realizar su identificación personal.
Una vez cumplido el proceso de autenticación de la identidad, el solicitante firma la solicitud de su certificado digital ante la Autoridad de Registro correspondiente, con lo que quedan aceptadas las condiciones de emisión y uso del certificado digital.

La solicitud de certificado que no haya finalizado el proceso de identificación, caducará a los TREINTA (30) días de su generación.

3.1. - Asignación de nombres de suscriptores.

3.1.1. -Tipos de Nombres.

El nombre a utilizar es el que surge de la documentación presentada por el solicitante, de acuerdo al apartado que sigue:

3.1.2. - Necesidad de Nombres Distintivos.

Se indicarán las siguientes denominaciones, según el tipo de certificados que se emitan.

Para los certificados de Aplicaciones:

a) *"commonName"* (OID 2.5.4.3: Nombre común): al nombre de la aplicación, servicio o de la unidad operativa responsable del servicio.

b) *"organizationalUnitName"* (OID 2.5.4.11: Nombre de la suborganización): contiene las unidades operativas relacionadas con el servicio, en caso de existir, pudiendo utilizarse varias instancias de este atributo de ser necesario.

c) *"organizationName"* (OID 2.5.4.10: Nombre de la organización): está presente y coincide con el nombre de la Persona Jurídica Pública o Privada responsable del servicio o aplicación.

d) *"serialNumber"* (OID 2.5.4.5: Nro. *de* serie): está presente y contiene el número de identificación de la Persona Jurídica Pública o Privada responsable del servicio o aplicación, expresado como texto y respetando el siguiente formato y codificación: "[código de identificación]" "[nro. de identificación]".

El valor para el campo [código de identificación] es: "CUIT": Clave Única de Identificación Tributaria para las Personas Jurídicas argentinas.

e) *"countryName"* (OID 2.5.4.6: Código de país): está presente y representa el país de emisión de los certificados, codificado según el estándar [IS03166] de DOS (2) caracteres.

Para los certificados de Personas Humanas:

a) *"commonName"* (OID 2.5.4.3: Nombre común): está presente y se corresponde con el nombre que figura en el Documento de Identidad del suscriptor, acorde a lo establecido en el punto 3.2.3.

b) *"serialNumber"* (OID 2.5.4.5: Nro. de serie): está presente y contiene el tipo y número de identificación del titular, expresado como texto y respetando el siguiente formato y codificación: "[tipo de documento]" "[nro. de documento]"

Los valores posibles para el campo [tipo de documento] son:

a) En caso de ciudadanos argentinos o residentes: “CUIT” o “CUIL”:

Clave Única de Identificación Tributaria o Laboral (según corresponda).

b) En caso de extranjeros:

- "PA" [país]: Número de Pasaporte y código de país emisor. El atributo [país] está codificado según el estándar [IS03166] de DOS (2) caracteres.
- "EX" [país]: Número y tipo de documento extranjero aceptado en virtud de acuerdos internacionales. El atributo [país] está codificado según el estándar [IS03166] de DOS (2) caracteres.

c) *"countryName"* (OID 2.5.4.6: Código de país): está presente y representa el país de emisión de los certificados, codificado según el estándar [IS03166] de DOS (2) caracteres.

Para los certificados de Personas Jurídicas Públicas o Privadas:

a) "commonName" (OID 2.5.4.3: Nombre común): coincide con la denominación de la Persona Jurídica Pública o Privada o con el nombre de la unidad operativa responsable del servicio.

b) "organizationalUnitName" (OID 2.5.4.11: Nombre de la suborganización): puede contener las unidades operativas relacionadas con el suscriptor, pudiendo utilizarse varias instancias de este atributo de ser necesario.

c) "organizactionName": (OID 2.5.4.10: Nombre de la organización): coincide con el nombre de la Persona Jurídica Pública o Privada.

d) "serialNumber" (OID 2.5.4.5: Nro de serie): está presente y contiene el número de identificación de la Persona Jurídica Pública o Privada, expresado como texto y respetando el siguiente formato y codificación: "[código de identificación]" "[nro de identificación]".

Los valores posibles para el campo [código de identificación] son:

a) “CUIT”: Clave Única de Identificación Tributaria para las Personas Jurídicas argentinas.

b) “ID” [país]: Número de Identificación Tributaria para Personas Jurídicas extranjeras. El atributo [país] está codificado según el estándar [ISO 3166] de DOS (2) caracteres.

e) "countryName" (OID 2.5.4-6: Código de país): está presente y representa el país de emisión de los certificados, codificado según el estándar [IS03166] de 2 caracteres.

Para los Certificados de Autoridad de Sello de Tiempo.

a) "commonName" (OID 2.5.4.3: Nombre común): Indica el nombre del servicio.

b) "organizationalUnitName" (OID 2.5.4.11: Nombre de la suborganización): puede contener las unidades operativas relacionadas con el suscriptor, pudiendo utilizarse varias instancias de este atributo de ser necesario.

c) "organizactionName": (OID 2.5.4.10: Nombre de la organización): coincide con el nombre de la Persona Jurídica Pública o Privada.

d) "serialNumber" (OID 2.5.4.5: Nro de serie): está presente y contiene el número de identificación de la Persona Jurídica Pública o Privada, expresado como texto y respetando el siguiente formato y codificación: "[código de identificación]" "[nro de identificación]".

Los valores posibles para el campo [código de identificación] son:

a) “CUIT”: Clave Única de Identificación Tributaria para las Personas Jurídicas argentinas.

b) “ID” [país]: Número de Identificación Tributaria para Personas Jurídicas extranjeras. El atributo [país] está codificado según el estándar [ISO 3166] de DOS (2) caracteres.

e) "countryName" (OID 2.5.4-6: Código de país): está presente y representa el país de emisión de los certificados, codificado según el estándar [IS03166] de 2 caracteres.

Para los Certificados de Autoridad de Sello de Competencia:

a) "commonName" (OID 2.5.4.3: Nombre común): Indica indicar el nombre de la Autoridad de Competencia..

b) "organizationalUnitName" (OID 2.5.4.11: Nombre de la suborganización): puede contener las unidades operativas relacionadas con el suscriptor, pudiendo utilizarse varias instancias de este atributo de ser necesario.

c) "organizactionName": (OID 2.5.4.10: Nombre de la organización): coincide con el nombre de la Persona Jurídica Pública o Privada.

d) "serialNumber" (OID 2.5.4.5: Nro de serie): está presente y contiene el número de identificación de la Persona Jurídica Pública o Privada, expresado como texto y respetando el siguiente formato y codificación: "[código de identificación]" "[nro de identificación]".

Los valores posibles para el campo [código de identificación] son:

a) “CUIT”: Clave Única de Identificación Tributaria para las Personas Jurídicas argentinas.

e) "countryName" (OID 2.5.4-6: Código de país): está presente y representa el país de emisión de los certificados, codificado según el estándar [IS03166] de 2 caracteres.

3.1.3. - Anonimato o uso de seudónimos.

No se emitirán certificados anónimos o cuyo Nombre Distintivo contenga UN (1) seudónimo.

3.1.4. - Reglas para la interpretación de nombres.

Todos los nombres representados dentro de los certificados emitidos bajo la presente Política coinciden con los correspondientes al documento de identidad del suscriptor o con la documentación presentada por la persona jurídica. Las discrepancias o conflictos que puedan generarse si los datos de los solicitantes o suscriptores contienen caracteres especiales, se tratarán de modo de asegurar la precisión de la información contenida en el certificado.

3.1.5. - Unicidad de nombres.

El nombre distintivo debe ser único para cada suscriptor, pudiendo existir más de un certificado con igual nombre distintivo si corresponde al mismo suscriptor. El procedimiento de resolución de homonimias se basa en la utilización del número de identificación laboral o tributaria, tanto en el caso de personas humanas como jurídicas.

3.1.6. - Reconocimiento, autenticación y rol de las marcas registradas.

No se admite la inclusión de marcas comerciales, marcas de servicios o nombres de fantasía como nombres distintivos en los certificados, excepto en el caso de personas jurídicas o aplicaciones, en los que se aceptará en base a la documentación presentada. El certificador se reserva el derecho de tomar todas las decisiones referidas a posibles conflictos sobre la utilización y titularidad de cualquier nombre entre sus suscriptores conforme su normativa al respecto. En caso de conflicto, la parte que solicite el certificado debe demostrar su interés legítimo y su derecho a la utilización de un nombre en particular.

3.2. - Registro inicial

Se describen los procedimientos a utilizar para autenticar, como paso previo a la emisión de UN (1) certificado, la identidad y demás atributos del solicitante que se presente ante el certificador o ante la Autoridad de Registro operativamente vinculada. Se establecen los medios admitidos para recibir los requerimientos de certificados y para comunicar su aceptación.

El certificador cumple con lo establecido en los artículos 14, inciso b) y 21, inciso a) de la Ley de Firma Digital Nº 25.506, y normas complementarias.

3.2.1. Métodos para comprobar la posesión de la clave privada.

El certificador comprueba que el solicitante se encuentra en posesión de la clave privada mediante la verificación de la solicitud del certificado digital en formato PKCS#10, el que no incluye dicha clave, Las claves siempre son generadas por el solicitante. En ningún caso el certificador licenciado ni sus autoridades de registro podrán tomar conocimiento o acceder bajo ninguna circunstancia a las claves de los solicitantes o titulares de los certificados, conforme el artículo 21 inciso b) de la Ley N° 25.506, y del artículo 21 inciso 3 del Anexo al Decreto Reglamentario N° 182/2019 y complementarias.

3.2.2 - Autenticación de la identidad de Personas Jurídicas Públicas o Privadas.

Se indicará como “No Aplicable” cuando solo se emitan certificados para Personas Humanas.

Los procedimientos de autenticación de la identidad de los suscriptores de los certificados de personas jurídicas públicas o privadas comprenden los siguientes aspectos:

a) El requerimiento debe efectuarse únicamente por intermedio del responsable autorizado a actuar en nombre del suscriptor para el caso de certificados de personas jurídicas o de quien se encuentre a cargo del servicio, aplicación o sitio web.
b) La Autoridad de Registro, verificará la identidad del responsable antes mencionado y su autorización para gestionar el certificado correspondiente.
c) El responsable mencionado en el apartado a) deberá validar su identidad mediante documentación que acredite su condición de persona jurídica.
d) La identidad de la Persona Jurídica titular del certificado, responsable del servicio o aplicación deberá ser verificada mediante documentación que acredite su condición de tal.

El Certificador cumple con las siguientes exigencias reglamentarias impuestas por el artículo 21, inciso i) de la Ley Nº 25.506, relativo a la conservación de la documentación de respaldo de los certificados emitidos e inciso f) de la misma ley, relativo a la recolección de datos personales necesarios para su emisión. Se conserva la documentación que respalda el proceso de identificación de la persona responsable de la custodia de las claves criptográficas. El responsable autorizado a

cargo del servicio o aplicación presta su consentimiento expresando la confirmación de que la información incluida en el certificado es correcta.

Los Oficiales de Registro de las Autoridades de Registro, en el marco de la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA, deberán capturar la fotografía digital del rostro y la huella dactilar de los solicitantes y suscriptores de certificados de firma digital.

3.2.3. - Autenticación de la identidad de Personas Humanas.

Se indicará como “No Aplicable” cuando solo se emitan certificados para Personas Jurídicas.

Se describen los procedimientos de autenticación de la identidad de los suscriptores de los certificados dé Personas Humanas.

Se exige la presencia física del solicitante o suscriptor del certificado ante el certificador o la Autoridad de Registro con la que se encuentre operativamente vinculado. La verificación se efectúa mediante la presentación de los siguientes documentos:

- De poseer nacionalidad argentina, se requiere Documento Nacional de Identidad.
- De tratarse de extranjeros, se requiere Documento Nacional de Identidad argentino o Pasaporte válido u otro documento válido aceptado en virtud de acuerdos internacionales.

En todos los casos, se conservará UNA (1) copia digitalizada de la documentación de respaldo del proceso de autenticación por parte del certificador o de la Autoridad de Registro operativamente vinculada.

Se consideran obligatorias las exigencias reglamentarias impuestas por la Ley Nº 25.506, su modificatoria y complementarias, en particular, lo establecido en el artículo 21, inciso i) de la mencionada ley relativo a la conservación de la documentación de respaldo de los certificados emitidos e inciso f) de la misma ley, relativo a la recolección de datos personales.

Adicionalmente, el Certificador celebra UN (1) acuerdo con el solicitante o suscriptor, conforme el Anexo V de la resolución 946/2021 de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS

a) El artículo 21, inciso i) de la Ley Nº 25.506 relativo a la conservación de la documentación de respaldo de los certificados emitidos.

b) El artículo 21, inciso f) de la Ley Nº 25.506 relativo a la recolección de datos personales.

c) El artículo 21, inciso 3. del Decreto Nº 182/19 relativo a generar, exigir o tomar conocimiento de la clave privada del suscriptor.

d) El artículo 21, inciso 14. del Decreto Nº 182/19 relativo a la protección de datos personales.

La Autoridad de Registro deberá verificar que el dispositivo criptográfico utilizado por el solicitante, si fuera el caso, cumple con las especificaciones técnicas establecidas por el ente licenciante.

e) El Articulo 1 de la Resolución SMA N° 116-E/2017, relativo a la captura de la fotografía digital del rostro y la huella dactilar de los solicitantes y suscriptores de certificados de firma digital.

La Autoridad de Registro verifica que el dispositivo criptográfico utilizado por el solicitante, si fuera el caso, cumple con las especificaciones técnicas establecidas por el Ente Licenciante.

3.2.4. - Información no verificada del suscriptor.

Se conserva la información referida al solicitante que no hubiera sido verificada.
Adicionalmente, se cumple con lo establecido en el apartado 3 del inciso b) del artículo 14 de la Ley N' 25.506.

3.2.5. - Validación de autoridad.

Según lo dispuesto en el punto 3.2.2., el certificador o la Autoridad de Registro con la que se encuentre operativamente vinculado, verifica la autorización de la Persona Humana que actúa en nombre de la Persona Jurídica para gestionar el certificado correspondiente.

3.2.6. - Criterios para la interoperabilidad.

Los certificados emitidos pueden ser utilizados por sus titulares en forma interoperable para firmar digitalmente cualquier documento o transacción, así como para autenticación o cifrado.

3.3. - Identificación y autenticación para la generación de nuevo par de claves (Rutina de Re Key).

3.3.1. - Renovación con generación de nuevo par de claves (Rutina de Re Key).

En el caso de certificados digitales de personas humanas o jurídicas, la renovación en este apartado aplica a la generación de UN (1) nuevo par de claves y su correspondiente certificado:

a) después de la revocación de UN (1) certificado.
b) después de la expiración de UN (1) certificado.
c) antes de la expiración de UN (1) certificado.
d) En los casos a) y b) se exigirá el cumplimiento de los procedimientos previstos en el punto 3.2.3. Autenticación de la identidad de Persona Humana.

3.3.2. - Generación de UN (1) certificado con el mismo par de claves.

En el caso de certificados digitales de personas humanas o jurídicas, la renovación en este apartado aplica a la emisión de UN (1) nuevo certificado sin que haya un cambio en la clave pública o en ningún otro dato del suscriptor. La renovación se podrá realizar siempre que el certificado se encuentre vigente.
A los fines de la obtención del certificado, no se exigirá la presencia física del suscriptor, debiendo éste remitir la constancia firmada digitalmente del inicio del trámite de renovación. En los certificados de aplicaciones, incluyendo los de servidores, se deberá tramitar UN (1) nuevo certificado, según lo indicado en el apartado anterior.

3.4. - Requerimiento de revocación.

El suscriptor podrá pedir la revocación de su certificado a través de alguno de los siguientes medios:

a) Por correo electrónico firmado digitalmente a la dirección: revocacion.pki@boxcustodia.com
b) Ingresando al sitio web de la **AC - BOX CUSTODIA DE ARCHIVOS S.A**. a la siguiente URL: https://pki.boxcustodia.com accediendo con su usuario y utilizando el código de revocación que le fuera asignado al momento de la emisión del certificado.

c) Personalmente presentándose ante la Autoridad de Registro correspondiente con documento de identidad que permita acreditar su identidad.

Los sitios de revocación estarán disponibles durante las VEINTICUATRO (24) horas los SIETE (7) días de la semana.

La revocación también podrá ser solicitada por la Autoridad de Registro o por la Autoridad Certificante de **BOX CUSTODIA DE ARCHIVOS S.A.**

Las causales de revocación de un certificado son las detalladas en el punto 4.9.1. de la Política Única de Certificación.

d) Se procederá a revocar un certificado en los siguientes casos:

1) Cuando lo solicite el titular del certificado por cualquier causa, incluida el haber tomado conocimiento de que su clave privada esté comprometida y haya dejado de ser segura.
2) Si AC - BOX CUSTODIA FIRMA DIGITAL determina que el certificado fue emitido en base a una información falsa, que en el momento de la emisión hubiera sido objeto de verificación.
3) Si AC - BOX CUSTODIA FIRMA DIGITAL determina que los procedimientos de emisión y/o verificación han dejado de ser seguros.
4) En caso que la Organización que haya adoptado el uso de certificados de firma digital emitidos por la AC - BOX CUSTODIA FIRMA DIGITAL, notifique a la Autoridad de Registro que la información contenida en el certificado ha dejado de ser exacta.
5) Cuando fuere solicitado por resolución judicial o de la Autoridad de Aplicación de la Ley Nº 25.506 debidamente fundada.
6) Si AC - BOX CUSTODIA FIRMA DIGITAL determina que el certificado dejó de cumplir con las políticas y normas legales y reglamentarias de la Infraestructura de Firma Digital de la República Argentina (IFDRA).
7) Por fallecimiento del titular, declaración judicial de ausencia con presunción de fallecimiento o declaración judicial de incapacidad, en el caso de persona humana comunicada fehacientemente por sus herederos o autoridad judicial competente a AC - BOX CUSTODIA FIRMA DIGITAL
8) Por cese del responsable autorizado, en el caso de personas jurídicas comunicada fehacientemente por el nuevo responsable autorizado de la persona jurídica a AC - BOX CUSTODIA FIRMA DIGITAL

9) Por cambio en los atributos de un certificado, aun cuando hubieran sido válidos al tiempo de su emisión.
10) Por cese de la existencia de la Persona Jurídica, comunicada fehacientemente por el responsable autorizado de la misma a AC - BOX CUSTODIA FIRMA DIGITAL
11) Por cese de la Licencia del Certificador
12) Por haberse resuelto el contrato que AC - BOX CUSTODIA FIRMA DIGITAL hubiera suscripto con la Organización a la cual perteneciese el Suscriptor, o lo convenido entre las partes, en el caso que corresponda.

4. CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS.

4.1. - Solicitud de certificado.

4.1.1. - Solicitantes de certificados.

Se describen las condiciones que deben cumplir los solicitantes de certificados.

4.1.2. - Solicitud de certificado.

Las solicitudes sólo podrán ser iniciadas por el solicitante en el caso de certificados de personas humanas y por el representante legal o apoderado con poder suficiente a dichos efectos, o por el Responsable del Servicio, aplicación o sitio web, autorizado a tal fin, en el caso de personas jurídicas.
Dicho solicitante debe presentar la documentación prevista en los apartados 3.2.2. - Autenticación de la identidad de Personas Jurídicas Públicas o Privadas y 3.2.3. - Autenticación de la identidad de Personas Humanas, así como la constancia de C.U.I.L.
Deberá también demostrar la pertenencia a la comunidad de suscriptores prevista en el apartado 1.3.3. Suscriptores de certificados.

a) Solicitud de certificado de persona humana:

El proceso de solicitud puede ser iniciado solamente por el interesado, quien posteriormente debe acreditar fehacientemente su identidad y deberá completar los datos solicitados.

Todo solicitante o suscriptor que se postule para obtener un certificado debe completar una solicitud, en el sitio web https://pki.boxcustodia.com/ del Certificador, que estará sujeta a revisión y aprobación por la AR.

El solicitante debe tener una dirección de correo electrónico e informarla en su solicitud, a los fines de ser notificado de la emisión de su certificado.

El solicitante debe elegir realizar su identificación ante la Autoridad de Registro Central o alguna de las Autoridades de Registro Delegadas si las hubiera.

Una vez ingresados sus datos y como paso previo a la generación del par de claves, seleccionará el nivel de seguridad del certificado requerido (alto o normal).

Adicionalmente, el solicitante deberá leer y aceptar el Acuerdo con Suscriptores para continuar el proceso. Como medida de seguridad se envía la solicitud del certificado a la dirección del correo electrónico declarado en la solicitud, requiriendo la confirmación de la misma.

Si se confirma la recepción del correo electrónico, la aplicación procederá a generar el par de claves y el requerimiento de certificado digital en formato PKCS#10 por software, nivel normal, o por hardware, nivel alto, si el solicitante así lo hubiera indicado.

Una vez generadas las claves, la aplicación del· Certificador valida el requerimiento PKCS#10 y genera el PIN de revocación del certificado y envía un nuevo correo electrónico al solicitante, en la dirección por él informada en su solicitud.

b) Solicitud de certificado de persona jurídica pública o privada.

La solicitud de un certificado de persona jurídica pública o privada, puede ser realizada por su representante legal, apoderado, administrador o responsable autorizado, quien deberá acreditar su identidad según lo establecido en el apartado 3.2.2. "Autenticación de la identidad de Personas Jurídicas Públicas o Privadas".

Debe contar con una dirección de correo electrónico e informarla en su solicitud, a los fines de ser notificado de la emisión de su certificado.

El proceso de solicitud puede ser iniciado solamente por el representante legal, apoderado, administrador o responsable autorizado de la persona jurídica pública o privada a favor de la cual se emitirá el certificado.

Una vez iniciado, el solicitante deberá leer y. aceptar el Acuerdo con Suscriptores para continuar el proceso. Como medida de seguridad se envía la solicitud del certificado a la dirección del correo electrónico declarada, requiriendo la confirmación de la misma. Si se confirma la recepción del correo electrónico, la aplicación procederá a generar el par de claves y el requerimiento de certificado digital en formato PKCS#10 por software, nivel normal, o por hardware, nivel alto, si el solicitante así lo hubiera indicado.

Completada la solicitud, el solicitante deberá confirmar todos los datos presentes en la misma seleccionando o la Autoridad de Registro Central o alguna de las Autoridades Delegadas de **BOX CUSTODIA DE ARCHIVOS S.A.** si las hubiere.

Una *vez* verificados los datos de la solicitud, se le envía un correo electrónico a la dirección de correo declarada a fin de solicitar su confirmación para una *vez* obtenida ésta generar el par de claves. Generadas las claves, la aplicación de **BOX CUSTODIA DE ARCHIVOS** S.A. valida el requerimiento PKCS#10 y genera el **PIN** de revocación del certificado y envía un nuevo correo electrónico al solicitante, en la dirección por él informada en su solicitud.

Solicitud de certificados de aplicación

La solicitud de emisión de certificado debe ser iniciada exclusivamente por el representante legal, apoderado, administrador o responsable autorizado de la persona jurídica a la que representa quien tendrá a su cargo acreditar su identidad según se indica en el apartado

4.1.3."Autenticación de la identidad de Personas Jurídicas Públicas o Privadas".

El solicitante deberá contar con una dirección de correo electrónico e informarla en su solicitud, a los fines de ser notificado de la emisión de su certificado.

El proceso de solicitud puede ser iniciado solamente por el representante legal, apoderado, administrador o responsable autorizado de la persona jurídica pública o privada a favor de la cual se emitirá el certificado.

Cuando el solicitante contará con un dispositivo criptográfico, éste deberá iniciar la solicitud en el dispositivo. Completada la solicitud, el solicitante deberá confirmar todos los datos presentes en la misma seleccionando o la Autoridad de Registro Central o alguna de las Autoridades Delegadas de BOX CUSTODIA DE ARCHIVOS S.A. si las hubiere.

Una vez verificados los datos de la solicitud, se le envía un correo electrónico a la dirección de correo declarada a fin de solicitar su confirmación para una vez obtenida ésta generar el par de claves. Generadas las claves, la aplicación de BOX CUSTODIA DE ARCHIVOS S.A. válida el requerimiento PKCS#10 y genera el PIN de revocación del certificado y envía un nuevo correo electrónico al solicitante, en la dirección por él informada en su solicitud.

Adicionalmente al procedimiento descripto en los puntos a), b) y c), se habilitará una modalidad "itinerante" por la que la Autoridad de Registro Central o Delegada concurre al lugar donde se encuentra el solicitante a fin de efectuar la validación de su identidad y condición de suscriptor.

4.2. - Procesamiento de la solicitud del certificado.

La aprobación de los certificados para personas humanas, personas jurídicas o para aplicaciones está sujeta a que el solicitante cumpla con todos los requisitos solicitados para la obtención del certificado que solicita y a la verificación presencial de la identidad del solicitante.

Si la solicitud es rechazada, se le informará al solicitante por mail firmado digitalmente por el Oficial de Registro, a la dirección de correo electrónico que hubiera declarado en su solicitud.

Si la solicitud es aprobada, se le comunicará de la misma manera, informando al suscriptor que su certificado se encuentra disponible para su descarga e instalación.

Con relación a la documentación acompañada por el solicitante al momento de presentarse ante el Oficial de Registro de la Autoridad de Registro Central o Delegada según sea el caso, deberá ser resguardada por el término de DIEZ (10) años a partir de la expiración del certificado o de su revocación.

4.3. - Emisión del certificado.

4.3.1. - Proceso de emisión de un certificado.

Cumplidos los recaudos del proceso enunciado en el apartado 4.1.2. Solicitud de certificado y una vez aprobada la solicitud de certificado por la Autoridad de Registro correspondiente, la Autoridad Certificante AC - BOX CUSTODIA FIRMA DIGITAL emitirá el certificado firmándolo digitalmente y lo pondrá a disposición del suscriptor.

En el mismo sentido, se emitirá un certificado ante una solicitud de renovación.

4.3.2. - Notificación de emisión.

Una vez finalizado el proceso de solicitud de un certificado, la AC - BOX CUSTODIA FIRMA DIGITAL, enviará de manera automática e inmediata al suscriptor del certificado, un correo electrónico notificándole de la emisión de su certificado indicándole como descargarlo. La dirección del correo electrónico al que se notifica la emisión del certificado, fue verificada y validada durante el proceso de solicitud del certificado.

4.4. - Aceptación del certificado.

Un certificado emitido a favor de un suscriptor se considera aceptado por su titular una vez que el suscriptor firmó el Acuerdo con Suscriptores y que el certificado haya sido puesto a su disposición.

4.5.- Uso del par de claves y del certificado.

4.5.1. - Uso de la clave privada y del certificado por parte del suscriptor.

Según lo establecido en la Ley Nº 25.506, en su artículo 25, el suscriptor debe:

a) Mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, e impedir su divulgación;
b) Utilizar UN (1) dispositivo de creación de firma digital técnicamente confiable;
c) Solicitar la revocación de su certificado al certificador ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma;
d) Informar sin demora al certificador el cambio de alguno de los datos contenidos en el certificado digital que hubiera sido objeto de verificación.

4.5.2. Uso de la clave pública y del certificado por parte de Terceros Usuarios.

Los Terceros Usuarios deben:

a) Conocer los alcances de la presente Política Única de Certificación;
b) Verificar la validez del certificado digital.

4.6. Renovación del certificado sin generación de un nuevo par de claves.

Se aplica el punto 3.3.2.- Generación de UN (1) certificado con el mismo par de claves.

4.7. Renovación del certificado con generación de un nuevo par de claves.

En el caso de certificados digitales de Personas Humanas, la renovación del certificado posterior a su revocación o luego de su expiración requiere por parte del suscriptor el cumplimiento de los procedimientos previstos en el punto 3.2.3. - Autenticación de la identidad de Personas Humanas.

Si la solicitud de UN (1) nuevo certificado se realiza antes de la expiración del anterior, no habiendo sido este revocado, no se exigirá la presencia física, debiendo el solicitante remitir la constancia firmada digitalmente del inicio del trámite de renovación.

Para los certificados de aplicaciones, incluyendo los de servidores, los responsables deben tramitar UN (1) nuevo certificado en todos los casos, cumpliendo los pasos requeridos en el apartado 3.2.2. Autenticación de la identidad de Personas Jurídicas Públicas o Privadas.

4.8. Modificación del certificado.

El suscriptor se encuentra obligado a notificar al certificador licenciado cualquier cambio en alguno de los datos contenidos en el certificado digital, que hubiera sido objeto de verificación, de acuerdo a lo dispuesto en el inciso d) del artículo 25 de la Ley Nº 25.506.

En cualquier caso, procede la revocación de dicho certificado y de ser requerido, la solicitud de uno nuevo.

4.9. - Suspensión y Revocación de Certificados.

Los certificados serán revocados de manera oportuna y sobre la base de UNA (1) solicitud de revocación de certificado validada.

El estado de suspensión no es admitido en el marco de la Ley Nº 25.506.

4.9.1. Causas de revocación.

El Certificador procederá a revocar los certificados digitales que hubiera emitido en los siguientes casos:

a) A solicitud del titular del certificado digital o del responsable autorizado para el caso de los certificados de Personas Jurídicas o aplicación.
b) Si determinara que el certificado fue emitido en base a información falsa, que al momento de la emisión hubiera sido objeto de verificación.
c) Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.
d) Por Resolución Judicial.
e) Por Resolución de la Autoridad de Aplicación debidamente fundado.
f) Por fallecimiento del titular.
g) Por declaración judicial de ausencia con presunción de fallecimiento del titular.
h) Por declaración judicial de incapacidad del titular.
i) Si se determina que la información contenida en el certificado ha dejado de ser válida.
j) Cuando la clave privada asociada al certificado, o el medio en que se encuentre almacenada, se encuentren comprometidos o corran peligro de estarlo.
k) Ante incumplimiento por parte del suscriptor de las obligaciones establecidas en el Acuerdo con Suscriptores.
l) Si se determina que el certificado no fue emitido de acuerdo a los lineamientos de la Política Única de Certificación, del Manual de Procedimientos, de la Ley Nº 25.506, y su modificatoria, sus normas reglamentarias..

El Certificador, de corresponder, revocará el certificado en un plazo no superior a las VEINTICUATRO (24) horas de recibido el requerimiento de revocación.

4.9.2. - Autorizados a solicitar la revocación.

Se encuentran autorizados para solicitar la revocación de UN (1) certificado:

a) En el caso de los certificados de personas humanas, el suscriptor del certificado.
b) En el caso de los certificados de persona jurídica o de aplicación, el responsable autorizado que efectuara el requerimiento.
c) En el caso de los certificados de persona jurídica o de aplicación, el responsable debidamente autorizado por la Persona Jurídica que brinda el servicio o es titular del certificado o la aplicación.
d) El Certificador o la Autoridad de Registro.
e) El Ente Licenciante.
f) La Autoridad Judicial.

g) La Autoridad de Aplicación.

4.9.3. - Procedimientos para la solicitud de revocación.

El certificador garantiza que:

a) Se identifica debidamente al solicitante de la revocación según se establece en el apartado 3.4.
b) Las solicitudes de revocación, así como toda acción efectuada por el certificador o la autoridad de registro en el proceso, están documentadas y conservadas en sus archivos.
c) Se documentan y archivan las justificaciones de las revocaciones aprobadas.
d) Una vez efectuada la revocación, se actualiza el estado del certificado en el repositorio y se incluye en la próxima lista de certificados revocados a ser emitida.
e) El suscriptor del certificado revocado es informado del cambio de estado de su certificado.

En caso de tratarse de certificados aprobados por Autoridades de Registro Delegadas, las solicitudes de revocación deberán dirigirse a la correspondiente Autoridad de Registro. Los números telefónicos y direcciones de correo electrónico de contacto de cada uno de ellos se encuentran disponibles en el sitio web de la **AC - BOX CUSTODIA FIRMA DIGITA**L (https://pki.boxcustodia.com/). El suscriptor podrá efectuar la revocación a través de alguno de los siguientes medios:

a) Por correo electrónico firmado digitalmente a la dirección: revocacion.pki@boxcustodia.com
b) Ingresando al sitio web de la **AC - BOX CUSTODIA DE ARCHIVOS S.A**. a la siguiente URL: https://pki.boxcustodia.com accediendo con su usuario y utilizando el código de revocación que le fuera asignado al momento de la emisión del certificado.
c) Personalmente presentándose ante la Autoridad de Registro correspondiente con documento de identidad que permita acreditar su identidad.

Los sitios de revocación estarán disponibles durante las VEINTICUATRO (24) horas los SIETE (7) días de la semana. Disponibilidad del servicio de consulta

Una vez efectuada la revocación, se actualiza el estado del certificado en el repositorio y se incluye en la próxima lista de certificados revocados a ser emitida.

4.9.4. - Plazo para la solicitud de revocación.

El titular de un certificado debe requerir su revocación en forma inmediata cuando se presente alguna de las circunstancias previstas en el apartado 4.9.1.

El servicio de recepción de solicitudes de revocación se encuentra disponible en forma permanente SIETE POR VEINTICUATRO (7x24) horas cumpliendo con lo establecido en el artículo 21, inciso 8 del Decreto Nº 182/19.

4.9.5. - Plazo para el procesamiento de la solicitud de revocación.

El plazo entre la recepción de la solicitud y el cambio de la información de estado del certificado indicando que la revocación ha sido puesta a disposición de los Terceros Usuarios, no superará en ningún caso las VEINTICUATRO (24) horas.

4.9.6. Requisitos para la verificación de la lista de certificados revocados.

Los Terceros Usuarios deben validar el estado de los certificados, mediante el control de la lista de certificados revocados, a menos que utilicen otro sistema con características de seguridad y confiabilidad por lo menos equivalentes.

La autenticidad y validez de las listas de certificados revocados también debe ser confirmada mediante la verificación de la firma digital del certificador que la emite y de su período de validez.

AC - BOX CUSTODIA DE ARCHIVOS S.A cumple con lo establecido en el artículo 21, inciso 9 del Anexo al Decreto Nº 182/2019 relativo al repositorio de certificados revocados y las obligaciones establecidas en la Resolución 946/2021.

4.9.7. - Frecuencia de emisión de listas de certificados revocados.

El Certificador genera y publica una Lista de Certificados Revocados con una frecuencia diaria, cada VEINTICUATRO (24) horas, con listas complementarias (delta CRL) en modo horario.

4.9.8.- Vigencia de la lista de certificados revocados.

La vigencia de cada lista de certificados revocados es de VEINTICUATRO (24) horas.

El Certificador posee un servicio en línea de revocación de certificados y de verificación de su estado. Ambos servicios se encuentran disponibles SIETE POR VEINTICUATRO (7x24) horas, sujetos a un razonable calendario de mantenimiento. La lista de

certificados revocados indicará su fecha de vigencia y la fecha de su próxima actualización.

4.9.9. - Disponibilidad del servicio de consulta sobre revocación y de estado del certificado.

AC - BOX CUSTODIA DE ARCHIVOS pone a disposición de los interesados la posibilidad de verificar el estado de un certificado por medio del acceso a la lista de certificados revocados y de otros medios de verificación de estado en línea (OCSP).

Se informarán los detalles del servicio de consulta de la lista de certificados ·revocados. Si el certificador ofrece adicionalmente el servicio de verificación en línea del estado de certificados, deberá informarlo.

AC - BOX CUSTODIA DE ARCHIVOS pone a disposición de los terceros usuarios:

a) La información relativa a las características de los servicios de verificación de estado.
b) La disponibilidad de tales servicios y los procedimientos que se seguirán en caso de no disponibilidad.

En el caso de las aplicaciones propias de **BOX CUSTODIA DE ARCHIVOS S.A**. donde se utilizan los certificados emitidos por la **AC - BOX CUSTODIA FIRMA DIGITAL** realizan la consulta sobre la lista de Certificados Revocados en forma automática.

4.9.10. - Requisitos para la verificación en línea del estado de revocación.

Los terceros usuarios están obligados a validar el estado de los certificados mediante el control de la lista de certificados revocados o mediante el acceso al servicio OCSP que se describe más adelante.

Los suscriptores y terceros usuarios están obligados a confirmar la autenticidad y validez de la lista de certificados revocados mediante la verificación de la firma digital de la **AC – BOX CUSTODIA FIRMA DIGITAL** y de su período de validez.

La **AC - BOX CUSTODIA FIRMA DIGITAL** garantiza el acceso permanente, eficiente y gratuito de los titulares de certificados y de terceros usuarios al repositorio de certificados.

La **AC - BOX CUSTODIA FIRMA DIGITAL** posee un servicio en línea de revocación de certificados y de verificación de su estado. Ambos servicios se encuentran disponibles

SIETE POR VEINTICUATRO (7x24) horas, sujetos a un razonable período de mantenimiento.

Las características operacionales de ambos servicios se encuentran disponibles en su sitio web.

El uso del protocolo OCSP permite, mediante su consulta, determinar el estado de validez de un certificado digital y representa una alternativa a la consulta a la CRL, la que también estará disponible. El servicio OCSP se provee en el siguiente sitio web: Servicio OCSP - IdentidadDigital (boxcustodia.com)

4.9.11.- Otras formas disponibles para la divulgación de la revocación.

El Certificador no utiliza otros medios para la divulgación del estado de revocación de los certificados que los contemplados en la presente Política Única de Certificación.

4.9.12.- Requisitos específicos para casos de compromiso de claves.

En caso de compromiso de su clave privada, el titular del certificado correspondiente se encuentra obligado a comunicar inmediatamente dicha circunstancia al certificador mediante alguno de los mecanismos previstos en el apartado 4.9.3. - Procedimientos para la solicitud de revocación.

4.9.13.- Causas de suspensión.

El estado de suspensión no es admitido en el marco de la Ley Nº 25.506 y modificatoria.

4.9.14. ·Autorizados a solicitar la suspensión.

El estado de suspensión no es admitido en el marco de la Ley Nº 25.506 y modificatoria.

4.9.15. - Procedimientos para la solicitud de suspensión.

El estado de suspensión no es admitido en el marco de la Ley Nº 25.506 y modificatoria.

4.9.16. - Límites del periodo de suspensión de un certificado.

El estado de suspensión no es admitido en el marco de la Ley Nº 25.506 y modificatoria.

4.10.- Estado del certificado.

4.10.1. - Características técnicas.

Servicios prestados:

- Lista de Certificados revocados (CRL)
- Servicio OCSP

Respecto a la CRL, se emite cada VEINTICUATRO (24) horas y delta CRLs en modo horario.
Con respecto a OCSP, permite verificar si el certificado se encuentra vigente a o ha sido revocado.

4.10.2. - Disponibilidad del servicio.

Se encuentran disponibles SIETE POR VEINTICUATRO (7x24) horas sujeto a un razonable calendario de mantenimiento, a partir de su sitio web: https://pki.boxcustodia.com

4.10.3. - Aspectos operativos.

No existen otros aspectos a mencionar.

4.11. - Desvinculación del suscriptor.

Una vez expirado el certificado o si este fuera revocado, de no tramitar un nuevo certificado, su titular se considera desvinculado de los servicios del certificador.
e igual forma se producirá la desvinculación, ante el cese de las operaciones del certificador.

4.12. - Recuperación y custodia de claves privadas.

El certificador licenciado no podrá bajo ninguna circunstancia realizar la recuperación de claves privadas de los titulares de certificados digitales, en virtud de lo dispuesto en el inciso b) del artículo 21 de la Ley Nº 25.506. El suscriptor se encuentra obligado a mantener el control exclusivo de su clave privada, no compartirla e impedir su divulgación, de acuerdo a lo dispuesto en el inciso a) del artículo 25 de la ley antes mencionada.

4.13. – Custodia centralizada de claves.

La AC - BOX CUSTODIA FIRMA DIGITAL es prestador de servicios de confianza para el servicio de firma digital con custodia centralizada

De acuerdo a lo establecido en el Art 1 de la Resolución 86/2020 de la SECRETARÍA DE INNOVACIÓN PÚBLICA, la AC - BOX CUSTODIA FIRMA DIGITAL provee el servicio de custodia centralizada de claves criptográficas, realizando asimismo la generación y el proceso de firma digital el cual lo realiza en un sistema técnicamente confiable y seguro conforme a los lineamientos establecidos en la Ley Nro 25.506, sus modificatorias y en el anexo a la Resolución 86/2020, cumpliendo con las normas de seguridad acordes a estándares internacionales y de auditoría establecidas por la Autoridad de Aplicación.

La clave privada del suscriptor es generada en el módulo criptográfico del dispositivo criptográfico provisto por BOX CUSTODIA DE ARCHIVOS S.A el cual tiene una certificación FIPS 140-2 nivel 3, siendo este dispositivo independiente del que se utiliza para la custodia de la clave privada de la AC - BOX CUSTODIA FIRMA DIGITAL

La generación de claves es realizada exclusivamente con datos de exclusivo conocimiento y control del suscriptor. Asimismo el sistema utilizado por la AC - BOX CUSTODIA FIRMA DIGITAL no permite que se tome conocimiento de las claves privadas de los suscriptores.

El proceso de creación de firma digital es realizado en el módulo criptográfico del dispositivo criptográfico provisto por la AC - BOX CUSTODIA FIRMA DIGITAL.

La AC - BOX CUSTODIA FIRMA DIGITAL cuenta con un sitio principal y uno de contingencia para garantizar la continuidad del servicio. El sitio de contingencia es una réplica del sitio principal contando con un dispositivo de creación de claves con certificación FIPS 140-2 nivel 3. Ambos dispositivos, el principal y la contingencia se encuentran en las instalaciones habilitadas para la operación de la AC - BOX CUSTODIA FIRMA DIGITAL

5. - CONTROLES DE SEGURIDAD FÍSICA, OPERATIVOS Y DE GESTIÓN.

Se describen a continuación los procedimientos referidos a los controles de seguridad física, de gestión y operativos implementados por el certificador. La descripción detallada se efectuará en el Plan de Seguridad.

5.1. - Controles de seguridad física.

Se cuenta con controles de seguridad relativos a:

a) Construcción y ubicación de instalaciones.
b) Niveles de acceso físico.
c) Comunicaciones, energía y ambientación.
d) Exposición al agua.
e) Prevención *y* protección contra incendios.
f) Medios de almacenamiento.
g) Disposición de material de descarte.
h) Instalaciones de seguridad externas.

5.2. Controles de Gestión.

Se cuenta con controles de seguridad relativos a:

I. Definición de roles afectados al proceso de certificación.
II. Número de personas requeridas por función.
III. Identificación *y* autenticación para cada rol.
IV. Separación de funciones.

5.3. Controles de seguridad del personal

Se cuenta con controles de seguridad relativos a:

a) Calificaciones, experiencia e idoneidad del personal, tanto de aquellos que cumplen funciones críticas como de aquellos que cumplen funciones administrativas, de seguridad, limpieza, etcétera.
b) Antecedentes laborales.
c) Entrenamiento *y* capacitación inicial.
d) Frecuencia de procesos de actualización técnica.
e) Frecuencia de rotación de cargos.
f) Sanciones a aplicar por acciones no autorizadas.
g) Requisitos para contratación de personal.
h) Documentación provista al personal, incluidas tarjetas y otros elementos de identificación personal.

5.4. Procedimientos de Auditoría de Seguridad.

Se mantienen políticas de registro de eventos, cuyos procedimientos detallados serán desarrollados en el Manual de Procedimientos.

Se cuenta con procedimientos de auditoría de seguridad sobre los siguientes aspectos:

a) Tipo de eventos registrados. Se respeta lo establecido en el Anexo II Sección 3 de la Resolución 946/2021.
b) Frecuencia de procesamiento de registros.
c) Período de guarda de los registros. Se respeta lo establecido en el inciso i) del artículo 21 de la Ley Nº 25.506 respecto a los certificados emitidos.
d) Medidas de protección de los registros, incluyendo privilegios de acceso.
e) Procedimientos de resguardo de los registros.
f) Sistemas de recolección y análisis de registros.
g) Notificaciones del sistema de recolección y análisis de registros.
h) Evaluación de vulnerabilidades.

5.5. - Conservación de registros de eventos.

Se han desarrollado e implementado políticas de conservación de registros, cuyos procedimientos detallados se encuentran desarrollados en el Manual de Procedimientos.

Los procedimientos cumplen con lo establecido por el artículo 21, inciso i) de la Ley Nº 25.506 relativo al mantenimiento de la documentación de respaldo de los certificados digitales emitidos.

Se respeta lo establecido en el Anexo II Sección 3 respecto del registro de eventos.

Existen procedimientos de conservación y guarda de registros en los siguientes aspectos, que se encuentran detallados en el Manual de Procedimientos:

a) Tipo de registro archivado. Se respeta lo establecido en el Anexo II Sección 3 de la Resolución 946/2021.
b) Período de guarda de los registros.
c) Medidas de protección de los registros archivados, incluyendo privilegios de acceso.
d) Procedimientos de resguardo de los registros.
e) Sistemas de recolección y análisis de registros.
f) Procedimientos para obtener y verificar la información archivada.

5.6. Cambio de claves criptográficas.

El par de claves criptográficas que **BOX CUSTODIA DE ARCHIVOS S.A.** genera para su Autoridad Certificante (**AC- BOX CUSTODIA FIRMA DIGITAL**) es generado en un ambiente seguro con motivo del licenciamiento de la presente Política Única de Certificación y tendrá una vigencia de DIEZ (10) años.

En todos los casos el cambio de claves criptográficas de BOX CUSTODIA DE ARCHIVOS S.A. implica la emisión de un nuevo certificado por parte de la AC Raíz de la REPÚBLICA ARGENTINA. Si la clave privada de BOX CUSTODIA DE ARCHIVOS S.A. se encontrase comprometida, se procederá a la revocación inmediata de su certificado y esa clave ya no podrá ser usada en el proceso de emisión de certificados.

BOX CUSTODIA DE ARCHIVOS S.A. tomará los recaudos necesarios para efectuar con suficiente antelación la renovación de su licencia y la obtención del certificado, si correspondiese.

Si por algún motivo resultase necesario cambiar el par de claves de un certificado vigente, el suscriptor deberá solicitar la revocación de su certificado e iniciar el proceso de solicitud de un nuevo certificado.

Los procedimientos a seguir para distribuir una nueva clave pública a los usuarios de un certificador luego de un cambio de claves pueden ser los mismos que fueron utilizados para distribuir la clave que se reemplaza. La nueva clave puede ser incluida en un certificado firmado digitalmente con la clave que será reemplazada, salvo que esta última esté comprometida.

5.7. - Compromiso y recuperación ante desastres.

Se describen los requerimientos relativos a la recuperación de los recursos del certificador en caso de falla o desastre. Estos requerimientos serán desarrollados en el Plan de Contingencia.

Se han desarrollado procedimientos referidos a:

a) Identificación, registro, reporte y gestión de incidentes.
b) Recuperación ante falla inesperada o sospecha de falla de componentes de hardware, software y datos.
c) Recuperación ante compromiso o sospecha de compromiso de la clave privada del certificador.

d) Continuidad de las operaciones en un entorno seguro luego de desastres.

Los procedimientos cumplen con lo establecido por el artículo 20 del Decreto Nº 182/19 en lo relativo a los servicios de infraestructura tecnológica prestados por un tercero.

5.8. - Plan de Cese de Actividades.

Se describen los requisitos y procedimientos a ser adoptados en caso de finalización de servicios del certificador o de una o varias de sus autoridades certificantes o de registro. Estos requerimientos son desarrollados en su Plan de Cese de Actividades.

Se han implementado procedimientos referidos a:

a) Notificación al ente licenciante, suscriptores, terceros usuarios, otros certificadores y otros usuarios vinculados.
b) Custodia de archivos y documentación e identificación de su custodio.

El responsable de la custodia de archivos y documentación cumple con idénticas exigencias de seguridad que las previstas para el certificador o su autoridad certificante o de registro que cesó.

Se contempla lo establecido por el artículo 44 de la Ley Nº 25.506 de Firma Digital en lo relativo a las causales de caducidad de la licencia. Asimismo, los procedimientos cumplen lo dispuesto por el artículo 20 del Decreto Nº 182/19, en lo relativo a los servicios de infraestructura tecnológica prestados por un tercero y las obligaciones establecidas en la presente resolución y sus correspondientes anexos.

6. - CONTROLES DE SEGURIDAD TÉCNICA.

Se describen las medidas de seguridad implementadas por el certificador para proteger las claves criptográficas y otros parámetros de seguridad críticos. Además, se incluyen los controles técnicos que se implementarán sobre las funciones operativas del certificador, Autoridades de Registro, repositorios, suscriptores.

6.1. Generación e instalación del par de claves criptográficas.

La generación e instalación del par de claves serán consideradas desde la perspectiva de las Autoridades Certificantes del Certificador, de las autoridades de registro y de los

suscriptores. Para cada una de estas entidades deberán abordarse los siguientes temas:

a) Responsables de la generación de claves.

b) Métodos de generación de claves, indicando si se efectúan por software o por hardware.

c) Métodos de entrega y distribución de la clave pública en forma segura.

d) Características y tamaños de las claves.

e) Controles de calidad de los parámetros de generación de claves.

f) Propósitos para los cuales pueden ser utilizadas las claves y restricciones para dicha utilización.

6.1.1. Generación del par de claves criptográficas.

Se describen los aspectos relativos a la generación del par de claves de las Autoridades Certificantes del Certificador, de las claves de los Oficiales de Registro de las Autoridades de Registro, y de las claves de los suscriptores. Se describe el tipo de soporte utilizado para la generación de claves. Se respeta lo establecido en el Anexo II Sección 2 respecto de generación del par de claves.

AC - BOX CUSTODIA FIRMA DIGITAL, luego del otorgamiento de la licencia por parte de la Autoridad de Aplicación para esta Política Única de Certificación, generará el par de claves criptográficas en un ambiente seguro con la participación de personal autorizado, sobre dispositivos criptográficos FIPS 140-2 Nivel 3. Para la generación del par de claves se utilizará el algoritmo RSA de 4096 bits.

En el caso de las AR, cada Oficial de Registro generará y almacenará su par de claves utilizando un dispositivo criptográfico homologado FIPS 140-2 Nivel 3 y utilizando el algoritmo RSA con un tamaño mínimo de 2048 bits.

Las claves criptográficas de los suscriptores son generadas y almacenadas por ellos. Los suscriptores generan sus claves mediante el algoritmo RSA con un tamaño mínimo de 2048 bits.

El par de claves del suscriptor de un certificado emitido en los términos de esta Política Única de Certificación debe ser generado de manera tal que su clave privada se encuentre bajo su exclusivo y absoluto control. El suscriptor es considerado titular del par de claves; como tal, está obligado a generarlas en un sistema confiable y a no revelar su clave privada a terceros bajo ninguna circunstancia.

6.1.2. - Entrega de la clave privada.

En todos los casos, se cumple con la obligación de abstenerse de generar, exigir o por cualquier otro medio tomar conocimiento o acceder a los datos de creación de firmas de los suscriptores (incluyendo los roles vinculados a las actividades de registro), establecido por artículo 21, inciso b) de la Ley Nº 25.506 y el artículo 21, inciso 3 del Anexo al Decreto Nº 182/2019..

6.1.3. - Entrega de la clave pública al emisor del certificado.

La clave pública del suscriptor del certificado es transferida a la **AC - BOX CUSTODIA FIRMA DIGITAL**, a través de la aplicación correspondiente, durante el proceso de solicitud de su certificado. La **AC - BOXCUSTODIA FIRMA DIGITAL** por su parte utilizará técnicas de "prueba de posesión" para determinar que los solicitantes se encuentran en posesión de la clave privada asociada a dicha clave pública.

El requerimiento de un certificado se emite en formato PKCS#10, o bien en el formato que lo reemplace en el futuro.

Los procesos de solicitud utilizan el formato PKCS#10 para implementar la "prueba de posesión", remitiendo los datos del solicitante y su clave pública dentro de una estructura firmada con su clave privada.

El procedimiento descripto asegura que:

- La clave pública no pueda ser cambiada durante la transferencia.
- Los datos recibidos por el Certificador se encuentran vinculados a dicha clave pública
- El remitente posee la clave privada que corresponde a la clave pública transferida.

6.1.4. - Disponibilidad de la clave pública del certificador.

El certificado del Certificador *y* su cadena de certificación se encuentran a disposición de los suscriptores *y* terceros usuarios en un repositorio en línea de acceso público a través de Internet, accesible a partir de Descargar Certificados - IdentidadDigital (boxcustodia.com)

6.1.5. Tamaño de claves.

Se definirá el tamaño de las claves criptográficas asociadas con los certificados emitidos según la Política Única de Certificación. Se deberá respetar lo establecido en el Anexo II Sección 2 respecto de las longitudes mínimas de las claves

La longitud de las claves criptográficas del certificado del Certificador es de 4096 bits.

La longitud de las claves criptográficas de los certificados de suscriptores emitidos por el Certificador es de 2048 bits como mínimo.

El algoritmo de firma utilizado es SHA-2 con RSA.

Las claves criptográficas que utilizan los certificados de servicios relacionados con la firma digital son de DOS MIL CUARENTA Y OCHO (2048) bits con algoritmo RSA como mínimo. En el caso particular de las autoridades de sello de tiempo, las claves criptográficas son de CUATRO MIL NOVENTA Y SEIS (4096) bits con algoritmo RSA como mínimo.

Las claves criptográficas que utilicen las autoridades de registro para realizar actividades tales como aprobar solicitudes, renovaciones, revocaciones y demás servicios de certificación son de DOS MIL CUARENTA Y OCHO (2048) bits con algoritmo RSA como mínimo.

6.1.6. - Generación de parámetros de claves asimétricas.

No se establecen condiciones especiales para la generación de parámetros de claves asimétricas más allá de los que corresponden con el algoritmo de generación RSA según su especificación técnica.

6.1.7. - Propósitos de utilización de claves (campo "KeyUsage" en certificados X.509 v.3).

Las claves criptográficas de los suscriptores de los certificados pueden ser utilizados para firmar digitalmente, para funciones de autenticación *y/o* para cifrado.

6.2. Protección de la clave privada y controles sobre los dispositivos criptográficos.

La protección de la clave privada debe ser considerada desde la perspectiva del certificador, de los repositorios, de las Autoridades de Registro *y* de los suscriptores,

siempre que sea aplicable. Para cada una de estas entidades deberán abordarse los siguientes temas:

a) Estándares utilizados para la generación del par de claves.
b) Número de personas involucradas en el control de la clave privada.
c) En caso de existir copias de resguardo de la clave privada, controles de seguridad establecida sobre ellas.
d) Procedimiento de almacenamiento de la clave privada en un dispositivo criptográfico.
e) Responsable de activación de la clave privada y acciones a realizar para su activación.
f) Duración del periodo de activación de la clave privada y procedimiento a utilizar para su desactivación.
g) Procedimiento de destrucción de la clave privada.
h) Requisitos aplicables al dispositivo criptográfico utilizado para el almacenamiento de las claves privadas.

6.2.1. - Controles *y* estándares para dispositivos criptográficos.

Para la generación y el almacenamiento de las claves criptográficas, AC - BOX CUSTODIA FIRMA DIGITAL, las Autoridades de Registro y los suscriptores que opten por un nivel Alto para sus certificados, utilizan los dispositivos referidos en el apartado 6.1.1.

Se respeta lo establecido en el Anexo II Sección 2 de la Resolución 946/2021 respecto de los estándares para dispositivos criptográficos.

La clave privada del suscriptor Persona Humana, Persona Jurídica y Aplicación es generada y almacenada, de la siguiente forma,

a) Por “hardware” sobre dispositivos criptográficos de propiedad del suscriptor;
b) Por “software”,
c) “Servicio de custodia centralizada de claves criptográficas”, que se encuentra integrado con los servicios de AC - BOX CUSTODIA FIRMA DIGITAL, cumpliendo los requisitos de seguridad correspondiente.

6.2.2. - Control "M de N" de clave privada.

Los controles empleados para la activación de las claves se basan en la presencia de M de N con M mayor a 2. Estos controles son desarrollados con mayor detalle en los documentos específicos.

6.2.3. - Recuperación de clave privada.

Ante una situación que requiera recuperar su clave privada, y siempre que ésta no se encuentre comprometida, el Certificador cuenta con procedimientos para su recuperación.

Esta sólo puede ser realizada por personal autorizado, sobre dispositivos criptográficos seguros y exclusivamente en el nivel de seguridad donde se realicen las operaciones críticas de la AC- BOX CUSTODIA FIRMA DIGITAL.

No se implementan mecanismos de resguardo y recuperación de las claves privadas de las AR y de los suscriptores. Estos deberán proceder a la revocación del certificado y a tramitar una nueva solicitud de emisión de certificado, si así correspondiere.

6.2.4. - Copia de seguridad de clave privada.

La AC - BOX CUSTODIA FIRMA DIGITAL genera una copia de seguridad de la clave privada del Certificador BOX CUSTODIA DE ARCHIVOS S.A. a través de un procedimiento que garantiza su integridad y confidencialidad. No se mantienen copias de las claves privadas de los suscriptores de certificados ni de los Oficiales de Registro.

6.2.5. - Archivo de clave privada.

Las copias de resguardo de la clave privada de la Autoridad Certificante BOX CUSTODIA DE ARCHIVOS S.A. son conservadas en lugares seguros, al igual que sus elementos de activación, bajo los niveles de seguridad requeridos por la normativa vigente.

BOX CUSTODIA DE ARCHIVOS S.A almacena las copias de reguardo de su clave privada a través de un procedimiento que garantiza su integridad y confidencialidad, conservándola en un lugar seguro, al igual que sus elementos de activación.

6.2.6. - Transferencia de claves privadas en dispositivos criptográficos.

El par de claves criptográficas de AC - BOX CUSTODIA FIRMA DIGITAL se genera y almacena en dispositivos criptográficos conforme a lo establecido en la presente Política, salvo en el caso de las copias de resguardo que también están soportados en dispositivos criptográficos homologados FIPS 140-2 nivel 3.

El par de claves criptográficas de las AR y de los suscriptores de certificados de nivel de seguridad Alto es almacenado en el mismo dispositivo criptográfico FIPS 140-2 nivel 3 donde se genera, no permitiendo su exportación.

6.2.7. -Almacenamiento de claves privadas en dispositivos criptográficos.

Las claves privadas de los suscriptores que tengan dispositivos criptográficos propios son generadas y almacenadas en esos dispositivos y estarán homologados como FIPS 140-2 nivel 3 y no permiten su exportación.

Las claves privadas de los suscriptores que utilizan el “Servicio de custodia centralizada de claves criptográficas” son generadas, almacenadas y utilizadas en dispositivos, validados como FIPS 140-2 nivel 3.

6.2.8. - Método de activación de claves privadas.

La clave privada de la **AC - BOX CUSTODIA FIRMA DIGITAL** se activa previa autenticación de los responsables de su control aplicándose un procedimiento seguro que requiere la participación de los poseedores de claves de activación según el control M de N, quienes validan las operaciones críticas, autorizando su ejecución por medio de llaves especiales que obran en su poder.

Los responsables de la activación de las claves privadas deberán identificarse frente al sistema según corresponda al rol asignado y en un orden determinado por medio de distintos mecanismos de autenticación ya sea llaves de seguridad, claves, etc.

Las Autoridades de Registro y los suscriptores de certificados que usen dispositivos criptográficos tienen acceso a su clave privada personal a través de una contraseña de acceso al dispositivo criptográfico y la contraseña de la clave privada.

6.2.9. - Método de desactivación de claves privadas.

La desactivación de la clave privada de la AC - BOX CUSTODIA FIRMA DIGITAL se lleva adelante mediante el proceso de desactivación de partición previa autorización de los responsables de su control a través de un procedimiento seguro y cuando se requiera utilizar temporalmente un equipamiento de respaldo o se realicen tareas de mantenimiento.

6.2.10. - Método de destrucción de claves privadas.

Se especifican las políticas a seguir para la destrucción segura de la clave privada y de sus copias de seguridad ante cualquier hecho que motivara el final de la vida útil de un certificado, tales como su revocación o expiración. Estos controles son desarrollados con mayor detalle en los documentos específicos.

En caso de cese de actividades de la AC - BOX CUSTODIA FIRMA DIGITAL o de compromiso de su clave privada, se destruirán los dispositivos de soporte de su clave privada mediante un procedimiento que garantice su destrucción total y segura según el último estado del arte disponible a la fecha.

6.2.11. - Requisitos de los dispositivos criptográficos.

AC - BOX CUSTODIA FIRMA DIGITAL, luego del otorgamiento de la licencia por parte de la Autoridad de Aplicación para esta Política Única de Certificación, generará el par de claves criptográficas en un ambiente seguro con la participación de personal autorizado, sobre dispositivos criptográficos FIPS 140-2 Nivel 3. Para la generación del par de claves se utilizará el algoritmo RSA de 4096 bits.

En el caso de las AR, cada Oficial de Registro generará y almacenará su par de claves utilizando un dispositivo criptográfico homologado FIPS 140-2 Nivel 3 y utilizando el algoritmo RSA con un tamaño mínimo de 2048 bits.

Las claves criptográficas de los suscriptores son generadas y almacenadas por ellos, de acuerdo con los niveles de seguridad establecidos en el apartado 1.3.1. En el caso que se utilicen dispositivos criptográficos, estos deberán ser homologados FIPS 140-2 Nivel 3. Los suscriptores generan sus claves mediante el algoritmo RSA con un tamaño mínimo de 2048 bits.

La capacidad del módulo criptográfico utilizado por el Servicio de custodia centralizada de claves criptográficas es expresada en cumplimiento como mínimo del estándar FIPS 140- 2 nivel 3

6.3. - Otros aspectos de administración de claves.

6.3.1. ·Archivo permanente de la clave pública.

Los certificados emitidos a suscriptores y a los Oficiales de Registro como así también el de la AC - BOX CUSTODIA FIRMA DIGITAL son almacenados bajo un esquema de redundancia y respaldados en forma periódica sobre dispositivos de solo lectura, lo cual, sumado a la firma de los mismos, garantiza su integridad.

Los certificados se almacenan en formato estándar bajo codificación internacional DER.

Las políticas y controles de seguridad implementados para recuperar la clave pública archivada, incluyendo el software y hardware, se hallan descriptos en el Plan de Contingencia.

6.3.2. - Período de uso de clave pública y privada.

Las claves privadas correspondientes a los certificados emitidos por el certificador podrán ser utilizadas por los suscriptores únicamente durante el período de validez de los certificados. Ese período tiene una validez de DOS (2) años para todos los certificados de persona humana o jurídica. Las correspondientes claves públicas podrán ser utilizadas durante el período establecido por las normas legales vigentes, a fin de posibilitar la verificación de las firmas generadas durante su período de validez, según se establece en el apartado anterior.

El par de claves criptográficas del certificado de AC - BOX CUSTODIA FIRMA DIGITAL tiene una validez de DIEZ (10) años

6.4. - Datos de activación.

Se entiende por datos de activación, a diferencia de las claves, a los valores requeridos para la operatoria de los dispositivos criptográficos y que necesitan estar protegidos.

Se establecen medidas suficientes de seguridad para proteger los datos de activación requeridos para la operación de los dispositivos criptográficos de los usuarios de certificados.

6.4.1. - Generación e instalación de datos de activación.

Los datos de activación del dispositivo criptográfico del certificador tienen un control "M de “N" en base a "M" Poseedores de claves de activación, que deben estar presentes de un total de "N" Poseedores posibles.

Ni el Certificador ni las AR implementan mecanismos de respaldo de contraseñas y credenciales de acceso a las claves privadas de los suscriptores u Oficiales de Registro o a sus dispositivos criptográficos, si fuera aplicable.

La AC - BOX CUSTODIA FIRMA DIGITAL establece medidas de seguridad para proteger adecuadamente los datos de activación de la clave privada de los suscriptores de certificados contra usos no autorizados.

6.4.2. - Protección de los datos de activación.

Las Autoridades de Registro y los Suscriptores son responsables de la custodia de sus respectivos dispositivos criptográficos y de la no divulgación de la contraseña de acceso del dispositivo criptográfico ni de la contraseña de la clave privada.

Ni BOX CUSTODIA DE ARCHIVOS S.A., ni la Autoridad de Registro Central, ni las Autoridades de Registro Delegadas implementan mecanismos de respaldo de las contraseñas de la clave privada ni de la contraseña de acceso del dispositivo criptográfico de Autoridades de Registro ni de Suscriptores.

La AC - BOX CUSTODIA FIRMA DIGITAL establece los siguientes procedimientos de control sobre su clave privada:

a) Se establecen al menos DOS (2) responsables de su control.
b) Se establece un procedimiento de activación de clave privada.
c) Se establece un procedimiento de destrucción de la clave privada.

Los datos de activación de la clave privada de la AC - BOX CUSTODIA FIRMA DIGITAL están protegidos por mecanismos de seguridad implementados en el nivel 6 de máxima seguridad.

6.4.3. - Otros aspectos referidos a los datos de activación.

Es responsabilidad de los Oficiales de Registro y de los suscriptores de certificados emitidos por la AC - BOX CUSTODIA FIRMA DIGITAL, elegir contraseñas fuertes para la protección de sus claves privadas y para el acceso a los dispositivos criptográficos que utilicen, si fuera aplicable.

6.5. Controles de seguridad informática.

6.5.1. Requisitos Técnicos específicos.

Se establecen los requisitos de seguridad referidos al equipamiento y al software del certificador, cuyo detalle se encuentra en el Manual de Procedimientos.

Dichos requisitos se vinculan con los siguientes aspectos:

a) Control de acceso a los servicios y roles afectados al proceso de certificación.
b) Separación de funciones entre los roles afectados al proceso de certificación.
c) Identificación y autenticación de los roles afectados al proceso de certificación.
d) Utilización de criptografía para las sesiones de comunicación y bases de datos.
e) Archivo de datos históricos y de auditoría del certificador y usuarios.
f) Registro de eventos de seguridad.
g) Prueba de seguridad relativa a servicios de certificación.
h) Mecanismos confiables para identificación de roles afectados al proceso de certificación.

i) Mecanismos de recuperación para claves y sistema de certificación.

Estas funciones pueden ser provistas por el sistema operativo, o bien a través de una combinación del sistema operativo, software de certificación y controles físicos.
Las funcionalidades mencionadas son provistas a través de una combinación del sistema operativo, software aplicativo y controles físicos.
La descripción de los controles de seguridad establecidos sobre los servidores del Certificador se incluye en el Plan de Seguridad.

6.5.2.- Requisitos de seguridad computacional.

El certificador cumple con las siguientes calificaciones de seguridad sobre los productos en los que se basa la implementación:
Los servidores que conforman la Autoridad Certificante se encuentran alojados dentro del datacenter de la **AC - BOX CUSTODIA FIRMA DIGITAL**, en el de Área Máxima de Seguridad (AMS), construida para tal fin, con los estándares requeridos para este tipo de ambientes.
Los módulos criptográficos de hardware (HSM) utilizados por AC - BOX CUSTODIA FIRMA DIGITAL están certificado por el NIST (National lnstitute of Standards and Technology) sobre la base del Estándar FIPS 140-2 Nivel 3.
Las aplicaciones del núcleo de la PKI de AC - BOX CUSTODIA FIRMA DIGITAL se basan en servicios adaptados de la solución EJBCA, corriendo sobre servidores Linux redundantes. Esta solución de software libre es totalmente modular y escalable.
Los dispositivos criptográficos utilizados por las AR están certificados por NIST (National lnstitute of Standards and Technology) sobre la base del Estándar FIPS 140-2 Nivel 3.
Los dispositivos criptográficos utilizados por suscriptores de nivel de seguridad Alto están certificados por NIST (National lnstitute of Standards and Technology) sobre la base del Estándar FIPS 140-2 Nivel 3.

6.6.- Controles Técnicos del ciclo de vida de los sistemas.

BOX CUSTODIA DE ARCHIVOS S.A. mantiene el control de los equipos y de la documentación de la configuración de los sistemas que prevén, registrándolo toda modificación o actualización a cualquiera de ellos.

El esquema de seguridad física del SMS de la Autoridad Certificante AC - BOX CUSTODIA FIRMA DIGITAL previene que terceros no autorizados puedan ingresar indebidamente a sus instalaciones. El control periódico de integridad del sistema de la Autoridad Certificante AC - BOX CUSTODIA FIRMA DIGITAL advierte sobre cualquier cambio realizado, lo identifica y permite comprobar su validez.

6.6.1. - Controles de desarrollo de sistemas.

El Certificador cumple con procedimientos específicos para el diseño y desarrollo de sistemas entre los que se encuentran:

- Separación de ambientes de desarrollo, prueba y producción
- Control de versiones para los componentes desarrollados

6.6.2. - Controles de gestión de seguridad.

Se documenta y controla la configuración del sistema, así como toda modificación o actualización, habiéndose implementado un método de detección de modificaciones no autorizadas. Existen controles respecto a la integridad del sistema de archivos de la AC - BOX CUSTODIA FIRMA DIGITAL que permiten controlar si hubo alteraciones no autorizadas.

6.6.3. - Controles de seguridad del ciclo de vida del software.

No aplica.

6.7.- Controles de seguridad de red.

Los servicios que provee AC - BOX CUSTODIA FIRMA DIGITAL que se encuentran conectados a una red de comunicación pública, son protegidos por la tecnología apropiada que garantiza su seguridad. Los análisis se realizaran como mínimo cada SEIS (6) MESES.

6.8. - Certificación de fecha y hora.

La AC - BOX CUSTODIA FIRMA DIGITAL brinda el servicio de Sellos de Tiempo para la certificación de fecha y hora. Este servicio está basado en la especificación de los

estándares RFC 3161 - "Internet X 509 Public Key lnfrastructure (TSP), ETSI TS 102 023, Time-Stamp Protocol, Electronic Signatures and lnfrastructures (ESI) Policy requirements for time-stamping authorities,
ETSI TS 101. 861, "Time stamping profile" y a su especificación equivalente RFC 3628 – “Requirements for time-stamping authorities” y está sincronizado con una fuente de hora confiable.

6.9. – Servicio de emisión de Sello de Competencia y/o Atributo

En caso de corresponder, se indicarán las especificaciones de los servicios de emisión de sellos de competencia y/o atributo prestados por el Certificador, según lo establecido en el RFC 5755 “An Internet Attribute Certificate Profile for Authorization”.

7. - PERFILES DE CERTIFICADOS Y DE LISTAS DE CERTIFICADOS REVOCADOS.

Los certificados emitidos por el Certificador respaldados por esta Política Única de Certificación cumplen con lo establecido en la especificación ITU X509 versión 3 (ISO/IEC 9594-8), adoptada como Estándar Técnico de la Infraestructura de Firma Digital de la República Argentina.
AC - BOX CUSTODIA FIRMA DIGITAL adhiere a las recomendaciones de los siguientes documentos en relación al perfil de los certificados:

- RFC 3739 "Internet X.509 Public Key lnfrastructure Qualified Certificates Profile" [RFC3739].
- RFC 5280 "Internet X.509 Public Key lnfrastructure Certificate and Certificate Revocation List (CRL) Profile" [RFC5280].

7 .1.- Perfil del certificado.

Todos los certificados serán emitidos conforme con lo establecido en la especificación ITU X.509 versión 3 o en su defecto, determine el Ente Licenciante, y deben cumplir con las indicaciones establecidas en el apartado 2 del Anexo IV - Perfiles de los Certificados y de las Listas de Certificados Revocados de la Resolución 946/2021.

a) Perfil del certificado de la persona humana.

Los siguientes campos se encuentran presentes en los certificados emitidos a Personas Humanas por la AC- BOX CUSTODIA FIRMA DIGITAL:

Campos Atributos Extensiones	**Valor/OID**	**Observaciones**
Versión (Versión)	2	Corresponde a versión 3
Número de serie (SerialNumber)	hasta 20 octetos 2.5.4.5	Entero positivo asignado unívocamente por la AC – BOX CUSTODIA FIRMA DIGITAL a cada certificado.
Algoritmo de Firma (Signature Algorithm)	Sha2RSA 1.2.840.113549.1.1.11	Algoritmo usado por el certificador para firmar.
Nombre distintivo del emisor (Issuer)		
commonName	AC- BOX CUSTODIA FIRMA DIGITAL 2.5.4.3	Identificación de la Autoridad Certificante
serialNumber	CUIT 30704582370 2.5.4.5	CUIT del Certificador
organizationName	BOX CUSTODIA DE ARCHIVOS S.A 2.5.4.10	Denominación del Certicador Licenciado
stateOrProvinceName	Ciudad Autónoma de Buenos Aires 2.5.4.8	Ciudad en la que se encuentra el Certificador.
countryName	AR 2.5.4.6	País del Certificador Licenciado
Validez (desde, hasta) (Validity (Not before,not after))		
notBefore	<fecha y hora de emisión UTC> yyyy/mm/ddhh:mm:ss huso-horario	Fecha y hora en que el periodo de vigencia del certificado comienza.
notAfter	<fecha y hora de emisión UTC+ periodo> yyyy/mm/ddhh:mm:ss	Fecha y hora en que el periodo de vigencia del certificado termina.

		El periodo para este perfil es 2 (dos) años como máximo.
Nombre distintivo del suscriptor (Subject)		
commonName	<Nombre y Apellidos> 2.5.4.3	Datos que surgen del Documento Nacional de Identidad presentado por titular
serialNumber	CUIL <Número de Identificacion> o PA <Pasaporte y código de país> o EX <Número u tipo de documento extranjero> 2.5.4.5	Número de identificación tributaria: CUIL de la persona humana En caso de extranjeros: “PA” [país]: Número de Pasaporte y código de país emisor. El atributo [país] Está codificado según el estándar [ISO3166] de DOS (2) caracteres. “EX” [país]: Número y tipo de documento extranjero aceptado en virtud de acuerdos internacionales. El atributo [país] está codificado según el estándar [ISO3166] de DOS (2) caracteres.
countryName	AR 2.5.4.6	Código de País de acuerdo a ISO3166
Clave pública del suscriptor (SubjectPublic Key Info)		
publickeyalgorithm	RSA 1.2.840.11.35.49.1.1.1	Tipo de algoritmo de clave pública utilizado.
publickeylength	2048 bits	Longitud de la clave pública del suscriptor.
Clave pública del suscriptor (SubjectPublicKey Info)	<Clave pública del suscriptor>	Valor de la clave pública del suscriptor

Restricciones básicas (Basic constraints)	Tipo de asunto = Entidad final pathLengthConstraint = Null 2.5.29.19	Define el certificado como de entidad final.
Usos de clave (Key Usage)	digitalSignature = 1 nonRepudiation = 1 keyEncipherment = 1 dataEncipherment = 1 keyAgreement = 1 keyCertSign = 0 cRLSign = 0 encipherOnly = 1 decipherOnly = 1 2.5.29.15	Propósito para el cual será utilizada la clave contenida en el certificado
Identificador de clave del Suscriptor (Subject Key Identifier)	Valor de hash de 32 bytes	Contiene un hash de 32 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints)	Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints) [1]Punto de distribución CRL Dirección URL= https://pki.boxcustodia.com/crl 2.5.29.31	URL del punto de distribución
Política de Certificación (CertificatePolicies)	OID de la Política de Certificación de BOX CUSTODIA DE ARCHIVOS = 2.16.32.1.1.6 Información de la Política de Certificación: Ubicación (URI): https://pkidocs.boxcustodia.com/acdocs/Politica_Unica.pdf Texto de aviso = Certificado emitido por un Certificador Licenciado en el marco de Ley 25.506	OID de la Política de Certificación de BOX CUSTODIA DE ARCHIVOS S.A., otorgado por la ONTI, URI de la Política de Certificación y texto obligatorio para los certificados de la IFDRA.
Identificador de la Clave de la Autoridad Certificante (AuthorityKeyIdentifier)	Valor de hash de 20 bytes 2.5.29.35	Contiene un hash de 20 bytes del atributo clave pública del AC BCFD que emitió el certificado.

Uso Extendido de Clave (Extended Key Usage)	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4)	Usos adicionales de la clave pública a los enumerados en el campo keyUsage.
Nombres Alternativos del Suscriptor (SubjectAlternativeName)	<Dirección de correo electrónico> 2.5.29.17	Dirección de mail del suscriptor verificada por circuito seguro compatible con RFC 822.(Campo optativo)
Acceso Información Emisor (AuthorityInformation Access)	CA Issuer: URL http://pkidocs.boxcustodia.com/accerts/06.crt OCSP: https://ocsp.pki.boxcustodia.com/	URL de la información para acceder al certificado de AC – BOX CUSTODIA DE FIRMA DIGITAL y al servicio de OCSP.
QCStatement	OID= 2.16.32.1.10.1 (claves generadas por software) OID=2.16.32.1.10.2.1, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 1. OID=2.16.32.1.10.2.2, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 2. OID= 2.16.32.1.10.2.3 (claves generadas por disp. FIPS 140-2 nivel 3)	Declaración del certificado calificado.

b) Perfil del certificado de la Personas Jurídicas

Campos Atributos Extensiones	**Valor/OID**	**Observaciones**
Versión (Version)	2	Corresponde a versión 3

Número de serie (SerialNumber)	hasta 20 octetos 2.5.4.5	Entero positivo asignado unívocamente por la AC – BOX CUSTODIA FIRMA DIGITAL a cada certificado.
Algoritmo de Firma (Signature Algorithm)	Sha2RSA 1.2.840.113549.1.1.11	Algoritmo usado por el certificador para firmar.
Nombre distintivo del emisor (Issuer)		
commonName	AC- BOX CUSTODIA FIRMA DIGITAL 2.5.4.3	Identificación de la Entidad Certificante
serialNumber	CUIT 30704582370 2.5.4.5	CUIT del Certificador
organizationName	BOX CUSTODIA DE ARCHIVOS S.A 2.5.4.10	Denominación del Certificador Licenciado
stateOrProvinceName	Ciudad Autónoma de Buenos Aires 2.5.4.8	Ciudad en la que se encuentra el Certificador.
countryName	AR 2.5.4.6	País del Certificador Licenciado
Validez (desde, hasta) (Validity (Not before,not after))		
notBefore	<fecha y hora de emisión UTC> yyyy/mm/ddhh:mm:ss huso-horario	Fecha y hora en que el periodo de vigencia del certificado comienza.
notAfter	<fecha y hora de emisión UTC+ periodo> yyyy/mm/ddhh:mm:ss	Fecha y hora en que el periodo de vigencia del certificado termina. El periodo para este perfil es 2 (dos) años como máximo.
Nombre distintivo del suscriptor (Subject)		
commonName	Nombre de la persona jurídica 2.5.4.3	Denominación de la Persona Jurídica
organizationName	Nombre de la organización 2.5.4.10	Nombre de la Persona Jurídica Pública o Privada.

organizationUnitName	Unidad Operativa del Suscriptor 2.5.4.11	Denominación de la Unidad Operativa del relacionada con el Suscriptor.
serialNumber	CUIT <Número de CUIT> 2.5.4.5	CUIT de la Persona Jurídica
countryName	AR 2.5.4.6	
Clave Pública del suscriptor (SubjectPublic Key Info)		
Publickeyalgorithm	RSA 1.2.840.11.35.49.1.1.1	Tipo de algoritmo de clave pública utilizado
Publickeylength	2048 bits	Longitud de la clave pública del suscriptor
SubjectPublicKey Info	<Clave pública del suscriptor>	Valor de la clave pública del suscriptor.
Restricciones básicas (Basic Constraints)	Tipo de asunto = Entidad final pathLengthConstraint = Null 2.5.29.19	Define el certificado como de entidad final
Usos de clave (Key Usage)	digitalSignature = 1 nonRepudiation = 1 keyEncipherment = 1 dataEncipherment = 1 keyAgreement = 1 keyCertSign = 0 cRLSign = 0 encipherOnly = 1 decipherOnly = 1 2.5.29.15	Propósito para el cual será utilizada la clave contenida en el certificado
Identificador de clave del Suscriptor (Subject Key Identifier)	Valor de hash de 32 bytes	Contiene un hash de 32 bytes del atributo clave pública del suscriptor
untos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints)	Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints) [1]Punto de	URL del punto de distribución

	distribución CRL Dirección URL= https://pki.boxcustodia.com/crl 2.5.29.31	
Política de Certificación (CertificatePolicies)	OID de la Política de Certificación de BOX CUSTODIA DE ARCHIVOS = 2.16.32.1.1.6 Información de la Política de Certificación: Ubicación (URI): https://pkidocs.boxcustodia.com/acdocs/Politica_Unica.pdf Texto de aviso = Certificado emitido por un Certificador Licenciado en el marco de Ley 25.506	OID de la Política de Certificación de BOX CUSTODIA DE ARCHIVOS S.A., otorgado por la ONTI, URI de la Política de Certificación y texto obligatorio para los certificados de la IFDRA.
Identificador de la Clave de la Autoridad Certificante	Valor de hash de 20 bytes 2.5.29.35	Contiene un hash de 20 bytes del atributo clave pública del AC BCFD que emitió el certificado.
Uso Extendido de Clave (Extended Key Usage)	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4) 2.5.29.37	Usos adicionales de la clave pública a los enumerados en el campo keyUsage
Nombres Alternativos del Suscriptor (SubjectAlternativeName)		
commonName	Nombres y Apellidos 2.5.4.3	Datos de la Persona Humana a cargo de la custodia de la clave privada
serialNumber	<Tipo><Número de documento> 2.5.4.5	Datos CUIL del poseedor de las claves
Title	<Nombre de la función> 2.5.4.12	Relación que vincula a la Persona Humana con la Persona Jurídica
Acceso Información Emisor (AuthorityInformation Access)	CA Issuer: URL http://pkidocs.boxcustodia.com/accerts/06.crt OCSP: https://ocsp.pki.boxcustodia.com/	URL de la información para acceder al certificado de AC – BOX CUSTODIA DE FIRMA DIGITAL y al servicio de OCSP.

QCStatement	OID= 2.16.32.1.10.1 (claves generadas por software) OID=2.16.32.1.10.2.1, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 1. OID=2.16.32.1.10.2.2, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 2. OID= 2.16.32.1.10.2.3 (claves generadas por disp. FIPS 140-2 nivel 3)	Declaración del certificado calificado.

c) Perfil del certificado para Aplicaciones.

Los siguientes campos se encuentran presentes en los certificados de aplicaciones emitidos por la AC -BOX CUSTODIA FIRMA DIGITAL.

Campos Atributos Extensiones	**Valor/OID**	**Observaciones**
Versión (Version)	2	Corresponde a versión 3
Número de serie (SerialNumber)	hasta 20 octetos 2.5.4.5	Entero positivo asignado unívocamente por la AC – BOX CUSTODIA FIRMA DIGITAL a cada certificado.
Algoritmo de Firma (Signature Algorithm)	Sha2RSA 1.2.840.113549.1.1.11	Algoritmo usado por el certificador para firmar.
Nombre distintivo del emisor (Issuer)		
commonName	AC- BOX CUSTODIA FIRMA DIGITAL 2.5.4.3	Identificación de la Entidad Certificante
serialNumber	CUIT 30704582370 2.5.4.5	CUIT del Certificador

organizationName	BOX CUSTODIA DE ARCHIVOS S.A 2.5.4.10	Denominación del Certificador Licenciado
stateOrProvinceName	Ciudad Autónoma de Buenos Aires 2.5.4.8	Ciudad en la que se encuentra el Certificador.
countryName	AR 2.5.4.6	País del Certificador Licenciado
Validez (desde, hasta) (Validity (Not before,not after))		
notBefore	<fecha y hora de emisión UTC> yyyy/mm/ddhh:mm:ss huso-horario	Fecha y hora en que el periodo de vigencia del certificado comienza.
notAfter	<fecha y hora de emisión UTC+ periodo> yyyy/mm/ddhh:mm:ss	Fecha y hora en que el periodo de vigencia del certificado termina. El periodo para este perfil es 3 (tres) años como máximo.
Nombre distintivo del suscriptor (Subject)		
commonName	Denominación de la aplicación 2.5.4.3	Denominación de la aplicación
organizationName	O=nombre dela Persona Jurídica responsable de la aplicación 2.5.4.10	Nombre de la Persona jurídica responsable de la aplicación o el servicio.
organizationUnitName	OU=Unidad Operativa relacionada con la aplicación 2.5.4.11	Contiene las Unidades operativas relacionadas con el servicio o aplicación, en caso de existir, pudiendo utilizarse varias instancias de este atributo de ser necesario.
serialNumber	SN= CUIT <Número de la Persona Jurídica responsable de la aplicación> 2.5.4.5	<CUIT> <Número de identificación tributaria de la Persona Jurídica responsable de la aplicación>

countryName	C=AR 2.5.4.6	
Clave Pública del suscriptor (SubjectPublic Key Info)		
Publickeyalgorithm	RSA 1.2.840.11.35.49.1.1.1	Tipo de algoritmo de clave pública utilizado
Publickeylength	2048 bits	Longitud de la clave pública del suscriptor
SubjectPublicKey Info	<Clave pública del suscriptor>	Valor de la clave pública del suscriptor.
Restricciones básicas (Basic Constraints)	Tipo de asunto = Entidad final PathLengthConstraint = Null 2.5.29.19	Define el certificado como de entidad final
Usos de clave (Key Usage)	digitalSignature = 1 nonRepudiation = 1 keyEncipherment = 1 dataEncipherment = 1 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0 2.5.29.15	Propósito para el cual será utilizada la clave contenida en el certificado
Identificador de clave del Suscriptor (Subject Key Identifier)	Valor de hash de 32 bytes 2.5.29.14	Contiene un hash de 32 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints)	Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints) [1]Punto de distribución CRL Dirección URL= https://pki.boxcustodia.com/crl 2.5.29.31	URL del punto de distribución

Política de Certificación (CertificatePolicies)	OID de la Política de Certificación de BOX CUSTODIA DE ARCHIVOS = 2.16.32.1.1.6 Información de la Política de Certificación: Ubicación (URI): https://pkidocs.boxcustodia.com/acdocs/Politica_Unica.pdf Texto de aviso = Certificado emitido por un Certificador Licenciado en el marco de Ley 25.506	OID de la Política de Certificación de BOX CUSTODIA DE ARCHIVOS S.A., otorgado por la ONTI, URI de la Política de Certificación y texto obligatorio para los certificados de la IFDRA.
Identificador de la Clave de la Autoridad Certificante	Valor de hash de 32 bytes 2.5.29.35	Contiene un hash de 32 bytes del atributo clave pública del AC BCFD que emitió el certificado.
Uso Extendido de Clave (Extended Key Usage)	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4) 2.5.29.37	Usos adicionales de la clave pública a los enumerados en el campo keyUsage
Acceso Información Emisor (AuthorityInformation Access)	CA Issuer: URL http://pkidocs.boxcustodia.com/accerts/06.crt OCSP: https://ocsp.pki.boxcustodia.com/	URL de la información para acceder al certificado de AC – BOX CUSTODIA DE FIRMA DIGITAL y al servicio de OCSP.
QCStatement	OID= 2.16.32.1.10.1 (claves generadas por software) OID=2.16.32.1.10.2.1, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 1. OID=2.16.32.1.10.2.2, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 2. OID= 2.16.32.1.10.2.3 (claves generadas por disp. FIPS 140-2 nivel 3)	Declaración del certificado calificado.

d) Perfil del certificado para Autoridad Sello de Competencia

Campos Atributos Extensiones	**Valor/OID**	**Observaciones**
Versión (Version)	2	Corresponde a versión 3
Número de serie (SerialNumber)	hasta 20 octetos 2.5.4.5	Entero positivo asignado unívocamente por la AC – BOX CUSTODIA FIRMA DIGITAL a cada certificado.
Algoritmo de Firma (Signature Algorithm)	Sha2RSA 1.2.840.113549.1.1.11	Algoritmo usado por el certificador para firmar.
Nombre distintivo del emisor (Issuer)		
commonName	AC- BOX CUSTODIA FIRMA DIGITAL 2.5.4.3	Identificación de la Entidad Certificante
serialNumber	CUIT 30704582370 2.5.4.5	CUIT del Certificador
organizationName	BOX CUSTODIA DE ARCHIVOS S.A 2.5.4.10	Denominación del Certificador Licenciado
stateOrProvinceName	Ciudad Autónoma de Buenos Aires 2.5.4.8	Ciudad en la que se encuentra el Certificador.
countryName	AR 2.5.4.6	País del Certificador Licenciado
Validez (desde, hasta) (Validity (Not before,not after))		
notBefore	<fecha y hora de emisión UTC> yyyy/mm/ddhh:mm:ss huso-horario	Fecha y hora en que el periodo de vigencia del certificado comienza.
notAfter	<fecha y hora de emisión UTC+ periodo> yyyy/mm/ddhh:mm:ss	Fecha y hora en que el periodo de vigencia del certificado termina. El periodo para este perfil es 2 (dos) años como máximo.
Nombre distintivo del suscriptor (Subject)		

commonName	< nombre de la Autoridad de Competencia > 2.5.4.3	Indica el nombre de la Autoridad de Competencia
serialNumber	<CUIT> <Número de CUIT> 2.5.4.5	CUIT de la Persona Jurídica pública o privada
organizationName	<Responsable del servicio> 2.5.4.10	Nombre de la Persona Jurídica Pública o Privada responsable del servicio.
organizationUnitName	<Unidad operativa> 2.5.4.11	Nombre de la unidad operativa relacionada con el suscriptor
countryName	AR 2.5.4.6	
Clave Pública del suscriptor		
Publickeyalgorithm	RSA 1.2.840.11.35.49.1.1.1	Tipo de algoritmo de clave pública utilizado
Publickeylength	4096 bits	Longitud de la clave pública del suscriptor
SubjectPublicKey Info	<Clave pública del suscriptor>	Valor de la clave pública del suscriptor.
Restricciones básicas (Basic Constraints)	Tipo de asunto = Entidad final pathLengthConstraint = Null 2.5.29.19	Define el certificado como de entidad final
Usos de clave (Key Usage)	digitalSignature = 1 nonRepudiation = 1 keyEncipherment = 0 dataEncipherment =0 keyAgreement = 0 keyCertSign = 1 cRLSign = 0 encipherOnly = 0	Propósito para el cual será utilizada la clave contenida en el certificado

	decipherOnly = 0 2.5.29.15	
Identificador de clave del Suscriptor (Subject Key Identifier)	Valor de hash de 32 bytes	Contiene un hash de 32 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints)	Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints) [1]Punto de distribución CRL Dirección URL= https://pki.boxcustodia.com/crl 2.5.29.31	URL del punto de distribución
Política de Certificación (CertificatePolicies)	OID de la Política de Certificación de BOX CUSTODIA DE ARCHIVOS = 2.16.32.1.1.6 Información de la Política de Certificación: Ubicación (URI): https://pkidocs.boxcustodia.com/acdocs/Politica_Unica.pdf Texto de aviso = Certificado emitido por un Certificador Licenciado en el marco de Ley 25.506	OID de la Política de Certificación de BOX CUSTODIA DE ARCHIVOS S.A., otorgado por la ONTI, URI de la Política de Certificación y texto obligatorio para los certificados de la IFDRA.
Identificador de la Clave de la Autoridad Certificante	Valor de hash de 32 bytes 2.5.29.35	Contiene un hash de 32 bytes del atributo clave pública del AC BCFD que emitió el certificado.
Uso Extendido de Clave (Extended Key Usage)	OCSPSigning (1.3.6.1.5.5.7.3.9) Autenticación del cliente (1.3.6.1.5.5.7.3.2) 2.5.29.37	Usos adicionales de la clave pública a los enumerados en el campo keyUsage
Acceso Información Emisor (AuthorityInformation Access)	CA Issuer: URL http://pkidocs.boxcustodia.com/accerts/06.crt OCSP: https://ocsp.pki.boxcustodia.com/	URL de la información para accede al certificado de ACBOX CUSTODIA FIRMA DIGITAL y al servicios

QCStatement	OID= 2.16.32.1.10.2.3 (claves generadas por disp. FIPS 140-2 nivel 3)	Declaración del certificado calificado

e) Perfil del certificado para Autoridad de Sello de Tiempo.

Campos Atributos Extensiones	**Valor/OID**	**Observaciones**
Versión (Version)	2	Corresponde a versión 3
Número de serie (SerialNumber)	hasta 20 octetos 2.5.4.5	Entero positivo asignado unívocamente por la AC – BOX CUSTODIA FIRMA DIGITAL a cada certificado.
Algoritmo de Firma (Signature Algorithm)	Sha2RSA 1.2.840.113549.1.1.11	Algoritmo usado por el certificador para firmar.
Nombre distintivo del emisor (Issuer)		
commonName	AC- BOX CUSTODIA FIRMA DIGITAL 2.5.4.3	Identificación de la Entidad Certificante
serialNumber	CUIT 30704582370 2.5.4.5	CUIT del Certificador
organizationName	BOX CUSTODIA DE ARCHIVOS S.A 2.5.4.10	Denominación del Certicador Licenciado
stateOrProvinceName	Ciudad Autónoma de Buenos Aires 2.5.4.8	Ciudad en la que se encuentra el Certificador.
countryName	AR 2.5.4.6	País del Certificador Licenciado
Validez (desde, hasta) (Validity (Not before,not after))		
notBefore	<fecha y hora de emisión UTC> yyyy/mm/ddhh:mm:ss huso-horario	Fecha y hora en que el periodo de vigencia del certificado comienza.
notAfter	<fecha y hora de emisión UTC+ periodo> yyyy/mm/ddhh:mm:ss	Fecha y hora en que el periodo de vigencia del certificado termina.

		El periodo para este perfil es 2 (dos) años como máximo.
Nombre distintivo del suscriptor (Subject)		
commonName	<Nombre del Servicio> 2.5.4.3	Denominación del servicio de emisión del Sello de Tiempo
serialNumber	<CUIT> <Número de CUIT> 2.5.4.5	CUIT de la Persona Jurídica pública o privada
organizationName	<Responsable del Servicio> 2.5.4.10	Nombre de la Persona Jurídica Pública o Privada responsable del servicio.
organizationUnitName	<Unidad operativa> 2.5.4.11	Nombre de la unidad operativa relacionada con el suscriptor
countryName	AR 2.5.4.6	
Clave Pública del suscriptor		
Publickeyalgorithm	RSA 1.2.840.11.35.49.1.1.1	Tipo de algoritmo de clave pública utilizado
Publickeylength	2048 bits	Longitud de la clave pública del suscriptor
SubjectPublicKey Info	<Clave pública del suscriptor>	Valor de la clave pública del suscriptor.
Restricciones básicas (Basic Constraints)	Tipo de asunto = Entidad final pathLengthConstraint = Null 2.5.29.19	Define el certificado como de entidad final
Usos de clave (Key Usage)	digitalSignature = 1 nonRepudiation = 1 keyEncipherment = 0 dataEncipherment =0 keyAgreement = 0 keyCertSign = 0 cRLSign = 0	Propósito para el cual será utilizada la clave contenida en el certificado

	encipherOnly = 0 decipherOnly = 0 2.5.29.15	
Identificador de clave del Suscriptor (Subject Key Identifier)	Valor de hash de 32 bytes	Contiene un hash de 32 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints)	Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints) [1]Punto de distribución CRL Dirección URL= https://pki.boxcustodia.com/crl 2.5.29.31	URI del punto de distribución
Política de Certificación (CertificatePolicies)	OID de la Política de Certificación de BOX CUSTODIA DE ARCHIVOS = 2.16.32.1.1.6 Información de la Política de Certificación: Ubicación (URI): https://pkidocs.boxcustodia.com/acdocs/Politica_Unica.pdf Texto de aviso = Certificado emitido por un Certificador Licenciado en el marco de Ley 25.506	OID de la Política de Certificación de BOX CUSTODIA DE ARCHIVOS S.A., otorgado por la ONTI, URI de la Política de Certificación y texto obligatorio para los certificados de la IFDRA.
Identificador de la Clave de la Autoridad Certificante	Valor de hash de 32 bytes 2.5.29.35	Contiene un hash de 32 bytes del atributo clave pública del AC BCFD que emitió el certificado.
Uso Extendido de Clave (Extended Key Usage)	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Certificación digital de fecha y hora (1.3.6.1.5.5.7.3.8) 2.5.29.37	Autenticación del cliente Certificación digital de fecha y hora
Acceso Información Emisor (AuthorityInformation Access)	CA Issuer: URL http://pkidocs.boxcustodia.com/accerts/06.crt OCSP: https://ocsp.pki.boxcustodia.com/	URL de la información para acceder al certificado de ACBOX CUSTODIA FIRMA DIGITAL y al servicios

QCStatement	OID= 2.16.32.1.10.1 (claves generadas por software) OID=2.16.32.1.10.2.1, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 1. OID=2.16.32.1.10.2.2, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 2. OID= 2.16.32.1.10.2.3 (claves generadas por disp. FIPS 140-2 nivel 3)	Declaración del certificado calificado

f) Perfil del certificado para el servicio de consulta OCSP

Campos Atributos Extensiones	**Valor/OID**	**Observaciones**
Versión (Version)	2	Corresponde a versión 3
Número de serie (SerialNumber)	hasta 20 octetos 2.5.4.5	Entero positivo asignado unívocamente por la AC – BOX CUSTODIA FIRMA DIGITAL a cada certificado.
Algoritmo de Firma (Signature Algorithm)	Sha2RSA 1.2.840.113549.1.1.11	Algoritmo usado por el certificador para firmar.
Nombre distintivo del emisor (Issuer)		
commonName	AC- BOX CUSTODIA FIRMA DIGITAL 2.5.4.3	Identificación de la Entidad Certificante
serialNumber	CUIT 30704582370 2.5.4.5	CUIT del Certificador
organizationName	BOX CUSTODIA DE ARCHIVOS S.A 2.5.4.10	Denominación del Certificador Licenciado
stateOrProvinceName	Ciudad Autónoma de Buenos Aires 2.5.4.8	Ciudad en la que se encuentra el Certificador.

countryName	AR 2.5.4.6	País del Certificador Licenciado
Validez (desde, hasta) (Validity (Not before,not after))		
notBefore	<fecha y hora de emisión UTC> yyyy/mm/ddhh:mm:ss huso-horario	Fecha y hora en que el periodo de vigencia del certificado comienza.
notAfter	<fecha y hora de emisión UTC+ periodo> yyyy/mm/ddhh:mm:ss	Fecha y hora en que el periodo de vigencia del certificado termina. El periodo para este perfil es 10 (diez) años como máximo.
Nombre distintivo del suscriptor (Subject)		
commonName	Servicio OCSP 2.5.4.3	Denominación del servicio
serialNumber	<CUIT> <Número de CUIT> 2.5.4.5	CUIT de la empresa BOX CUSTODIA DE ARCHIVOS S.A.
organizationName	BOX CUSTODIA DE ARCHIVOS S.A 2.5.4.10	Denominación del Certificador Licenciado
countryName	AR 2.5.4.6	País del Certificador Licenciado
Clave Pública del suscriptor		
Publickeyalgorithm	RSA 1.2.840.11.35.49.1.1.1	Tipo de algoritmo de clave pública utilizado
ublickeylength	2048 bits	Longitud de la clave pública del suscriptor
SubjectPublicKey Info	<Clave pública del suscriptor>	Valor de la clave pública del suscriptor.
Restricciones básicas (Basic Constraints)	Tipo de asunto = Entidad final pathLengthConstraint = Null 2.5.29.19	Define el certificado como de entidad final

Usos de clave (Key Usage)	digitalSignature = 1 nonRepudiation = 1 keyEncipherment = 0 dataEncipherment =0 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0 2.5.29.15	Propósito para el cual será utilizada la clave contenida en el certificado
Identificador de clave del Suscriptor (Subject Key Identifier)	Valor de hash de 32 bytes	Contiene un hash de 32 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints)	Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints) [1]Punto de distribución CRL Dirección URL= https://pki.boxcustodia.com/crl 2.5.29.31	URI del punto de distribución
Política de Certificación (CertificatePolicies)	OID de la Política de Certificación de BOX CUSTODIA DE ARCHIVOS = 2.16.32.1.1.6 Información de la Política de Certificación: Ubicación (URI): https://pkidocs.boxcustodia.com/acdocs/Politica_Unica.pdf Texto de aviso = Certificado emitido por un Certificador Licenciado en el marco de Ley 25.506	OID de la Política de Certificación de BOX CUSTODIA DE ARCHIVOS S.A., otorgado por la ONTI, URI de la Política de Certificación y texto obligatorio para los certificados de la IFDRA.
Identificador de la Clave de la Autoridad Certificante	Valor de hash de 20 bytes 2.5.29.35	Contiene un hash de 20 bytes del atributo clave pública del AC BCFD que emitió el certificado.

Uso Extendido de Clave (Extended Key Usage)	OCSPSigning (1.3.6.1.5.5.7.3.9) 2.5.29.37	Corresponde a las respuestas del servicio OCSP
Acceso Información Emisor (AuthorityInformation Access)	CA Issuer: URL http://pkidocs.boxcustodia.com/accerts/06.crt OCSP: https://ocsp.pki.boxcustodia.com/	URL de la información para acceder al certificado de ACBOX CUSTODIA FIRMA DIGITAL y al servicio de OCSP.
QCStatement	OID= 2.16.32.1.10.1 (claves generadas por software) OID=2.16.32.1.10.2.1, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 1. OID=2.16.32.1.10.2.2, cuando las claves sean generadas en dispositivos que cuenten con certificación FIPS 140 (Versión 2) nivel 2. OID= 2.16.32.1.10.2.3 (claves generadas por disp. FIPS 140-2 nivel 3)	Declaración del certificado calificado

7.1.1. - Número de versión

Los certificados emitidos corresponden al estándar X.509 y contienen el valor 2 correspondiente a la versión 3.

7.1.2. - Extensiones

Key Usage

El “keyusage” indica el uso del certificado de acuerdo con el RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and CRL Profile”. Es una EXTENSIÓN CRÍTICA.

Extensión Políticas de Certificación

En la extensión de “certificatepolicies” (Políticas de Certificación) se detalla el nombre del dominio de la CA y el directorio creado para el Repositorio de dicho documento. Es una EXTENSIÓN CRÍTICA. Se incluye OID de la Política de Certificación. Ese OID es asignado por la Autoridad de Aplicación a solicitud del ente licenciante.

Nombre Alternativo Del Sujeto

La extensión “subjectAltName”, es una EXTENSIÓN NO CRÍTICA. En los certificados de personas jurídicas públicas o privadas que no identifiquen a un servicio se incluyen los datos identificatorios de la persona humana a cargo de la custodia de la clave privada del mismo. Adicionalmente, esta extensión “SubjectAlternativeName” permite asociar identidades adicionales al suscriptor de un certificado.

Las opciones definidas incluyen una dirección del correo electrónico, un nombre DNS, una dirección IP y un identificador uniforme de recurso (URI). Esta extensión debe utilizarse para consignar las direcciones de correo electrónico de los suscriptores en lugar del atributo “email” del campo “subject”.

Restricciones Básicas (Basic Constraints)

La extensión “BasicConstraints” permite identificar si el suscriptor de un certificado es un certificador e indica la longitud máxima de las rutas de certificación válidas que el certificado incluye. Esta extensión está presente en todos los certificados. Los certificados de certificador deben contener el atributo “ca” con valor TRUE es una EXTENSIÓN CRÍTICA. Para los certificados de usuarios finales deben dos contienen los atributos “ca” con valor FALSE y PathLenConstraint=Null.

Uso de Claves Extendido (Extended Key Usage)

La extensión permite configurar los propósitos de la clave. La extensión NO ES CRÍTICA. Certificados para servicios de certificación digital de fecha y hora deben incluir el valor “idkp-timeStamping” (1.3.6.1.5.5.7.3.8).

Los Certificados en caso de ser utilizados para correo seguro, deben incluir el valor “id-kpemail-protection” (1.3.6.1.5.5. 7.3.4)

Contiene el valor id-kp-OCSPSigning (1.3.6.1.5.5.7.3.9) para los certificados de servicio OCSP.

7.1.3. - Identificadores de algoritmos

Los algoritmos utilizados son los especificados en el [RFC 4055] para RSA, [RFC 5480] para curvas elípticas o [RFC 5758] para DSA y ECDSA o los que, en su defecto, determine la Autoridad de Aplicación

7.1.4. - Formatos de nombre

Los formatos de nombres cumplen con lo establecido en el punto “3.1.2. Necesidad de Nombres Distintivos” de la Política Única de Certificación de la AC - BOX CUSTODIA FIRMA DIGITAL.

7.1.5. - Restricciones de nombre

Todos los nombres representados dentro de los certificados emitidos bajo la presente Política coinciden con “3.1.4. Reglas para la interpretación de nombres” y “3.1.5. Unicidad de nombres” de la Política Única de Certificación de la AC - BOX CUSTODIA FIRMA DIGITAL.

7.1.6. - OID de la Política Única de Certificación

El OID de la Política de Certificación que AC BOX CUSTODIA FIRMA DIGITAL utiliza para la emisión de sus certificados, fue asignado por la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS a solicitud del ente licenciante.

El campo “userNotice” incluye la leyenda “certificado emitido por un certificador licenciado en el marco de la Ley Nº 25.506”.

La extensión “CertificatePolicies” incluye la información sobre la Política de Certificación necesaria para la validación del certificado.

Esta extensión está presente en todos los certificados y es una EXTENSION CRITICA.

7.1.7. - Sintaxis y semántica de calificadores de Política

El calificador de la política está incluido en la extensión de “Certificate Policies” y contiene una referencia al URL con la Política de Certificación aplicable.

7.1.8. - Semántica de procesamiento para extensiones críticas

Sin estipulaciones.

7 .2 Perfil de la lista de certificados revocados.

En lo referente a CRLs la AC - BOX CUSTODIA FIRMA DIGIT**AL** adhiere a las recomendaciones del documento:

> RFC 5280 "Internet X.509 Public Key lnfrastructure Certificate and Certificate Revocation List (CRL) Profile" [RFC5280]

Las Listas de Certificados Revocados serán emitidas conforme con lo establecido en la especificación ITU X.509 versión 2 o la que, en su defecto, determine el Ente Licenciante, y cumplirán con las indicaciones establecidas el apartado “3 - Perfil de

CRLs” del Anexo IV – “Perfiles de los Certificados y de las Listas de Certificados Revocados”.

Los siguientes campos se encuentran presentes en la Lista de Certificados Revocados, emitida por la AC- BOX CUSTODIA FIRMA DIGITAL**:**

Campos Atributos Extensiones	**Valor/OID**	**Observaciones**
Versión (Version)	2	Corresponde a versión 3
Número de serie (SerialNumber)	hasta 20 octetos 2.5.4.5	Entero positivo asignado unívocamente por la AC – BOX CUSTODIA FIRMA DIGITAL a cada certificado.
Algoritmo de Firma (Signature Algorithm)	Sha2RSA 1.2.840.113549.1.1.11	Algoritmo usado por el certificador para firmar.
Nombre distintivo del emisor (Issuer)		
commonName	AC- BOX CUSTODIA FIRMA DIGITAL 2.5.4.3	Identificación de la Entidad Certificante
serialNumber	CUIT 30704582370 2.5.4.5	CUIT del Certificador
organizationName	BOX CUSTODIA DE ARCHIVOS S.A 2.5.4.10	Denominación del Certificador Licenciado
stateOrProvinceName	Ciudad Autónoma de Buenos Aires 2.5.4.8	Ciudad en la que se encuentra el Certificador.
countryName	AR 2.5.4.6	País del Certificador Licenciado
Día y hora de vigencia (thisUpdate)	<fecha y hora UTC> yyyy/mm/ddhh:mm:ss huso-horario	Fecha y hora efectivas de emisión, a partir de la cual entra en vigencia.
Proxima Actualización (nextUpdate)	<fecha y hora UTC> yyyy/mm/ddhh:mm:ss	Fecha y hora en que el periodo de vigencia del certificado termina.

Identificador de la Clave de la Autoridad Certificante (AuthrorityKeyIdentifier)	Valor de hash de 32 bytes 2.5.29.35	Contiene un hash de 32 bytes del atributo clave pública del AC BCFD que emitió la Lista de Certificados Revocados.
Número de CRL (CRL Number)	Número de la CRL OID – 2.5.29.20	Número incremental que identifica la CRL emitida
Identificador Delta CRL (Delta CRL Indicator)	Número de Delta CRL 2.5.29.27	Número que se incrementa cada vez que se emite una Delta CRL.
Certificados Revocados (RevokedCertifiactes)		
Fecha de Revocación	<fecha y hora UTC< yyyy/mm/ddhh:mm:ss huso-horario	Fecha y hora en que se revocó el certificado
Número de Serie del Certificado revocado (Serial Number)	Hasta 20 octetos 2.5.4.5	
Motivo de la Revocación	Motivo de acuerdo al RFC 5280	
Algoritmo de Identificación Huella Digital	SHA2	

7.2.1 Número de versión

El campo “versión” describe la versión de la CRL. Contienen el valor 1 (correspondiente a Versión 2

. 7.2.2 Extensiones de CRL (Lista de Certificados Revocados)

Identificación de Clave de la Autoridad Certificante (Authority Key Identifier)

La extensión “AuthorityKeyIdentifier” proporciona un medio para identificar la clave pública que corresponde a la clave privada utilizada para firmar una CRL. Esta extensión está presente en todas las listas de revocación de certificados.

Número de CRL (CRL Number)

La extensión “CRLNumber” contiene un número de secuencia creciente para una CRL y emisor dado. Esta extensión permite que los usuarios determinen fácilmente cuándo una

CRL particular reemplaza otra CRL. Esta extensión se encuentra en todas las listas de revocación de certificados.

Punto de Distribución del Emisor (Issuing Distribution Point)

La extensión “IssuingDistributionPoint” identifica el punto de distribución y el alcance de una CRL particular. Esta extensión es CRÍTICA.

Perfil de la consulta en línea del estado del certificado

La consulta en línea del estado de un certificado digital se realiza utilizando el Protocolo OCSP (On-Line Certificate Status Protocol). Es implementada conforme a lo previsto por la Resolución 946/2021 y lo indicado en la especificación RFC 6960.

7.3. - Perfil de la consulta en línea del estado del certificado.

La consulta en línea del estado de un certificado digital se realiza utilizando el Protocolo OCSP (On-Line Certificate Status Protocol). Deberá ser implementada conforme a lo indicado en la especificación RFC 6960 “X.509 Internet Public Key Infrastructure On Line Certificate Status Protocol – OCSP” y cumplir con las indicaciones establecidas en el apartado “4 - Perfil de la consulta en línea del estado del certificado” del Anexo IV – “Perfiles de los Certificados y de las Listas de Certificados Revocados”.

7.3.1 Consultas OCSP

Los siguientes datos se encuentran presentes en las consultas:

a) Versión (versión).
b) Requerimiento de servicio (service request).
c) Identificador del certificado bajo consulta (target certificate identifier).
d) Extensiones opcionales (optionals extensions), las cuales podrían ser procesadas por quien responde.

Al recibir la consulta OCSP, se determina:

a) Si el formato de la consulta es adecuado.
b) Si quien responde se encuentra habilitado para responder la consulta.
c) Si la consulta contiene la información que necesita quien responde.

Si alguna de estas condiciones no se cumpliera, da lugar a un mensaje de error. De lo contrario se devuelve una respuesta.

7.3.2 Respuestas OCSP

Todas las respuestas OCSP son firmadas digitalmente por la AC- BOX CUSTODIA FIRMA DIGITAL y contienen los siguientes datos:

a) Versión de la sintaxis de respuesta.

b) Identificador de quien responde.
c) Fecha y hora en la que se genera la respuesta.
d) Respuesta respecto al estado del certificado.
e) Extensiones opcionales.
f) Identificador (OID) único del algoritmo de firma.
g) Firma de la respuesta.

La respuesta a una consulta OCSP consiste en:

a) Identificador del certificado.
b) Valor correspondiente al estado del certificado.
c) Período de validez de la respuesta.
d) Extensiones opcionales.

Se especifican las siguientes respuestas posibles para el valor correspondiente al estado del certificado:

a) Válido (good), indicando una respuesta positiva a la consulta. Este valor indica que no existe un certificado digital con el número de serie contenido en la consulta, que haya sido revocado durante su vigencia.
b) Revocado (revoked), indicando que el certificado ha sido revocado.
c) Desconocido (unknown), indicando que quien responde no reconoce el número de serie incluido en la consulta, debido comúnmente a la inclusión de un emisor desconocido.

8. -AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES.

Este componente indicará aspectos específicos del proceso de auditoría, como ser:

a) Denominación de la entidad de auditoría.
b) Frecuencia y contextos para la realización de las auditorías.

c) Identificación y calificaciones de la entidad evaluadora.
d) Vinculación entre el certificador y la entidad evaluadora
e) Temas principales a evaluar en las auditorías.
f) Medidas a adoptar en caso de dictámenes no favorables.
g) Modalidad de comunicación de los informes de auditoría.

Se cumplen las exigencias reglamentarias impuestas por:

a) Los artículos 33 y 34 de la Ley Nº 25.506 de Firma Digital, respecto al sistema de auditoría y el artículo 21, inciso k) de la misma ley, relativo a la publicación de informes de auditoría.

b) Los artículos 6 a 8 del Decreto Nº 182/19, reglamentario de la Ley de Firma Digital, relativos al sistema de auditoría.

c) El Ente Licenciante de la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA realiza auditorías ordinarias al Certificador **BOX CUSTODIA DE ARCHIVOS S.A.,** a la Autoridad Certificante AC - **BOX CUSTODIA FIRMA DIGITAL** y a sus Autoridades de Registro, a fin de verificar el cumplimiento de los requisitos de licenciamiento.

d) Las auditorías tienen por objeto verificar el cumplimiento de los requisitos exigidos para obtener y mantener la condición de Certificador Licenciado y la aplicación de las políticas y procedimientos aprobados por el Ente Licenciante para la presente Política Única de Certificación.

e) Por su parte, BOX **CUSTODIA DE ARCHIVOS S.A.,** en su carácter de Certificador Licenciado, realizará auditorías periódicas a sus propias Autoridades de Registro autorizadas a funcionar con el objeto de verificar el cumplimiento de los procesos y procedimientos establecidos en la normativa regulatoria de Firma Digital.

f) La información relevante de los informes de las auditorías es publicada en el sitio web de la **AC - BOX CUSTODIA FIRMA DIGITAL**: https://boxcustodia.com/acdocs/Informe_Auditoria_2014.pdf

9. - ASPECTOS LEGALES Y ADMINISTRATIVOS.

9.1. -Aranceles.

Los certificados digitales emitidos bajo la presente Política son expedidos a favor de personas humanas y/o jurídicas a título oneroso, aplicándose aranceles diferenciales asociados a los distintos tipos de certificados.

Los aranceles serán consultados por medio de correo electrónico a comercial@boxcustodia.com

9.2. - Responsabilidad Financiera.

La responsabilidad financiera se origina en lo establecido por la Ley Nº 25.506 y su Decreto Nº 182/19 y en las disposiciones de la presente política.

9.3. – Confidencialidad

Se indican las previsiones en cuanto al tratamiento de información confidencial del certificador, estableciendo como mínimo los siguientes aspectos:

a) Alcance de la información considerada confidencial.
b) Tipos de información no considerada confidencial.
c) Responsabilidades de los roles involucrados

Toda información referida a solicitantes o suscriptores que sea recibida por el certificador o por las Autoridades de Registro operativamente vinculadas, será tratada en forma confidencial y no puede hacerse pública sin el consentimiento previo de los titulares de los datos, con excepción de que requerida judicialmente. La exigencia se extiende a toda otra información referida a los solicitantes y los suscriptores de certificados a la que tenga acceso el Certificador o sus Autoridades de Registro durante el ciclo de vida del certificado.

Lo precedentemente señalado no es aplicable cuando se trate de información que se transcriba en el certificado o sea obtenida de fuentes públicas.

9.3.1. - Información confidencial

Toda información remitida por el solicitante o suscriptor de un certificado al momento de efectuar un requerimiento es considerada confidencial y no es divulgada a terceros sin su consentimiento previo y expreso, salvo que sea requerida mediante resolución fundada en causa judicial por juez competente. La exigencia se extenderá también a toda otra información referida a los suscriptores de certificados a la que tenga acceso el certificador o la Autoridad de Registro durante el ciclo de vida del certificado.

Se especifica la información a ser tratada como confidencial por el certificador y por las Autoridades de Registro operativamente vinculadas, de acuerdo con lo establecido por las normas legales y reglamentarias vigentes.

Toda información referida a suscriptores que sea recibida en los requerimientos de certificados por la AC - BOX CUSTODIA FIRMA DIGITAL o por las Autoridades de Registro operativamente vinculadas es confidencial y no puede hacerse pública sin el consentimiento previo de aquellos, salvo que sea requerida judicialmente por juez competente. La exigencia se extiende a toda otra información referida a los solicitantes y suscriptores de certificados a la que tenga acceso la **AC - BOX CUSTODIA FIRMA DIGITAL** o sus Autoridades de Registro durante el ciclo de vida de los certificados.

Lo indicado no es aplicable cuando se trate de información que se transcriba en el certificado o sea obtenida de fuentes públicas.

BOX CUSTODIA DE ARCHIVOS S.A., en su carácter de Certificador, garantiza la confidencialidad frente a terceros de su clave privada, la que, al ser el punto de máxima confianza, será generada y custodiada conforme a lo que se especifique en la presente Política. Asimismo, se considera confidencial cualquier información:

- Resguardada en servidores o bases de datos y vinculada al proceso de gestión del ciclo de vida de los certificados digitales emitidos por el Certificador.
- Almacenada en cualquier soporte, incluyendo aquella que se transmita verbalmente, vinculada a procedimientos de certificación, excepto aquella declarada como no confidencial en forma expresa.
- Relacionada con los Planes de Contingencia, controles, procedimientos de seguridad y registros de auditoría pertenecientes al Certificador.
- Es considerada confidencial la información incluida en el Manual de Procedimientos de Seguridad y en el Plan de Contingencias de la AC - BOX CUSTODIA FIRMA

DIGITAL.

En todos los casos resulta de aplicación la Ley Nº 25.326 de protección de datos personales, su reglamentación y demás normas complementarias.

9.3.2.- Información no confidencial.

La siguiente información no se considera confidencial:

a) Contenido de los certificados y de las listas de certificados revocados.
b) Información sobre personas humanas o jurídicas que se encuentre disponible en certificados o en directorios de acceso público.
c) Políticas de Certificación y Manual de Procedimientos de Certificación (en sus aspectos no confidenciales).
d) Secciones públicas de la Política de Seguridad del certificador.
e) Política de privacidad del certificador.
f) Acuerdo con suscriptores.
g) Toda otra referida a personas humanas que se encuentre disponible en certificados o en directorios de acceso público.

9.3.3. - Responsabilidades de los roles involucrados.

La información confidencial podrá ser revelada ante un requerimiento emanado de juez competente como parte de un proceso judicial.

La información confidencial podrá ser revelada ante un requerimiento emanado de juez competente como parte de un proceso judicial o ante requerimiento de autoridad administrativa como parte de un proceso administrativo.

Toda divulgación de información referida a los datos de identificación del suscriptor o a cualquier otra información generada o recibida durante el ciclo de vida del certificado sólo podrá efectuarse previa autorización escrita del suscriptor del certificado.

No será necesario el consentimiento cuando:

- Los datos se hayan obtenido de fuentes de acceso público irrestricto;
- Los datos se limiten a nombre, documento nacional de identidad, pasaporte, documento de identidad expedido por país miembro del MERCOSUR u ocupación.
- Aquellos para los que el Certificador hubiera obtenido autorización expresa de su titular.

9.4. - Privacidad

Todos los aspectos vinculados a la privacidad de los datos personales estarán sujetos a la normativa vigente en materia de Protección de los Datos Personales (Ley Nº 25.326 y normas reglamentarias, complementarias y aclaratorias). Las consideraciones particulares se incluyen en la Política de Privacidad.

9.5 - Derechos de Propiedad Intelectual

Las aplicaciones y los sistemas informáticos generados por el Certificador con el objeto de desarrollar e implementar la **AC - BOX CUSTODIA FIRMA DIGITAL** son propiedad de **BOX CUSTODIA DE ARCHIVOS S.A**.

Los sistemas operativos y de soporte informático no desarrollados por **BOX CUSTODIA DE ARCHIVOS S.A.** cuentan con su respectiva licencia de uso.

Los datos propios de la **AC - BOX CUSTODIA FIRMA DIGITAL** incluidos en esta Política única de Certificación son de propiedad de **BOX CUSTODIA DE ARCHIVOS S.A.**

9.6. - Responsabilidades y garantías.

Se regirá por lo establecido en la Ley Nº 25.506, su Decreto Nº 182/19 y demás normativa aplicable en la materia.

Las partes contratantes se rigen por además por el Acuerdo con Suscriptores que es el contrato específico que regula la relación entre el suscriptor y el Certificador Licenciado **BOX CUSTODIA DE ARCHIVOS S.A.**

El Certificador no asumirá responsabilidad alguna en aquellos supuestos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados, en los supuestos de daños y perjuicios que resultaren del uso no autorizado de un certificado digital y en los supuestos donde las inexactitudes contenidas en el certificado resultaran de la información que hubiera presentado el suscriptor, siempre que el Certificador pueda demostrar que ha actuado con la debida diligencia.

Los alcances de la responsabilidad del Certificador se limitan a las consecuencias directas de la falta de cumplimiento de los procedimientos establecidos en la Política Única de Certificación, en relación a la emisión, renovación y revocación de certificados y en ningún momento será responsable por el mal uso de los certificados que pudiera hacerse, como tampoco por los daños y perjuicios derivados de la falta de consulta de la información disponible en Internet sobre la validez de los certificados, ni tampoco será responsable de los usos de los certificados en aplicaciones específicas.

El Certificador no será responsable por los daños o perjuicios que hubieran acontecido por culpa de un tercero, de la víctima, o la presencia de un hecho fortuito o de fuerza mayor que no le sea imputable, quedando eximido de resarcir total o parcialmente los daños causados a la víctima en caso de que probara su falta de culpa o que actuó diligentemente.
El Certificador no garantiza el acceso a la información cuando mediaran razones de caso fortuito o fuerza mayor (catástrofes naturales, cortes masivos de luz por períodos indeterminados, destrucción debido a eventos no previstos, ataques informáticos, etc.), ni asume responsabilidad por los daños que se deriven en forma directa o indirecta como consecuencia de estos casos.

9.7. - Deslinde de responsabilidad

El Certificador no asumirá responsabilidad alguna en aquellos supuestos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados, en los supuestos de daños y perjuicios que resultaren del uso no autorizado de un certificado digital y en los supuestos donde las inexactitudes contenidas en el certificado resultaran de la información que hubiera presentado el suscriptor, siempre que el Certificador pueda demostrar que ha actuado con la debida diligencia.
Los alcances de la responsabilidad del Certificador se limitan a las consecuencias directas de la falta de cumplimiento de los procedimientos establecidos en la Política Única de Certificación, en relación a la emisión, renovación y revocación de certificados y en ningún momento será responsable por el mal uso de los certificados que pudiera hacerse, como tampoco por los daños y perjuicios derivados de la falta de consulta de la información disponible en Internet sobre la validez de los certificados, ni tampoco será responsable de los usos de los certificados en aplicaciones específicas.
El Certificador no será responsable por los daños o perjuicios que hubieran acontecido por culpa de un tercero, de la víctima, o la presencia de un hecho fortuito o de fuerza mayor que no le sea imputable, quedando eximido de resarcir total o parcialmente los daños causados a la víctima en caso de que probara su falta de culpa o que actuó diligentemente.
El Certificador no garantiza el acceso a la información cuando mediaran razones de caso fortuito o fuerza mayor (catástrofes naturales, cortes masivos de luz por períodos indeterminados, destrucción debido a eventos no previstos, ataques informáticos, etc.), ni asume responsabilidad por los daños que se deriven en forma directa o. indirecta como consecuencia de estos casos.

9.8. - Limitaciones a la responsabilidad frente a terceros.

Aplican las limitaciones previstas por la Ley Nº 25.506 y sus normas reglamentarias y complementarias y el Acuerdo con Suscriptores firmado por los suscriptores con el Certificador Licenciado.

También aplica la limitación impuesta en casos de fuerza mayor conforme la definición establecida en el Código Civil y Comercial Unificado.

9.9. - Compensaciones por daños *y* perjuicios.

No aplica.

9.10. - Condiciones de vigencia.

La Política Única de Certificación empieza a ser efectiva una vez que el acto administrativo por el cual la Autoridad competente la aprueba sea publicado en el Boletín Oficial de la REPÚBLICA ARGENTINA.

La Política Única de Certificación deberá a su vez ser publicada en el correspondiente sitio de internet del Certificador Licenciado y los nuevos certificados deben ser emitidos cumpliendo las políticas determinadas en la nueva versión de la Política Única de Certificación.

La Política Única de Certificación estará en vigor mientras no sea derogada *y* reemplazada por una nueva versión.

9.11.- Avisos personales y comunicaciones con los participantes.

No aplicable.

9.12.- Gestión del ciclo de vida del documento.

Si el responsable del documento definido en el punto 1.5.1 del Formulario de Adhesión considerara pertinente la modificación del documento deberá someter a consideración y evaluación del Certificador Licenciado BOX CUSTODIA DE ARCHIVOS S.A. las correspondientes propuestas.

Si los cambios o modificaciones propuestas son aceptados, tendrán como resultado final la aprobación de una nueva versión de la Política Única de Certificación.

9.12.1. - Procedimientos de cambio.

Las modificaciones a la presente Política Única de Certificación, deberán ser aprobadas previamente por el ente licenciante conforme a lo establecido por el artículo 21 inciso q) de la Ley Nº 25.506, el Decreto Nº 182/2019 y por la resolución 946/2021. Toda Política Única de Certificación será sometida a la aprobación del Ente Licenciante durante el proceso de licenciamiento

9.12.2- Mecanismo y plazo de publicación y notificación.

Una copia de la versión vigente de la presente Política Única de Certificación se encuentra disponible en forma pública y accesible a través de Internet en el sitio web https://pkidocs.boxcustodia.com/acdocs/Politica_Unica.pdf Una vez que la Autoridad de Aplicación notifique al Certificador la aprobación de las modificaciones a la Política de Certificación, éste procederá a su publicación en el sitio web antes mencionado.

9.12.3. - Condiciones de modificación del OID.

No aplicable.

9.13. - Procedimientos de resolución de conflictos.

Cualquier controversia y/o conflicto resultante de la aplicación de esta Política Única de Certificación, deberá ser resuelto en sede administrativa de acuerdo a las previsiones de la Ley Nacional de Procedimientos Administrativos Nº 19.549 y su Decreto Reglamentario Nº1759/72.

La presente Política Única de Certificación se encuentra en un todo subordinado a las prescripciones de la Ley Nº 25.506 y su reglamentación.

Los titulares de certificados y los terceros usuarios podrán interponer ante el Ente Licenciante recurso administrativo por conflictos referidos a la prestación del servicio por parte del Certificador. Una vez agotada la vía administrativa, podrá interponerse acción judicial, siendo competente la Justicia en lo Contencioso Administrativo Federal.

El reclamo efectuado por un tercero usuario o por el titular de un certificado digital expedido por el Certificador, sólo será procedente previa acreditación de haberse efectuado reclamo ante este último con resultado negativo. Acreditada dicha circunstancia, el Ente Licenciante procederá a recibir, evaluar y resolver las denuncias mediante la instrucción del correspondiente trámite administrativo.

A los efectos del reclamo antes citado, se procederá de la siguiente manera:

a) Una vez recibido el reclamo en las oficinas del Certificador, este citará al reclamante a una audiencia y labrará un acta que deje expresa constancia de los hechos que motivan el reclamo y de todas y cada uno de los antecedentes que le sirvan de causa.
b) Una vez que el Certificador emita opinión, se notificará al reclamante y se le otorgará un plazo de CINCO (5) días hábiles administrativos para ofrecer y producir la prueba de su descargo.

El Certificador Licenciado resolverá en un plazo de DIEZ (1 O) días lo que estime corresponder, conforme a los criterios de máxima razonabilidad, equidad y pleno ajuste al bloque de legalidad vigente y aplicable.
En ningún caso, la Política Única de Certificación del certificador prevalecerá sobre lo dispuesto por la normativa vigente de firma digital.
El suscriptor o los terceros usuarios podrán accionar ante el ente licenciante, previo agotamiento del procedimiento ante el certificador licenciado correspondiente, el cual deberá proveer obligatoriamente al interesado de un adecuado procedimiento de resolución de conflictos.

9.14. - Legislación aplicable.

La legislación que respalda la interpretación, aplicación y validez de la Política Única de Certificación, es la Ley Nº 25.506 y su modificatoria, el Decreto Nº 182/2019 y su modificatorio, y su normativa complementaria.

9.15. - Conformidad con normas aplicables.

La legislación aplicable a la actividad del Certificador es la Ley Nº 25.506, el Decreto Nº 182/19 y toda otra norma complementaria dictada por la autoridad competente.

9.16. - Cláusulas adicionales.

No se establecen cláusulas adicionales.

9.17. - Otras cuestiones generales.

No aplica.

República Argentina - Poder Ejecutivo Nacional
Las Malvinas son argentinas

Hoja Adicional de Firmas
Anexo

Número: IF-2022-91402257-APN-SSIA#JGM

CIUDAD DE BUENOS AIRES
Miércoles 31 de Agosto de 2022

Referencia: Política Única de Certificación 2.3 - BOX/CUSTODIA DE ARCHIVOS S A

El documento fue importado por el sistema GEDO con un total de 90 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2022.08.31 11:19:07 -03:00

Luis Mariano PAPAGNI
Subsecretario
Subsecretaría de Innovación Administrativa
Jefatura de Gabinete de Ministros

Digitally signed by Gestion Documental Electronica
Date: 2022.08.31 11:19:08 -03:00