Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

661

ANEXO

POLÍTICA ÚNICA DE CERTIFICACIÓN

CERTIFICADOR LICENCIADO
BOX CUSTODIA DE ARCHIVOS S.A.

Versión 1.1

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

FOLIO 462

ANEXO

ÍNDICE

1- INTRODUCCIÓN.	7
1.1.- Descripción general.	7
1.2.- Nombre e Identificación del Documento.	7
1.3.- Participantes y aplicabilidad.	7
1.3.1.- Certificador.	8
1.3.2.- Autoridad de Registro.	8
1.3.3.- Suscriptores de certificados.	8
1.3.4.- Terceros Usuarios.	9
1.4.- Uso de los certificados.	9
1.5.- Administración de la Política.	9
1.5.1.- Responsable del Documento.	9
1.5.2.- Contacto.	9
1.5.3.-Procedimiento de aprobación de la Política Única de Certificación.	10
1.6. - Definiciones y Acrónimos.	10
1.6.1. – Definiciones.	10
1.6.2. – Acrónimos.	13
2. - RESPONSABILIDADES VINCULADAS A LA PUBLICACIÓN Y A LOS REPOSITORIOS.	14
2.1. – Repositorios.	14
2.2. – Publicación de Información del certificador.	14
2.3. – Frecuencia de publicación.	16
2.4. – Controles de acceso a la información.	16
3.- IDENTIFICACIÓN Y AUTENTICACIÓN.	17
3.1. – Asignación de nombres de suscriptores.	18
3.1.1. – Tipos de Nombres.	18
3.1.2. - Necesidad de Nombres Distintivos.	18
3.1.3. - Anonimato o uso de seudónimos.	22
3.1.4. - Reglas para la interpretación de nombres.	22
3.1.5. - Unicidad de nombres.	22
3.1.6. - Reconocimiento, autenticación y rol de las marcas registradas.	22
3.2. - Registro inicial.	23
3.2.1. - Métodos para comprobar la posesión de la clave privada.	23
3.2.2 - Autenticación de la identidad de Personas Jurídicas Públicas o Privadas	24
3.2.3. - Autenticación de la identidad de Personas Físicas.	25
3.2.4. - Información no verificada del suscriptor.	26

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

663

ANEXO

3.2.5. - Validación de autoridad. 26
3.2.6. - Criterios para la interoperabilidad. 26
3.3. - Identificación y autenticación para la generación de nuevo par de claves (Rutina de Re Key). 27
3.3.1. - Renovación con generación de nuevo par de claves (Rutina de Re Key). 27
3.3.2. - Generación de UN (1) certificado con el mismo par de claves. 27
3.4. - Requerimiento de revocación. 28
4. - CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS. 29
4.1. - Solicitud de certificado. 29
4.1.1. - Solicitantes de certificados. 29
4.1.2. - Solicitud de certificado. 29
4.2. – Procesamiento de la solicitud del certificado. 32
4.3. – Emisión del certificado. 33
4.3.1. – Proceso de emisión de un certificado. 33
4.3.2. - Notificación de emisión. 33
4.4. - Aceptación del certificado. 34
4.5. - Uso del par de claves y del certificado. 34
4.5.1. - Uso de la clave privada y del certificado por parte del suscriptor. 34
4.5.2. - Uso de la clave pública y del certificado por parte de Terceros Usuarios. 35
4.6. - Renovación del certificado sin generación de un nuevo par de claves. 35
4.7. - Renovación del certificado con generación de un nuevo par de claves. 35
4.8. - Modificación del certificado. 35
4.9. – Suspensión y Revocación de Certificados. 36
4.9.1. - Causas de revocación. 36
4.9.2. - Autorizados a solicitar la revocación. 37
4.9.3. - Procedimientos para la solicitud de revocación. 38
4.9.4. – Plazo para la solicitud de revocación. 39
4.9.5. – Plazo para el procesamiento de la solicitud de revocación. 39
4.9.6. - Requisitos para la verificación de la lista de certificados revocados. 39
4.9.7. - Frecuencia de emisión de listas de certificados revocados. 40
4.9.8.- Vigencia de la lista de certificados revocados. 40
4.9.9. - Disponibilidad del servicio de consulta sobre revocación y de estado del certificado. 40
4.9.10. - Requisitos para la verificación en línea del estado de revocación. 41
4.9.11. - Otras formas disponibles para la divulgación de la revocación. 42
4.9.12. - Requisitos específicos para casos de compromiso de claves. 42
4.9.13. - Causas de suspensión. 42
4.9.14. - Autorizados a solicitar la suspensión. 42
4.9.15. - Procedimientos para la solicitud de suspensión. 43

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

664

ANEXO

4.9.16. - Límites del periodo de suspensión de un certificado. 43
4.10. – Estado del certificado. 43
4.10.1. – Características técnicas. 43
4.10.2. – Disponibilidad del servicio. 43
4.10.3. – Aspectos operativos. 43
4.11. – Desvinculación del suscriptor. 44
4.12. – Recuperación y custodia de claves privadas. 44
5. - CONTROLES DE SEGURIDAD FÍSICA, OPERATIVOS Y DE GESTIÓN. 44
5.1. - Controles de seguridad física. 44
5.2. - Controles de Gestión. 45
5.3. - Controles de seguridad del personal 45
5.4. - Procedimientos de Auditoría de Seguridad. 46
5.5. - Conservación de registros de eventos. 46
5.6. - Cambio de claves criptográficas. 47
5.7. - Plan de respuesta a incidentes y recuperación ante desastres. 48
5.8. - Plan de Cese de Actividades. 49
6. - CONTROLES DE SEGURIDAD TÉCNICA. 49
6.1. - Generación e instalación del par de claves criptográficas. 50
6.1.1. - Generación del par de claves criptográficas. 50
6.1.2. - Entrega de la clave privada. 51
6.1.3. - Entrega de la clave pública al emisor del certificado. 51
6.1.4. - Disponibilidad de la clave pública del certificador. 52
6.1.5. - Tamaño de claves. 52
6.1.6. - Generación de parámetros de claves asimétricas. 52
6.1.7. - Propósitos de utilización de claves (campo "KeyUsage" en certificados X.509 v.3). 52
6.2. - Protección de la clave privada y controles sobre los dispositivos criptográficos. 53
6.2.1. – Controles y estándares para dispositivos criptográficos. 53
6.2.2. - Control "M de N" de clave privada. 54
6.2.3. - Recuperación de clave privada. 54
6.2.4. - Copia de seguridad de clave privada. 54
6.2.5. - Archivo de clave privada. 54
6.2.6. - Transferencia de claves privadas en dispositivos criptográficos 55
6.2.7. - Almacenamiento de claves privadas en dispositivos criptográficos. 55
6.2.8. - Método de activación de claves privadas. 55
6.2.9. - Método de desactivación de claves privadas. 56
6.2.10. - Método de destrucción de claves privadas. 56
6.2.11. – Requisitos de los dispositivos criptográficos. 57

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

665

ANEXO

6.3. - Otros aspectos de administración de claves. 57
6.3.1. - Archivo permanente de la clave pública. 57
6.3.2. - Período de uso de clave pública y privada. 58
6.4. - Datos de activación. 58
6.4.1. - Generación e instalación de datos de activación. 58
6.4.2. - Protección de los datos de activación. 59
6.4.3. - Otros aspectos referidos a los datos de activación. 59
6.5. - Controles de seguridad informática. 60
6.5.1. - Requisitos Técnicos específicos. 60
6.5.2. - Requisitos de seguridad computacional. 61
6.6. - Controles Técnicos del ciclo de vida de los sistemas. 61
6.6.1. - Controles de desarrollo de sistemas. 62
6.6.2. – Controles de gestión de seguridad. 62
6.6.3. - Controles de seguridad del ciclo de vida del software. 62
6.7. - Controles de seguridad de red. 62
6.8. – Certificación de fecha y hora. 63
7. - PERFILES DE CERTIFICADOS Y DE LISTAS DE CERTIFICADOS REVOCADOS. 63
7.1. - Perfil del certificado 64
7.2 Perfil de la lista de certificados revocados. 86
7.3. - Perfil de la consulta en línea del estado del certificado. 88
7.3.1. – Consultas OCSP. 88
7.3.2. - Respuestas OCSP. 88
8. – AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES. 88
9. – ASPECTOS LEGALES Y ADMINISTRATIVOS. 90
9.1. – Aranceles. 90
9.2. - Responsabilidad Financiera. 90
9.3. – Confidencialidad. 91
9.3.1. - Información confidencial. 91
9.3.2. - Información no confidencial. 93
9.3.3. – Responsabilidades de los roles involucrados. 93
9.4. – Privacidad. 94
9.5 - Derechos de Propiedad Intelectual 94
9.6. – Responsabilidades y garantías. 95
9.7. – Deslinde de responsabilidad. 96
9.8. – Limitaciones a la responsabilidad frente a terceros. 97
9.9. – Compensaciones por daños y perjuicios. 97
9.10. – Condiciones de vigencia. 97

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

666

ANEXO

9.11.- Avisos personales y comunicaciones con los participantes. 98
9.12.- Gestión del ciclo de vida del documento. 98
9.12.1. - Procedimientos de cambio. 98
9.12.2 – Mecanismo y plazo de publicación y notificación. 99
9.12.3. – Condiciones de modificación del OID. 99
9.13. - Procedimientos de resolución de conflictos. 99
9.14. - Legislación aplicable. 101
9.15. – Conformidad con normas aplicables. 101
9.16. – Cláusulas adicionales. 101
9.17. – Otras cuestiones generales. 101

3653 RF

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

667

ANEXO

241

1- INTRODUCCIÓN.

1.1.- Descripción general.

El presente documento establece las políticas que se aplican a la relación entre un certificador licenciado en el marco de la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA (Ley Nº 25.506) 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 física 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 GABINETE de la JEFATURA DE GABINETE DE MINISTROS, siendo la SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN que de ella depende, quien entiende en las funciones de ente licenciante.

1.2.- Nombre e Identificación del Documento.

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

b) Versión: 1.1

c) Fecha de aplicación:

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 http://pki.boxcustodia.com

3653 FF

1.3.- Participantes y aplicabilidad.

Integran la infraestructura del certificador las siguientes entidades:

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

668

ANEXO

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 http://pki.boxcustodia.com 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 físicas o jurídicas sean éstas públicas o privadas y aquellos que presten otros servicios relacionados con la firma digital, tales como los enunciados en el artículo 10 de la Decisión Administrativa Nº 927 de fecha 30 de octubre de 2014.

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.

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

669

ANEXO

1.3.4.- Terceros Usuarios.

Son Terceros Usuarios de los certificados emitidos bajo la presente Política Única de Certificación toda persona física 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. En el caso de los certificados de sitio seguro, serán Terceros Usuarios quienes verifiquen el certificado del servidor.

1.4.- Uso de los certificados.

Las claves correspondientes a los certificados digitales que se emitan bajo la presente Política Única de 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: http://pki.boxcustodia.com/

3653

1.5.2.- Contacto.

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

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

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

670

ANEXO

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: http://pki.boxcustodia.com

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

La Política Única de Certificación del Certificador Licenciado **BOX CUSTODIA DE ARCHIVOS S.A.** como así también el Formulario de Adhesión previsto en el Anexo I a la Decisión Administrativa Nº 927/14 fueron presentadas 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 N° 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:** la SECRETARÍA DE GABINETE de la JEFATURA DE GABINETE DE MINISTROS es la Autoridad de Aplicación de firma digital en la REPÚBLICA ARGENTINA.
- **Autoridad de Registro**: es la entidad que tiene a su cargo las funciones de:

• Recepción de las solicitudes de emisión de certificados.

• Validación de la identidad y autenticación de los datos de los titulares de certificados.

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

671

ANEXO

- 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.**
- Remisión de las solicitudes aprobadas al Certificador Licenciado **BOX CUSTODIA DE ARCHIVOS S.A.** con la que se encuentre operativamente vinculada.
- 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.
- Identificación y autenticación de los solicitantes de revocación de certificados.
- 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.
- Cumplimiento de las normas y recaudos establecidos para la protección de datos personales.
- 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.

Dichas funciones son delegadas por el certificador licenciado. Puede actuar en una instalación fija o en modalidad móvil, siempre que medie autorización del ente licenciante.

- **Certificado Digital:** Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular (artículo 13 de la Ley N° 25.506).

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

FOLIO 672 J.G.M.

ANEXO

- **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. (artículo 17 de la Ley N° 25.506).
- **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. (Anexo al Decreto N° 2628 de fecha 19 de diciembre de 2002).
- **Ente licenciante:** la SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN de la SECRETARÍA DE GABINETE de la JEFATURA DE GABINETE DE MINISTROS es Ente Licenciante.
- **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). (Anexo al Decreto N° 2628/02)
- **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). (Anexo al Decreto N° 2628/02)
- **Plan de Cese de Actividades:** conjunto de actividades a desarrollar por el certificador licenciado en caso de finalizar la prestación de sus servicios. (Anexo al Decreto N° 2628/02)
- **Plan de Continuidad de las operaciones:** Conjunto de procedimientos a seguir por el certificador licenciado ante situaciones de ocurrencia no previstas que comprometan la continuidad de sus operaciones.

2653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

673

ANEXO

- **Plan de Seguridad:** Conjunto de políticas, prácticas y procedimientos destinados a la protección de los recursos del certificador licenciado. (Anexo al Decreto N° 2628/02).
- **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). El resultado de una consulta a este servicio está firmado por el certificador que brinda el servicio.
- **Suscriptor o Titular de certificado digital:** Persona 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 física o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente. (artículo 3° del Decreto N° 724 de fecha 8 de junio de 2006).

3658

1.6.2. – Acrónimos.

CRL - Lista de Certificados Revocados ("Certificate Revocation List")

CUIT - Clave Única de Identificación Tributaria

IEC - International Electrotechnical Commission

IETF - Internet Engineering Task Force

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

674

ANEXO

OCSP - Protocolo en línea del estado de un certificado ("On line Certificate Status Protocol")

OID - Identificador de Objeto ("Object Identifier")

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) Formulario de Adhesión del Anexo I.

b) Política Única de Certificación en sus versiones vigente y anteriores

c) El modelo del Acuerdo con Suscriptores.

d) Los Términos y Condiciones con Terceros Usuarios ("relying parties")

e) Política de Privacidad.

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

FOLIO 675 J.G.M.

ANEXO

f) Manual de Procedimientos en sus aspectos de carácter público, versiones vigentes y anteriores.

g) Información relevante de los informes de su última auditoría.

h) Repositorio de certificados revocados.

i) Certificados del Certificador licenciado y acceso al de la Autoridad Certificante Raíz.

j) Su certificado digital.

k) Su certificado OCSP.

l) La lista de certificados revocados (CRL).

El Certificador está obligado a brindar el servicio de repositorio en cumplimiento de lo dispuesto en el artículo 21 de la Ley Nº 25.506, el Decreto Nº 2628/02, y en la presente Política Única de Certificación, como así también con las obligaciones establecidas en el artículo 21, inciso k) de la Ley Nº 25.506:

k) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, la lista de certificados digitales revocados, la Política Única de Certificación, la información relevante de los informes de la última auditoría de que hubiera sido objeto, su Manual de Procedimientos y toda información que determine la Autoridad de Aplicación.

También está obligado a cumplir con las obligaciones establecidas en el artículo 34, incisos g), h) y m) del Decreto Nº 2628/02:

g) Garantizar el acceso permanente, eficiente y gratuito de los titulares y terceros al repositorio de certificados revocados.

h) Mantener actualizados los repositorios de certificados revocados por el período establecido por la Autoridad de Aplicación.

3653 FF

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

676

ANEXO

m) Cumplir con las normas y recaudos establecidos para la protección de datos personales.

2.3. – 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 http://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 N° 25.326 y lo dispuesto por el inciso h) del artículo 21 de la Ley N° 25.506, el solicitante o titular de un certificado digital podrá solicitar el acceso a toda la información relativa a las tramitaciones realizadas.

3653

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:

a) El solicitante efectúa el requerimiento de certificado ingresando al siguiente sitio web: http://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

3653 FF

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

FOLIO 678

ANEXO

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 los proveedores de servicios de firma digital o de aplicación:

a) "*commonName*" (OID 2.5.4.3: Nombre común): DEBE corresponder 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): DEBE contener a 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): DEBE estar presente y DEBE coincidir con el nombre de la Persona Jurídica Pública o Privada responsable del servicio o aplicación.

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

ANEXO

d) "*serialNumber*" (OID 2.5.4.5: Nro. de serie): DEBE estar presente y DEBE contener 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): DEBE estar presente y DEBE representar el país de emisión de los certificados, codificado según el estándar [ISO3166] de DOS (2) caracteres.

Para los certificados de Personas Físicas:

a) "*commonName*" (OID 2.5.4.3: Nombre común): DEBE estar presente y DEBE corresponderse 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): DEBE estar presente y DEBE contener 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/CUIL": Clave Única de Identificación Tributaria o Laboral.

b) En caso de extranjeros:

- "PA" [país]: Número de Pasaporte y código de país emisor. El atributo [país] DEBE estar codificado según el estándar [ISO3166] de DOS (2) caracteres.

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

680

ANEXO

- "EX" [país]: Número y tipo de documento extranjero aceptado en virtud de acuerdos internacionales. El atributo [país] DEBE estar codificado según el estándar [ISO3166] de DOS (2) caracteres.

c) "*countryName*" (OID 2.5.4.6: Código de país): DEBE estar presente y DEBE representar el país de emisión de los certificados, codificado según el estándar [ISO3166] de DOS (2) caracteres.

Para los certificados de Personas Jurídicas Públicas o Privadas:

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

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

c) "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.

d) "serialNumber" (OID 2.5.4.5: Nro de serie): DEBE estar presente y DEBE contener 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:

I. "CUIT": Clave Única de Identificación Tributaria para las Personas Jurídicas argentinas.

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

681

ANEXO

II. "ID" [país]: Número de identificación tributario para Personas Jurídicas extranjeras. El atributo [país] DEBE estar codificado según el estándar [ISO3166] de 2 caracteres.

"countryName" (OID 2.5.4.6: Código de país): DEBE estar presente y DEBE representar el país de emisión de los certificados, codificado según el estándar [ISO3166] de 2 caracteres.

Para los certificados de sitio seguro:

a) "*commonName*" (OID 2.5.4.3: Nombre común): DEBE contener la denominación del sitio web de Internet que se busca proteger.

b) "*organizationalUnitName*" (OID 2.5.4.11: Nombre de la Suborganización): DEBE contener a las unidades operativas de las que depende el sitio web, de corresponder, pudiendo utilizarse varias instancias de este atributo de ser necesario.

c) "*organizationName*" (OID 2.5.4.10: Nombre de la Organización): DEBE estar presente y DEBE coincidir con el nombre de la Persona Jurídica Pública o Privada responsable del sitio web.

d) "*serialNumber*" (OID 2.5.4.5: Nro. de serie): DEBE estar presente y DEBE contener 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.

- "countryName" (OID 2.5.4.6: Código de país): DEBE estar presente y DEBE representar el país de emisión de los certificados, codificado según el estándar [ISO3166] de DOS (2) caracteres.

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

682

ANEXO

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 físicas como jurídicas.

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

3653 FF

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 DEBE cumplir con lo establecido en:

I. El artículo 21, inciso a) de la Ley de Firma Digital N° 25.506 y el artículo 34, inciso e) de su reglamentario, Decreto N° 2628/02, relativos a la información a brindar a los solicitantes.

II. El artículo 14, inciso b) de la Ley de Firma Digital N° 25.506 relativo a los contenidos mínimos de los certificados.

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 inciso b) del artículo 21 de la Ley N° 25.506.

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

FOLIO 684

ANEXO

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

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) El certificador o la autoridad del registro, en su caso, 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 según lo dispuesto en el apartado siguiente.

d) La identidad de la Persona Jurídica titular del certificado o responsable del servicio, aplicación o sitio web deberá ser verificada mediante documentación que acredite su condición de tal.

El certificador DEBE cumplir con las siguientes exigencias reglamentarias impuestas por:

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 34, inciso m) del Decreto Nº 2628/02 relativo a la protección de datos personales.

2653

Debe conservarse la documentación que respalda el proceso de identificación de la persona responsable de la custodia de las claves criptográficas.

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

685

ANEXO

El responsable autorizado o a cargo del servicio, aplicación o sitio web debe firmar UN (1) acuerdo que contenga la confirmación de que la información incluida en el certificado es correcta.

3.2.3. - Autenticación de la identidad de Personas Físicas.

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

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:

a) El artículo 21, inciso i) de la Ley N° 25.506 relativo a la conservación de la documentación de respaldo de los certificados emitidos.

b) El artículo 21, inciso f) de la Ley N° 25.506 relativo a la recolección de datos personales.

3653

c) El artículo 34, inciso i) del Decreto N° 2628/02 relativo a generar, exigir o tomar conocimiento de la clave privada del suscriptor.

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

686

ANEXO

d) El artículo 34, inciso m) del Decreto Nº 2628/02 relativo a la protección de datos personales.

Adicionalmente, el certificador debe celebrar UN (1) acuerdo con el solicitante o suscriptor, conforme el Anexo V de la Decisión Administrativa Nº 927/14, del que surge su conformidad respecto a la veracidad de la información incluida en el certificado.

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.

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 Física 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.

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

687

ANEXO

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 físicas 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.

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 Personas Físicas.

Si la solicitud del nuevo certificado se realiza antes de la expiración del certificado, 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.

En los certificados de personas jurídicas o de aplicaciones, incluyendo los de servidores, se deberá tramitar UN (1) nuevo certificado, cumpliendo los pasos requeridos en el apartado 3.2.2. Autenticación de la identidad de Personas Jurídicas Públicas o Privadas.

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

En el caso de certificados digitales de personas físicas 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.

3653

A los fines de la obtención del certificado, no se exigirá la presencia física del suscriptor,

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

688

ANEXO

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:

http://pki.boxcustodia.com accediendo con su usuario y utilizando el código de revocación que le fuera asignado al momento de la emisión del certificado.

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.

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

FOLIO 689

ANEXO

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 físicas 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 Físicas, así como la constancia de C.U.I.T. o 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 física:

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 http://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.

2653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

690

ANEXO

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.

3653

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.

c) Solicitud de certificados de sitio seguro o 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 3.2.2. "Autenticación de la identidad de Personas Jurídicas Públicas o Privadas".

El solicitante deberá completar la correspondiente solicitud aclarando si se trata de un certificado para sitio seguro o si se trata de un certificado de aplicaciones.

Debe contar con una dirección de correo electrónico e informarla en su solicitud, a los fines

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

COORDINACIÓN DE DESPACHO Y PROTOCOLIZACIÓN FOLIO 692 Nº ..... J.G.N.

ANEXO

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 contara 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.** 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.

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 físicas, personas jurídicas, de sitio seguro 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.

3653 FF

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

FOLIO 693

ANEXO

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.

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

FOLIO 0241

ANEXO

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 N° 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.

De acuerdo a lo establecido en la Decisión Administrativa N° 927/14:

- Proveer toda la información que le sea requerida a los fines de la emisión del certificado de modo completo y preciso.
- Utilizar los certificados de acuerdo a los términos y condiciones establecidos en la presente Política Única de Certificación.
- Tomar debido conocimiento, a través del procedimiento previsto en cada caso, del contenido de la Política Única de Certificación, del Manual de Procedimientos, del Acuerdo con Suscriptores y de cualquier otro documento aplicable.

3653 RF

COORDINACIÓN DE DESPACHO FOLIO 695 Nº J.G.M.

ANEXO

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 Físicas, 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 Físicas.

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.

3653

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 N° 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 solicitud del titular del certificado digital o del responsable autorizado para el caso de los certificados de Personas Jurídicas o aplicación (Nota para el certificador: se deberá indicar lo que corresponda).
- Si determinara que el certificado fue emitido en base a información falsa, que al momento de la emisión hubiera sido objeto de verificación.
- Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.
- Por Resolución Judicial.
- Por Resolución de la Autoridad de Aplicación.
- Por fallecimiento del titular.
- Por declaración judicial de ausencia con presunción de fallecimiento del titular.
- Por declaración judicial de incapacidad del titular.

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

FOLIO 697 J.G.M.

ANEXO

- Si se determina que la información contenida en el certificado ha dejado de ser válida.
- Cuando la clave privada asociada al certificado, o el medio en que se encuentre almacenada, se encuentren comprometidos o corran peligro de estarlo.
- Ante incumplimiento por parte del suscriptor de las obligaciones establecidas en el Acuerdo con Suscriptores.
- 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 N° 25.506, del Decreto N° 2628/02 y demás normativa sobre firma digital.
- Por revocación de su propio certificado digital.

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) El suscriptor del certificado.

b) El responsable autorizado que efectuara el requerimiento, en el caso de certificados de persona jurídica o de aplicación.

c) El responsable autorizado por la Persona Jurídica que brinda el servicio o es titular del certificado o la aplicación, en el caso de los certificados de aplicación.

d) El responsable autorizado por la Persona Jurídica responsable del sitio web, en el caso de certificados de sitio seguro.

e) Aquellas personas habilitadas por el suscriptor del certificado a tal fin, previa acreditación fehaciente de tal autorización.

3653 FF

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

FOLIO 1698

ANEXO

f) El certificador o la Autoridad de registro operativamente vinculada.

g) El ente licenciante.

h) La autoridad judicial competente.

i) 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 DIGITAL** (http://pki.boxcustodia.com).

El suscriptor podrá efectuar la revocación a través de alguno de los medios indicados en el punto 3.4 del Formulario de Adhesión a la Política Única de Certificación y de esta Política Única de Certificación.

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

ANEXO

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 34, inciso f) del Decreto Nº 2628/02.

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.

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

FOLIO 700 Nº ..... J.G.M.

ANEXO

El certificador cumple con lo establecido en el artículo 34, inciso g) del Decreto Nº 2628/02 relativo al acceso al repositorio de certificados revocados y las obligaciones establecidas en la Decisión Administrativa Nº 927/14 y sus correspondientes Anexos.

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.

El certificador 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.

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.

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

24 1

FOLIO 701

ANEXO

El certificador debe poner 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.

c) Todas las características opcionales de tales servicios.

El único mecanismo válido para la verificación del estado de los certificados es a través de las Listas de Certificados Revocados.

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.

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

702

ANEXO

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: http://ocsp.pki.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.

4.9.14. - Autorizados a solicitar la suspensión.

3653

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

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

FOLIO 703 Nº ..... J.G.M.

ANEXO

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.

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.

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://www.pki.boxcustodia.com.

4.10.3. – Aspectos operativos.

No existen otros aspectos a mencionar.

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

704

ANEXO

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.

De 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 o custodia de claves privadas de los titulares de certificados digitales, en virtud de lo dispuesto en el inciso b) del artículo 21 de la Ley N° 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.

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.

3653

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.

3653 AF

f) Sanciones a aplicar por acciones no autorizadas.

g) Requisitos para contratación de personal.

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

COORDINACIÓN DE DESPACHO Y PROTOCOLIZACIÓN
FOLIO 206
N°
J.G.M.

ANEXO

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. Debe respetarse lo establecido en el Anexo II Sección 3.

b) Frecuencia de procesamiento de registros.

c) Período de guarda de los registros. Debe respetarse lo establecido en el inciso i) del artículo 21 de la Ley N° 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 (internos vs. externos).

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 N° 25.506 relativo al mantenimiento de la documentación de respaldo de los certificados digitales emitidos.

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

COORDINACIÓN DE DESPACHO Y PROMULGACIÓN FOLIO 707 Nº..... J.G.M.

ANEXO

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. Debe respetarse lo establecido en el Anexo II Sección 3.

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) Requerimientos para los registros de certificados de fecha y hora.

f) Sistemas de recolección y análisis de registros (internos vs. externos).

g) 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. Por su parte la licencia tiene una vigencia de CINCO (5) 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.

3653

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

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

708

ANEXO

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. - Plan de respuesta a incidentes 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 Continuidad de las Operaciones.

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 33 del Decreto Nº 2628/02 en lo relativo a los servicios de infraestructura tecnológica prestados por un tercero.

2653 FF

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

709

ANEXO

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) Revocación del certificado del certificador y de los certificados emitidos.

c) Transferencia de la 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 N° 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 33 del Decreto N° 2628/02, reglamentario de la Ley de Firma Digital, en lo relativo a los servicios de infraestructura tecnológica prestados por un tercero y las obligaciones establecidas en la Decisión Administrativa N° 927/14 y sus correspondientes Anexos.

6. - CONTROLES DE SEGURIDAD TÉCNICA.

3653

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

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

710

ANEXO

controles técnicos que se implementarán sobre las funciones operativas del certificador, Autoridades de Registro, repositorios, suscriptores, etcétera.

6.1. - Generación e instalación del par de claves criptográficas.

6.1.1. - Generación del par de claves criptográficas.

El Certificador, 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 2 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 2. 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.

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

FOLIO 711 J.G.M.

ANEXO

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 la Ley Nº 25.506, artículo 21, inciso b) y el Decreto Nº 2628/02, artículo 34, inciso i).

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 parteutilizará 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.

3653 ff

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

712

ANEXO

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 https://pki.boxcustodia.com

6.1.5. - Tamaño de 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-1 con RSA.

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 para cifrado.

3683

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

713

ANEXO

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:

- Estándares utilizados para la generación del par de claves.
- Número de personas involucradas en el control de la clave privada.
- En caso de existir copias de resguardo de la clave privada, controles de seguridad establecidos sobre ellas.
- Procedimiento de almacenamiento de la clave privada en un dispositivo criptográfico.
- Responsable de activación de la clave privada y acciones a realizar para su activación.
- Duración del período de activación de la clave privada y procedimiento a utilizar para su desactivación.
- Procedimiento de destrucción de la clave privada.
- 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, el Certificador, 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.

Debe respetarse lo establecido en el Anexo II Sección 2 de la Decisión Administrativa Nº 927/14 respecto de los estándares para dispositivos criptográficos.

241

COORDINACIÓN DE GESTIÓN Y PROTOCOLIZACIÓN
FOLIO
714
J.G.M.

ANEXO

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.

3653 FF

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

COORDINACIÓN DE DESPACHO Y PROTOCOLIZACIÓN
FOLIO
715
J.G.M.

ANEXO

activación, bajo los niveles de seguridad requeridos por la normativa vigente.

El Certificador 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, de acuerdo a lo dispuesto por la Decisión Administrativa N° 927/14 en cuanto a los niveles de reguardo de claves.

6.2.6. - Transferencia de claves privadas en dispositivos criptográficos.

El par de claves criptográficas del Certificador 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 2 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 2 y no permiten su exportación.

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,

3653 FF

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.

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

FOLIO 717

ANEXO

6.2.11. – Requisitos de los dispositivos criptográficos.

El Certificador, 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 2 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 2. Los suscriptores generan sus claves mediante el algoritmo RSA con un tamaño mínimo de 2048 bits.

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

3053

COORDINACIÓN DE DESPACHO Y PROTOCOLIZACIÓN
FOLIO
718
Nº
J.G.M.

ANEXO

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. 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.

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

3653 FF

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.

3653 FF

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

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

COORDINACIÓN DE DESPACHO Y PROTOCOLIZACIÓN FOLIO 720 Nº..... J.G.M.

ANEXO

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.

3653 FF

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

FOLIO 721

ANEXO

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 hadware (HSM) utilizados por **AC - BOX CUSTODIA FIRMA DIGITAL** están certificado por el NIST (National Institute 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 Institute of Standards and Technology) sobre la base del Estándar FIPS 140-2 Nivel 2.

Los dispositivos criptográficos utilizados por suscriptores de nivel de seguridad Alto están certificados por NIST (National Institute of Standards and Technology) sobre la base del Estándar FIPS 140-2 Nivel 2.

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.

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

COORDINACIÓN DE DESPACHO Y PROTOCOLIZACIÓN FOLIO 722 Nº..... J.G.M.

ANEXO

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 el Certificador que se encuentran conectados a una red de

comunicación pública, son protegidos por la tecnología apropiada que garantiza su seguridad.

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 previsto en el artículo 10 de la Decisión Administrativa Nº 927/14.

Este servicio está basado en la especificación de los estándares RFC 3161 – "Internet X. 509 Public Key Infrastructure, ETSI TS 102 023, Time-Stamp Protocol, Electronic Signatures and Infrastructures (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.

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 los requerimientos de la Decisión Administrativa Nº 927/14 y 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.

El Certificador adhiere a las recomendaciones de los siguientes documentos en relación al perfil de los certificados:

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

3653

ANEXO

7.1. - Perfil del certificado.

Todos los certificados serán emitidos conforme con lo establecido en la especificación ITU X.509 versión 3 o la que en su defecto, determine el Ente Licenciante, y deben cumplir con las indicaciones establecidas en la sección "2 - Perfil de certificados digitales" del Anexo IV de la Decisión Administrativa N° 927/14.

a) Perfil del certificado de la **persona física**.

Los siguientes campos se encuentran presentes en los certificados emitidos a **Personas Físicas** 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 (SignatureAlgorithm)	sha1RSA 1.2.840.113549.1.1.5	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	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	País del Certificador Licenciado

	2.5.4.6	
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 período de vigencia del certificado comienza
notAfter	<fecha y hora de emisión UTC+ periodo> yyyy/mm/ddhh:mm:ss huso-horario	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	<Nombres y Apellidos> 2.5.4.3	Datos que surgen del Documento Nacional de Identidad presentado por el titular
serialNumber	CUIT/CUIL <Número de identificación> o PA <Pasaporte y código de país> o EX <Número y tipo de documento extranjero> 2.5.4.5	Número de identificación tributaria: CUIT/CUIL de la persona física En caso de extranjeros: "PA" [país]: Número de Pasaporte y código de país emisor. El atributo [país] DEBE estar 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] DEBE estar 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 (SubjectPublic Key Info)	<Clave pública del suscriptor>	Valor de la clave pública del suscriptor
Restricciones básicas (Basic Constraints)	Tipo de asunto = Entidad final pathLenghtConstraint = Null 2.5.29.19	Define el certificado como de entidad final

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

726

ANEXO

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 20 bytes	Contiene un hash de 20 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=http://pki.boxcustodia.com/crl [2]Punto de distribución CRL Dirección URL=http://pki1.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): http://pki.boxcustodia.com/cps.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.

3653 FF

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

FOLIO 727

ANEXO

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: URI http://pki.boxcustodia.com/crt/BCFD.crt OCSP: http://ocsp.pki.boxcustodia.com/	URL de la información para acceder al certificado de AC - BOX CUSTODIA FIRMA DIGITAL y al servicio de OCSP
QCStatment	OID= 2.16.32.1.10.2.2 (claves generadas por disp. FIPS 140-2 nivel 2) OID= 2.16.32.1.10.1 (claves generadas por software) 1.3.6.1.5.5.7.1.3	Declaración del certificado calificado

b) Los siguientes campos se encuentran presentes en los certificados de **Personas Jurídicas** 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 (SignatureAlgorithm)	sha1RSA 1.2.840.113549.1.1.5	Algoritmo usado por el certificador para firmar
Nombre distintivo del emisor (Issuer)		

3653 FF

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

FOLIO 723 Nº ..... COORDINACIÓN DE DESREGULACIÓN Y SIMPLIFICACIÓN J.G.M.

ANEXO

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 período de vigencia del certificado comienza
notAfter	<fecha y hora de emisión UTC+ periodo> yyyy/mm/ddhh:mm:ss huso-horario	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	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/CUIL<Número de CUIT> 2.5.4.5	CUIT/CUIL 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
SubjectPublic Key Info	<Clave pública del suscriptor>	Valor de la clave pública del suscriptor

3653 FF

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

COORDINACIÓN DE DESPACHO Y PROTOCOLIZACIÓN FOLIO 729 Nº ..... J.G.M.

ANEXO

Restricciones básicas (Basic Constraints)	Tipo de asunto = Entidad final pathLenghtConstraint = 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 utiliza la clave contenida en el certificado
Identificador de clave del Suscriptor (Subject Key Identifier)	Valor de hash de 20 bytes	Contiene un hash de 20 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=http://pki.boxcustodia.com/crl [2]Punto de distribución CRL Dirección URL=http://pki1.boxcustodia.com/crl 2.5.29.31	URI del punto de distribución
Política de Certificación (CertificationPolicies)	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): http://pki.boxcustodia.com/cps.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

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

FOLIO 730 Nº ..... J.G.M.

ANEXO

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) 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 Física a cargo de la custodia de la clave privada
serialNumber	<Tipo><Número de documento> 2.5.4.5	Datos CUIT/CUIL del poseedor de las claves
title	<Nombre de la función> 2.5.4.12	Relación que vincula la Persona Física con la Persona Jurídica
Acceso Información Emisor (AuthorityInformation Access)	CA Issuer: URI http://pki.boxcustodia.com/crt/BCFD.crt OCSP: http://ocsp.pki.boxcustodia.com/	URL de la información para acceder al certificado de AC - BOX CUSTODIA FIRMA DIGITAL y al servicio de OCSP
QCStatment	OID= 2.16.32.1.10.2.2 (claves generadas por disp. FIPS 140-2 nivel 2) OID= 2.16.32.1.10.2.3 (claves generadas por disp. FIPS 140-2 nivel 3) OID= 2.16.32.1.10.1 (claves generadas por software) 1.3.6.1.5.5.7.1.3	Declaración del certificado calificado

3653 FF

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

COORDINACIÓN DE DESPACHO Y PROTOCOLIZACIÓN FOLIO 731 Nº ..... J.G.M.

ANEXO

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 (SignatureAlgorithm)	sha1RSA 1.2.840.113549.1.1.5	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 período de vigencia del certificado comienza
notAfter	<fecha y hora de emisión UTC+ periodo> yyyy/mm/ddhh:mm:ss huso-horario	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)		

3653 FF

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

732

ANEXO

commonName	Denominación de la aplicación 2.5.4.3	Nombre de la aplicación, servicio o de la unidad operativa responsable del servicio
organizationName	< Nombre de la organización >2.5.4.10	Nombre de la Persona Jurídica pública o privada responsable de la aplicación
organizationalUnitName	< Nombre de la suborganización>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	CUIT/CUIL <Número de CUIT> 2.5.4.5	<CUIT/CUIL><Número de identificación tributaria de la Persona Jurídica pública o privada responsable de la aplicación>
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
SubjectPublic Key Info	<Clave pública del suscriptor>	Valor de la clave pública del suscriptor
Restricciones básicas (Basic Constraints)	Tipo de asunto = Entidad final pathLenghtConstraint = 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 20 bytes	Contiene un hash de 20 bytes del atributo clave pública del suscriptor

3653 FF

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

FOLIO 733

ANEXO

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=http://pki.boxcustodia.com/crl [2]Punto de distribución CRL Dirección URL=http://pki1.boxcustodia.com/crl 2.5.29.31	URI del punto de distribución
Política de Certificación (CertificationPolicies)	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): http://pki.boxcustodia.com/cps.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 - BOX CUSTODIA FIRMA DIGITAL que emitió el certificado.
Uso Extendido de Clave (Extended Key Usage)	Autenticación del cliente (1.3.6.1.5.5.7.3.2) OCSPSigning (1.3.6.1.5.5.7.3.9) 2.5.29.37	Usos adicionales de la clave pública a los enumerados en el campo keyUsage
Acceso Información Emisor (AuthorityInformation Access)	CA Issuer: URI http://pki.boxcustodia.com/crt/BCFD.crt OCSP: http://ocsp.pki.boxcustodia.com/	URL de la información para acceder al certificado de ACBOX CUSTODIA FIRMA DIGITAL y al servicio de OCSP

2653 FF

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

FOLIO 737

ANEXO

QCStatment	OID= 2.16.32.1.10.2.2 (claves generadas por disp. FIPS 140-2 nivel 2) OID= 2.16.32.1.10.2.3 (claves generadas por disp. FIPS 140-2 nivel 3) OID= 2.16.32.1.10.1 (claves generadas por software) 1.3.6.1.5.5.7.1.3	Declaración del certificado calificado

d) Perfil del certificado para **Sitios Seguros**.

Los siguientes campos se encuentran presentes en los certificados de sitios seguros 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 DIGITA La cada certificado
Algoritmo de Firma (SignatureAlgorithm)	sha1RSA 1.2.840.113549.1.1.5	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

3653 FF

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

FOLIO 735

ANEXO

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 período de vigencia del certificado comienza
notAfter	<fecha y hora de emisión UTC+ periodo> yyyy/mm/ddhh:mm:ss huso-horario	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 del Sitio Web de Internet 2.5.4.3	Denominación del sitio web de Internet que se busca proteger
serialNumber	CUIT/CUIL <Número de CUIT> 2.5.4.5	<CUIT/CUIL><Número de identificación tributaria de la Persona Jurídica pública o privada responsable del Sitio Web>
organizationName	<Nombre de la empresa u organismo> 2.5.4.10	Nombre de la Persona Jurídica pública o privada responsable del sitio web.
organizationalUnitName	<Unidad operativa de la organización> 2.5.4.11	Nombre de la unidad operativa de la que depende el sitio web.
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
SubjectPublic Key Info	<Clave pública del suscriptor>	Valor de la clave pública del suscriptor
Restricciones básicas (Basic Constraints)	Tipo de asunto = Entidad final pathLenghtConstraint = Null 2.5.29.19	Define el certificado como de entidad final
Usos de clave (Key Usage)	digitalSignature = 1 nonRepudiation = 1 keyEncipherment = 1 dataEncipherment= 0 keyAgreement = 1 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0	Propósito para el cual será utilizada la clave contenida en el certificado

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

ANEXO

	2.5.29.15	
Identificador de clave del Suscriptor (Subject Key Identifier)	Valor de hash de 20 bytes	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados (CRLDistribution Points)	Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints) [1]Punto de distribución CRL Dirección URL=http://pki.boxcustodia.com/crl [2]Punto de distribución CRL Dirección URL=http://pki1.boxcustodia.com/crl 2.5.29.31	URI del punto de distribución
Política de Certificación (CertificationPolicies)	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): http://pki.boxcustodia.com/cps.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 - BOX CUSTODIA FIRMA DIGITAL que emitió el certificado.
Uso Extendido de Clave (Extended Key Usage)	Autenticación del servidor (1.3.6.1.5.5.7.3.1) Autenticación del cliente (1.3.6.1.5.5.7.3.2)	Usos adicionales de la clave pública a los enumerados en el campo keyUsage

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

737

ANEXO

Nombres Alternativos del Suscriptor (SubjectAlternativeName) : IP/DNS/URI		
Acceso Información Emisor (AuthorityInformation Access)	CA Issuer: URI http://pki.boxcustodia.com/crt/BCFD.crt OCSP: http://ocsp.pki.boxcustodia.com/	URL de la información para acceder al certificado de ACBOX CUSTODIA FIRMA DIGITAL y al servicio de OCSP
QCStatment	OID= 2.16.32.1.10.1 (claves generadas por software) 1.3.6.1.5.5.7.1.3	Declaración del certificado calificado

e) Los siguientes campos se encuentran presentes en los **certificados para Autoridades de Competencia**, 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 (SignatureAlgorithm)	sha1RSA 1.2.840.113549.1.1.5	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

3653 FF

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

732

ANEXO

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 período de vigencia del certificado comienza
notAfter	<fecha y hora de emisión UTC+ periodo> yyyy/mm/ddhh:mm:ss huso-horario	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	<Nombre del Servicio> 2.5.4.3	Denominación del Servicio de emisión del Sello 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
organizationalUnitName	<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
Clave pública del suscriptor (SubjectPublickeyInfo)	<Clave pública del suscriptor>	Valor de la clave pública del suscriptor
Restricciones básicas (Basic Constraints)	Tipo de asunto = Entidad final pathLenghtConstraint = Null 2.5.29.19	Define el certificado como de entidad final

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

ANEXO

Usos de clave (Key Usage)	digitalSignature = 1 nonRepudiation = 1 keyEncipherment =0 dataEncipherment =0 keyAgreement =0 keyCertSign = 1 cRLSign = 1 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 20 bytes	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados (CRLDistribution Points)	Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints) [1]Punto de distribución CRL Dirección URL=http://pki.boxcustodia.com/crl [2]Punto de distribución CRL Dirección URL=http://pki1.boxcustodia.com/crl 2.5.29.31	URI del punto de distribución
Política de Certificación (CertificationPolicies)	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): http://pki.boxcustodia.com/cps.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.

3653 FF

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

740

ANEXO

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	Corresponde a las respuestas del servicio OCSP
Acceso Información Emisor (AuthorityInformation Access)	CA Issuer: URI http://pki.boxcustodia.com/crt/BCFD.crt OCSP: http://ocsp.pki.boxcustodia.com/	URL de la información para acceder al certificado de AC - BOX CUSTODIA FIRMA DIGITAL y al servicio de OCSP
QCStatment	OID= 2.16.32.1.10.2.2 (claves generadas por disp. FIPS 140-2 nivel 2) OID= 2.16.32.1.10.2.3 (claves generadas por disp. FIPS 140-2 nivel 3) 1.3.6.1.5.5.7.1.3	Declaración del certificado calificado

f) Los siguientes campos se encuentran presentes en los certificados para Autoridades de **Sello de Tiempo**, 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 (SignatureAlgorithm)	sha1RSA 1.2.840.113549.1.1.5	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 del Certificador

3653 FF

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

741

ANEXO

	CUIT 30704582370 2.5.4.5	
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 período de vigencia del certificado comienza
notAfter	<fecha y hora de emisión UTC+ periodo> yyyy/mm/ddhh:mm:ss huso-horario	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	<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/CUIL 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
organizationalUnitName	<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	4096bits	Longitud de la clave pública del suscriptor
Clave pública del suscriptor (SubjectPublickeyInfo)	<Clave pública del suscriptor>	Valor de la clave pública del suscriptor
Restricciones básicas (Basic	Tipo de asunto = Entidad final pathLenghtConstraint = Null 2.5.29.19	Define el certificado como de entidad final

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

242

ANEXO

Constraints)		
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 20 bytes	Contiene un hash de 20 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=http://pki.boxcustodia.com/crl [2]Punto de distribución CRL Dirección URL=http://pki1.boxcustodia.com/crl 2.5.29.31	URI del punto de distribución
Política de Certificación (CertificationPolicies)	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): http://pki.boxcustodia.com/cps.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

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

743

ANEXO

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) 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: URI http://pki.boxcustodia.com/crt/BCFD.crt OCSP: http://ocsp.pki.boxcustodia.com/	URL de la información para acceder al certificado de AC - BOX CUSTODIA FIRMA DIGITAL y al servicio de OCSP
QCStatment	OID= 2.16.32.1.10.2.2 (claves generadas por disp. FIPS 140-2 nivel 2) OID= 2.16.32.1.10.2.3 (claves generadas por disp. FIPS 140-2 nivel 3) 1.3.6.1.5.5.7.1.3	Declaración del certificado calificado

g) Los siguientes campos se encuentran presentes en los certificados del **servicio de consulta OCSP**, 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 (SignatureAlgorithm)	sha1RSA 1.2.840.113549.1.1.5	Algoritmo usado por el certificador para firmar

8653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

FOLIO 744 Nº ..... J.G.M. COORDINACIÓN DE ASESORAMIENTO Y LEGALIZACIÓN

ANEXO

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 período de vigencia del certificado comienza
notAfter	<fecha y hora de emisión UTC+ periodo> yyyy/mm/ddhh:mm:ss huso-horario	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 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
organizationName	BOX CUSTODIA DE ARCHIVOS S.A. 2.5.4.10	Denominación 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
Publickeylength	2048 bits	Longitud de la clave pública del suscriptor

3653 FF

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

745

ANEXO

Clave pública del suscriptor (SubjectPublickeyInfo)	<Clave pública del suscriptor>	Valor de la clave pública del suscriptor
Restricciones básicas (Basic Constraints)	Tipo de asunto = Entidad final pathLenghtConstraint = 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 20 bytes	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints)	[1]Punto de distribución CRL Dirección URL=http://pki.boxcustodia.com/crl/BCFD.crl 2.5.29.31	URI del punto de distribución
Política de Certificación (CertificationPolicies)	OID de la Política de Certificación de BOX CUSTODIA DE ARCHIVOS S.A. , URI de la Política: http://pki.boxcustodia.com/cps.pdf Texto de aviso=certificado emitido por un certificador licenciado en el marco de la 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.

3653

ANEXO

Uso Extendido de Clave (Extended Key Usage)	OCSPSigning (1.3.6.1.5.5.7.3.9)	Corresponde a las respuestas del servicio OCSP
Acceso Información Emisor (AuthorityInformation Access)	CA Issuer: URI http://pki.boxcustodia.com/crt/BCFD.crt OCSP: http://ocsp.pki.boxcustodia.com/	URL de la información para acceder al certificado de AC - BOX CUSTODIA FIRMA DIGITAL y al servicio de OCSP
QCStatment	OID= 2.16.32.1.10.2.2 (claves generadas por disp. FIPS 140-2 nivel 2) OID= 2.16.32.1.10.2.3 (claves generadas por disp. FIPS 140-2 nivel 3) 1.3.6.1.5.5.7.1.3	Declaración del certificado calificado

7.2 Perfil de la lista de certificados revocados.

En lo referente a CRLs la **AC – BOX CUSTODIA FIRMA DIGITAL** adhiere a las recomendaciones del documento:

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

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)	1	Corresponde a versión 2
Algoritmo de Firma (SignatureAlgorithm)	sha1RSA 1.2.840.113549.1.1.5	Algoritmo usado por el certificador para firmar

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

FOLIO 747

ANEXO

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 entre en vigencia
Próxima Actualización (nextUpdate)	<fecha y hora UTC> yyyy/mm/ddhh:mm:ss huso-horario	Fecha y hora de emisión de la próxima Lista de Certificados Revocados
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 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
Indicador 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	

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

FOLIO 748

ANEXO

(ReasonCode)		
Algoritmo de Identificación Huella Digital	SHA1	
Versión de CA	V0.0	

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 y cumplir con las indicaciones establecidas en la sección "4 - Perfil de la consulta en línea del estado del certificado" del Anexo IV de la Decisión Administrativa Nº 927/14 – "Perfiles de los Certificados y de las Listas de Certificados Revocados".

7.3.1. – Consultas OCSP.

A completar sobre la base de lo establecido en el documento referido en el apartado 4.1 del Anexo IV de la Decisión Administrativa Nº 927/14.

7.3.2. - Respuestas OCSP.

A completar sobre la base de lo establecido en el documento referido en el apartado 4.3 del Anexo IV de la Decisión Administrativa Nº 927/14.

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.

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

COORDINACIÓN DE DESPACHO Y PROTOCOLIZACIÓN FOLIO 749 J.C.M.

ANEXO

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 18 a 21 del Decreto Nº 2628/02, reglamentario de la Ley de Firma Digital, relativos al sistema de auditoría y el artículo 20 del mismo, vinculado a conflicto de intereses.

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.

3653

f) La información relevante de los informes de las auditorías es publicada en el sitio web de la **AC – BOX CUSTODIA FIRMA DIGITAL**: http://pki.boxcustodia.com.

9. – ASPECTOS LEGALES Y ADMINISTRATIVOS.

9.1. – Aranceles.

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

Los aranceles para las distintas clases de certificados serán publicados en el siguiente sitio web de **BOX CUSTODIA DE ARCHIVOS S.A.**:

http://pki.boxcustodia.com

9.2. - Responsabilidad Financiera.

Se incluyen las cláusulas que establezcan la responsabilidad por daños potenciales que podrían sufrir los suscriptores de certificados y los terceros usuarios, en razón del posible incumplimiento de lo dispuesto en las normas legales y reglamentarias y en la Política Única de Certificación y de los recursos con los que cuenta el certificador para afrontarlos.

En caso de existir seguros de responsabilidad civil debe proveerse información que los respalde.

La responsabilidad financiera se origina en lo establecido por la Ley Nº 25.506 y su Decreto Nº 2628/02 y en las disposiciones de la presente política.

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

751

ANEXO

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.

3653 FF

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

752

ANEXO

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.

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

753

ANEXO

- 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 caso resulta de aplicación la Ley N° 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 físicas 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) Toda otra referida a personas físicas 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.

3653

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.

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

754

ANEXO

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.**

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

755

ANEXO

9.6. – Responsabilidades y garantías.

Se regirá por lo establecido en la Ley Nº 25.506, su Decreto Nº 2628/02, la Decisión Administrativa Nº 927/14 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

3653

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

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

FOLIO 757

ANEXO

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

3653

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 la Ley Nº 25.506, artículo 21, inciso q) y por la Decisión Administrativa Nº 927/14 y sus anexos respectivos.

Toda Política Única de Certificación es sometida a aprobación del ente licenciante durante el proceso de licenciamiento.

Todo cambio a la Política Única de Certificación debe ser comunicado al suscriptor.

Adicionalmente, el certificador licenciado incluirá la información específica correspondiente a esta sección, la cual surge del Anexo I de la Decisión Administrativa Nº 927/14.

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

FOLIO 759

ANEXO

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 http://pki.boxcustodia.com/

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 N° 19.549 y su Decreto Reglamentario N° 1759/72.

La presente Política Única de Certificación se encuentra en un todo subordinado a las prescripciones de la Ley N° 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

3653

Jefatura de Gabinete de Ministros
Secretaría de Gabinete

241

FOLIO 760

ANEXO

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 (10) 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.

3653

FOLIO 761

ANEXO

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, el Decreto Nº 2628/02, y toda otra norma complementaria dictada por la autoridad competente.

9.15. – Conformidad con normas aplicables.

La legislación aplicable a la actividad del Certificador es la Ley N° 25.506, el Decreto N° 2628/02, la Decisión Administrativa N° 927/14 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.

3653