Box CUSTODIA Y GESTIÓN DIGITAL

MANUAL DE PROCEDIMIENTOS

AUTORIDAD CERTIFICANTE
BOX CUSTODIA DE ARCHIVOS S.A.

Versión 2.3 (Abril 2022)

www.boxcustodia.com

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

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

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

Índice

1. INTRODUCCIÓN

1.1. Descripción General

El presente manual establece los procedimientos relacionados con la Emisión y Administración de los Certificados Digitales de la Autoridad Certificante de BOX CUSTODIA DE ARCHIVOS S.A., (en adelante "AC - BOX CUSTODIA FIRMA DIGITAL"), en el marco de la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA (Ley Nº 25.506 y sus modificatoria) y los solicitantes, suscriptores y terceros usuarios de los certificados que éste emita. Un certificado vincula los datos de verificación de Firma Digital de una persona humana o jurídica o con una aplicación a un conjunto de datos que permiten identificar a dicha entidad, conocida como suscriptor del certificado.
La Autoridad de Aplicación de la Infraestructura de Firma Digital antes mencionada es la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS.

Los procedimientos requerirán para su ejecución, las funciones instrumentadas por el Sistema Informático de la AC - BOX CUSTODIA FIRMA DIGITAL, desarrollado por BOX CUSTODIA DE ARCHIVOS S.A.

1.2. Identificación

a) Nombre: Manual de Procedimientos para Certificados Digitales de la AC - BOX CUSTODIA FIRMA DIGITAL;
b) Versión: 2.2;
c) Fecha de aplicación: A partir de su aprobación por el Ente Licenciante;
d) OID: 2.16.32.1.1.6;
e) Lugar o sitio de publicación: se publica en el sitio web de la AC - BOX CUSTODIA FIRMA DIGITAL https://pki.boxcustodia.com/

1.3. Participantes y aplicabilidad.

1.3.1. Certificador.

Los procedimientos descriptos en el presente manual, en sus partes pertinentes, son de aplicación obligatoria para BOX CUSTODIA DE ARCHIVOS S.A.

1.3.2. Autoridad de Registro (AR).

Los procedimientos descriptos en el presente manual, en sus partes pertinentes, son de aplicación obligatoria para la Autoridad de Registro Central y Autoridades de Registro Delegadas.

En la Autoridad de Registro se realizan las funciones de "Verificación de Identidad de los Solicitantes" de Certificados Digitales y la "Gestión de Trámites asociados".

La AC - BOX CUSTODIA FIRMA DIGITAL instrumentará un módulo que se corresponde con las funciones de las Autoridades de Registro, en adelante AR, el que será operado por el Responsable de AR, y por los Oficiales de Registro designados.

En los documentos anexos al presente Manual, “Procedimientos de las Autoridades de Registro de la AC - BOX CUSTODIA FIRMA DIGITAL”, se establecerán los procedimientos para las designaciones necesarias y para su funcionamiento, entre ellos, de su responsable y de sus Oficiales de Registro titular y suplentes, así como también sus responsabilidades y cumplimiento de funciones en relación con el proceso de gestión de Certificados Digitales.

1.3.3. Suscriptores de certificados.

Los procedimientos descriptos en el presente Manual, en sus partes pertinentes a cada Clase de Certificado, son de aplicación obligatoria para los Solicitantes y Suscriptores de Certificados.

Los solicitantes de los Certificados Digitales deberán ser persona humana o jurídica, sean éstas públicas o privadas, y aquellos que presten otros servicios relacionados con la firma digital que puedan firmar digitalmente transacciones, documentación, y todas las acciones necesarias para formalizar actos, procesos, funciones de gestión documental pública o privada, procesos de despapelización y/o digitalización, desarrollo e implementación de sistemas o aplicativos que protejan la autoría e integridad de la documentación tratada, e intervenida, a través del uso de la Firma Digital, utilizando Certificados emitidos por la AC – BOX CUSTODIA FIRMA DIGITAL, conforme el marco normativo especificado en la Política Única de Certificación de la referida Autoridad Certificante.

Los certificados digitales contemplados en la Política Única de Certificación de la AC - BOX CUSTODIA FIRMA DIGITAL y que se regulan en este manual se distinguen en las siguientes clases:

- Certificado de Aplicaciones.
- Certificado de Persona Humana.
- Certificado de Persona Jurídica o Privadas.
- Certificado para Autoridad de Sellos de Tiempo.
- Certificado para Autoridades de Competencia.

Cada una de estas Clases de Certificados se podrá emitir con dos tipos de soporte de clave:

a) Almacenes criptográficos implementados por software;
b) Almacenes criptográficos implementados por hardware, por medio de un dispositivo criptográfico.

Además de los perfiles de Certificados anteriormente enunciados, la AC - BOX CUSTODIA FIRMA DIGITAL, emitirá también un Certificado para Servicios de Estado en Línea (OCSP), donde el suscriptor es la propia AC - BOX CUSTODIA FIRMA DIGITAL, usado este certificado para brindar el servicio de verificación en línea del estado de un certificado.

La clase de certificado determinará su posibilidad de utilización por parte de los sistemas que implementen el esquema de Firma Digital.

1.3.4. Terceros Usuarios

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

1.4. Uso de los certificados

Las claves correspondientes a los certificados digitales que se emitan bajo la presente Política Única 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 del Manual de Procedimientos

1.5.1. Responsable del Documento

Este manual es administrado por BOX CUSTODIA DE ARCHIVOS S.A.

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

Correo electrónico: info@pki.boxcustodia.com

Teléfono: +54 11 5032 2355

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

1.5.2. Contacto

BOX CUSTODIA DE ARCHIVOS S.A. es el responsable del registro, mantenimiento e interpretación del presente manual.

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

Domicilio: Perú Nº 277, piso 4, oficina 1. (C1066AAG) CIUDAD AUTÓNOMA DE BUENOS AIRES.

Correo electrónico: info@pki.boxcustodia.com

Teléfono: +54 11 5032 2355

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

1.5.3. Procedimiento de aprobación de la Política Única de Certificación

El presente Manual de Procedimientos ha sido aprobado por el Ente Licenciante de Firma Digital de la República Argentina. La primera edición de este Manual de procedimiento fue presentada ante el Ente Licenciante durante el proceso de licenciamiento, el que fue aprobado por la Resolución de la SECRETARÍA DE GABINETE de la JEFATURA DE GABINETE DE MINISTROS Nº 43 del 15 de mayo de 2015.

1.6. - Definiciones y Acrónimos.

1.6.1. - Definiciones.

Se incluirán las definiciones de los conceptos relevantes utilizados en la Política de

Certificación, incluyendo los siguientes:

- **Autoridad de Aplicación:** la SECRETARÍA DE INNOVACIÓN PÚBLICA 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:
  a) Recepción de las solicitudes de emisión de certificados.
  b) Validación de la identidad y autenticación de los datos de los titulares de certificados.
  c) Validación de otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue el Certificador Licenciado BOX CUSTODIA DE ARCHIVOS S.A.
  d) Remisión de las solicitudes aprobadas al Certificador Licenciado BOX CUSTODIA DE ARCHIVOS S.A. con la que se encuentre operativamente vinculada.
  e) Recepción y validación de las solicitudes de revocación de certificados; y su direccionamiento al Certificador Licenciado BOX CUSTODIA DE ARCHIVOS S.A. con el que se vinculen.
  f) Identificación y autenticación de los solicitantes de revocación de certificados.
  g) Archivo y la conservación de toda la documentación respaldatoria del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por el certificador licenciado.
  h) Cumplimiento de las normas y recaudos establecidos para la protección de datos personales.
  i) Cumplimiento de las disposiciones que establezca la Política Única de Certificación y el Manual de Procedimientos del Certificador Licenciado con el que se encuentre vinculada, en la parte que resulte aplicable.

  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.
- **Autoridad de Sello de Tiempo:** Entidad que acredita la fecha y hora cierta, asignada a un documento o registro electrónico por una tercera parte confiable y firmada digitalmente por ella.

- **Autoridad de Sello de Competencia:** Entidad que acredita competencias, roles, funciones o relaciones laborales del titular de un certificado de firma digital.
- **Certificado Digital:** Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular (artículo 13 de la Ley N° 25.506).
- **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 Nº 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.
- **Ente licenciante:** Es el encargado de aprobar las Políticas Únicas de Certificación, el Manual de Procedimiento, el Plan de Seguridad, el Plan de Cese de Actividades y el Plan de Contingencia, presentados por los Certificadores solicitantes de la licencia o licenciados en el marco de la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA.
- **Lista de certificados revocados** Lista de certificados que han sido dejados sin efecto en forma permanente por el Certificador Licenciado, la cual ha sido firmada digitalmente y publicada por el mismo. En inglés: Certificate Revocation List (CRL). (CRL por sus siglas en ingles)
- **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). (CPS por sus siglas en inglés)
- **Plan de Cese de Actividades:** conjunto de actividades a desarrollar por el certificador licenciado en caso de finalizar la prestación de sus servicios.
- **Plan de Contingencia:** Conjunto de procedimientos a seguir por el Certificador Licenciado ante situaciones de ocurrencia no previstas que comprometan la continuidad de sus operaciones.
- **Plan de Seguridad:** Conjunto de políticas, prácticas y procedimientos destinados a la protección de los recursos del certificador licenciado.

- **Política de Privacidad:** conjunto de declaraciones que el Certificador Licenciado se compromete a cumplir de manera de resguardar los datos de los solicitantes y suscriptores de certificados digitales por él emitidos.

- **Servicio OCSP (Protocolo en línea del estado de un certificado - "Online Certificate Status Protocol"):** servicio de verificación en línea del estado de los certificados. El OCSP es un método para determinar el estado de revocación de un certificado digital usando otros medios que no sean el uso de Listas de Revocación de Certificados (CRL).
- **Suscriptor o Titular de Certificado Digital:** Persona, jurisdicción o entidad a cuyo nombre se emite un certificado y que posee una clave privada que se corresponde con la clave pública contenida en el mismo.
- **Tercero Usuario:** persona humana o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente.

1.6.2. - Acrónimos.

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

CUIT - Clave Única de Identificación Tributaria

IEC - International Electrotechnical Commission

IETF - Internet Engineering Task Force

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

OID - Identificador de Objeto ("Object Identifier'')

ONTI - Oficina Nacional de Tecnologías de Información

RFC - Request For Comments

2. RESPONSABILIDADES VINCULADAS A LA PUBLICACIÓN Y A LOS REPOSITORIOS

2.1. Repositorios

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

2.2. Publicación de Información del Certificador

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

a) Política Única de Certificación en sus versiones vigentes y anteriores

b) Acuerdo con Suscriptores.

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

d) Política de Privacidad.

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

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

g) Repositorio de certificados revocados.

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

i) Consulta de certificados emitidos (indicando su estado).

La publicación se realiza cumpliendo los procedimientos que se detallan en el punto 8.- "Administración de Especificaciones" del presente Manual de Procedimientos.

2.3. Listado de Autoridades de Registro - Frecuencia de publicación

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

Independientemente de un suceso de Revocación de un Certificado, la Lista de Certificados Revocados (CRL) se renovará cada 24 horas, aunque no tuviere modificaciones.

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 actualización del resto de la información contenida en el Repositorio, se realizarán en un plazo menor a 24 horas, siempre que se hubiere cumplido con los procedimientos de Administración de Especificaciones del punto 8. del presente Manual.

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

2.4. Controles de acceso a la información

Se garantizan los controles de los accesos al certificado del certificador, a la Lista de Certificados Revocados y a las versiones anteriores y actualizadas de la Política de Certificación y a su Manual de Procedimientos (excepto en sus aspectos confidenciales).

Solo se revelará información confidencial o privada, si es requerida judicialmente o en el marco de procedimientos administrativos.

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

BOX CUSTODIA DE ARCHIVOS S.A. garantiza el acceso permanente, eficiente y gratuito de los titulares y terceros a la información publicada en su repositorio incluyendo la lista de certificados

revocados y a disponer y dedicar los recursos necesarios para garantizar la seguridad de los datos almacenados, desde el punto de vista técnico y jurídico.

2.5. Repositorios de Certificados y Listas de Revocación.

La AC - BOX CUSTODIA FIRMA DIGITAL proveerá información del Estado de Validez de los Certificados emitidos, a través de su sitio web " https://pki.boxcustodia.com/ ". Una vez en el sitio web, deberá ingresarse el número de Certificado Digital sobre el cual quiera consultarse su correspondiente estado, y el servicio emitirá un mensaje acorde al estado del Certificado consultado. El Repositorio de Certificados se actualizará inmediatamente después de ocurrida una emisión de un Certificado Digital. Por su parte toda vez determinada la necesidad de Revocación de un Certificado Digital, el mismo será revocado inmediatamente por medio de la AC - BOX CUSTODIA FIRMA DIGITAL. La actualización de la lista de certificados digitales revocados se cumplirá en forma automática y sincrónica con la correspondiente operación de revocación de la AC - BOX CUSTODIA FIRMA DIGITAL. Independientemente de ello, la lista se renueva cada 24 horas aunque no hubieran ocurrido novedades. De este modo, salvo contingencias operativas, la publicación del estado de los certificados digitales revocados en el sitio web de la AC - BOX CUSTODIA FIRMA DIGITAL será de forma inmediata para su consulta por parte de Terceros Usuarios. La Lista de Certificados Digitales Revocados incluirá la Fecha y la Hora de su última actualización.

El acceso a la Lista de Certificados revocados es público, no estableciéndose ninguna clase de restricción. Se encuentra disponible en el sitio web de la AC - BOX CUSTODIA FIRMA DIGITAL "https://pki.boxcustodia.com/crl "o bien se puede acceder al estado de los certificados por medio del servicio Online Certificate Status Protocol (OCSP) a través del sitio https://ocsp.pki.boxcustodia.com/. El servicio OCSP deberá configurarse en las aplicaciones cliente de los terceros usuarios, mediante la identificación de la autoridad certificante y la provisión de la URL del servicio.

2.6.- Confidencialidad.

2.6.1. - Información confidencial.

La divulgación de información considerada confidencial, a petición de autoridad judicial o competente, será autorizada en última instancia por el Responsable de la AC - BOX CUSTODIA FIRMA DIGITAL, quien decidirá sobre la conveniencia de la oportunidad y medio en que se realizará la comunicación del contenido al requirente.

2.6.2. - Información no confidencial.

La información no confidencial que tenga que ver con la AC - BOX CUSTODIA FIRMA DIGITAL está accesible libremente desde Intranet en el sitio web https://pki.boxcustodia.com/ , en las secciones o repositorios correspondientes.

2.6.3. – Publicación de información sobre la revocación o suspensión de un certificado.

El acceso a las listas de certificados revocados es público y está disponible en el sitio web de la AC - BOX CUSTODIA FIRMA DIGITAL "https://pki.boxcustodia.com/crl ", bajo los procedimientos especificados en el punto 2.6.4. – "Repositorios de certificados y listas de revocación" del presente Manual de Procedimientos. De acuerdo con la Ley Nº 25.506, el estado de Suspensión no está, ni será admitido.

2.6.4. – Divulgación de información a autoridades judiciales.

Cuando existiese un pedido formal de información emanado de una Autoridad Judicial, sobre cualquiera de los datos o información de un suscriptor o grupo de ellos, incluyéndose expresamente pero no limitándose a la de "carácter confidencial", se le dará el tratamiento detallado en el punto 2.6.1. – "Información confidencial" correspondiente al presente Manual de Procedimientos.

2.6.5. – Divulgación de información como parte de un proceso judicial o administrativo.

Se aplicará idéntico procedimiento que el punto 2.6.4.- "Divulgación de información a autoridades judiciales".

2.6.6. - Divulgación de información por solicitud del suscriptor.

De acuerdo con la Ley Nº 25.326 de Protección de los Datos Personales, todo suscriptor de un certificado digital puede tener acceso a sus datos de identificación u otra información vinculada al ciclo de vida de su certificado digital. A esos efectos deberá efectuar la correspondiente solicitud por escrito ante su AR.

En caso que sea necesario divulgar información referida a los datos de identificación del suscriptor de un certificado digital, el suscriptor deberá otorgar la autorización correspondiente. La comunicación fehaciente al suscriptor explicando los motivos del requerimiento deberá estar avalada por el Responsable de la AC - BOX CUSTODIA FIRMA DIGITAL, y podrá efectuarse por escrito o mediante una notificación desde el portal de suscriptor de la AC - BOX CUSTODIA FIRMA DIGITAL.

2.6.7. – Otras circunstancias de divulgación de información.

Cualquier otra circunstancia de divulgación de información no prevista en los apartados anteriores, será autorizada en última instancia por el Responsable de la AC - BOX CUSTODIA FIRMA DIGITAL, quien decidirá sobre la conveniencia de la oportunidad y medio en que se realizará la divulgación de la información en trato.

3. IDENTIFICACIÓN Y AUTENTICACIÓN.

3.1. - Asignación de nombres de suscriptores.

3.1.1. - Tipos de Nombres.

Para el CUIT/CUIL/CDI indicado en el punto 3.2.- "Registro inicial" del presente Manual de Procedimientos, la AC - BOX CUSTODIA FIRMA DIGITAL mostrará como nombre y apellido del solicitante aquellos obrantes en sus registros. Si al momento de ingresar su solicitud el solicitante encontrara que el nombre o apellido mostrados por el sistema, no coincidieran con los de su documento de identidad, deberá ingresar los de éste último. En caso que tenga solicitudes de certificados en trámite, o certificados válidos, no podrá cambiarlos. La modificación de estos datos sólo impacta en el sistema de la AC - BOX CUSTODIA FIRMA DIGITAL. Si tuviera que efectuar correcciones sobre su CUIL/CUIT/CDI, deberá efectuar los procedimientos indicados en el punto 3.1.6.- "Procedimiento de resolución de disputas sobre nombres" de este manual

3.1.2. Necesidad de Nombres Distintivos

Los atributos mínimos incluidos en los certificados con el fin de identificar unívocamente a su titular se encuentran definidos en el apartado 3.1.2. de la Política Única de Certificación.

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. Respecto de la interpretación de ciertos caracteres especiales que pudieran estar presentes en el nombre o apellido del solicitante/suscriptor, éste último deberá reflejarlos de manera acorde a como están escritos en su documento de identificación personal.

3.1.5. Unicidad de nombres

El nombre distintivo es 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 persona humana como jurídica.

3.1.6.- Procedimiento de resolución de disputas sobre nombres.

En la solicitud sólo se aceptarán números de CUIL/CUIT/CDI válidos para la emisión. En caso de conflictos el solicitante o suscriptor deberá solicitar la resolución del inconveniente ante el organismo responsable del nombre en cuestión: para el caso de un CUIL, la Administración Nacional de la Seguridad Social (ANSES), para el caso de un CUIT/CDI, deberá resolverlo ante una dependencia de BOX CUSTODIA DE ARCHIVOS S.A. El solicitante tiene la opción en el sistema informático de la AC, de corregir sus datos de nombre y apellido al momento de solicitar un certificado, corrección que tendrá efecto únicamente a los fines del certificado digital. La modificación de datos del padrón deberá realizarse por otra vía ante la autoridad que corresponda. Para la resolución de disputas

sobre nombres ante el caso de una incongruencia, error, omisión o duplicación de datos de identificador de usuario en el CUIL/CUIT/CDI del solicitante de un certificado digital, que no hayan podido ser resueltas efectivamente por los organismos administradores o responsables de esos datos, se podrá recurrir a la AC - BOX CUSTODIA FIRMA DIGITAL mediante la presentación de una nota en su Mesa de Entradas, dirigida al Responsable de la AC - BOX CUSTODIA FIRMA DIGITAL, explicando el caso. BOX CUSTODIA DE ARCHIVOS S.A. evaluará en instancias administrativas la situación planteada

3.1.7. Reconocimiento, autenticación y rol de las marcas registradas

No se admite la inclusión de marcas comerciales, marcas de servicios o nombres de fantasía como nombres distintivos en los certificados, excepto en el caso de personas jurídicas o aplicaciones, en los que se aceptará en base a la documentación presentada.

El certificador se reserva el derecho de tomar todas las decisiones referidas a posibles conflictos sobre la utilización y titularidad de cualquier nombre entre sus suscriptores conforme su normativa al respecto. En caso de conflicto, la parte que solicite el certificado demostrará su interés legítimo y su derecho a la utilización de un nombre en particular.

3.2. - Registro inicial.

El solicitante de un certificado digital que será otorgado por la AC - BOX CUSTODIA FIRMA DIGITAL, ingresará al sitio web de la AC - BOX CUSTODIA FIRMA DIGITAL " https://pki.boxcustodia.com/ ", luego seleccionar la opción de "Gestionar Certificados".

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

El certificador cumple con lo establecido en:

a) El artículo 21, inciso a) de la Ley de Firma Digital Nº 25.506 y el artículo 21, inciso 7) de su reglamentario, Decreto Nº 182/19, relativos a la información a brindar a los solicitantes.
b) El artículo 14, inciso b) de la Ley de Firma Digital Nº 25.506 relativo a los contenidos mínimos de los certificados.

Proceso de registro inicial:

- El solicitante efectúa el requerimiento de certificado contactándose con el área comerciad de la AC - BOX CUSTODIA FIRMA DIGITAL solicitando el instructivo correspondiente. La información de contacto junto con el acuerdo de suscriptores y los formularios de suscripción se encuentra en el sitio web: https://pki.boxcustodia.com .
- El solicitante se presenta a la Autoridad de Registro de la AC - BOX CUSTODIA FIRMA DIGITAL con la documentación completa y debidamente firmada.

- El Oficial de Registro controla que la documentación cumpla con lo previsto en los puntos 3.1.9 y 3.1.10, según corresponda. El proceso de solicitud no puede continuar sin la correcta compleción de este punto.
- El Oficial de Registro verifica la identidad del representante a partir de la documentación de respaldo presentada por éste y firma la solicitud, dando conformidad y por terminado este punto.
- El Oficial de Registro procesa y aprueba la solicitud en el sistema de la AC.
- Por último, el Oficial de Registro conforma el legajo del suscriptor con toda la documentación presentada en este acto.

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

En el caso de las solicitudes para certificados digitales de seguridad alta, el solicitante generará su par de claves usando su propio dispositivo criptográfico en la Autoridad de Registro o bien utilizando el mecanismo de "Custodia centralizada de claves" descripto en el punto 4.13 de la Política Única de Certificación de la la AC - BOX CUSTODIA FIRMA DIGITAL. Las claves criptográficas, en ambos casos, son generadas por el solicitante. Luego el solicitante entregará su solicitud de certificado en formato PKCS#10, el cual no incluye la clave privada. De esta forma queda garantizada la posesión de la clave privada exclusivamente por parte del solicitante o suscriptor. El personal de la Autoridad de Registro se abstendrá de generar, exigir, tomar conocimiento o acceder bajo ninguna circunstancia a la clave privada del suscriptor.

3.2.2 Autenticación de la identidad de personas jurídicas públicas o privadas.

La verificación de la identidad de los Solicitantes de los Certificados de Personas Jurídicas se lleva a cabo mediante la acreditación del carácter (Representante Legal, Apoderado o Administrador) y la constatación de los datos del número, apellidos, nombres y foto obrantes en el documento de identidad válido que el solicitante presenta en la AR. Para la verificación de la identidad requerida en la Política Única de Certificación de la AC – BOX CUSTODIA FIRMA DIGITAL se establece que la documentación requerida al solicitante de un certificado digital es:

a) Original y Fotocopia del Documento de Identidad vigente, del responsable de custodiar la clave;
b) Nota de la Persona Jurídica Solicitante, confirmando la solicitud del Certificado requerido, el Carácter del Solicitante y el plazo de vigencia del Certificado requerido;
c) Certificación del Empleador, que acredite que el Solicitante cumple las funciones establecidas en el punto 1.3.3. de esta Política Única de Certificación;
d) Acuerdo del Suscriptores firmado;
e) Recibo que acredite el pago del Certificado correspondiente;
f) Registro y presentación de los documentos que se detallan a continuación, los que deberán ser presentados en copia certificada por Escribano Público, según correspondieren:

I. Estatuto o Contrato Social, correspondiente a la Persona Jurídica;

II. Acta de Directorio, o documento que acredite la representación invocada o vinculación, y el periodo de vigencia de la misma;

III. Constancia de Inscripción en el Registro Público de Comercio;

IV. Constancia de Inscripción en AFIP;

V. DNI de todos los socios, en caso de Sociedades Irregulares;

VI. Acta de distribución de cargos;

VII. Poder General Amplio, o Poder Especial que autoriza la solicitud de Certificado, de Firma Digital;

VIII. Revocación de poderes

El Oficial de Registro verificará que la documentación presentada corresponda a la persona que lo exhibe.

La documentación exhibida deberá estar en buen grado de conservación, y sus datos deberán ser concordantes con los obrantes en la solicitud. La foto deberá ser actual y reflejar concordancia con los aspectos físicos más característicos de la persona identificada. Las Autoridades de Registro conservarán la documentación de respaldo del proceso de verificación de identidad, inclusive aquella que no hubiera sido verificada durante este proceso, cumpliéndose las exigencias del artículo 21 inc. f) e i) de la Ley Nº 25.506 y el artículo 21 inc. 14) del Decreto Nº 182/19.

Adicionalmente se procede a la captura de la fotografía digital del rostro y la huella dactilar de los solicitantes y suscriptores de certificados de firma digital, almacenando la fotografía digital en formato JPEG y la imagen y la minucia de la huella dactilar de acuerdo al estándar ISO/IEC 19794-2. El Suscriptor de un Certificado firmará su ejemplar del Acuerdo con Suscriptores que, entre otras, contiene la declaración de que la información que presentó para ser incluida en el certificado es correcta.

3.2.3. - Autenticación de la identidad de persona humana

La verificación de la identidad de los solicitantes de los certificados de persona humana se lleva a cabo mediante la contrastación de los datos de número, apellidos, nombres y foto obrantes en el documento de identidad válido que el solicitante presenta en el Puesto de Atención de la AR. Para la verificación de la identidad requerida en la Política de Certificación de la AC - BOX CUSTODIA FIRMA DIGITAL se establece que la documentación requerida al solicitante de un certificado digital es:

1.- Argentinos nativos o naturalizados y extranjeros: original y fotocopia del documento nacional de identidad, libreta cívica o libreta de enrolamiento. Los extranjeros deberán presentar el original y fotocopia del pasaporte o cédula del MERCOSUR (de tratarse de un país limítrofe).

2.- Extranjeros con residencia en el país -incluida la temporaria o transitoria- que no posean documento nacional de identidad: original y fotocopia de la cédula de identidad, o del certificado o

comprobante que acredite el número de expediente asignado por la Dirección Nacional de Migraciones, donde conste el carácter de su residencia

El Oficial de Registro verificará que el documento presentado corresponda a la persona que lo exhibe. El documento exhibido deberá estar en buen grado de conservación, y sus datos deberán ser concordantes con los obrantes en la solicitud. La foto deberá ser actual y reflejar concordancia con los aspectos físicos más característicos de la persona identificada. Los Puestos de Atención de la AR conservarán la documentación de respaldo del proceso de verificación de identidad, inclusive aquella que no hubiera sido verificada durante este proceso, cumpliéndose las exigencias del artículo 21 inc. f) e i) de la Ley Nº 25.506 y el artículo 21 inc. 14) del Decreto Nº 182/19.

Adicionalmente se procede a la captura de la fotografía digital del rostro y la huella dactilar de los solicitantes y suscriptores de certificados de firma digital, almacenando la fotografía digital en formato JPEG y la imagen y la minucia de la huella dactilar de acuerdo al estándar ISO/IEC 19794-2. El suscriptor de un certificado firmará su ejemplar del Acuerdo con Suscriptores que, entre otras, contiene la declaración de que la información que presentó para ser incluida en el certificado es correcta.

Casos de no aprobación: se indican a continuación los casos en que no se aprobará una solicitud de certificado digital y el procedimiento correspondiente.

a) No es posible validar la identidad del solicitante Si la identidad del solicitante no ha podido ser validada satisfactoriamente por medio de los procedimientos indicados para el alta de un certificado digital, el Oficial de Registro no aprobará la solicitud y se realizará lo siguiente:

a.1. - El Oficial de Registro debe informar al solicitante acerca de los elementos y/o pasos faltantes para finalizar satisfactoriamente el proceso de validación de su identidad.

a.2.- El solicitante tiene un plazo de TREINTA (30) días corridos a partir de la generación de la solicitud, para proveer la información faltante o complementaria que se le solicite.

a.3.- En caso de no completarse el trámite pasado dicho plazo, la solicitud será revocada automáticamente por el sistema de la AC - BOX CUSTODIA FIRMA DIGITAL y el solicitante reinicia el proceso de solicitud de emisión del certificado digital, efectuando un nuevo requerimiento.

b) El dispositivo criptográfico provisto por el solicitante no está homologado

Si el dispositivo criptográfico provisto por el solicitante no está aprobado por la AC - BOX CUSTODIA FIRMA DIGITAL, el Oficial de Registro no aprobará la solicitud y se realizará lo siguiente:

b.1.- El Oficial de Registro informa al solicitante que no es posible aprobar su solicitud debido a que el dispositivo criptográfico que pretende utilizar no está aprobado por la AC - BOX CUSTODIA FIRMA DIGITAL.

b.2.- El solicitante tiene un plazo de TREINTA (30) días corridos a partir de la generación de la solicitud, para presentarse nuevamente en el Puesto de Atención con un dispositivo criptográfico homologado por la AC - BOX CUSTODIA FIRMA DIGITAL, oportunidad en que deberá repetirse la verificación de identidad del solicitante.

b.3.- En caso de no completarse el trámite pasado dicho plazo, la solicitud será revocada automáticamente por el sistema de la AC - BOX CUSTODIA FIRMA DIGITAL y el solicitante reinicia el proceso de solicitud de emisión del certificado, efectuando un nuevo requerimiento.

c) Revocación de Solicitud

En caso que una solicitud no sea aprobada en alguna de sus instancias en el término de TREINTA (30) días corridos desde su generación, caducará en forma automática por la ejecución de reglas internas del aplicativo de la AC - BOX CUSTODIA FIRMA DIGITAL. El solicitante deberá realizar una nueva solicitud.

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 Nº 25.506.

3.2.5. Validación de autoridad

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

3.2.6. Criterios para la interoperabilidad

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

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

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

En el caso de certificados digitales de persona humana o jurídica, 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 Persona Humana.

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 3.1-10. 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 persona humana o jurídica, la renovación en este apartado aplica a la emisión de UN (1) nuevo certificado sin que haya un cambio en la clave pública o en ningún otro dato del suscriptor. La renovación se podrá realizar siempre que el certificado se encuentre vigente.

A los fines de la obtención del certificado, no se exigirá la presencia física del suscriptor, debiendo éste remitir la constancia firmada digitalmente del inicio del trámite de renovación.

En los certificados de aplicaciones, incluyendo los de servidores, se deberá tramitar UN (1) nuevo certificado, según lo indicado en el apartado anterior.

3.4. Requerimiento de revocación

La AC - BOX CUSTODIA FIRMA DIGITAL admite y procesa solicitudes de revocación recibidas de los suscriptores o sus terceros autorizados. Por medio del mismo se especifica a un tercero para que actúe en representación de su titular en los trámites habilitados para este Servicio de Delegación. El titular de un Certificado Digital emitido por la AC - BOX CUSTODIA FIRMA DIGITAL, puede solicitar la revocación de un certificado digital del cual es suscriptor, mediante alguno de los siguientes procedimientos:

a) Por correo electrónico firmado digitalmente a la dirección: revocacion.pki@boxcustodia.com
b) Ingresando al sitio web de la AC - BOX CUSTODIA DE ARCHIVOS S.A. a la siguiente URL: https://pki.boxcustodia.com accediendo con su usuario y utilizando el código de revocación que le fuera asignado al momento de la emisión del certificado.
c) Personalmente presentándose ante la Autoridad de Registro correspondiente con documento de identidad que permita acreditar su identidad. Los sitios de revocación estarán disponibles durante las VEINTICUATRO (24) horas los SIETE (7) días de la semana. La revocación también podrá ser solicitada por la Autoridad de Registro o por la Autoridad Certificante de BOX CUSTODIA DE ARCHIVOS S.A. Las causales de revocación de un certificado son las detalladas en el punto 4.9.1. de la Política Única de Certificación
d) Se procederá a revocar un certificado en los siguientes casos:
    1) Cuando lo solicite el titular del certificado por cualquier causa, incluida el haber tomado conocimiento de que su clave privada esté comprometida y haya dejado de ser segura.

2) Si AC - BOX CUSTODIA FIRMA DIGITAL determina que el certificado fue emitido en base a una información falsa, que en el momento de la emisión hubiera sido objeto de verificación.
3) Si AC - BOX CUSTODIA FIRMA DIGITAL determina que los procedimientos de emisión y/o verificación han dejado de ser seguros.
4) En caso que la Organización que haya adoptado el uso de certificados de firma digital emitidos por la AC - BOX CUSTODIA FIRMA DIGITAL, notifique a la Autoridad de Registro que la información contenida en el certificado ha dejado de ser exacta.
5) Cuando fuere solicitado por resolución judicial o de la Autoridad de Aplicación de la Ley Nº 25.506 debidamente fundada.
6) Si AC - BOX CUSTODIA FIRMA DIGITAL determina que el certificado dejó de cumplir con las políticas y normas legales y reglamentarias de la Infraestructura de Firma Digital de la República Argentina (IFDRA).
7) Por fallecimiento del titular, declaración judicial de ausencia con presunción de fallecimiento o declaración judicial de incapacidad, en el caso de persona humana comunicada fehacientemente por sus herederos o autoridad judicial competente a AC - BOX CUSTODIA FIRMA DIGITAL
8) Por cese del responsable autorizado, en el caso de personas jurídicas comunicada fehacientemente por el nuevo responsable autorizado de la persona jurídica a AC - BOX CUSTODIA FIRMA DIGITAL
9) Por cambio en los atributos de un certificado, aun cuando hubieran sido válidos al tiempo de su emisión.
10) Por cese de la existencia de la Persona Jurídica, comunicada fehacientemente por el responsable autorizado de la misma a AC - BOX CUSTODIA FIRMA DIGITAL
11) Por cese de la Licencia del Certificador
12) Por haberse resuelto el contrato que AC - BOX CUSTODIA FIRMA DIGITAL hubiera suscripto con la Organización a la cual perteneciese el Suscriptor, o lo convenido entre las partes, en el caso que corresponda.

3.4.1 Revocación a solicitud del titular del certificado digital

El titular puede solicitar la revocación de un certificado digital mediante alguno de los siguientes procedimientos:

a. Por medio de la página web de la AC - BOX CUSTODIA FIRMA DIGITAL Existe una página web disponible las 24 horas para este servicio de revocación de certificados digitales.

I. Acceder a la página web https://pki.boxcustodia.com/ ingresando su usuario y contraseña.

II. Acceder a sus certificados generados y seleccionar de sus certificados vigentes el perfil de certificado a revocar.

III. Seleccionar la Opción Revocar y confirmar esta acción ingresando la Clave de Revocación (Dicha clave fue entregada al momento de obtener su certificado por la Autoridad de registro).

IV. Seguidamente el sistema le solicitara que ingrese el motivo de esta revocación.

V. El sistema notificara por correo electrónico que el trámite web ha sido realizado.

b. Por medio de la Mesa de Ayuda de la AC - BOX CUSTODIA FIRMA DIGITAL

Existe una Mesa de Ayuda disponible las 24 horas para este servicio de revocación de certificados digitales.

I. Llamar telefónicamente a la Mesa de Ayuda.
II. Identificarse con su nombre completo o nombre de usuario del sistema y optativamente indicar la identificación (nro. de serie) del certificado digital que desea revocar. Si no recuerda el número de serie y posee más de un certificado activo, la Mesa de Ayuda brindará indicios sobre los certificados existentes para poder individualizarlos (fechas, clase, etc.)
III. El titular deberá informar el Código de Revocación Telefónica que tenga válido en ese momento (dicho código es el que eligió en el momento en que solicitó su primer certificado digital).
IV. Manifestar su decisión de revocar el certificado digital indicando al operador telefónico las causas de la solicitud.
V. El Operador de la Mesa de Ayuda de la AC BOX CUSTODIA FIRMA DIGITAL deberá ejecutar la opción de "Revocación de Certificado Digital" del Sistema Informático de AC BOX CUSTODIA FIRMA DIGITAL, con los datos que le fueron suministrados en los pasos anteriores.
VI. El Operador informara al suscriptor el resultado de la operación, enviándose al correo del suscriptor el detalle de la revocación

c. Personalmente en un Puesto de Atención de la AR

I. Presentarse personalmente en un Puesto de Atención de la AR de la AC - BOX CUSTODIA FIRMA DIGITAL dentro de los horarios de atención, informando sus datos y la identificación del certificado digital que desea revocar.

II. Manifestar al Oficial de Registro las causas de la solicitud de revocación.

III. El Oficial de Registro deberá ejecutar la opción de "Revocación de Certificado Digital" del Sistema Informático de la AC BOX CUSTODIA FIRMA DIGITAL, con los datos que le fueron suministrados en los pasos anteriores.

IV. El Oficial de Registro notificará al suscriptor el resultado de la operación y se enviará un correo electrónico al suscriptor informando de la operación de revocación ejecutada.

d. A través de un tercero autorizado

Se admite un pedido de revocación efectuado por un tercero, que fue autorizado previamente por el Titular de un Certificado. El Tercero acepta dicha designación. La

próxima vez que ingrese al portal de suscriptor de la AC, verá desplegadas en pantalla las opciones de identificación con la cual está habilitado para ingresar (la suya propia y su/s representado/s). En caso que opte por su representado verá un menú restringido del titular de los certificados, donde podrá identificar y revocar el/los certificado/s.

3.4.2 Revocación por parte de la AC BOX CUSTODIA FIRMA DIGITAL

Al detectarse la presencia de algún causal de revocación por parte de la AC - BOX CUSTODIA FIRMA DIGITAL en la legislación vigente, el Responsable de la AR revocará el o los certificados digitales que corresponda/n.

a. Revocación de un único certificado digital.
   I. El Responsable de AR constatará que la causa de la revocación del certificado digital en cuestión esté dentro de las previstas por la política correspondiente al presente manual.
   II. Se ejecutará la opción "Revocación de Certificado Digital por parte de la AR" del Sistema Informático de la AC BOX CUSTODIA FIRMA DIGITAL, con los datos del titular y del certificado digital en cuestión, colocar su causa y deberá firmar la transacción con su dispositivo criptográfico.

b. Revocación de múltiples certificados digitales

El Sistema Informático de la AC - BOX CUSTODIA FIRMA DIGITAL prevé medios para realizar revocaciones múltiples en caso de existir varios certificados digitales afectados por un mismo causal de revocación, para facilitar la tarea. Este tipo de revocaciones son realizadas por el Responsable de AR mediante el menú correspondiente y se aplica el mismo procedimiento que para el caso de un único certificado digital.

4. CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS

4.1. Solicitud de certificado

4.1.1. Solicitantes de certificados

Todo potencial suscriptor de un certificado digital en los términos del presente documento (en adelante el “solicitante”) que desee obtener un certificado digital, iniciará el trámite de solicitud ingresando al sitio web de la AC - BOX CUSTODIA FIRMA DIGITAL “ https://pki.boxcustodia.com/ ” e ingresar al menú de “Mis Certificados”, previamente registrándose al sistema cuando se lo solicite, pudiendo realizar pedidos de acuerdo a los 6 tipos de perfiles de certificados disponibles. Los certificados digitales de suscriptor que emite la AC - BOX CUSTODIA FIRMA DIGITAL bajo la Política de Certificación que se corresponde con el presente Manual de Procedimientos, son de tres clases, los cuales a su vez pueden ser de cualquiera de los 6 tipos de perfiles de certificados definidos en las Políticas de Certificación de AC - BOX CUSTODIA FIRMA DIGITAL:

a. Implementado por medio de un dispositivo criptográfico.

b. OCSP: El suscriptor es la AC - BOX CUSTODIA FIRMA DIGITAL, usado en relación con el servicio de verificación en línea del estado de un certificado.

La clase de certificado determina su posibilidad de uso y aplicabilidad en los sistemas que implementen la firma digital. Los navegadores soportados por el Sistema Informático de AC - BOX CUSTODIA FIRMA DIGITAL, en las estaciones de trabajo de los suscriptores son:

a. Internet Explorer 9 o superior;

b. Firefox 26 o superior;

c. Chrome 38 o superior;

Se requiere tener instalado en estos navegadores Java 1.6.0.22 o superior.

4.1.2. Solicitud de certificado

La **AC - BOX CUSTODIA FIRMA DIGITAL** emite Certificados Digitales para Persona Humana y Jurídica como se describe en el punto 7.1 Perfil del certificado, en la Política de Certificación de **AC - BOX CUSTODIA FIRMA DIGITAL**. Además se realizará lo siguiente:

- ***a.*** Acceder al Portal de suscriptor para efectuar una solicitud de certificado de firma digital, consignando los datos que allí se soliciten.
- ***b.*** No poseer sanciones dictadas por autoridades competentes que impidan el otorgamiento de un certificado digital.
- ***c.*** Cumplir con lo establecido en la Política de Certificación, y demás documentos asociados en lo que tenga relación con la solicitud de certificado que se presenta.
- ***d.*** Cumplir con las condiciones establecidas en el Acuerdo con Suscriptores que habrá de firmar.

Si el solicitante cumpliera las condiciones para recibir un dispositivo criptográfico provisto por la **AC - BOX CUSTODIA FIRMA DIGITAL**, el sistema informático le notificará tal circunstancia al realizar la solicitud y le indicará la lista de los Puestos de Atención de la AR de la **AC - BOX CUSTODIA FIRMA DIGITAL** en las cuales podría retirar el mencionado dispositivo y completar el trámite.

4.2. Procesamiento de la solicitud del certificado

4.2.1. Presentación de la solicitud

a. Se deben cumplir los siguientes pasos para el certificado Implementado por medio de un dispositivo criptográfico

En la estación de trabajo del solicitante:

I. El solicitante deberá ingresar a “Mis Certificados” / “Nueva Solicitud”. El sistema mostrará y describirá cada uno de los perfiles de certificado disponibles para realizar una solicitud. El solicitante deberá seleccionar el tipo de perfil de certificado que cumpla con sus requerimientos.

II. El sistema mostrará el formulario a cargar por el solicitante según el perfil de certificado que haya seleccionado. Además mostrara como ayuda por cada cuadro de texto una descripción del dato que cargará el solicitante.

III. El solicitante cargará todos los datos para generar la solicitud. Además seleccionará en el tipo de seguridad la opción “Hardware” para la generación de claves.
IV. El solicitante deberá leer y aceptar el Acuerdo de Suscriptores y finalmente presionar en la opción “Generar Solicitud”.
V. El sistema generará el HASH de los datos cargados como un control adicional.
VI. El solicitante deberá imprimir el comprobante de solicitud, el cual incluye los datos cargados anteriormente y su HASH generado.
VII. Su pedido queda pendiente de procesamiento en el sistema informático de la AC y asociado al Puesto de Atención mencionado.

4.2.2. Aprobación de la solicitud

a) El Oficial de Registro evaluará la solicitud de certificado, verificando la identidad del solicitante en forma presencial y demás datos pertinentes, y en caso de corresponder dará curso favorable a la solicitud. Una vez admitida la solicitud, el Oficial de Registro efectuará la verificación de identidad del solicitante.

b) En caso de que el tipo de seguridad sea por hardware:

- Si el dispositivo criptográfico sea provisto por la **AC - BOX CUSTODIA FIRMA DIGITAL**, el Oficial Certificador imprimirá el correspondiente recibo en el cual constarán los datos de la unidad a entregar con sus correspondientes instructivos y software, y el solicitante deberá conformarlo.

- Si el dispositivo criptográfico sea provisto por el solicitante, el Oficial Certificador constatará que el mismo esté homologado.

- El solicitante y Oficial de Registro en una terminal en la AR inicializarán el dispositivo criptográfico, y el solicitante desde esa terminal deberá ingresar a la opción "Mis Certificados / Generar Claves" para generar el par de claves y guardar la clave privada en su dispositivo criptográfico. El solicitante seleccionará la solicitud correspondiente e ingresará la opción de generar claves e ingresara la longitud de claves deseada (2048).

c) En caso que se utilice el servicio de custodia centralizada de claves:

- El dispositivo criptográfico es provisto por la **AC - BOX CUSTODIA FIRMA DIGITAL**, el Oficial Certificador imprimirá el correspondiente recibo en el cual constarán la solicitud del suscriptor del uso del servicio.
- El solicitante y Oficial de Registro en una terminal en la AR o en una terminal del solicitante, inicializarán el proceso, y el solicitante desde esa terminal deberá ingresar a la opción "Mis Certificados / Generar Claves" para generar el par de claves y guardar la clave privada en el dispositivo criptográfico provisto por la **AC - BOX CUSTODIA FIRMA DIGITAL**. El solicitante seleccionará la solicitud correspondiente e ingresará la opción de generar claves e ingresará la longitud de claves deseada (2048).

d) El Oficial Certificador aprobará la solicitud y le entregará el "Código de Activación" y el "Código de Revocación" del certificado digital que el suscriptor deberá conservar para utilizarlo en la aceptación y revocación del certificado

4.2.3. Generación de certificado del suscriptor

Para cualquier tipo de seguridad seleccionado, el solicitante ingresa a la opción "Mis Certificados / Finalizar Solicitud".

El solicitante deberá seleccionar una de las solicitudes pendientes de finalización y para esa solicitud ingresará el código de activación válido para esa solicitud. Una vez verificado se procederá según el tipo de certificado.

En el caso de un certificado digital implementado por hardware, el solicitante cumplirá los siguientes pasos:

I. El solicitante conecta el dispositivo criptográfico a un puerto USB.
II. El solicitante ingresa la clave personal.
III. El sistema verifica el código de activación.
IV. El sistema calcula y verifica que el HASH de la solicitud sea el mismo.
V. Si la solicitud pudo procesarse correctamente, el sistema lo informará al solicitante, instalando el certificado en el dispositivo criptográfico instalado.

En el caso de un certificado digital utilice el servicio de custodia centralizada de claves, el solicitante realiza los siguientes pasos:

I. El solicitante se conecta a la interfaz web del servicio de custodia centralizada.
II. El solicitante ingresa la clave del dispositivo.
III. El sistema verifica el código de activación.
IV. El sistema calcula y verifica que el HASH de la solicitud sea el mismo.
V. Si la solicitud pudo procesarse correctamente, el sistema lo informará al solicitante, instalando el certificado en el módulo criptográfico del dispositivo criptográfico provisto por BOX CUSTODIA DE ARCHIVOS S.A el cual tiene una certificación FIPS 140-2 nivel 3.

4.2.4. Solicitud de renovación del Certificado

Un suscriptor puede solicitar la renovación de su certificado digital dentro de su período de validez, con un máximo de DOS (2) renovaciones desde la emisión del certificado digital original. El suscriptor entiende que este proceso de renovación no se aplica cuando se deba cambiar algún dato del certificado a renovar. La renovación de un certificado digital de suscriptor no implica generar un nuevo par de claves.

Transcurrido el período de validez del par de claves asociadas al certificado, el certificado digital asociado no podrá renovarse y dichas claves no deberán ser usadas por el suscriptor, de acuerdo a lo indicado en el *punto 6.3.2 del presente Manual*.

El sistema informático de la **AC - BOX CUSTODIA FIRMA DIGITAL**, colocará un mensaje en el portal del suscriptor TREINTA (30) días antes de vencimiento del certificado, y adicionalmente enviará un mail desde la cuenta " renovaciones@boxcustodia.com " a la dirección que el suscriptor tenga consignada en el sistema.

Para el caso de certificados digitales con Seguridad Media (por software) y Seguridad Alta (por hardware), el procedimiento es ingresar al sistema de la **AC - BOX CUSTODIA FIRMA DIGITAL**, iniciar sesión, ingresar al menú de "Mis Certificados / Certificados Generados", identificar el certificado a renovar, seleccionar el certificado a renovar y efectuar la acción de renovación. El botón de acción para la renovación aparecerá automáticamente a partir del momento en que resten 30 días para su vencimiento. Una vez concluida exitosamente, deberá importar el nuevo certificado a su estación de trabajo.

4.3. Emisión del certificado

4.3.1. Proceso de emisión de un certificado

a. Antes de 30 días corridos a partir de la creación de la solicitud, el solicitante se presenta con la documentación requerida en el Puesto de Atención que eligió, donde se efectúa la verificación de identidad. De resultar satisfactoria, el Oficial de Registro ingresa, al módulo de AR del Sistema Informático de la **AC - BOX CUSTODIA FIRMA DIGITAL**, y con su propio dispositivo criptográfico pre-aprueba la solicitud. De no resultar satisfactoria la verificación de identidad, se aplica el procedimiento *"Casos de no aprobación"* establecido en el punto 3.2.3. - Autenticación de la identidad de persona humana.

b. El Oficial de Registro será notificado por el módulo de AR del Sistema Informático de la **AC - BOX CUSTODIA FIRMA DIGITAL** si el solicitante fue seleccionado para recibir un dispositivo criptográfico por parte de la **AC - BOX CUSTODIA FIRMA DIGITAL**, en cuyo caso procederá a ejecutar la opción *"Entrega de dispositivo criptográfico"* de dicho sistema, imprimir el correspondiente recibo en el cual constarán los datos de la unidad a entregar y requerir al solicitante que firme dicho recibo en su presencia.

c. Si el solicitante optó por traer su propio dispositivo criptográfico, el Oficial de Registro deberá verificar, mediante la herramienta de verificación de su módulo de AR, que el mismo se corresponde con alguno de los modelos homologados por la **AC - BOX CUSTODIA FIRMA DIGITAL**, debiendo en caso contrario aplicar se aplica el procedimiento *"Casos de no aprobación"* establecido en el punto 3.2.3. - Autenticación de la identidad de persona humana.

d. Si el solicitante optó por la utilización del servicio de custodia centralizada de claves, el Oficial de Registro deberá verificar, mediante la herramienta de verificación de su módulo de AR, debiendo en caso contrario aplicar el procedimiento *"Casos de no aprobación"* establecido en el punto 3.2.3. - Autenticación de la identidad de persona humana..

e. Continuando en el Puesto de Atención, el solicitante, con la presencia del Oficial de Registro verificando el uso del dispositivo homologado, ingresa al Portal del Solicitante/suscriptor, identificar la solicitud de certificado ya aprobada en el menú de *"Mis Certificados / Finalizar Solicitud"*, y seleccionar la opción de generar certificado. Se

conecta el dispositivo criptográfico a un puerto USB de dicha estación de trabajo, e indicar al mismo que lo genere. Si el dispositivo criptográfico falla y no es posible realizar la importación, se aplica el procedimiento *"Casos de no aprobación"* establecido en el punto 3.2.3. - Autenticación de la identidad de persona humana..

f. El Oficial de Registro aprueba la emisión del certificado desde su portal de AR firmando la solicitud, y entregar el código de aceptación y código de revocación de certificado al solicitante.

4.3.2. Notificación de emisión

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

4.4. Aceptación del certificado

Previo a la descarga del certificado a su nombre, el suscriptor deberá controlar el contenido del mismo y, en caso de estar de acuerdo, proceder a descargar e instalar el certificado.

En caso de error u omisión en el contenido del certificado, el suscriptor deberá revocarlo al momento de recibirlo y no hacer uso del mismo; caso contrario el suscriptor acepta la exactitud del contenido asume las obligaciones y responsabilidades establecidas por esta "Política Única de Certificación".

Para cualquier tipo de seguridad el solicitante deberá ingresar a la opción "Mis Certificados / Finalizar Solicitud".

Luego, deberá seleccionar una de las solicitudes pendientes de finalización y para esa solicitud ingresar el código de activación válido. Si la solicitud pudo procesarse correctamente, el sistema lo informará al solicitante y descargará una aplicación local que el solicitante ejecutará en su computadora para que el certificado se instale en el almacén de claves donde se generaron las claves. Alternativamente podrá descargar el archivo del certificado e instalarlo manualmente donde corresponda.

En el caso de un certificado digital implementado por hardware, antes de ingresar el código de activación, el solicitante deberá conectar el dispositivo criptográfico e ingresar la clave del dispositivo.

En el caso de la utilización del servicio de custodia centralizada de claves, el solicitante deberá ingresar la clave de acceso al dispositivo.

El suscriptor puede probar su dispositivo, firmando un texto de prueba disponible en el portal de la AC. En cualquier caso, en que la importación de un certificado digital al dispositivo criptográfico no sea satisfactoria, o en el caso que el solicitante deba recibir por parte de la **AC - BOX CUSTODIA FIRMA DIGITAL** un dispositivo criptográfico y que por cualquier circunstancia no se disponga de

alguno en el Puesto de Atención, mientras se cumpla el plazo de validez de la solicitud, podrá repetirse el proceso de importación. Pasado el mismo, deberá realizarse una nueva solicitud.

4.5. Uso del par de claves y del certificado

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

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

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

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

Los Terceros Usuarios deben:

a) Conocer los alcances establecidos en la Política Única de Certificación de AC - BOX CUSTODIA FIRMA DIGITAL;
b) Verificar la validez del certificado digital.

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

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

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

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

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

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

4.8. Modificación del certificado

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

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

4.9. Suspensión y Revocación de Certificados

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

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

4.9.1. Causas de revocación

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

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

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

4.9.2. Autorizados a solicitar la revocación

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

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

f) La Autoridad Judicial.
g) La Autoridad de Aplicación.

4.9.3. Procedimientos para la solicitud de revocación

El certificador garantiza que:

a) Se identifica debidamente al solicitante de la revocación según se establece en el apartado "3.4. - Requerimiento de revocación".
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 (https://pki.boxcustodia.com/web/identidaddigital/autoridades-de-registro).

El suscriptor podrá efectuar la revocación a través de alguno de los medios indicados en el punto "3.4. - Requerimiento de revocación" de la Política Única de Certificación.

El titular puede solicitar la revocación de un certificado digital mediante alguno de los siguientes procedimientos:

a) Por medio de la página web de la AC - BOX CUSTODIA FIRMA DIGITAL
   Existe una página web disponible las 24 horas para este servicio de revocación de certificados digitales.
   I. Acceder a la página web https://pki.boxcustodia.com/ ingresando su usuario y contraseña.
   II. Acceder a sus certificados generados y seleccionar de sus certificados vigentes el perfil de certificado a que desea revocar.
   III. Seleccionar la Opción Revocar y confirmar esta acción ingresando la Clave de Revocación (Dicha clave fue entregada al momento de obtener su certificado por la Autoridad de registro).
   IV. Seguidamente el sistema le solicitará que ingrese el motivo de esta revocación.
   V. El sistema notificará por correo electrónico que el trámite web ha sido realizado.
b) Por medio de la Mesa de Ayuda de la AC - BOX CUSTODIA FIRMA DIGITAL
   Existe una Mesa de Ayuda disponible las 24 horas para este servicio de revocación de certificados digitales.
   I. Llamar telefónicamente a la Mesa de Ayuda.
   II. Identificarse con su nombre completo o nombre de usuario del sistema y optativamente indicar la identificación (nro. de serie) del certificado digital que

desea revocar. Si no recuerda el número de serie y posee más de un certificado activo, la Mesa de Ayuda brindará indicios sobre los certificados existentes para poder individualizarlos (fechas, clase, etc.).

III. El titular deberá informar el Código de Revocación Telefónica que tenga válido en ese momento (dicho código es el que eligió en el momento en que solicitó su primer certificado digital fue entregado al momento de generar su certificado).

IV. Manifestar su decisión de revocar el certificado digital indicando al operador telefónico las causas de la solicitud.

V. El Operador de la Mesa de Ayuda de la AC - BOX CUSTODIA FIRMA DIGITAL deberá ejecutar la opción de "Revocación de Certificado Digital" del Sistema Informático de AC - BOX CUSTODIA FIRMA DIGITAL, con los datos que le fueron suministrados en los pasos anteriores.

VI. El Operador informará al suscriptor el resultado de la operación, enviándose al correo del suscriptor el detalle de la revocación.

c) Personalmente en un Puesto de Atención de la AR

I. Presentarse personalmente en un Puesto de Atención de la AR de la AC - BOX CUSTODIA FIRMA DIGITAL dentro de los horarios de atención, informando sus datos y la identificación del certificado digital que desea revocar.

II. Manifestar al Oficial de Registro las causas de la solicitud de revocación.

III. El Oficial de Registro deberá ejecutar la opción de "Revocación de Certificado Digital" del Sistema Informático de la AC - BOX CUSTODIA FIRMA DIGITAL, con los datos que le fueron suministrados en los pasos anteriores.

IV. El Oficial de Registro notificará al suscriptor el resultado de la operación y se enviará un correo electrónico al suscriptor informando de la operación de revocación ejecutada.

d) A través de un tercero autorizado

Se admite un pedido de revocación efectuado por un tercero, que fue autorizado previamente por el Titular de un Certificado.

El Tercero acepta dicha designación. La próxima vez que ingrese al portal de suscriptor de la AC, verá desplegadas en pantalla las opciones de identificación con la cual está habilitado para ingresar (la suya propia y su/s representado/s). En caso que opte por su representado verá un menú restringido del titular de los certificados, donde podrá identificar y revocar el/los certificado/s.

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 requerirá su revocación en forma inmediata cuando se presente alguna de las circunstancias previstas en el apartado 4.9.1.

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

4.9.5. Plazo para el procesamiento de la solicitud de revocación

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

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

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

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

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

.

4.9.7. Frecuencia de emisión de listas de certificados revocados

El Certificador genera y publica una Lista de Certificados Revocados con una frecuencia diaria, cada VEINTICUATRO (24) horas.

4.9.8. Vigencia de la lista de certificados revocados

La vigencia de cada lista de certificados revocados es de VEINTICUATRO (24) horas.
AC - BOX CUSTODIA DE ARCHIVOS posee un servicio en línea de revocación de certificados y de verificación de su estado. Ambos servicios se encuentran disponibles SIETE POR VEINTICUATRO (7x24) horas, sujetos a un razonable calendario de mantenimiento. La lista de certificados revocados indicará su fecha de vigencia y la fecha de su próxima actualización.

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

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

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

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

a) La información relativa a las características de los servicios de verificación de estado.

b) La disponibilidad de tales servicios y los procedimientos que se seguirán en caso de no disponibilidad.

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

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

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

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

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

La AC - BOX CUSTODIA FIRMA DIGITAL posee un servicio en línea de revocación de certificados y de verificación de su estado. Ambos servicios se encuentran disponibles SIETE POR VEINTICUATRO (7x24) horas, sujetos a un razonable período de mantenimiento.

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

El uso del protocolo OCSP permite, mediante su consulta, determinar el estado de validez de un certificado digital y representa una alternativa a la consulta a la CRL, la que también estará disponible. El servicio OCSP se provee en el siguiente sitio web: https://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 Política Única de Certificación de AC - BOX CUSTODIA FIRMA DIGITAL.

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 4.8.3. - Procedimientos para la solicitud de revocación.

4.9.13. Causas de suspensión

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

4.9.14. Autorizados a solicitar la suspensión

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

4.9.15. Procedimientos para la solicitud de suspensión

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

4.9.16. Límites del periodo de suspensión de un certificado

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

4.10. Estado del certificado

4.10.1. Características técnicas

Servicios prestados:

- Lista de Certificados revocados (CRL)
- Servicio OCSP

Respecto a la CRL, se emite cada VEINTICUATRO (24) horas y delta CRLs en modo horario.

Con respecto a OCSP, permite verificar si el certificado se encuentra vigente a o ha sido revocado.

4.10.2 Disponibilidad del servicio

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

4.10.3. Aspectos operativos

No existen otros aspectos a mencionar.

4.11. Desvinculación del suscriptor

Una vez expirado el certificado o si este fuera revocado, de no tramitar un nuevo certificado, su titular se considera desvinculado de los servicios del certificador.

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 Nº 25.506. El suscriptor se encuentra obligado a mantener el control exclusivo de su clave privada, no compartirla e impedir su divulgación, de acuerdo a lo dispuesto en el inciso a) del artículo 25 de la ley antes mencionada.

4.13. – Custodia centralizada de claves.

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

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

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

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

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

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

5. CONTROLES DE SEGURIDAD FÍSICA, FUNCIONALES Y PERSONALES

5.1. Controles de Seguridad Física

El Responsable de Seguridad efectuará periódicamente una verificación del estado de los recintos operativo y alternativo de la AC - BOX CUSTODIA FIRMA DIGITAL, por medio de las facilidades remotas de monitoreo y/o presencialmente.

Para el ingreso al recinto exclusivo de la AC - BOX CUSTODIA FIRMA DIGITAL, los niveles de acceso a trasponer por parte de los Testigos y el personal afectado a las funciones de la AC, serán facilitados por el personal de BOX CUSTODIA DE ARCHIVOS S.A. que administra el acceso al Área de Máxima Seguridad (AMS).

5.1.1. Construcción y ubicación de instalaciones

El centro de cómputos donde se encuentran instalados los activos informáticos que componen la AC - BOX CUSTODIA FIRMA DIGITAL, conforma un Ambiente de Máxima Seguridad (AMS).

Dicho AMS es una construcción modular constituida de piso, laterales, techo y estructura propia, que permite su ampliación y traslado, protección refractaria al calor, barrera contra la propagación de humedad, campos magnéticos e ignífugo. Posee características específicas para la protección de equipamientos electrónicos, centros de datos, medios magnéticos, papeles y demás portadores de datos.

5.1.2. Niveles de acceso físico

Se encuentran implementados cinco niveles de acceso físico.

A tal efecto se define como primer nivel al ingreso al predio, el cual se efectúa mediante tarjeta de proximidad.

El segundo nivel, representa el acceso al edificio, con la misma tecnología descripta.

El tercer nivel, es el acceso a la sala de operaciones NOC (Network Operations Center o Centro de Operaciones de la Red), mediante la identificación por medio de una clave en un teclado numérico asociado a la presentación de una tarjeta magnética.

El cuarto nivel es el de acceso a la AMS propiamente dicha, con la identificación biométrica de huella digital asociada a la presentación de una tarjeta magnética.

El quinto nivel, es el acceso a la sala donde se alojan el servidor criptográfico y los servidores del sistema de la AC - BOX CUSTODIA FIRMA DIGITAL.

A partir de allí, los servidores se encuentran instalados en racks, y poseen instaladas cámaras de monitoreo y accesos.

5.1.3. Energía y aire acondicionado

La energía es provista desde la red pública, contando el edificio con una cámara transformadora de media tensión, desde la cual se distribuyen en el tablero principal. Asimismo, se dispone de un sistema de UPS (Uninterruptible Power Suply o Unidad de Energía Ininterrumpible), que se activa en forma automática ante la ocurrencia de algún corte del suministro externo. El sistema de UPS es respaldado a su vez por grupos moto-generadores, los cuales arrancan en forma automática en caso de corte del suministro de la red pública y proporcionan un suministro ininterrumpido de energía eléctrica. Las salidas de las UPS en el AMS para los servidores. Respecto de las condiciones de aire acondicionado, el AMS cuenta con acondicionadores, en una configuración redundante que mantiene a uno de ellos en stand-by (preparado para actuar en caso de falla del otro).

5.1.4. Monitoreo ambiental

El sistema de monitoreo ambiental del AMS cuenta con sensores de temperatura, humedad ambiente y humo.

5.1.5. Prevención y protección contra incendio

El AMS cuenta internamente con un sistema propio de detección consistente en una red de sensores de humo.

5.1.6. Medios de almacenamiento

El AMS cuenta con una sala dedicada para el resguardo físico de los medios de almacenamiento. Asimismo, en la sala de servidores se encuentran ubicaciones de seguridad con protección con capacidad para el resguardo de medios.

5.1.7. Disposición de material de descarte

Para la destrucción de información sensitiva, presente en los medios ópticos de respaldo, se inutilizarán ambas caras con un medio adecuado en presencia del Administrador de Servidores, el

Responsable de Seguridad y los Testigos según el control “M de N” establecido, constando en el Libro de Actas de la AC - BOX CUSTODIA FIRMA DIGITAL lo actuado.

El mismo procedimiento se utilizará si deben destruirse cintas de respaldo, desarmando la cinta y cortándola en porciones menores a 1 metro de longitud.

5.1.8. Sitio alternativo

BOX CUSTODIA DE ARCHIVOS S.A. mantiene en existencia capacidades externas de procesamiento fuera del lugar donde reside el Sistema Informático de la AC, a los efectos de prever la disponibilidad de los recursos necesarios de hardware y software, para que puedan mantenerse los servicios indispensables en caso de contingencia.

5.1.9. Sensores presenciales y de ambiente de la sala de la AC

Tanto en el sitio operativo como en el alternativo, existen sensores de temperatura, humedad y movimiento que activan a la alarma del AMS. Se graba en video la actividad en la sala según estos parámetros de activación.

5.2. Controles de Gestión

5.2.1. Roles

Las funciones relacionadas con la AC - BOX CUSTODIA FIRMA DIGITAL, son llevadas a cabo por personal calificado, el cual realiza sus funciones de acuerdo a los roles asignados, los que se listan a continuación:

a) Responsable de la AC - BOX CUSTODIA FIRMA DIGITAL: es la máxima autoridad responsable de la AC BOX CUSTODIA FIRMA DIGITAL ante la Autoridad de Aplicación, los Suscriptores y los Terceros Usuarios. Es responsable de custodiar una ACS para establecer el quórum del Mundo de Seguridad que custodia el HSM además de una OCS que está incluida en este y protege las claves de la AC, además habilita el Libro de Actas de BOX CUSTODIA DE ARCHIVOS. En relación a la Política de Certificación, implementa las recomendaciones de las auditorías y administra las versiones. En el Plan de Seguridad, reporta de forma fehaciente a la Autoridad de Aplicación todos los incidentes que afecten a la seguridad. Autoriza y administra la aplicación del Plan de Contingencia, notificando a la Autoridad de Aplicación. Participa en el Plan de Cese de Actividades, notificando a la Autoridad de Aplicación.
b) Responsable de Seguridad: encargado de establecer los filtros, restricciones, y controles, que permitan resguardar la información de la AC BOX CUSTODIA FIRMA DIGITAL, y del control y asignación de acceso físico a los recintos. Poseedor ACS para formar parte del quórum del Mundo de Seguridad y de una OCS que integra el quórum que protege la clave privada de la AC dentro del HSM. Interviene en el soporte al proceso de habilitación y baja de las Autoridades de Registro. Poseedor de una ACS que participa en el proceso de generación y resguardo de los respaldos del HSM. Participa activamente en la ejecución del Plan de Seguridad, de Contingencia y de Cese de Actividades.
c) Administrador de Servicios Críticos: es el personal que administra los servidores de la AC (Core y Publicación). Encargado de conexionar y energizar el equipo en su sitio definitivo.

Participa en el proceso de inicialización realizando la instalación de software en los servidores y creación en el Sistema Informático de la AC - BOX CUSTODIA FIRMA DIGITAL la Autoridad de Registro, a los efectos de emitir el primer certificado digital de usuario. Aplica instalaciones o actualizaciones a los servidores y ejecuta rutinas periódicas de control de registro de ejecuciones, a efectos de mantener el equipamiento operativo. Además administra el dispositivo criptográfico HSM (Hardware Security Module o Módulo de Seguridad por Hardware). Participa en la inicialización del dispositivo, la generación de respaldos y la restauración de los mismos ante contingencias.

Poseedor ACS para formar parte del quórum del Mundo de Seguridad y de una OCS que integra el quórum que protege la clave privada de la AC dentro del HSM Ejecuta rutinas periódicas de control, a efectos de mantener el equipamiento operativo, y participa en el proceso de cese de actividades de las claves de la AC. Interviene en el proceso de inicialización de los dispositivos, participa en el resguardo y en la recuperación de los datos del Mundo de Seguridad.

d) Responsable de Comunicaciones: Administra las comunicaciones que dan soporte a la infraestructura de firma en la AC - BOX CUSTODIA FIRMA DIGITAL.

e) Definidores: es un comité formado por el Responsable de la AC, el responsable de Seguridad y el Administrador de servicios Críticos, dicho comité es el responsable de realizar las definiciones relativas a las Políticas de Certificación, operativas, procedimentales, de seguridad física y lógica, planes de contingencia y de cese de actividades.

f) Desarrolladores de software: es el personal encargado de desarrollar las aplicaciones informáticas que dan soporte a los servicios de la AC - BOX CUSTODIA FIRMA DIGITAL.

g) Homologadores: es un comité conformado por el Responsable de Seguridad, el Administrador de Servidores y el Responsable de Comunicaciones encargado de evaluar el software desarrollado, previamente a su puesta en producción.

h) Responsable de AR: es el responsable de elaborar y mantener el plan de implantación y administración de la Autoridad de Registro de la AC - BOX CUSTODIA FIRMA DIGITAL, de sus Puestos de Atención y del personal afectado a los mismos. Participa activamente en el proceso de inicio de la AC solicitando el primer certificado que emita la misma.

i) Responsable de Puesto de Atención: es el responsable de la operación de un Puesto de Atención de la Autoridad de Registro de la AC - BOX CUSTODIA FIRMA DIGITAL, con capacidad de recibir y aprobar solicitudes de certificados digitales. Revoca certificados por presentación personal de su titular o autorizado. Coordina y administra los recursos que le competen en su Puesto de Atención. Es nombrado por el Responsable de la AR.

j) Oficial de Registro: Personal de un Puesto de Atención, con capacidad de recibir y aprobar solicitudes de certificados digitales. Revoca certificados por presentación personal de su titular o autorizado. Interviene en el proceso de emisión de certificado, identificando al solicitante, recibiendo la solicitud, y aprobando el trámite, de corresponder. Suscribe la documentación respectiva de las solicitudes aprobadas.

k) Testigos: Validan las operaciones críticas autorizando la ejecución de las mismas por medio de llaves ACS que obran en su poder, y que conforman el control “M de N” establecido. Participa en la inicialización de los dispositivos, en los procesos de generación de respaldos

y de restauración ante contingencias. Participa en el proceso de cese de actividades de las claves de la AC.

l) Mesa de Ayuda: personal encargado de las funciones de Mesa de Ayuda, en relación a las gestiones de certificados, temas de Firma Digital en general y/o en particular, atención de consultas de terceros usuarios, recepciona y deriva incidentes. Interviene eventualmente en el proceso de revocación de certificados por medio de la recepción del Código de Revocación Telefónica. Su par de claves es generado y almacenado en dispositivos criptográficos certificados bajo normas FIPS 140-2 Nivel 2.

m) Auditor: personal encargado de las funciones de auditoría.

5.2.2. Correspondencia roles – Accesos del HSM.

En relación al HSM de la AC - BOX CUSTODIA FIRMA DIGITAL, la posesión de los accesos para la autorización de funciones en relación a los roles es:

a) ACS se utiliza para la autorización carga o molificación de la funcionalidad del Mundo de Seguridad (Security World) el cual da las condiciones generales para la inicialización segura del ambiente, para cargar el Mundo de seguridad se puede hacer solamente con el quórum de ACS que se haya definido al momento de crearlo. En nuestro caso este control M de N, tres necesarios de seis posibles. Las seis ACS posibles son distribuidas entre el Responsable de la AC, el Responsable de Seguridad, Responsable de Comunicaciones, el Administrador de Servicios Críticos y dos testigos.

b) OCS Se utiliza para protección de la clave privada de nuestra AC y para la protección de la Clave privada de nuestro Servicio de Respuesta OCSP. Este grupo de tarjetas conforman un control M de N donde el quórum será tres necesarias de seis posibles. Las seis posibles son distribuidas entre el Responsable de Seguridad, el Administrador de Servicios Críticos, el Responsable de Comunicaciones y dos testigos.

5.2.3. Roles – Altas y modificaciones de roles

La asignación y/o modificación de los roles deberá ser realizada mediante disposición por parte del Responsable de la. AC - BOX CUSTODIA FIRMA DIGITAL. La misma prevé tanto los roles asignados a los titulares como a los sustitutos previstos en situaciones normales de operación.

5.2.4. Roles - Cese de funciones – Reemplazo

En caso de renuncia, remoción del cargo o cambio de rol asignado de cualquier funcionario relacionado con la AC - BOX CUSTODIA FIRMA DIGITAL, el personal sustituto previsto lo reemplazará. En estos casos el personal que no continúe con sus actividades se comunicará al Responsable de la AC - BOX CUSTODIA FIRMA DIGITAL de BOX CUSTODIA DE ARCHIVOS S.A., para que se inhabiliten las funciones del mismo en relación a la AC - BOX CUSTODIA FIRMA DIGITAL.

5.3. Controles de Seguridad del Personal

La AC - BOX CUSTODIA FIRMA DIGITAL cumple los mismos procedimientos de administración de personal establecidos para BOX CUSTODIA DE ARCHIVOS S.A.

BOX CUSTODIA DE ARCHIVOS S.A. mantiene controles para proveer seguridad en las prácticas de contratación y administración del personal, a fin de respaldar la confiabilidad de sus operaciones.

El personal que desempeña funciones en la AC - BOX CUSTODIA FIRMA DIGITAL está sujeto a evaluaciones de desempeño anual de índole profesional integral, conservándose la respectiva evidencia al respecto.

El personal que desempeña funciones en la AC - BOX CUSTODIA FIRMA DIGITAL no podrá estar sumariado, y será preventivamente apartado de dichas funciones en caso que se le iniciare uno, hasta el término de su resolución.

BOX CUSTODIA DE ARCHIVOS S.A. tiene procedimientos que minimizan los riesgos de error humano, robo, fraude o uso inadecuado de instalaciones.

Las responsabilidades en materia de seguridad son explicitadas en la etapa de inducción, incluidas en los contratos y monitoreadas durante el desempeño del empleado.

Los candidatos a ocupar los roles son adecuadamente seleccionados, especialmente si se trata de tareas críticas.

Todo el personal de la AC - BOX CUSTODIA FIRMA DIGITAL cumple o ha cumplido un proceso de selección previo a su incorporación que incluye los siguientes controles:

Verificación de antecedentes laborales:

a) El área de Recursos Humanos de BOX CUSTODIA DE ARCHIVOS S.A., por medio de sus oficinas competentes, conserva constancia de los antecedentes laborales de los candidatos en los correspondientes legajos de personal o en los sistemas de evaluación de desempeño.

Es responsabilidad de dichas oficinas la verificación de la aptitud de los candidatos mediante el chequeo de los antecedentes y referencias presentadas, entrevistas personales u otros mecanismos de selección adecuados, para una precalificación.

La selección entre los candidatos que hayan aprobado el paso previo anterior está a cargo del área de desarrollo de la AC - BOX CUSTODIA FIRMA DIGITAL.

Finalizado el proceso de selección, los candidatos seleccionados son nombrados en los roles respectivos por el Responsable de la AC - BOX CUSTODIA FIRMA DIGITAL, comunicándose dicho nombramiento por escrito a cada uno de los interesados, quienes se notificarán mediante la confección del “Acuerdo de Confidencialidad y Compromiso de Cumplimiento” del Anexo A del presente documento.

Las actuaciones de nombramientos y de los acuerdos firmados serán conservadas en los archivos de la AC - BOX CUSTODIA FIRMA DIGITAL bajo la custodia del Responsable de Seguridad.

Los roles definidos en las Políticas de Certificación de la AC - BOX CUSTODIA FIRMA DIGITAL son desempeñados por diferentes responsables. Ninguno de los nombrados concentrará más de una

función, aun cuando fuera en forma transitoria. En caso de ausencia temporaria, el responsable será reemplazado por su correspondiente sustituto.

5.4. Procedimientos de auditoría de seguridad

El Certificador mantiene registros de auditoría de todas las operaciones que realiza, protegiendo su integridad en medios de almacenamiento seguros y conservándolos por un período mínimo de DIEZ (10) años.

Asimismo, se mantendrán registros no informatizados de toda aquella información generada en formato de papel. Estos registros se encuentran disponibles tanto para la auditoría interna, como del Ente Licenciante y de otros organismos o entidades que tengan competencias al respecto.

Los principales procedimientos implementados a fin de respaldar la realización de las auditorías sobre la AC son los siguientes:

a) Tipo de eventos registrados.
   Los tipos de eventos que se registrarán son los relacionados a la administración del ciclo de vida de: las claves criptográficas, los certificados y los dispositivos criptográficos. Además, se registrarán los eventos relacionados a la solicitud de certificados y a los eventos de seguridad. Siguiendo lo establecido en el Anexo II Sección 3 de la Resolución 946/2021.
b) Frecuencia de procesamiento de registros.
   Los registros se procesarán periódicamente de acuerdo al tipo y se detalla la frecuencia en cada proceso descripto al final de la sección.
c) Período de guarda de los registros.
   Los registros se almacenarán por un periodo de 10 años según lo establecido en el inciso i) del artículo 21 de la Ley Nº 25.506 respecto a los certificados emitidos.
d) Medidas de protección de los registros, incluyendo privilegios de acceso.
   Las medidas de protección de los registros, incluyendo los privilegios de acceso se adecuan a las definiciones establecidas en la política de seguridad de la AC.
e) Procedimientos de resguardo de los registros.
   Las copias de respaldo se conservarán y almacenarán en lugares ignífugos, con acceso restringido y con condiciones ambientales adecuadas. Dichas copias poseerán rótulos identificatorios y serán solo accesibles por personal autorizado.
   Las copias de seguridad se almacenan en las instalaciones productivas y de contingencia como medida preventiva para asegurar la recuperación total de la información en caso de ser necesario.
f) Sistemas de recolección y análisis de registros (internos vs. externos).
   El SGSI posee un registro de logs centralizados que unifica los registros de los distintos puntos.
g) Notificaciones del sistema de recolección y análisis de registros.
   Desde el registro de logs centralizados se pueden establecer alertas de acuerdo al tipo de evento.
h) Evaluación de vulnerabilidades.

Debido a la necesidad de evaluar y tratar los riesgos de seguridad de la información para cumplir con las normativas legales vigentes se ha establecido una Política específica de Gestión de Riesgos de Seguridad de la Información la cual determina y establece todos los mecanismos adecuados para la evaluación y tratamiento de riesgos sobre los activos de información.

Los principales procedimientos implementados a fin de respaldar la realización de las auditorías sobre la AC-BOX CUSTODIA FIRMA DIGITAL son los siguientes:

a) Registro de logs de auditoría
   Procesamiento: semanal
   Archivo: trimestral
   Período de conservación: DIEZ (10) años
   Métodos de protección contra borrado o modificación: implementados a través de mecanismos de hash.
   Resguardo: se conservan dos copias en lugar físico seguro
b) Notificación de eventos significativos: todo el personal del Certificador es responsable cumplir un procedimiento de notificación de eventos que puedan comprometer la seguridad de los sistemas.
c) Informes de vulnerabilidad

Los Registros de logs de auditoría son generados por el Responsable de Auditoria según rol definido.

Tanto los logs de auditoria como lo informes de vulnerabilidades y las constancias de notificación de eventos de seguridad se mantienen a disposición de los organismos autorizados a efectuar auditorías sobre el Certificador. El procedimiento para su generación y mantenimiento se encuentra especificado en el Plan de Seguridad.

5.4.1. Generación y mantenimiento de archivos de auditoría

Los archivos de auditoría son generados automáticamente por el Sistema Informático de la AC - BOX CUSTODIA FIRMA DIGITAL, sin intervención de operadores.

La AR de la AC - BOX CUSTODIA FIRMA DIGITAL, bajo el esquema descentralizado en Puestos de Atención, tiene a disposición del organismo auditor toda la documentación que reciba o genere como respaldo del proceso de validación de la identidad de los solicitantes y suscriptores de certificados, que se conservará en lugar seguro dentro del ámbito de cada Puesto de Atención de la AR por DIEZ (10) años. En el caso de los certificados de suscriptores, el plazo se contará desde la fecha de vencimiento del certificado digital o de su revocación, lo que suceda en último término.

El Responsable de Seguridad mantiene controles que proveen seguridad en lo relativo a que:

a) Se mantiene un registro de eventos significativos referidos al ambiente del certificador;
b) La administración de claves y de certificados sea registrada en forma adecuada y completa;
c) Se mantiene la confidencialidad e integridad de los registros de eventos actuales y archivados;
d) Los registros de eventos se archivan en forma completa y confidencial y,

e) Los registros de eventos son revisados periódicamente por personal autorizado.

5.4.1.1. Eventos registrables

La AC - BOX CUSTODIA FIRMA DIGITAL lleva registro de los siguientes eventos:

	Información Registrada
Siempre	• Fecha y hora del registro. • Número de serie o secuencia del registro. • Tipo de registro. • Fuente del registro (ej.: terminal, puerto, etc.) • Identificación de la entidad que efectuó el registro.
	Eventos a Registrar
Administración del ciclo de vida de las claves	• Generación del par de claves del certificador • Instalación de claves criptográficas manuales y sus resultados (con identidad del operador). • Resguardo de las claves del certificador. • Almacenamiento de las claves del certificador. • Recuperación de las claves del certificador. • Utilización de las claves del certificador. • Archivo de las claves del certificador. • Destrucción de claves del certificador. • Identificación de quien autoriza una operación de administración de claves. • Identificación de quien maneja datos relativos a las claves (tal como componentes de claves, o claves almacenadas en dispositivos portátiles u otros medios). • Custodia de las claves o de dispositivos o medios que almacenan las claves. • Vulneración de la clave privada.
Administración del ciclo de vida de los certificados	• Recepción de solicitudes de certificados (inicial, renovación y de remisión de claves). • Transferencia de claves públicas para su certificación. • Cambios en los datos de identificación de una entidad. • Generación de certificados. • Distribución de la clave pública del certificador. • Solicitudes de revocación de certificados. • Generación y emisión de listas de certificados revocados. • Acciones tomadas relativas a la expiración de un certificado.
Administración del ciclo de vida de los dispositivos criptográficos	• Recepción del dispositivo. • Ingreso o retiro del dispositivo del lugar de almacenamiento. • Utilización de dispositivos. • Desinstalación del dispositivo. • Remisión de un dispositivo para servicio técnico o reparación. • Retiro / Baja / Descarga de un dispositivo.

Solicitud de Certificados	• Tipos de documentos identificatorios presentados por el solicitante. • Localización del archivo de las copias de las solicitudes de certificados y de los documentos de identificación. • Identificación de la entidad que acepta la solicitud. • Identificación de la Autoridad de Registro, de ser aplicable.
Eventos de seguridad	• Archivos de seguridad sensibles o registros leídos o escritos, incluyendo el registro diario de eventos. • Borrado de datos de seguridad sensibles. • Cambios en los perfiles de seguridad. • Utilización de mecanismos de identificación y autenticación, hayan o no sido exitosos (incluyendo intentos múltiples de autenticación fallida). • Caídas del sistema, fallas en el hardware y otras anomalías. • Acciones desarrolladas por los operadores y administradores del sistema y/u oficiales de seguridad informática. • Cambios de/ en los datos identificatorios de una entidad. • Decisiones de obviar procesos de encriptación / autenticación. • Accesos al sistema del certificador o a cualquier componente relacionado.
	Observaciones generales
Información sensible	Los registros de eventos no reflejaran los valores en texto plano de claves privadas o contraseñas.
Sincronización de eventos	Los sistemas de horario de las computadoras estaran sincronizados para permitir un correcto registro de eventos. La sincronización se realiza según la hora oficial, con un desvío no mayor a 1seg. Toda información de tiempo deberá estar expresada en UTC.

5.4.1.2. Copias de resguardo de archivos de transacciones de auditoría

Las copias de resguardo de los archivos de transacciones de auditoría de la AC - BOX CUSTODIA FIRMA DIGITAL se encontrarán a disposición del organismo auditor.

En forma periódica, y cumpliendo los mismos estándares para los sistemas informáticos de la AC - BOX CUSTODIA FIRMA DIGITAL para el resguardo diario, semanal y mensual, el sistema resguarda los datos. Cada 30 días, el Responsable de Seguridad se asegura que sendas copias del último respaldo disponible sean trasladadas al cofre ignífugo ubicado en el AMS del sitio operativo y del sitio alternativo.

Para el traslado y el almacenamiento seguro de los resguardos del HSM productivo, de su mundo de seguridad y OCS, el Responsable de Seguridad trasladará los mismos a un sitio alternativo seguro y físicamente junto al del HSM productivo, inmediatamente después de haberlos realizado. Los resguardos se alojarán cofre dentro del AMS a tal efecto dispuesta en el sitio alternativo. El sitio alternativo dispone de condiciones similares de seguridad física que el de la AC - BOX CUSTODIA FIRMA DIGITAL.

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 presente Manual de Procedimientos.

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

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

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

a) Tipo de registro archivado. Se respeta lo establecido en el Anexo II Sección 3 de la Resolución 946/2021.

b) Período de guarda de los registros.

c) Medidas de protección de los registros archivados, incluyendo privilegios de acceso.

d) Procedimientos de resguardo de los registros.

e) Sistemas de recolección y análisis de registros.

f) Procedimientos para obtener y verificar la información archivada.

AC - BOX CUSTODIA FIRMA DIGITAL mantiene un sistema de registro de eventos sobre cada una de las siguientes actividades. Para cada evento se registrará:

a) Fecha y hora de ocurrencia
b) Número de serie o secuencia
c) Tipo de evento
d) Fuente del registro
e) Identificación de la entidad que efectuó el registro

Administración del ciclo de vida de las claves criptográficas:

a) Generación y almacenamiento de las claves criptográficas del Certificador.
b) Resguardo de las claves criptográficas del Certificador.
c) Recuperación de las claves criptográficas del Certificador.
d) Utilización de las claves criptográficas del Certificador.

e) Archivo de las claves criptográficas del Certificador.
f) Retiro del servicio de datos relacionado con las claves criptográficas.
g) Destrucción de las claves criptográficas.
h) Identificación de la entidad que autoriza una operación de administración de claves criptográficas.
i) Identificación de la entidad que administra los datos relativos a las claves criptográficas.
j) Compromiso de la clave privada.

Administración del ciclo de vida de los certificados:

a) Recepción de solicitudes de certificados
b) Transferencia de claves públicas para la emisión de certificados.
c) Cambios en los datos de la solicitud del certificado.
d) Generación de certificados.
e) Distribución de la clave pública del certificado.
f) Solicitud de revocación del certificado
g) Generación y emisión de CRL.
h) Acciones tomadas en relación con la expiración de un certificado.

Administración del ciclo de vida de los dispositivos criptográficos:

a) Recepción del dispositivo.
b) Ingreso o retiro del dispositivo del lugar de almacenamiento.
c) Instalación del dispositivo.
d) Uso del dispositivo.
e) Desinstalación del dispositivo.
f) Envío de un dispositivo para servicio técnico o reparación.
g) Retiro, baja o borrado de información del dispositivo.

Información relacionada con la solicitud de certificados:

a) Tipos de documentos de identificación presentados por el solicitante.
b) Otra información de identificación, en caso de ser aplicable.
c) Ubicación del archivo de las copias de las solicitudes de certificados y de los documentos de identificación.
d) Identificación de la entidad que recibe y acepta la solicitud.
e) Método utilizado para validar los documentos de identificación.
f) Identificación de la Autoridad de Registro, de ser posible.

Eventos de seguridad:

a) Archivos sensibles de seguridad o registros leídos o escritos incluyendo el registro diario de eventos.
b) Borrado de datos sensibles de seguridad.

c) Cambios en los perfiles de seguridad.
d) Registros de intentos exitosos y fallidos de accesos al sistema, los datos y los recursos.
e) Caídas del sistema, fallas en el hardware y software u otras anomalías.
f) Acciones desarrolladas por los operadores y administradores de sistemas y responsables de seguridad.
g) Cambios en la relación entre el Certificador, la AC-BOX CUSTODIA FIRMA DIGITAL y las AR y el personal relacionado con el proceso de certificación.
h) Decisiones de no utilizar procesos o procedimientos de cifrado y/o autenticación.
i) Accesos al sistema de la AC- BOX CUSTODIA FIRMA DIGITAL o a cualquiera de sus componentes.

5.6. Cambio de claves criptográficas

El cambio de las claves criptográficas de la AC - BOX CUSTODIA FIRMA DIGITAL, podrá ocurrir por la necesidad de:

a) Sustituir las claves que van a ser retiradas, originado por el vencimiento del certificado de la AC.
b) Modificar la información contenida en el certificado, de importancia tal que obligue a solicitar un nuevo certificado a la Autoridad de Aplicación.
c) Producir el cese de la actual Política Única de Certificación y la tramitación de una nueva licencia.

En todos los casos este cambio de clave implica la emisión de un nuevo certificado por parte de la Autoridad de Aplicación a favor de la AC - BOX CUSTODIA FIRMA DIGITAL.

La clave privada que es objeto de cambio continuará siendo utilizada para firmar la lista de certificados revocados correspondiente a la Política bajo la cual fueron emitidos, hasta el plazo de validez del último certificado digital emitido con esa clave privada. En ese momento se revocará el certificado objeto del cambio y se destruirá la clave privada asociada al mismo.

Si la clave privada de la AC - BOX CUSTODIA FIRMA DIGITAL está comprometida, la Autoridad de Aplicación revocará su certificado y esa clave ya no podrá ser usada para firmar, ni siquiera CRLs. Los certificados de los suscriptores quedarán sin sustento en una situación equivalente a la de revocados.

5.7. Compromiso y recuperación ante desastres

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

Se han desarrollado procedimientos referidos a:

a) Identificación, registro, reporte y gestión de incidentes.

b) Recuperación ante falla inesperada o sospecha de falla de componentes de hardware, software y datos.

c) Recuperación ante compromiso o sospecha de compromiso de la clave privada del certificador.

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

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

5.8 Plan de Cese de Actividades

Se describen los requisitos y procedimientos a ser adoptados en caso de finalización de servicios del certificador o de una o varias de sus autoridades certificantes o de registro.

Estos requerimientos son desarrollados en su Plan de Cese de Actividades.

Se han implementado procedimientos referidos a:

a) Notificación al ente licenciante, suscriptores, terceros usuarios, otros certificadores y otros usuarios vinculados.

b) Custodia de archivos y documentación e identificación de su custodio.

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

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

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1. Generación e instalación de claves

La generación e instalación del par de claves serán consideradas desde la perspectiva de las Autoridades Certificantes del Certificador, de las autoridades de registro y de los suscriptores. Para cada una de estas entidades deberán abordarse los siguientes temas:

a) Responsables de la generación de claves.

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

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

d) Características y tamaños de las claves.

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

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

6.1.1. Generación del par de claves criptográficas

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

AC - BOX CUSTODIA FIRMA DIGITAL, luego del otorgamiento de la licencia por parte de la Autoridad de Aplicación para esta Política Única de Certificación, generará el par de claves criptográficas en un ambiente seguro con la participación de personal autorizado, sobre dispositivos criptográficos FIPS 140-2 Nivel 3. Para la generación del par de claves se utilizará el algoritmo RSA de 4096 bits con un período de vigencia de DIEZ (10) años.

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

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

BOX CUSTODIA DE ARCHIVOS S.A. es responsable de su par de claves criptográficas, no revela su clave privada a terceros bajo ninguna circunstancia y la almacena en un medio que garantiza su integridad y confidencialidad, estando en todo momento bajo el exclusivo control de ella, garantizando que es única y que se encuentra protegida contra réplicas fraudulentas.

Respecto del Certificador, la generación del par de claves de la **AC - BOX CUSTODIA FIRMA DIGITAL** se llevará a cabo según lo detallado en el documento bajo el título de *"Ceremonia Inicial"*.

Respecto de los responsables de la Autoridad de Registro, previa designación de su función por parte del Responsable de la **AC - BOX CUSTODIA FIRMA DIGITAL**, la generación y resguardo del par de claves criptográficas se efectuará mediante el procedimiento descrito en el documento titulado "Procedimientos de la Autoridad de Registro".

6.1.2. Entrega de la clave privada

Según lo establecido en "6.1.2. Entrega de la clave privada" de la Política Única de Certificación de **AC - BOX CUSTODIA FIRMA DIGITAL**.

6.1.3. Entrega de la clave pública al emisor del certificado

Según lo establecido en "6.1.3. Entrega de la clave pública" de la Política Única de Certificación de **AC - BOX CUSTODIA FIRMA DIGITAL**.

6.1.4. Disponibilidad de la clave pública del certificador

La AC - BOX CUSTODIA FIRMA DIGITAL publica en su repositorio de acceso libre "https://pki.boxcustodia.com/" su certificado digital, su certificado OCSP y los que compongan su cadena de certificación, estando disponibles las 24 horas los 365 días del año.

6.1.5. Tamaño de claves

Según lo establecido en "6.1.5. Tamaño de claves" de la Política Única de Certificación de **AC - BOX CUSTODIA FIRMA DIGITAL**.

6.1.6. Generación de parámetros de claves asimétricas

Según lo establecido en "6.1.6. Generación de parámetros de claves asimétricas" de la Política Única de Certificación de **AC - BOX CUSTODIA FIRMA DIGITAL**.

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

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

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

La protección de la clave privada debe ser considerada desde la perspectiva del certificador, de los repositorios, de las Autoridades de Registro *y* de los suscriptores, siempre que sea aplicable. Para cada una de estas entidades deberán abordarse los siguientes temas:

a) Estándares utilizados para la generación del par de claves.

b) Número de personas involucradas en el control de la clave privada.

c) En caso de existir copias de resguardo de la clave privada, controles de seguridad establecida sobre ellas.

d) Procedimiento de almacenamiento de la clave privada en un dispositivo criptográfico.

e) Responsable de activación de la clave privada y acciones a realizar para su activación.

f) Duración del periodo de activación de la clave privada y procedimiento a utilizar para su desactivación.

g) Procedimiento de destrucción de la clave privada.

Requisitos aplicables al dispositivo criptográfico utilizado para el almacenamiento de las claves privadas.

6.2.1. Estándares para dispositivos criptográficos

Para la generación y el almacenamiento de claves criptográficas, AC - BOX CUSTODIA FIRMA DIGITAL utiliza dispositivos de las siguientes características:

a) Para la generación de las claves criptográficas del Certificador: dispositivos que cumplen con las características definidas en FIPS 140-2 para el nivel 3.

b) Para la generación de las claves criptográficas utilizadas para la firma de información de estado de certificados: dispositivos que cumplen FIPS 140-2 nivel 3
c) Para certificados de suscriptores de nivel de seguridad Alto, el solicitante genera su par de claves y almacena la clave privada en un dispositivo criptográfico especial que cumplen con las características definidas en FIPS 140-2 para el nivel 3.

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

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

6.2.2. Control “M de N” de clave privada

La AC - BOX CUSTODIA FIRMA DIGITAL implementa el procedimiento que requiere la participación de funcionarios denominados “testigos”, poseedor de ACS, para los siguientes tipos de operación en el HSM:

a) Configuración inicial o reconfiguraciones
b) Alta/Modificación/Baja de Políticas
c) Creación/Modificación/Baja del Mundo de Seguridad
d) Actualización de Versiones de FW y/o SW
e) Reponer las OCS.
f) Modificar las OCS.
g) Generación/Destrucción de claves criptográficas
h) Generación/Restauración de resguardos

El valor adoptado para “M” es de 3 (tres) y para “N” es de 6 (seis).

6.2.3. Recuperación de clave privada

Ante una situación que requiera recuperar la clave privada de la AC - BOX CUSTODIA FIRMA DIGITAL y que no fuera producto de su compromiso, la misma se realizará con la presencia de los funcionarios testigos, el Administrador de Infraestructuras Criticas, el Administrador de Comunicaciones y el Responsable de Seguridad. La recuperación de la clave privada requiere la restauración del.

El prendimiento para la restauración de un resguardo del HSM se realizará desde un terminal dentro del recinto de la AC - BOX CUSTODIA FIRMA DIGITAL, mediante los siguientes pasos:

a) HSM

El procedimiento para la restauración de un resguardo del HSM operativo exige la presencia del Responsable de Seguridad, del Administrador de HSM, del Administrador de Partición y de los testigos involucrados según el nivel “M de N” establecido, con los OCS y ACS del equipo operativo.

Se realiza desde un terminal dentro del recinto operativo de la AC - BOX CUSTODIA FIRMA DIGITAL siguiendo los pasos detallados en el Anexo Backup y Recuperación del HSM.

Si la clave privada de la AC - BOX CUSTODIA FIRMA DIGITAL estuviera comprometida, se procederá a su inmediata destrucción, se caducarán todos los certificados digitales creados con dicha clave y se notificará a los suscriptores en un plazo inferior a las 24 horas.

6.2.4. Copia de seguridad de clave privada

La copia de seguridad de la clave privada y del certificado OCSP, se realiza mediante un resguardo del Mundo de Seguridad y los OCS del HSM, siguiendo el Anexo Backup y Recuperación del HSM

Cuando la clave privada de la AC - BOX CUSTODIA FIRMA DIGITAL está desactivada, el dispositivo criptográfico que la contiene permanece bajo el mismo control de seguridad física descripto en el punto 5 de la presente Política de Certificación.

6.2.5. Archivo de clave privada

La clave privada de la AC - BOX CUSTODIA FIRMA DIGITAL es archivada garantizando su integridad y confidencialidad.

En el Anexo Backup y Recuperación del HSM se establecen los procedimientos de archivo de la clave privada del Certificador.

6.2.6. Transferencia de claves privadas en dispositivos criptográficos

El par de claves criptográficas de la AC - BOX CUSTODIA FIRMA DIGITAL y del certificado OCSP se genera y almacena en dispositivos criptográficos conforme lo establecido en la Política Única de Certificación. Sólo se realizan dos transferencias de la clave privada de la AC - BOX CUSTODIA FIRMA DIGITAL y del certificado OCSP, correspondientes a sendos backups, uno para el sitio de operaciones principal y el otro para el sitio alternativo, utilizando los procedimientos de resguardo propios de los dispositivos criptográficos utilizados.

La clave privada de la AC - BOX CUSTODIA FIRMA DIGITAL, se crea dentro del dispositivo criptográfico en el momento de la Ceremonia Inicial. En caso necesario, la incorporación posterior de la misma clave privada al dispositivo criptográfico de la AC - BOX CUSTODIA FIRMA DIGITAL, se realiza mediante la restauración del resguardo correspondiente. Ambos eventos son llevados a cabo por medio de procedimientos que involucran a personal técnico, de seguridad y funcionarios testigos que garantizan la seguridad e integridad de la clave creada o restaurada.

En los dispositivos criptográficos de suscriptores de certificados digitales, la clave privada es generada y almacenada por el mismo dispositivo, sin transferirse ni extraerse bajo ninguna circunstancia.

La creación y almacenamiento de la clave privada para los suscriptores, se realiza cuando el solicitante inserta su dispositivo criptográfico en la estación de trabajo del Puesto de Atención provista a tal fin, seleccionando la opción "Generar Certificado

6.2.7. Almacenamiento de claves privadas

Este punto se encuentra descripto en el apartado 6.2.6 del presente Manual de Procedimientos.

6.2.8. Método de activación de claves privadas

Para la activación de la clave privada de la AC - BOX CUSTODIA FIRMA DIGITAL se aplica el procedimiento que requiere la participación de los testigos según el control “M de N”. El procedimiento se mencionó en el punto 6.2.6. – “Incorporación de claves privadas en dispositivos criptográficos” del presente Manual de Procedimientos.

Para la activación de la clave privada de suscriptores se aplican los procedimientos de los puntos 4.4 del presente Manual de Procedimientos.

6.2.9. Método de desactivación de claves privadas

La desactivación de claves privadas se lleva adelante mediante el procedimiento de desactivación provisto por el fabricante y llevado adelante por el Administrador de Servicios Críticos y el Responsable de Seguridad.

6.2.10. Método de destrucción de claves privadas

La destrucción del par de claves en una partición del Hardware Security Module (HSM) de la AC - BOX CUSTODIA FIRMA DIGITAL se realiza en forma remota desde el Terminal del HSM.

El proceso lo llevan adelante el Responsable de Seguridad y el Administrador del Servicios Críticos siguiendo las recomendaciones del fabricante.

En caso de cese de actividades del Certificador o de compromiso de la clave privada de la AC – BOX CUSTODIA FIRMA DIGITAL, los dispositivos criptográficos serán reformateados e inicializados nuevamente por personal autorizado.

6.2.11. Requisitos de los dispositivos criptográficos

El dispositivo criptográfico utilizado por el certificador se encuentra certificado por NIST (National Institute of Standards and Technology) con FIPS 140-2 Nivel 3.

Los dispositivos criptográficos utilizados por suscriptores en certificados están certificados por NIST (National Institute of Standards and Technology) con FIPS 140-2 Nivel 3.

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

6.3. Otros aspectos de administración de claves

6.3.1. Archivo permanente de la clave pública

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

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

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

.

6.3.2. Período de uso de clave pública y privada

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

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

6.4. Datos de activación

6.4.1. Generación e instalación de datos de activación

Los datos de activación del sistema informático de la AC - BOX CUSTODIA FIRMA DIGITAL tienen un control “M de N”. Cada procedimiento de activación de datos sobre el HSM se detalla en el anexo del presente manual bajo el título del Anexo II “Procedimiento para la ceremonia de emisión de certificado de la Autoridad Certificante de la AC - BOX CUSTODIA FIRMA DIGITAL” del presente Manual de Procedimientos. Mediante estos procedimientos se asegura el correcto uso de los datos de activación.

Los datos de activación de los dispositivos criptográficos de los Oficiales Certificadores, de los Responsables de los Puestos de Atención y del Responsable de AR, están garantizados mediante el uso de una clave de acceso a los dispositivos.

6.4.2. Protección de los datos de activación

La pérdida, robo o hurto del dispositivo criptográfico de la AC o los del personal afectado a sus funciones, deberá ser denunciada inmediatamente al Responsable de Seguridad, ya que mientras no se proceda en tal sentido las operaciones registradas durante ese lapso serán responsabilidad del poseedor del mismo.

La pérdida, robo o hurto del dispositivo criptográfico de un suscriptor o de su certificado digital, implica que el suscriptor o autorizado deban solicitar inmediatamente su revocación a la AC - BOX CUSTODIA FIRMA DIGITAL.

Cada suscriptor es único responsable por todas las operaciones que queden registradas bajo el dispositivo criptográfico que posee asignado.

Los suscriptores colocan una clave de protección del dispositivo criptográfico inmediatamente después de recibido o activado el certificado digital, en los intervalos requeridos por el dispositivo o ante la sospecha de revelación del mismo.

A efectos de la elección de la clave de protección no se utiliza combinaciones que posean propiedades de deducibilidad, como por ejemplo fechas conspicuas, repeticiones o sucesiones periódicas, métodos posicionales, etc. Los dispositivos criptográficos provistos por la AC - BOX CUSTODIA FIRMA DIGITAL están configurados para cumplir estos preceptos.

De ningún modo se hará préstamo del dispositivo criptográfico, ni dar a conocer su clave de protección o código de activación.

Los datos de activación son tratados como información confidencial y no estarán expuestos en medios accesibles por terceros. Las personas responsables de su custodia no divulgarán su condición.

Las pautas para la protección de los datos de activación de las claves privadas de los dispositivos de los suscriptores, quienes serán responsables del cumplimiento de las mismas, son mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, impedir su divulgación y aplicar las medidas de seguridad necesarias para evitar que terceros puedan tomar conocimiento de cualquier dato privado relacionado con su certificado digital.

6.4.3. Otros aspectos referidos a los datos de activación

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

6.5. Controles de seguridad informática

6.5.1. Requisitos Técnicos específicos

BOX CUSTODIA ARCHIVOS S.A., de manera de cumplimentar su política de seguridad informática, cumplimenta los siguientes requisitos:

6.5.1.1.

La autenticación del personal de BOX CUSTODIA ARCHIVOS S.A. involucrado en la operatoria del sistema informático de la AC - BOX CUSTODIA FIRMA DIGITAL, se implementa por medio de un dispositivo de autenticación externo. La aprobación de solicitudes de emisión, revocación y renovación de certificados es firmada digitalmente por el personal de los Puestos de Atención utilizando el dispositivo criptográfico que aloja su certificado digital de Clase 4.

6.5.1.2.

Para garantizar una adecuada segregación de funciones, existen roles para cada una de las principales actividades y responsabilidades de la AC - BOX CUSTODIA FIRMA DIGITAL, que se detallan en el punto 5.2.1.- “Roles” del presente Manual de Procedimientos.

6.5.1.3.

La identificación y autenticación del personal involucrado en el proceso de certificación u otras operaciones dentro de la AC - BOX CUSTODIA FIRMA DIGITAL, se efectúa con los medios descriptos en el punto a), de manera de garantizar y asegurar la autoría y legitimidad de las operaciones.

6.5.1.4.

Se utiliza criptografía para las sesiones de comunicación y acceso a las bases de datos mediante el estándar Secure Socket Level (SSL).

6.5.1.5.

En el sistema informático de la AC se almacenan en archivos los datos históricos y de auditoría del certificador. En los Puestos de Atención y en relación al proceso de certificación y a los trámites involucrados de los solicitantes de certificados, se almacenan los originales y/o copias de la documentación respaldatoria del proceso.

6.5.1.6.

Se registran los eventos de seguridad producidos en el proceso de certificación mediante los registros de auditoría del sistema de la AC.

6.5.1.7.

Se efectúan pruebas de seguridad periódicas relativas a los servicios de certificación, de acuerdo a los procedimientos indicados en el Plan de Seguridad, punto 19.- “Control de Acceso”.

6.5.1.8.

Para la identificación confiable de los roles afectados al proceso de certificación, el sistema identifica a los usuarios, atribuyéndole el perfil que le corresponda (Oficial de Registro, Responsable del Puesto de Atención o Responsable de AR) dentro del sistema de la AC - BOX CUSTODIA FIRMA DIGITAL.

6.5.1.9.

Para la recuperación de claves y el sistema de certificación, están disponibles la planilla de configuración del sistema y los archivos de seguridad en el sitio alternativo.

6.5.2. Requisitos de seguridad computacional

Todo el equipamiento afectado a las tareas sensibles de la AC - BOX CUSTODIA FIRMA DIGITAL se encuentra ubicado en la sala de acceso exclusivo, bajo los niveles de acceso requeridos por la normativa vigente.

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

6.6.1. Controles de desarrollo de sistemas

BOX CUSTODIA DE ARCHIVOS S.A. utiliza metodologías de desarrollo e implementación de sistemas basadas en el modelo OWASP (Open Web Application Security Project o Proyecto Abierto de Seguridad de Aplicaciones Web). Las áreas desarrolladoras de sistemas informáticos dedicadas a proyectos de seguridad, autenticación y firma digital han recibido documentación referencial procedente de este modelo, cuyos fundamentos se detallan en la página de Internet www.owasp.org.

6.6.2. Controles de gestión de seguridad

BOX CUSTODIA DE ARCHIVOS S.A. mantiene el control de los equipos por medio del inventario y la documentación de la configuración del sistema, así como toda modificación o actualización. Los

controles son auditados en forma periódica según las especificaciones correspondientes de la Política de Seguridad.

6.6.3. Calificaciones de seguridad del ciclo de vida del software

No hay procedimientos aplicables a este punto.

6.7. Controles de seguridad de red

BOX CUSTODIA DE ARCHIVOS S.A. posee mecanismos de control de acceso basados en una estructura separada de autenticación y de autorización de acceso a los sistemas, por medio del módulo de administración de usuarios de la AC - BOX CUSTODIA FIRMA DIGITAL, que es administrado por el Responsable de la AR.

BOX CUSTODIA DE ARCHIVOS S.A. posee un sistema de protección integral de sus activos informáticos, mediante la implementación de soluciones tipo "firewall" (filtrado de paquetes) y sistemas de detección de intrusiones online.

6.8. Certificación de Fecha y Hora

La AC - BOX CUSTODIA FIRMA DIGITAL brinda el servicio de Sellos de Tiempo para la certificación de fecha y hora. Este servicio está basado en la especificación de los estándares RFC 3161 - "Internet X. 509 Public Key Infrastructure (TSP), 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.

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

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

7. PERFILES DE CERTIFICADOS Y DE LISTAS DE CERTIFICADOS REVOCADOS

Los certificados emitidos por el Certificador respaldados por esta Política Única de Certificación cumplen con lo establecido en la especificación ITU X509 versión 3 (ISO/IEC 9594-8), adoptada como Estándar Técnico de la Infraestructura de Firma Digital de la República Argentina.

AC - BOX CUSTODIA FIRMA DIGITAL adhiere a las recomendaciones de los siguientes documentos en relación al perfil de los certificados:

- RFC 3739 "Internet X.509 Public Key Infrastructure Qualified Certificates Profile" [RFC3739].
- RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate

Revocation List (CRL) Profile" [RFC5280].

7.1. Perfil del certificado

Resulta de aplicación lo establecido en el apartado 7.1. de la Política Única de Certificación respecto al perfil del certificado de persona humana, de persona jurídica, de aplicaciones y de proveedores de servicios de firma digital.

7.2. Perfil de la lista de certificados revocados

Resulta de aplicación lo establecido en el apartado 7.2. de la Política Única de Certificación.

7.3. Perfil del certificado OCSP

Resulta de aplicación lo establecido en el apartado 7.3. de la Política Única de Certificación.

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

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

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

Se cumplen las exigencias reglamentarias impuestas por:

a) Los artículos 33 y 34 de la Ley Nº 25.506 de Firma Digital, respecto al sistema de auditoría y el artículo 21, inciso k) de la misma ley, relativo a la publicación de informes de auditoría.
b) Los artículos 6 a 8 del Decreto Nº 182/19, reglamentario de la Ley de Firma Digital, relativos al sistema de auditoría.
c) El Ente Licenciante de la Infraestructura de Firma Digital de la REPÚBLICA ARGENTINA realiza auditorías ordinarias al Certificador BOX CUSTODIA DE ARCHIVOS S.A., a la Autoridad Certificante AC - BOX CUSTODIA FIRMA DIGITAL y a sus Autoridades de Registro, a fin de verificar el cumplimiento de los requisitos de licenciamiento.
d) Las auditorías tienen por objeto verificar el cumplimiento de los requisitos exigidos para obtener y mantener la condición de Certificador Licenciado y la aplicación de las políticas y procedimientos aprobados por el Ente Licenciante para la presente Política Única de Certificación.

e) Por su parte, BOX CUSTODIA DE ARCHIVOS S.A., en su carácter de Certificador Licenciado, realizará auditorías periódicas a sus propias Autoridades de Registro autorizadas a funcionar con el objeto de verificar el cumplimiento de los procesos y procedimientos establecidos en la normativa regulatoria de Firma Digital.
f) La información relevante de los informes de las auditorías es publicada en el sitio web de la AC - BOX CUSTODIA FIRMA DIGITAL: https://pki.boxcustodia.com/ .

En base a lo dispuesto por las normas vigentes, la AC - BOX CUSTODIA FIRMA DIGITAL, en su calidad de certificador licenciado se encuentra sujeta a las auditorías de carácter interno y externo. Las auditorías externas pueden ser del Ente Licenciante de la Infraestructura Nacional de Firma Digital de la República Argentina o de servicios contratados a terceros.

El Ente Licenciante realiza las auditorías en base a sus programas los que son comunicados e informados oportunamente.

Los servicios externos son contratados como mínimo una vez al año para realizar una auditoría general.

Los aspectos a evaluar se encuentran establecidos en el artículo 27 de la Ley N° 25.506 y otras normas reglamentarias.

Los informes resultantes de las auditorías son elevados a las autoridades de Box Custodia de Archivos S.A.. Sus aspectos relevantes son publicados en forma permanente e ininterrumpida en su sitio web.

El certificador cumple las exigencias reglamentarias impuestas por:

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

9. ASPECTOS LEGALES Y ADMINISTRATIVOS

9.1. Aranceles

El servicio prestado por BOX CUSTODIA DE ARCHIVOS S.A. será arancelado para los solicitantes y suscriptores de certificados.

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

9.2. Responsabilidad Financiera

La responsabilidad financiera se origina en lo establecido por la Ley Nº 25.506 y su Decreto Nº 182/19 y en las disposiciones establecidas en la Política Única de Certificación.

9.3. Confidencialidad

Toda información referida a solicitantes o suscriptores de certificados que sea recibida por el Certificador o por las AR operativamente vinculadas, será tratada en forma confidencial y no puede hacerse pública sin el consentimiento previo de los titulares de los datos, salvo que sea 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 AR durante el ciclo de vida del certificado.

Lo indicado 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

Resulta de aplicación lo establecido en el apartado 9.3.1 de la Política Única de Certificación.

9.3.2. Información no confidencial

Resulta de aplicación lo establecido en el apartado 9.3.2. de la Política Única de Certificación.

9.3.3. Responsabilidades de los roles involucrados

Resulta de aplicación lo establecido en el apartado 9.3.3. de la Política Única de Certificación.

9.4. Privacidad

Resulta de aplicación lo establecido en el apartado 9.4. de la Política Única de Certificación.

9.5 Derechos de Propiedad Intelectual

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

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

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

9.6. Responsabilidades y garantías

Resulta de aplicación lo establecido en el apartado 9.6. de la Política Única de Certificación.

9.7. Deslinde de responsabilidad

Resulta de aplicación lo establecido en el apartado 9.7. de la Política Única de Certificación.

9.8. Limitaciones a la responsabilidad frente a terceros

Resulta de aplicación lo establecido en el apartado 9.8. de la Política Única de Certificación.

9.9. Compensaciones por daños y perjuicios

Resulta de aplicación lo establecido en el apartado 9.9. de la Política Única de Certificación.

9.10. Condiciones de vigencia

Resulta de aplicación lo establecido en el apartado 9.10. de la Política Única de Certificación.

9.11. Avisos personales y comunicaciones con los participantes

No aplicable.

9.12. Gestión del ciclo de vida del documento

9.12.1. Procedimientos de cambio

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

9.12.2. Mecanismo y plazo de publicación y notificación

AC - BOX CUSTODIA FIRMA DIGITAL, una vez notificada de la aprobación de las modificaciones a los documentos indicados en el apartado 9.12.1 por parte de la Autoridad de Aplicación, y siempre que se trate de documentos de carácter público, publicará en su sitio web las modificaciones aprobadas, indicando, en cada caso, el texto reemplazado. Asimismo, se publicará el texto de las nuevas versiones de los mencionados documentos.

Los suscriptores que posean certificados vigentes a la fecha de aplicación del cambio serán notificados por correo electrónico en las direcciones declaradas en los correspondientes certificados.

Los documentos vigentes de carácter público y sus versiones anteriores se encuentran disponibles en su sitio web https://pki.boxcustodia.com/

9.12.3. Condiciones de modificación del OID

No aplicable.

9.13. Procedimientos de resolución de conflictos

Resulta de aplicación lo establecido en el apartado 9.13. de la Política Única de Certificación.

9.14. Legislación aplicable

Resulta de aplicación lo establecido en el apartado 9.14. de la Política Única de Certificación.

9.15. Conformidad con normas aplicables

Resulta de aplicación lo establecido en el apartado 9.15. de la Política Única de Certificación.

9.16. Cláusulas adicionales

No se establecen cláusulas adicionales.

9.17. Otras cuestiones generales

No aplicable

República Argentina - Poder Ejecutivo Nacional
Las Malvinas son argentinas

Hoja Adicional de Firmas
Anexo

Número: IF-2022-91402105-APN-SSIA#JGM

CIUDAD DE BUENOS AIRES
Miércoles 31 de Agosto de 2022

Referencia: Manual de Procedimientos 2.3 - BOX/CUSTODIA DE ARCHIVOS S A

El documento fue importado por el sistema GEDO con un total de 68 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2022.08.31 11:18:54 -03:00

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

Digitally signed by Gestion Documental Electronica
Date: 2022.08.31 11:18:55 -03:00