


MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN

CERTIFICADOR LICENCIADO


PRISMA MEDIOS DE PAGO S.A.

Versión: 2.0

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 2 de 59


Versiones y modificaciones de este documento

Ver	Mod	Fecha	Autor	Validación	Descripción
1	0	Julio 2015	PRISMA MEDIOS DE PAGO S.A.		Versión inicial
2	0	Mayo 2017	PRISMA MEDIOS DE PAGO S.A.		Adecuación del documento a la Resolución 399-E/16 del MINISTERIO DE MODERNIZACIÓN.


	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 3 de 59

Contenido


1.	INTRODUCCIÓN.....	9
1.1.	Descripción General	9
1.2.	Nombre e identificación del documento.....	9
1.3.	Participantes	10
1.3.1.	Certificador	10
1.3.2.	Autoridad de registro	10
1.3.3.	Suscriptores de certificados	10
1.3.4.	Terceros Usuarios.....	11
1.4.	Uso de los certificados.....	11
1.5.	Administración del Manual de Procedimientos.....	11
1.5.1.	Responsable del documento.....	11
1.5.2.	Contactos	11
1.5.3.	Procedimiento de aprobación del Manual de Procedimientos	12
1.6.	Definiciones y Acrónimos	12
1.6.1.	Definiciones.....	12
1.6.2.	Acrónimos	14
2.	RESPONSABILIDADES VINCULADAS A LA PUBLICACIÓN Y A LOS REPOSITORIOS	15
2.1.	Repositorios	15
2.2.	Publicación de información del certificador	15
2.3.	Frecuencia de publicación	15
2.4.	Controles de acceso a la información.....	15
3.	IDENTIFICACIÓN Y AUTENTICACIÓN	16
3.1.	Asignación de nombres de suscriptores.....	16
3.1.1.	Tipos de Nombres.....	16
3.1.2.	Necesidad de Nombres Distintivos.....	16
3.1.3.	Anonimato o uso de seudónimos.....	18
3.1.4.	Reglas para la interpretación de nombres.....	18

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 4 de 59


3.1.5.	Unicidad de nombres.....	19
3.1.6.	Reconocimiento, autenticación y rol de las marcas registradas	19
3.2.	Registro Inicial.....	19
3.2.1.	Métodos para comprobar la posesión de clave privada.....	20
3.2.2.	Autenticación de la identidad de personas jurídicas públicas o privadas	20
3.2.3.	Autenticación de la identidad de personas físicas	21
3.2.4.	Información no verificada del suscriptor	22
3.2.5.	Validación de Autoridad	22
3.2.6.	Criterios de Interoperabilidad.....	23
3.3.	Identificación y autenticación para la generación de un nuevo par de claves	23
3.3.1.	Renovación con generación de nuevo par de claves (rutina de Re-Key).....	23
3.3.2.	Generación de UN (1) certificado con el mismo par de claves	23
3.4.	Requerimiento de revocación.....	24
4.	CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS.....	25
4.1.	Solicitud de Certificado.....	25
4.1.1.	Solicitantes de certificado.....	25
4.1.2.	Solicitud de certificado	25
4.2.	Procesamiento de la solicitud del certificado	26
4.3.	Emisión del certificado	26
4.3.1.	Proceso de Emisión de certificado	26
4.3.2.	Notificación de Emisión	26
4.4.	Aceptación del certificado	26
4.5.	Uso del par de claves y del certificado	26
4.5.1.	Uso de la clave privada y del certificado por parte del suscriptor	26
4.5.2.	Uso de la clave pública y del certificado por parte de Terceros Usuarios.....	27
4.6.	Renovación del certificado sin generación de un nuevo par de claves.....	27
4.7.	Renovación del certificado con generación de un nuevo par de claves.....	27
4.8.	Modificación del certificado	28
4.9.	Suspensión y Revocación de certificados	28
4.9.1.	Causas de revocación	28

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 5 de 59


4.9.2.	Autorizados a solicitar la revocación	29
4.9.3.	Procedimientos para la solicitud de revocación	29
4.9.4.	Plazo para la solicitud de revocación.....	30
4.9.5.	Plazo para el procesamiento de la solicitud de revocación	30
4.9.6.	Requisitos para la verificación de la lista de certificados revocados.....	30
4.9.7.	Frecuencia de emisión de listas de certificados revocados	31
4.9.8.	Vigencia de la lista de certificados revocados.....	31
4.9.9.	Disponibilidad del servicio de consulta sobre revocación y estado del certificado	31
4.9.10.	Requisitos para la verificación en línea del estado de revocación.....	31
4.9.11.	Otras formas disponibles para la divulgación de la revocación	31
4.9.12.	Requisitos específicos para casos de compromiso de claves	31
4.9.13.	Causas de suspensión	31
4.9.14.	Autorizados a solicitar la suspensión.....	31
4.9.15.	Procedimientos para la solicitud de suspensión	31
4.9.16.	Límites del período de suspensión de un certificado	32
4.10.	Estado del certificado	32
4.10.1.	Características técnicas.....	32
4.10.2.	Disponibilidad del servicio	32
4.10.3.	Aspectos Operativos.....	32
4.11.	Desvinculación del suscriptor.....	32
4.12.	Recuperación y custodia de claves privadas.....	32
5.	CONTROLES DE SEGURIDAD FÍSICA, OPERATIVOS Y DE GESTIÓN	33
5.1.	Controles de seguridad física	33
5.2.	Controles de gestión.....	33
5.3.	Controles de seguridad del personal.....	33
5.4.	Procedimientos de Auditoría de Seguridad	34
5.5.	Conservación de registros de eventos.....	35
5.6.	Cambio de claves criptográficas.....	35
5.7.	Plan de respuesta a incidentes y recuperación ante desastres	35
5.8.	Plan de cese de actividades	36

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 6 de 59


6.	CONTROLES DE SEGURIDAD TECNICA	36
6.1.	Generación e instalación del par de claves criptográficas.....	36
6.1.1.	Generación del par de claves criptográficas	36
6.1.2.	Entrega de la clave privada al suscriptor	37
6.1.3.	Entrega de la clave pública al emisor del certificado	37
6.1.4.	Disponibilidad de la clave pública del certificador	37
6.1.5.	Tamaño de claves	37
6.1.6.	Generación de parámetros de claves asimétricas.....	37
6.1.7.	Propósitos de utilización de claves (campo “KeyUsage” en certificados X.509 v.3)	37
6.2.	Protección de la clave privada y controles sobre los dispositivos criptográficos	38
6.2.1.	Estándares para dispositivos criptográficos.....	38
6.2.2.	Control “M de N” de clave privada.....	38
6.2.3.	Recuperación de clave privada	38
6.2.4.	Copia de seguridad de clave privada	38
6.2.5.	Archivo de clave privada	38
6.2.6.	Transferencia de claves privadas en dispositivos criptográficos.....	38
6.2.7.	Almacenamiento de claves privadas en dispositivos criptográficos	38
6.2.8.	Método de activación de claves privadas	39
6.2.9.	Método de desactivación de claves privadas	39
6.2.10.	Método de destrucción de claves privadas	39
6.2.11.	Requisitos de los dispositivos criptográficos.....	39
6.3.	Otros aspectos de administración de claves.....	39
6.3.1.	Archivo permanente de la clave pública.....	39
6.3.2.	Período de uso de clave pública y privada.....	39
6.4.	Datos de activación	40
6.4.1.	Generación e instalación de datos de activación	40
6.4.2.	Protección de los datos de activación	40
6.4.3.	Otros aspectos referidos a los datos de activación	40
6.5.	Controles de seguridad informática.....	40
6.5.1.	Requisitos técnicos específicos.	40

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 7 de 59

6.5.2.	Requisitos de seguridad computacional	41
6.6.	Controles Técnicos del ciclo de vida de los sistemas	41
6.6.1.	Controles de desarrollo de sistemas	41
6.6.2.	Controles de gestión de seguridad	41
6.6.3.	Calificaciones de seguridad del ciclo de vida del software	41
6.7.	Controles de seguridad de red	41
6.8.	Certificación de fecha y hora	41
7.	PERFILES DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS.....	42
7.1.	Perfil del certificado	42
7.2.	Perfil de la lista de certificados revocados	49
7.3.	Perfil de la consulta en línea del estado del certificado	49
8.	AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES.....	50
9.	ASPECTOS GENERALES LEGALES Y ADMINISTRATIVOS.	50
9.1.	Aranceles	50
9.2.	Responsabilidad Financiera	50
9.3.	Confidencialidad.....	50
9.3.1.	Información confidencial	51
9.3.2.	Información no confidencial	51
9.3.3.	Responsabilidad de los roles involucrados	51
9.4.	Privacidad	52
9.5.	Derechos de propiedad intelectual	52
9.6.	Responsabilidades y garantías	52
9.7.	Deslinde de la responsabilidad	52
9.8.	Limitaciones a la responsabilidad frente a terceros.....	53
9.9.	Compensaciones por daños y perjuicios	53
9.10.	Condiciones de Vigencia	53
9.11.	Avisos personales y comunicaciones con los participantes.....	54
9.12.	Gestión del ciclo de vida del documento.....	54
9.12.1.	Procedimientos de cambio	54
9.12.2.	Mecanismo y plazo de publicación y notificación	54

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 8 de 59

9.12.3.	Condiciones de modificación del OID.....	54
9.13.	Procedimientos de resolución de conflictos.....	54
9.14.	Legislación aplicable	55
9.15.	Conformidad con normas aplicables	55
9.16.	Cláusulas adicionales	59
9.17.	Otras cuestiones generales.....	59

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 9 de 59

1. INTRODUCCIÓN

1.1. Descripción General

El presente Manual describe el conjunto de procedimientos utilizados por el Certificador cuyas funciones son ejercidas por PRISMA MEDIOS DE PAGO S.A. (en adelante el Certificador) en el cumplimiento de sus responsabilidades de administración de certificados digitales emitidos a favor de sus suscriptores, en el marco de la Ley N° 25.506 de firma digital, el Decreto N° 2628 del 19 de diciembre de 2002, la Decisión Administrativa N° 927 del 30 de noviembre de 2014 y demás normas reglamentarias.

Este Manual de Procedimientos forma parte de la documentación técnica emitida por el Certificador junto con los siguientes documentos:

- a) Política Única de Certificación.
- b) Plan de Seguridad (incluyendo política y procedimientos de seguridad).
- c) Plan de Continuidad de Operaciones.
- d) Plan de Cese de Actividades.
- e) Acuerdo con Suscriptores.
- f) Términos y Condiciones con Terceros Usuarios.
- g) Política de Privacidad.
- h) Plataforma tecnológica.


1.2. Nombre e identificación del documento

Nombre: Manual de Procedimientos de Certificación de PRISMA MEDIOS DE PAGO S.A.

Versión: 1.0

Fecha:

Lugar: se publica en el sitio web de la BANELCO AC, URL: <http://ac.banelco.com.ar/firma-digital/docs/>

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 10 de 59

1.3. Participantes

1.3.1. Certificador

PRISMA MEDIOS DE PAGOS S.A. en su carácter de Certificador, prestará servicios de certificación de acuerdo a lo establecido en la presente política.

Domicilio: Lavarden 247 (C1437FBE) – CABA – Buenos Aires – Argentina.

Teléfono: (54 11) 4345-5678

E-mail: contacto_ac@prismamp.com.ar

CUIT: 30-59891004-5.

1.3.2. Autoridad de registro

Las Autoridades de Registro de la BANELCO AC tienen por función la identificación y validación de identidad y de los otros datos de los solicitantes y suscriptores de certificados digitales que a su vez lleva implícita la tarea de verificación y guarda de la documentación presentada por los mismos.


La estructura de las Autoridades de Registro estará conformada de la siguiente manera:

- a) Autoridad de Registro Central: se encontrará y operará bajo la órbita directa de PRISMA MEDIOS DE PAGOS S.A., habilitándose la modalidad “itinerante” para su funcionamiento y;
- b) Autoridades de Registro Descentralizadas: funcionarán en distintas organizaciones previa aprobación de PRISMA MEDIOS DE PAGO S.A. Estas Autoridades de Registro operarán bajo el estricto control y supervisión de PRISMA MEDIOS DE PAGO S.A.

Las Autoridades de Registro habilitadas se publicarán en el sitio <http://ac.banelco.com.ar/firma-digital/AutoridadesDeRegistro.pdf> bajo el título “Autoridades de Registro”.

1.3.3. Suscriptores de certificados

Los suscriptores de certificados serán personas físicas o aquellas personas jurídicas que tengan por objetivo cualquiera de los usos de certificados digitales y emitidos a nombre de personas físicas, personas jurídicas, aplicaciones, sitio seguro y de autoridad de competencia y de sello de tiempo de acuerdo a lo definido, y en los términos expresados en la presente “Política única de Certificación”.

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 11 de 59

1.3.4. Terceros Usuarios

Son Terceros Usuarios de los certificados emitidos bajo la presente Política Única de Certificación, toda persona física o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente, de acuerdo al Anexo I del Decreto N° 2628 del 19 de diciembre de 2002. En el caso de los certificados de sitio seguro, serán Terceros Usuarios quienes verifiquen el certificado del servidor.

1.4. Uso de los certificados

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

1.5. Administración del Manual de Procedimientos

1.5.1. Responsable del documento

Será responsable de la presente Política Única de Certificación quien ejerza las funciones de Responsable de la autoridad certificante BANELCO AC de PRISMA MEDIOS DE PAGOS S.A.

E-mail: contacto_ac@prismamp.com.ar

Teléfono (5411) 4345-5678

1.5.2. Contactos

Datos del responsable del registro, mantenimiento e interpretación del Manual de Procedimientos (Responsable de la Autoridad Certificante BANELCO AC):

Responsable: Gerente de Autenticación

E-mail: autoridad.certificante@prismamp.com.ar


Teléfono: (5411) 4345-5678

Para consultas, reclamos y sugerencias referidas al proceso de certificación:

Centro de Contacto

Domicilio: Lavarden 247 (C1437FBE) – CABA – Buenos Aires, Argentina

E-mail: contacto_ac@prismamp.com.ar

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 12 de 59

Teléfono: (5411) 4345-5678

1.5.3. Procedimiento de aprobación del Manual de Procedimientos

El procedimiento a aplicar en la generación y aprobación de la documentación será el Procedimiento de Aprobación de Políticas, documentos y Procedimientos denominado:


P-AprobacionPolíticasNormasProcedimientos.

Una vez concluida la aprobación interna, se procederá a enviar al Ente Licenciante, y se establecerá una nueva versión del Manual de Procedimientos cuando se haya recibido la aprobación correspondiente.

1.6. Definiciones y Acrónimos


1.6.1. Definiciones

- Autoridad de Aplicación: la SECRETARIA DE MODERNIZACIÓN del MINISTERIO DE MODERNIZACIÓN.
- Autoridad de Registro: es la entidad que tiene a su cargo las funciones de:
 - o Recepción de las solicitudes de emisión de certificados.
 - o Validación de la identidad y autenticación de los datos de los titulares de certificados.
 - o Validación de otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue el Certificador Licenciado.
 - o Remisión de las solicitudes aprobadas al Certificador Licenciado con la que se encuentre operativamente vinculada.
 - o Recepción y validación de las solicitudes de revocación de certificados; y su direccionamiento al Certificador Licenciado con el que se vinculen.
 - o Identificación y autenticación de los solicitantes de revocación de certificados.
 - o 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.
 - o Cumplimiento de las normas y recaudos establecidos para la protección de datos personales.
 - o Cumplimiento de las disposiciones que establezca la Política de Certificación y el Manual de Procedimientos del Certificador Licenciado con el que se encuentre vinculada, en la parte que resulte aplicable.

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 13 de 59

Dichas funciones son delegadas por el certificador licenciado. Puede actuar en una instalación fija o en modalidad móvil, siempre que medie autorización de la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA del MINISTERIO DE MODERNIZACIÓN.

- 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 N° 25.506).
- Certificación digital de fecha y hora: indicación de la fecha y hora cierta, asignada a un documento o registro electrónico por una tercera parte confiable y firmada digitalmente por ella. (Anexo al Decreto N° 2628 de fecha 19 de diciembre de 2002).
- Ente licenciante: el MINISTERIO DE MODERNIZACIÓN, siendo dicho organismo y la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA, quienes entienden en las funciones de Ente Licenciante.
- Lista de certificados revocados: Lista de certificados que han sido dejados sin efecto en forma permanente por el Certificador Licenciado, la cual ha sido firmada digitalmente y publicada por el mismo. En ingles: Certificate Revocation List (CRL). (Anexo al Decreto N° 2628/02).
- Manual de Procedimientos: Conjunto de prácticas utilizadas por el certificador licenciado en la emisión y administración de los certificados. En ingles: Certification Practice Statement (CPS). (Anexo al Decreto N° 2628/02).
- Plan de Cese de Actividades: conjunto de actividades a desarrollar por el certificador licenciado en caso de finalizar la prestación de sus servicios. (Anexo al Decreto N° 2628/02).
- Plan de continuidad de las operaciones: Conjunto de procedimientos a seguir por el certificador licenciado ante situaciones de ocurrencia no previstas que comprometan la continuidad de sus operaciones.
- Plan de Seguridad: Conjunto de políticas, prácticas y procedimientos destinados a la protección de los recursos del certificador licenciado. (Anexo al Decreto N° 2628/02).
- Política de Privacidad: conjunto de declaraciones que el Certificador Licenciado se compromete a cumplir de manera de resguardar los datos de los solicitantes y suscriptores de certificados por el emitido.
- 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

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 14 de 59

Revocación de Certificados (CRL). El resultado de una consulta a este servicio está firmado por el certificador que brinda el servicio.

- Suscriptor o Titular de certificado digital: Persona o entidad a cuyo nombre se emite un certificado y que posee una clave privada que se corresponde con la clave pública contenida en el mismo.

- Tercero Usuario: persona física o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente. (Artículo 3° del Decreto N° 724/06).

1.6.2. Acrónimos

AC – Autoridad Certificante

CA- Certificate Authority

DRP – Disaster Recovery Plan

PRD – Plan de recupero ante desastres

CRL – Lista de Certificados Revocados

CUIT – Clave Única de Identificación Tributaria

CUIL – Clave Única de Identificación Laboral

DNI – Documento Nacional de Identidad

IEC – International Electrotechnical Commission


IETF – Internet Engineering Task Force

OID – Identificador de Objeto (“Object Identifier”)

RFC – Request for Comments

OCSP – Protocolo en línea del estado de un certificado (“Online Certificate Status Protocol”)

DNSAFD – Dirección Nacional de Sistemas de Administración y Firma Digital

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 15 de 59

2. RESPONSABILIDADES VINCULADAS A LA PUBLICACIÓN Y A LOS REPOSITORIOS

2.1. Repositorios

Los repositorios serán administrados por PRISMA MEDIOS DE PAGO S.A. y estarán ubicados en servidores propios.

2.2. Publicación de información del certificador

El Certificador garantizará el acceso a la información actualizada y vigente publicada en su repositorio de los siguientes elementos:

- a) Formulario de Adhesión del Anexo I
- b) Política Única de Certificación anteriores y vigente
- c) Acuerdo Tipo con suscriptores
- d) Términos y condiciones Tipo con terceros usuarios (“relying parties”)
- e) Política de Privacidad
- f) Manual de Procedimientos (parte pública)
- g) Información relevante de los informes de su última auditoría
- h) Repositorio de certificados revocados
- i) Certificados del certificador licenciado y acceso al de la Autoridad Certificante Raíz


2.3. Frecuencia de publicación

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

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.

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 16 de 59

En virtud de lo dispuesto por la Ley de Protección de Datos Personales N° 25.326 y por el inciso h) del artículo 21 de la ley N° 25.506, el solicitante o titular de un certificado digital podrá solicitar acceso a toda la información relativa a las tramitaciones realizadas.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. Asignación de nombres de suscriptores

3.1.1. Tipos de Nombres

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

3.1.2. Necesidad de Nombres Distintivos


Para los certificados de los proveedores de servicios de firma digital o de aplicación:

- “commonName” (OID 2.5.4.3: Nombre común): DEBE corresponder al nombre de la aplicación, servicio o de la unidad operativa responsable del servicio.
- “organizationalUnitName” (OID 2.5.4.11: Nombre de la suborganización): DEBE contener a las unidades operativas relacionadas con el servicio, en caso de existir, pudiendo utilizarse varias instancias de este atributo de ser necesario.
- “organizationName” (OID 2.5.4.10: Nombre de la organización): DEBE estar presente y DEBE coincidir con el nombre de la Persona Jurídica Pública o Privada responsable del servicio o aplicación.
- “serialNumber” (OID 2.5.4.5: Nro. de serie): DEBE estar presente y DEBE contener el número de identificación de la Persona Jurídica Pública o Privada responsable del servicio o aplicación, expresado como texto y respetando el siguiente formato y codificación: “[código de identificación]” “[nro. de identificación]”

El valor para el campo [código de identificación] es:

- “CUIT”: Clave Única de Identificación Tributaria para las Personas Jurídicas argentinas.
- “countryName” (OID 2.5.4.6: Código de país): DEBE estar presente y DEBE representar el país de emisión de los certificados, codificado según el estándar [ISO3166] de DOS (2) caracteres.

Para los certificados de Personas Físicas:

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 17 de 59

- “commonName” (OID 2.5.4.3: Nombre común): DEBE estar presente y DEBE corresponderse con el nombre que figura en el Documento de Identidad del suscriptor, acorde a lo establecido en el punto 3.2.3.
- “serialNumber” (OID 2.5.4.5: Nro. de serie): DEBE estar presente y DEBE contener el tipo y número de identificación del titular, expresado como texto y respetando el siguiente formato y codificación: “[tipo de documento]” “[nro. de documento]”

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


- En caso de ciudadanos argentinos o residentes: “CUIT/CUIL”: Clave Única de Identificación Tributaria o Laboral.
- En caso de extranjeros:
 - o “PA” [país]: Número de Pasaporte y código de país emisor. El atributo [país] DEBE estar codificado según el estándar [ISO3166] de DOS (2) caracteres.
 - o “EX” [país]: Número y tipo de documento extranjero aceptado en virtud de acuerdos internacionales [país] DEBE estar codificado según el estándar [ISO3166] de DOS (2) caracteres
- “countryName” (OID 2.5.4.6: Código de país): DEBE estar presente y DEBE representar el país de emisión de los certificados, codificado según el estándar [ISO3166] de DOS (2) caracteres.

Para los certificados de Personas Jurídicas Públicas o Privadas:

- “commonName” (OID 2.5.4.3: Nombre común): DEBE coincidir con la denominación de la Persona Jurídica Pública o Privada o con el nombre de la unidad operativa responsable del servicio (ej. Gerencia de Compras).
- “organizationalUnitName” (OID 2.5.4.11: Nombre de la suborganización): PUEDE contener las unidades operativas relacionadas con el suscriptor, pudiendo utilizarse varias instancias de este atributo de ser necesario.
- “organizationName” (OID 2.5.4.10: Nombre de la organización): DEBE coincidir con la denominación de la Persona Jurídica Pública o Privada.
- “serialNumber” (OID 2.5.4.5: Nro. de serie): DEBE estar presente y DEBE contener el número de identificación de la Persona Jurídica Pública o Privada, expresado como texto y respetando el siguiente formato y codificación: “[código de identificación]” “[nro. de identificación]”

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

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

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 18 de 59

- “ID” [país]: Número de identificación tributario para Personas Jurídicas extranjeras. El atributo [país] DEBE estar codificado según el estándar [ISO3166] de DOS (2) caracteres.
- “countryName” (OID 2.5.4.6: Código de país): DEBE estar presente y DEBE representar el país de emisión de los certificados, codificado según el estándar [ISO3166] de DOS (2) caracteres.

Para los certificados de Sitio Seguro:


- “commonName” (OID 2.5.4.3: Nombre común): DEBE contener la denominación del sitio web de Internet que busca proteger.
- “organizationalUnitName” (OID 2.5.4.11: Nombre de la suborganización): DEBE contener a las unidades operativas de las que depende el sitio web, de corresponder, pudiendo utilizarse varias instancias de este atributo de ser necesario.
- “organizationName” (OID 2.5.4.10: Nombre de la Organización): DEBE estar presente y DEBE coincidir con el nombre de la Persona Jurídica Pública o Privada responsable del sitio web.
- “serialNumber” (OID 2.5.4.5: Nro. de serie): DEBE estar presente y DEBE contener el número de identificación de la Persona Jurídica Pública o Privada responsable del servicio o aplicación, expresado como texto y respetando el siguiente formato y codificación: “[código de identificación]” “[nro. de identificación]”.
- El valor para el campo [código de identificación] es: “CUIT”: Clave Única de Identificación Tributaria para las Personas Jurídicas argentinas.
- “countryName” (OID 2.5.4.6: Código de país): DEBE estar presente y DEBE representar el país de emisión de los certificados, codificado según el estándar [ISO3166] de DOS (2) caracteres.
- Adicionalmente, el certificador licenciado incluirá la información específica correspondiente a esta sección, la cual surge del Anexo I.

3.1.3. Anonimato o uso de seudónimos

No se emitirán certificados anónimos o cuyo nombre distintivo contenga un seudónimo.

3.1.4. Reglas para la interpretación de nombres

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

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 19 de 59

3.1.5. Unicidad de nombres

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

3.1.6. Reconocimiento, autenticación y rol de las marcas registradas

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

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

3.2. Registro Inicial


El solicitante se contactará con el área comercial de Prisma Medios de Pago S.A. solicitando el “Instructivo de solicitud de certificado”, el “Formulario de Suscripción de Certificado” y el “Acuerdo con Suscriptores”. De estar disponibles, también podrá descargarlos desde el sitio Web de Banelco AC. La información de contacto se encuentra publicada en <http://ac.banelco.com.ar>.

El solicitante deberá presentarse ante la autoridad de registro con la documentación solicitada en el “Instructivo de solicitud de certificado” y el “Formulario de Suscripción de Certificado” debidamente completado y firmado.

El Oficial de Registro recibirá la documentación solicitada en el “Instructivo de solicitud de certificado” y controlará que se cumplan todos los puntos detallados en el “Checklist para suscripción de certificados”, en caso de faltar uno o más puntos devolverá la documentación al suscriptor informando tal condición para que el mismo lo complete para poder continuar con el proceso.

El Oficial de Registro verificará la identidad del solicitante, la documentación de respaldo de su representación y pago de aranceles. Luego, el Oficial de Registro firmará el “Formulario de Suscripción de Certificado” dando la conformidad correspondiente.

El Oficial de Registro cargará el pedido de certificado en el sistema de Administración de la CA.

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 20 de 59

El Oficial de Registro armará el legajo del suscriptor, el cual contendrá una copia de toda la documentación presentada en los puntos anteriores.

El certificador DEBE cumplir con lo establecido en:

- a) El artículo 21, inciso a) de la Ley de Firma Digital N°25.506 y el artículo 34, inciso e) de su reglamentario, Decreto N° 2628/02, relativos a la información a brindar a los solicitantes.
- b) El artículo 14, inciso b) de la Ley de Firma Digital N°25.506 relativo a los contenidos mínimos de los certificados.

3.2.1. Métodos para comprobar la posesión de clave privada

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


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

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

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

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

- a) El artículo 21, inciso i) de la Ley N° 25.506 relativo a la conservación de la documentación de respaldo de los certificados emitidos.
- b) El artículo 21, inciso f) de la Ley N° 25.506 relativo a la recolección de datos personales.

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 21 de 59

c) El artículo 34, inciso m) del Decreto N° 2628/02 relativo a la protección de datos personales.

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

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

La documentación requerida estará especificada en el documento Instructivo de Solicitud de Certificado publicado en <http://ac.banelco.com.ar>

A continuación se enumera la documentación necesaria a presentar por el solicitante:

Comprobante de CUIT expedido a su nombre y vigente.

Constancia de Inscripción en la AFIP.


Estatuto o Contrato Social.

La documentación respaldatoria del solicitante, a su vez estará dada por el tipo de Persona Jurídica a la cual representa.

TIPO DE SOCIEDAD	FIRMANTE	DOCUMENTACION A PRESENTAR
SOCIEDAD ANÓNIMA	PRESIDENTE	✓ COPIA DE ACTA DE DESIGNACIÓN
	APODERADO	✓ COPIA DE ACTA O COPIA DE PODER CON DESIGNACIÓN COMO TAL
SOCIEDAD DE RESPONSABILIDAD LIMITADA	SOCIO GERENTE	✓ CONTRATO CONSTITUTIVO
	APODERADO	✓ COPIA DE ACTA O COPIA DE PODER CON DESIGNACIÓN COMO TAL
ADMINISTRACION DE CONSORCIOS	PRESIDENTE	✓ COPIA DE ACTA DE ASAMBLEA
	ADMINISTRADOR	
MUNICIPIOS	INTENDENTE	✓ COPIA DE ACTA DE DESIGNACIÓN O NOMBRAMIENTO
	SECRETARIO DE HACIENDA	
ENTES GUBERNAMENTALES (EJ. RENTAS)	DIRECTOR DE FINANZAS	✓ COPIA DE ACTA DE DESIGNACIÓN O NOMBRAMIENTO
	SECRETARIO DE FINANZAS	
	SECRETARIO DE HACIENDA	
COLEGIOS	REPRESENTANTE LEGAL	✓ COPIA DE ACTA/CERTIFICADO/DECRETO O COPIA DE PODER CON DESIGNACIÓN COMO TAL
	APODERADO	
COOPERATIVAS	PRESIDENTE	✓ COPIA DE ACTA DE DESIGNACIÓN
	REPRESENTANTE LEGAL	✓ COPIA DE ACTA O COPIA DE PODER CON DESIGNACIÓN COMO TAL
	APODERADO	
CLUBES / MUTUALES / ASOCIACIONES CIVILES	PRESIDENTE	✓ COPIA DE ACTA DE DESIGNACIÓN
	APODERADO	✓ COPIA DE ACTA O COPIA DE PODER CON DESIGNACIÓN COMO TAL

3.2.3. Autenticación de la identidad de personas físicas

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

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 22 de 59

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

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

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

Se consideran obligatorias las exigencias reglamentarias impuestas por:

- a) El artículo 21, inciso i) de la Ley N° 25.506 relativo a la conservación de la documentación de respaldo de los certificados emitidos.
- b) El artículo 21, inciso f) de la Ley N° 25.506 relativo a la recolección de datos personales.
- c) El artículo 34, inciso i) del Decreto N° 2628/02 relativo a generar, exigir o tomar conocimiento de la clave privada del suscriptor.
- d) El artículo 34, inciso m) del Decreto N° 2628/02 relativo a la protección de datos personales.

Adicionalmente, el certificador deberá celebrar UN (1) acuerdo con el solicitante o suscriptor, conforme el Anexo IV de la Resolución 399 - E2016 05-10-2016, del que surge su conformidad respecto a la veracidad de la información incluida en el certificado.


La Autoridad de Registro deberá verificar que el dispositivo criptográfico utilizado por el solicitante, si fuera el caso, cumple con las especificaciones técnicas establecidas por la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA del MINISTERIO DE MODERNIZACIÓN.

3.2.4. Información no verificada del suscriptor

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

3.2.5. Validación de Autoridad

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

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 23 de 59

3.2.6. Criterios de 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 un nuevo par de claves

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

Cuando el Suscriptor requiera un nuevo par de claves, deberá revocar el certificado y solicitar la emisión de uno nuevo. Para esto, deberá realizar un nuevo proceso de solicitud.

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

- a) después de la revocación de UN (1) certificado.
- b) después de la expiración de UN (1) certificado.
- c) antes de la expiración de UN (1) certificado.

En los casos a) y b) se exigirá el cumplimiento de los procedimientos previstos en el punto 3.2.3. - Autenticación de la identidad de Personas Físicas.


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

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

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

En el caso de certificados digitales de personas físicas, 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 Persona Jurídica, Sitio seguro y Aplicaciones, incluyendo los de servidores, se deberá tramitar UN (1) nuevo certificado, según lo indicado en el apartado anterior.

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 24 de 59


3.4. Requerimiento de revocación

El suscriptor cuando se trate de certificados de persona física, o la persona física a cargo de la custodia de la clave privada para el resto de los casos, podrá revocar el certificado digital o pedir la revocación de su certificado a través de alguno de los siguientes medios.

a) Ingresando al sitio web del certificador en: <http://ac.banelco.com.ar/> suministrando el código de revocación provisto al momento de la emisión del certificado y su identificación en carácter de representante de la empresa.

La solicitud de revocación será recibida por un oficial del centro de contacto. El servicio de recepción de solicitudes de revocación se encuentra disponible las VEINTICUATRO (24) horas del día, salvo en ocasión de que se encuentren realizando tareas de mantenimiento.

b) El suscriptor puede optar por presentarse personalmente ante la Autoridad de Registro y completar el formulario de SolicitudDeRevocacionDeCertificado acreditando su identidad y representación para que el Oficial de Registro proceda a revocar el certificado.

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 25 de 59

4. CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS

4.1. Solicitud de Certificado

4.1.1. Solicitantes de certificado

El proceso de solicitud de emisión de certificado debe ser iniciado exclusivamente por personas físicas o en caso de certificados de personas jurídicas, a través de su representante legal, administrador o apoderado, quien luego deberá acreditar fehacientemente su identidad y vínculo según se indica en “3.2.2. - Autenticación de la identidad de personas jurídicas”.


4.1.2. Solicitud de certificado

Las solicitudes solo podrán ser iniciadas por el solicitante, en el caso de certificados de personas físicas, por el representante legal o apoderado con poder suficiente a dichos efectos, o por el Responsable del Servicio, aplicación o sitio web, autorizado a tal fin, en el caso de personas jurídicas.

Dicho solicitante debe presentar la documentación prevista en los apartados 3.2.2 – Autenticación de la identidad de Personas Jurídicas Públicas o Privadas y 3.2.3 - Autenticación de la identidad de Personas Físicas, así como la constancia de C.U.I.T. o C.U.I.L. Deberá también demostrar la pertenencia a la comunidad de suscriptores previstas en el apartado 1.3.3. Suscriptores de certificados.

Descripción del procedimiento:

- 1) El solicitante se contactará con el área comercial de Prisma Medios de Pago S.A. solicitando el “Instructivo de solicitud de certificado”, el “Formulario de Suscripción de Certificado” y el “Acuerdo con Suscriptores”. De estar disponibles, también podrá descargarlos desde el sitio Web de Banelco AC. La información de contacto se encuentra publicada en <http://ac.banelco.com.ar>.
- 2) El solicitante deberá presentarse ante la autoridad de registro con la documentación solicitada en el “Instructivo de solicitud de certificado” y el “Formulario de Suscripción de Certificado” debidamente firmado.
- 3) El Oficial de Registro recibirá la documentación solicitada en el “Instructivo de solicitud de certificado” y controlará que se cumplan todos los puntos detallados en el “Checklist para suscripción de certificados”, en caso de faltar uno o más puntos devolverá la documentación al suscriptor informando tal condición para que el mismo lo complete para poder continuar con el proceso.
- 4) El Oficial de Registro verificará la identidad del representante, la documentación de respaldo de su representación y pago de los aranceles. Luego, el Oficial de Registro firmará el “Formulario de Suscripción de Certificado” dando la conformidad correspondiente.

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 26 de 59

- 5) El Oficial de Registro cargará el pedido de certificado en el sistema de Administración de la CA.
- 6) El Oficial de Registro armará el legajo del suscriptor, el cual contendrá una copia de toda la documentación presentada en los puntos anteriores.

4.2. Procesamiento de la solicitud del certificado

Las solicitudes de certificados de personas físicas o jurídicas serán procesadas dentro de las 72hs hábiles de acuerdo al proceso de emisión de certificados.

Las solicitudes de certificados de aplicaciones aprobados serán procesadas dentro de las 96hs hábiles.

4.3. Emisión del certificado

4.3.1. Proceso de Emisión de certificado

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

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

4.3.2. Notificación de Emisión

La notificación se realiza al momento de la generación 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 el certificado.


En caso de que 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”.

4.5. Uso del par de claves y del certificado

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

Según lo establecido en la Ley N° 25.506, en su artículo 25, el suscriptor debe:

- a) Mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, e impedir su divulgación;

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 27 de 59

- b) Utilizar UN (1) dispositivo de creación de firma digital técnicamente confiable;
- c) Solicitar la revocación de su certificado al certificador ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma;
- d) Informar sin demora al certificador el cambio de alguno de los datos contenidos en el certificado digital que hubiera sido objeto de verificación.

De acuerdo a lo establecido en la presente Resolución:

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

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

Los Terceros Usuarios deben:

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


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

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

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

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

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

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 28 de 59

Para los certificados Persona Jurídica, Sitio seguro y 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 N° 25.506. En cualquier caso procede la revocación de dicho certificado y de ser requerido, la solicitud de uno nuevo.

4.9. Suspensión y Revocación de certificados


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

El estado de suspensión no es admitido en el marco de la Ley N° 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 se determina que el certificado fue emitido en base a una información falsa que al momento de la emisión hubiera sido objeto de verificación.
- c. Si se determina 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
- f. Por fallecimiento del titular o representante.
- g. Por declaración judicial de ausencia con presunción de fallecimiento del titular o representante.
- h. Si se determina que la información contenida en el certificado ha dejado de ser válida.
- i. Cuando la clave privada asociada al certificado, o el medio en que se encuentre almacenada, se encuentren comprometidos o corran peligro de estarlo.

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 29 de 59

j. Ante incumplimiento por parte del suscriptor de las obligaciones establecidas en el Acuerdo con Suscriptores.

k. Si se determina que el certificado no fue emitido de acuerdo a los lineamientos de la Política Única de Certificación, del Manual de Procedimientos, de la Ley N°25.506, del Decreto Reglamentario N°2628/02 y demás normativas sobre firma digital.

l. Por revocación de su propio certificado digital.

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

4.9.2. Autorizados a solicitar la revocación


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

- a. El suscriptor del certificado.
- b. El responsable autorizado que efectuara el requerimiento, en el caso de certificados de persona jurídica o de aplicación.
- c. El responsable autorizado por la Persona Jurídica que brinda el servicio o es titular del certificado o la aplicación, en el caso de los certificados de aplicación.
- d. El responsable autorizado por la Persona Jurídica responsable del sitio web, en el caso de certificados de sitio seguro.
- e. Aquellas personas habilitadas por el suscriptor del certificado a tal fin, previa acreditación fehaciente de tal autorización,
- f. El certificador o la Autoridad de registro operativamente vinculada.
- g. El ente licenciante.
- h. La autoridad judicial competente.
- i. La autoridad de Aplicación.

4.9.3. Procedimientos para la solicitud de revocación

El certificador garantiza que:

- a. Se identifica debidamente al solicitante de la revocación según se establece en el apartado 3.4.
- b. Las solicitudes de revocación, así como toda acción efectuada por el certificador o la autoridad de registro en el proceso, están documentadas y conservadas en sus archivos.

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 30 de 59

- 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.

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

- 1- Por correo electrónico firmado digitalmente a la dirección: revocación@prismamp.com.ar
- 2- Personalmente presentándose ante la Autoridad de Registro correspondiente con documento de identidad que permita acreditar su identidad.

4.9.4. Plazo para la solicitud de revocación

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

El servicio de recepción de solicitudes de revocación se encuentra disponible en forma permanente SIETE POR VEINTICUATRO (7x24) horas cumpliendo lo establecido en el artículo 34, inciso f) del Decreto N° 2628/02.

4.9.5. Plazo para el procesamiento de la solicitud de revocación


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

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

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

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

El certificador cumple con lo establecido en el artículo 34, inciso g) del Decreto N° 2628/02 relativo al acceso al repositorio de certificados revocados y las obligaciones establecidas en la presente Decisión Administrativa y sus correspondientes anexos.

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 31 de 59

4.9.7. Frecuencia de emisión de listas de certificados revocados

La lista de certificados revocados será emitida como mínimo cada VEINTICUATRO (24) horas o inmediatamente después de la revocación de un certificado.

4.9.8. Vigencia de la lista de certificados revocados

La vigencia de la lista de certificados revocados será de VEINTICUATRO (24) horas.

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

PRISMA MEDIOS DE PAGO S.A. a través de su sitio web <http://ac.banelco.com.ar> pondrá a disposición de los interesados la lista de certificados revocados para realizar la validación del estado de un certificado.

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

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 de la CRL, la que también estará disponible. El servicio OCSP se provee por medio del sitio web <http://ac.banelco.com.ar/ocsp>.

4.9.11. Otras formas disponibles para la divulgación de la revocación

PRISMA MEDIOS DE PAGO S.A. no dispondrá de otras formas de verificación por parte de terceros.

4.9.12. Requisitos específicos para casos de compromiso de claves

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

4.9.13. Causas de suspensión


El estado de suspensión de certificados no es admitido en el marco de la Ley N° 25.506.

4.9.14. Autorizados a solicitar la suspensión

El estado de suspensión de certificados no es admitido en el marco de la Ley N° 25.506

4.9.15. Procedimientos para la solicitud de suspensión

El estado de suspensión de certificados no es admitido en el marco de la Ley N° 25.506

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 32 de 59

4.9.16. Límites del período de suspensión de un certificado

El estado de suspensión de certificados no es admitido en el marco de la Ley N° 25.506

4.10. Estado del certificado

4.10.1. Características técnicas

La verificación del estado de los certificados podrá ser realizada mediante la consulta de la CRL disponible en el sitio de BANELCO AC <http://ac.banelco.com.ar/CRL/> y mediante la consulta en línea de su estado (OCSP), encontrándose ambos servicios disponibles.

4.10.2. Disponibilidad del servicio

Ambos servicios se encontrarán disponibles los siete días de la semana, las veinticuatro horas del día; en caso de contingencia del sitio primario, la funcionalidad se limitará al sitio público y funcionalidades de revocación y publicación de CRL durante las primeras veinticuatro horas, incluyendo el servicio de consulta en línea (OCSP).

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 operaciones del certificador.

4.12. Recuperación y custodia de claves privadas

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

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 33 de 59

5. CONTROLES DE SEGURIDAD FÍSICA, OPERATIVOS Y DE GESTIÓN

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

5.1. Controles de seguridad física

Se cuenta con controles de seguridad relativos a:

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

5.2. Controles de gestión


Se cuenta con controles de seguridad relativos a:

- a) Definición de roles afectados al proceso de certificación.
- b) Número de personas requeridas por función.
- c) Identificación y autenticación para cada rol.
- d) Separación de funciones.

5.3. Controles de seguridad del personal

Se cuenta con controles de seguridad relativos a:

- a) Calificaciones, experiencia e idoneidad del personal, tanto de aquellos que cumplen funciones críticas como de aquellos que cumplen funciones administrativas, de seguridad, limpieza, etcétera.
- b) Antecedentes laborales.
- c) Entrenamiento y capacitación inicial.
- d) Frecuencia de procesos de actualización técnica.
- e) Frecuencia de rotación de cargos.
- f) Sanciones a aplicar por acciones no autorizadas.

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 34 de 59

g) Requisitos para contratación de personal.

h) Documentación provista al personal, incluidas tarjetas y otros elementos de identificación personal.

5.4. Procedimientos de Auditoría de Seguridad

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

a) Tipo de eventos registrados. Debe respetarse lo establecido en el Anexo II Sección 3.

Se registrarán los eventos relacionados a la Administración del ciclo de vida de las claves criptográficas, del ciclo de vida de los certificados y del ciclo de vida de los dispositivos criptográficos. Asimismo, se registrarán los eventos relacionados a la solicitud de certificados y a los eventos de seguridad.

b) Frecuencia de procesamiento de registros.

Los registros se procesaran ante la ocurrencia del evento.

c) Periodo de guarda de los registros. Debe respetarse lo establecido en el inciso i) del artículo 21 de la Ley N° 25.506 respecto a los certificados emitidos.

Los registros se almacenaran por un periodo de 10 años.

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 las políticas de seguridad de la información de Prisma Medios de Pago S.A.

e) Procedimientos de resguardo de los registros.

Los registros se almacenaran dentro y fuera de las instalaciones de PRISMA MEDIOS DE PAGO como medida preventiva para asegurar la recuperación total de la información en caso de ser necesario.


Dichas copias de respaldo se conservarán y almacenarán en lugares ignífugos, con acceso restringido y con adecuadas condiciones ambientales según se establece en las políticas y controles de infraestructura física.

Las copias poseerán rótulos identificatorios y serán solo accesibles por personal autorizado a tal fin.

Adicionalmente, existirá un registro de los movimientos y traslado de las cintas y otros medios físicos de almacenamiento desde y hacia los depósitos ubicados fuera del edificio, así como de la identificación de las personas que los ingresen, días, horas y motivos.

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

No aplicable.

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 35 de 59

g) Notificaciones del sistema de recolección y análisis de registros.

No aplicable.

h) Evaluación de vulnerabilidades.

Con el objetivo de establecer mecanismos de evaluación y tratamiento de los riesgos de seguridad de la información que permitan cumplir con las normativas legales vigentes y de organismos de control, PRISMA MEDIOS DE PAGO ha establecido una Política específica de Gestión de Riesgos de Seguridad de la Información (L-SGSI-01 - POLITICA DE GESTION DE RIESGOS DE SEGURIDAD INFORMATICA), la cual determina y establece todos los mecanismos adecuados para la evaluación y tratamiento de riesgos sobre los activos de información de PRISMA MEDIOS DE PAGO.

5.5. Conservación de registros de eventos

Los procedimientos cumplen con lo establecido por el artículo 21, inciso i) de la Ley N° 25.506 relativo al mantenimiento de la documentación de respaldo de los certificados digitales emitidos.

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

5.6. Cambio de claves criptográficas

El certificado de la Autoridad Certificante con su respectiva clave pública embebida estará publicado en el sitio <http://ac.banelco.com.ar>.


Tres años previos al vencimiento de las mismas, PRISMA MEDIOS DE PAGO S.A. solicitará un nuevo certificado a la Autoridad Certificante Raíz de la República Argentina operada por la Autoridad de Aplicación.

5.7. Plan de respuesta a incidentes y recuperación ante desastres

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

Se han desarrollado procedimientos referidos a:

- a) Identificación, registro, reporte y gestión de incidentes.
- b) Recuperación ante falla inesperada o sospecha de falla de componentes de hardware, software y datos.
- c) Recuperación ante compromiso o sospecha de compromiso de la clave privada del certificador.
- d) Continuidad de las operaciones en un entorno seguro luego de desastres.

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 36 de 59

Los procedimientos cumplen con lo establecido por el artículo 33 del Decreto N° 2628/02 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 certificadoras o de registro. Estos requerimientos son desarrollados en su Plan de Cese de Actividades.

Se han implementado procedimientos referidos a:

- a) Notificación a la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA del MINISTERIO DE MODERNIZACIÓN, suscriptores, terceros usuarios, otros certificadoros y otros usuarios vinculados.
- b) Revocación del certificado del certificador y de los certificados emitidos.
- c) Transferencia de la custodia de archivos y documentación e identificación de su custodio.

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

Se contempla lo establecido por el artículo 44 de la Ley N° 25.506 de Firma Digital en lo relativo a las causales de caducidad de la licencia.

6. CONTROLES DE SEGURIDAD TECNICA

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


6.1. Generación e instalación del par de claves criptográficas

6.1.1. Generación del par de claves criptográficas

La clave privada de la Autoridad Certificante BANELCO AC es generada en ambientes seguros, por personal autorizado, sobre dispositivos criptográficos homologados FIPS 140-2 Nivel 3.

La Autoridad Certificante genera sus claves mediante el algoritmo RSA con un tamaño de 4096 bits.

La clave privada de las Autoridades de Registro es generada utilizando un dispositivo criptográfico FIPS 140-2 Nivel 2 o superior.

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 37 de 59

Las Autoridades de Registro y suscriptores generan sus claves mediante el algoritmo RSA con un tamaño mínimo de 2048 bits, excepto el caso de las Autoridades de Sello de Tiempo para las que son de 4096 bits.

6.1.2. Entrega de la clave privada al suscriptor

En todos los casos se cumple con la obligación de abstenerse de generar, exigir o por cualquier otro medio tomar conocimiento o acceder a los datos de creación de firmas de los suscriptores (incluyendo los roles vinculados a las actividades de registro), establecido por la Ley N°25.506, artículo 21, inciso b) y el Decreto N° 2628/02, artículo 34, inciso i).

6.1.3. Entrega de la clave pública al emisor del certificado

El Solicitante entrega la clave pública a la Autoridad Certificante durante el proceso de Solicitud.

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

6.1.4. Disponibilidad de la clave pública del certificador

Los certificados de la “Autoridad Certificante” y el certificado de la “Autoridad Certificante Raíz de la República Argentina” se encuentran disponibles en <http://ac.banelco.com.ar/>

La verificación de la validez de los certificados de los suscriptores de la presente política, se realiza automáticamente verificando la cadena de confianza del certificado del suscriptor donde se verifican el certificado de la Autoridad Certificante, la Autoridad Certificante Raíz y las listas de Certificados Revocados de ambas.

6.1.5. Tamaño de claves

La Autoridad Certificante utiliza clave RSA de 4096 bits.


Las Autoridades de Registro y Suscriptores utilizan clave RSA de 2048 bits, excepto el caso de las Autoridades de Sello de Tiempo para las que son de 4096 bits.

6.1.6. Generación de parámetros de claves asimétricas

Las claves se generan a través de un algoritmo RSA respetando su especificación.

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

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

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 38 de 59

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

6.2.1. Estándares para dispositivos criptográficos

La Autoridad Certificante utiliza dispositivos criptográficos por hardware según estándar FIPS 140-2 Nivel 3 y la Autoridad de Registro utilizará dispositivos criptográficos FIPS 140-2 Nivel 2 o superior.

6.2.2. Control “M de N” de clave privada

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

6.2.3. Recuperación de clave privada

Únicamente la Autoridad Certificante tendrá mecanismos de recuperación de su clave privada a partir de su copia de respaldo o backup. La recuperación se dará de acuerdo al procedimiento privado definido a tal fin.

6.2.4. Copia de seguridad de clave privada

El Certificador genera una copia de seguridad de la clave privada inmediatamente después de su generación a través de un procedimiento que garantiza su integridad y confidencialidad. Las mismas son almacenadas en dispositivos criptográficos seguros homologados FIPS 140-2 nivel 3.

6.2.5. Archivo de clave privada

La copia de resguardo de la clave privada de la Autoridad Certificante y los elementos necesarios para la activación son conservados bajo los niveles de seguridad exigidos por la DA 927/2014.

6.2.6. Transferencia de claves privadas en dispositivos criptográficos


Las copias de resguardo de la clave privada de la Autoridad Certificante BANELCO AC están soportadas en dispositivos criptográficos que cumplen con el estándar FIPS 140-2 nivel 3.

Las claves privadas de las Autoridades de Registro son generadas y almacenadas en dispositivos que cumplen con el estándar FIPS 140-2 nivel 2 o superior, los cuales no permiten su exportación.

6.2.7. Almacenamiento de claves privadas en dispositivos criptográficos

Las claves privadas de la Autoridad Certificante serán almacenadas en dispositivos criptográficos FIPS 140-2 nivel 3 al momento de la activación del dispositivo.

Las claves criptográficas de las Autoridades de Registro serán almacenadas en dispositivos criptográficos FIPS 140-2 nivel 2 o superior.

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 39 de 59

6.2.8. Método de activación de claves privadas

Para la activación de la clave privada de la Autoridad Certificante se aplica el control descrito en la sección “6.2.2. Control “M de N” de clave privada”. Los responsables necesarios para la activación deberán autenticarse en el sistema de acuerdo al rol y/o combinación de roles asignados.

Las Autoridades de Registro y Suscriptores poseen una contraseña autogenerada para el acceso al dispositivo criptográfico y clave privada, si fuera aplicable.

6.2.9. Método de desactivación de claves privadas

La desactivación de las claves privadas se realiza mediante el procedimiento de desactivación de partición; esto puede ocurrir cuando se exista la necesidad de utilizar temporalmente un equipamiento secundario o se realicen tareas de mantenimiento.

6.2.10. Método de destrucción de claves privadas

Las claves privadas se destruyen mediante procedimientos que imposibilitan su posterior recuperación o uso, bajo las mismas medidas de seguridad que se emplearon para su creación.

En el caso de claves privadas de las Autoridades de Registro y Suscriptores, la responsabilidad de la administración de las mismas corresponderá por cuenta de cada Autoridad de Registro o Suscriptor, incluida la tarea de destrucción de las claves.

6.2.11. Requisitos de los dispositivos criptográficos

Los dispositivos criptográficos utilizados por el Certificador Licenciado están certificados por el NIST (National Institute of Standards and Technology) cumplimentando el 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 de la Autoridad Certificante y los emitidos por ella son almacenados, publicados y respaldados bajo un esquema redundante y respaldados de forma periódica con permisos de solo lectura, sumado a la firma de cada uno de ellos, garantiza su integridad.

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 periodo de validez de los certificados. Las correspondientes claves públicas podrán ser utilizadas durante el periodo establecido por las normas legales vigentes, a fin de

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 40 de 59

posibilitar la verificación de las firmas generadas durante su periodo de validez, según se establece en el apartado anterior.

6.4. Datos de activación

Se entiende por datos de activación, a diferencia de las claves, a los valores requeridos para la operatoria de los dispositivos criptográficos y que necesitan estar protegidos. Se establecen medidas suficientes de seguridad para proteger los datos de activación requeridos para la operación de los dispositivos criptográficos de los usuarios de certificados.

6.4.1. Generación e instalación de datos de activación

La inicialización de los dispositivos criptográficos utilizados por las Autoridades de Registro y los Suscriptores es realizada por ellos mismos mediante la definición de una contraseña previa a la generación de la clave privada.

La generación e instalación de los datos de activación de la clave privada de la Autoridad Certificante se realiza durante la ceremonia inicial con todos los N participantes del control M de N descrito en la sección “6.2.2. Control “M de N” de clave privada”.

6.4.2. Protección de los datos de activación

Las Autoridades de Registro y los Suscriptores son los únicos responsables de la custodia y no divulgación de la contraseña de la clave privada.

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 Autoridad Certificante, elegir contraseñas robustas con inclusión de números, letras mayúsculas, letras minúsculas y caracteres especiales para la protección de sus claves privadas y acceso a los dispositivos criptográficos que utilicen.


6.5. Controles de seguridad informática

6.5.1. Requisitos técnicos específicos.

PRISMA MEDIOS DE PAGO S.A. en su carácter de Certificador Licenciado, cumple con los requisitos técnicos definidos por la normativa vigente.

Entre los controles técnicos se destacan :

- a. Control de accesos a los servicios y roles afectados al proceso de certificación

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 41 de 59

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

6.5.2. Requisitos de seguridad computacional

Los equipos que conforman la Autoridad Certificante se encuentran ubicados en un ámbito de máxima seguridad según los requerimientos establecidos para este tipo de ambientes.

Las características de seguridad del módulo criptográfico HSM Hardware Security Module, son las siguientes:

Certificación FIPS 140-2 Level 3, Common Criteria EAL4+

6.6. Controles Técnicos del ciclo de vida de los sistemas

6.6.1. Controles de desarrollo de sistemas

No aplicable.

6.6.2. Controles de gestión de seguridad

No aplicable.

6.6.3. Calificaciones de seguridad del ciclo de vida del software

No aplicable.

6.7. Controles de seguridad de red

Los servicios provistos por el Certificador Licenciado se encuentran protegidos por la infraestructura tecnológica apropiada que garantiza la seguridad.

6.8. Certificación de fecha y hora

El servicio de emisión de sellos de tiempo de BANELCO AC está basado en la especificación de los estándares RFC 3161 y está sincronizado con una fuente de hora confiable.

PRISMA MEDIOS DE PAGO	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 42 de 59

7. PERFILES DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS

7.1. Perfil del certificado

Todos los certificados serán emitidos conforme a lo establecido en la especificación ITU X.509 versión 3 o la que en su defecto, determine el Ente Licenciantes, y deben cumplir con las indicaciones establecidas en la sección “2 – Perfil de certificados digitales” del Anexo IV – Perfiles de los Certificados y de las Listas de Certificados Revocados.

Certificado para Persona Física


Cetificado x.509 v3	Nombre del campo	Contenido
Atributos	y OID	
Versión	Versión	V3 2 (correspondiente a versión 3)
Número de serie	serialNumber - 2.5.4.5	<Número de serie del certificado> (entero positivo asignado unívocamente por la AC Banelco a cada certificado de hasta 20 octetos)
Algoritmo de Firma	signatureAlgorithn	sha1RSA (1.2.840.113549.1.1.5)
Nombre distintivo del emisor (Issuer)	commonName - 2.5.4.3	CN=Banelco AC
	serial Number - 2.5.4.5	SERIALNUMBER=CUIT 30598910045
	organizationName - 2.5.4.10	O=PRISMA MEDIOS DE PAGO S.A.
	stateOrProvinceName - 2.5.4.8	S=Ciudad Autónoma de Buenos Aires
	countryName - 2.5.4.6	C=AR
Validez (desde, hasta)	notBefore	<fecha y hora de emisión UTC> yyyy/mm/dd hh:mm:ss huso-horario
	notAfter	<fecha y hora de emisión UTC+2 años> yyyy/mm/dd hh:mm:ss huso-horario
Nombre distintivo del suscriptor	commonName - 2.5.4.3	CN= APELLIDO NOMBRE
	serialNumber - 2.5.4.5	SERIALNUMBER=<CUIT/CUIL> <NUMERO>
	countryName - 2.5.4.6	C=AR
Clave pública del suscriptor (Subject Public Key Info)	publicKey Algorithm	RSA (1.2.840.11.35.49.1.1.1)
	Public key length	2048 bits
	Clave Pública del suscriptor	<Clave pública del suscriptor>
Restricciones básicas	basicConstraint - 2.5.29.19	Tipo de asunto = Entidad Final pathLengthConstraint=NULL
Usos de Clave	keyUsage - 2.5.29.15	digitalSignature=1 contentCommitment=1 keyEncipherment=1 dataEncipherment=1 keyAgreement=1 keyCertSign=0 cRLSign=0 encipherOnly=1 decipherOnly=1
Identificador de clave del suscriptor	subjectKeyIdentifier - 2.5.29.14	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados	CRLDistributionPoints - 2.5.29.31	[1] Punto de distribución: Nombre completo: Dirección: URL=http://ac.banelco.com.ar/firma-digital/crl/Banelcoac.crl
Política de Certificación	certificatePolicies - 2.5.29.32	[1] Política de certificación: OID de la Política Única = [1.1] Información de la Política de Certificación= CPS Ubicación: http://ac.banelco.com.ar/firma-digital/docs/Política%20de%20Certificación%20Banelco.pdf User notice=certificado emitido por un Certificador Licenciado en el marco de Ley 25.506.
Identificador de la Clave de la Autoridad Certificante	authorityKeyIdentifier - 2.5.29.35	keyidentifier=<Identificador de la clave de la AC> (contiene un hash de 20 bytes del atributo clave pública de la AC Banelco)
Uso Extendido de clave	extendedKeyUsage - 2.6.29.37	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4)
Nombres Alternativos del Suscriptor	subjectAltName - 2.5.29.17	Dirección de correo electrónico (campo optativo)
Información de Acceso de la AC	authorityInfoAccess - 1.3.6.1.5.5.7.1.1	URL=http://ac.banelco.com.ar/ocsp
Declaración del certificado calificado	QCStatment - 1.3.6.1.5.5.7.1.3	OID=2.16.32.1.10.2.2 (claves generadas por disp. FIPS 140-2 Nivel 2) OID=2.16.32.1.10.1 (claves generadas por software)

Certificado para Persona Jurídica

Cetificado x.509 v3	Nombre del campo y OID	Contenido
Versión	Versión	V3 2 (correspondiente a versión 3)
Número de serie	serialNumber - 2.5.4.5	<Número de serie del certificado> (entero positivo asignado unívocamente por la AC Banelco a cada certificado de hasta 20 octetos)
Algoritmo de Firma	signatureAlgorithm	sha1RSA (1.2.840.113549.1.1.5)
Nombre distintivo del emisor	commonName - 2.5.4.3	CN=Banelco AC
(Issuer)	serial Number - 2.5.4.5	SERIALNUMBER=CUIT 30598910045
	organizationName - 2.5.4.10	O=PRISMA MEDIOS DE PAGO S.A.
	stateOrProvinceName - 2.5.4.8	S=Ciudad Autónoma de Buenos Aires
	countryName - 2.5.4.6	C=AR
Validez (desde, hasta)	notBefore	<fecha y hora de emisión UTC> yyyy/mm/dd hh:mm:ss huso-horario
	notAfter	<fecha y hora de emisión UTC+3 años> yyyy/mm/dd hh:mm:ss huso-horario
Nombre distintivo del suscriptor	commonName - 2.5.4.3	CN= Razón Social o Denominación
	organizationName - 2.5.4.10	O=Debe coincidir con el nombre de la Persona Jurídica
	organizationUnitName - 2.5.4.11	OU=Unidad Organizacional del suscriptor area/departamento
(Subject DN)	serialNumber - 2.5.4.5	SERIALNUMBER=<CUIT/CUIL> <NUMERO>
	countryName - 2.5.4.6	C=AR
	publicKey Algorithm	RSA (1.2.840.11.35.49.1.1.1)
(Subject Public Key Info)	Public key length	2048 bits
	Clave Pública del suscriptor	<Clave pública del suscriptor>
Restricciones básicas	basicConstraint - 2.5.29.19	Tipo de asunto = Entidad Final pathLengthConstraint=Null
Usos de Clave	keyUsage - 2.5.29.15	digitalSignature=1 contentCommitment=1 keyEncipherment=1 dataEncipherment=1 keyAgreement=1 keyCertSign=0 cRLSign=0 encipherOnly=1 decipherOnly=1
Identificador de clave del suscriptor	subjectKeyIdentifier - 2.5.29.14	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados	CRLDistributionPoints - 2.5.29.31	[1] Punto de distribución: Nombre completo: Dirección: URL=http://ac.banelco.com.ar/firma-digital/crl/Banelcoac.crl
Política de Certificación	certificatePolicies - 2.5.29.32	[1] Política de certificación: OID de la Política Única = [1.1] Información de la Política de Certificación= CPS Ubicación: http://ac.banelco.com.ar/firma-digital/docs/Política%20de%20Certificación%20Banelco.pdf User notice=certificado emitido por un Certificador Licenciado en el marco de Ley 25.506.
Identificador de la Clave de la Autoridad Certificante	authorityKeyIdentifier - 2.5.29.35	keyIdentifier=<Identificador de la clave de la AC> (contiene un hash de 20 bytes del atributo clave pública de la AC Banelco)
Uso Extendido de clave	extendedKeyUsage - 2.6.29.37	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4)
Nombres Alternativos del Suscriptor	subjectAltName - 2.5.29.17	CN=APELLIDO Nombre de la persona física a cargo de la custodia de la clave privada SN= <CUIT/CUIL> <Número> T=<Relación que vincula a la persona física con la persona jurídica>
Información de Acceso de la AC	authorityInfoAccess - 1.3.6.1.5.5.7.1.1	URL=http://ac.banelco.com.ar/ocsp
Declaración del certificado calificado	QCStatement - 1.3.6.1.5.5.7.1.3	OID=2.16.32.1.10.2.3 (claves generadas por disp. FIPS 140-2 Nivel 3) OID=2.16.32.1.10.2.2 (claves generadas por disp. FIPS 140-2 Nivel 2) OID=2.16.32.1.10.1 (claves generadas por software)

Certificado para Aplicaciones

Certificado x.509 v3		
Atributos	Nombre del campo y OID	Contenido
Versión	Versión	V3 2 (correspondiente a versión 3)
Número de serie	serialNumber - 2.5.4.5	<Número de serie del certificado> (entero positivo asignado unívocamente por la AC Banelco a cada certificado de hasta 20 octetos)
Algoritmo de Firma	signatureAlgorithm	sha1RSA (1.2.840.113549.1.1.5)
Nombre distintivo del emisor (Issuer)	commonName - 2.5.4.3	CN=Banelco AC
	serial Number - 2.5.4.5	SERIALNUMBER=CUIT 30598910045
	organizationName - 2.5.4.10	O=PRISMA MEDIOS DE PAGO S.A.
	stateOrProvinceName - 2.5.4.8	S=Ciudad Autónoma de Buenos Aires
	countryName - 2.5.4.6	C=AR
Validez (desde, hasta)	notBefore	<fecha y hora de emisión UTC> yyyy/mm/dd hh:mm:ss huso-horario
	notAfter	<fecha y hora de emisión UTC+3 años> yyyy/mm/dd hh:mm:ss huso-horario
Nombre distintivo del suscriptor (Subject DN)	commonName - 2.5.4.3	CN= Denominación de la Aplicación
	organizationName 2.5.4.10	O=<Razón Social o Denominación>
	organizationUnitName - 2.5.4.11	OU=Unidad operativa relacionada con el servicio o aplicación
	serialNumber - 2.5.4.5	SERIALNUMBER=<CUIT/CUIL> <NUMERO>
	countryName - 2.5.4.6	C=AR
Clave pública del suscriptor (Subject Public Key Info)	publicKey Algorithm	RSA (1.2.840.11.35.49.1.1.1)
	Public key length	2048 bits
	Clave Pública del suscriptor	<Clave pública del suscriptor>
Restricciones básicas	basicConstraint - 2.5.29.19	Tipo de asunto = Entidad Final pathLengthConstraint=NULL
Usos de Clave	keyUsage - 2.5.29.15	digitalSignature=1 contentCommitment=1 keyEncipherment=1 dataEncipherment=1 keyAgreement=1 keyCertSign=0 cRLSign=0 encipherOnly=1 decipherOnly=1
Identificador de clave del suscriptor	subjectKeyIdentifier - 2.5.29.14	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados	CRLDistributionPoints - 2.5.29.31	[1] Punto de distribución: Nombre completo: Dirección: URL=http://ac.banelco.com.ar/firma-digital/crl/Banelcoac.crl
Política de Certificación	certificatePolicies - 2.5.29.32	[1] Política de certificación: OID de la Política Única = [1.1] Información de la Política de Certificación= CPS Ubicación: http://ac.banelco.com.ar/firma-digital/docs/Política%20de%20Certificación%20Banelco.pdf User notice=certificado emitido por un Certificador Licenciado en el marco de Ley 25.506.
Identificador de la Clave de la Autoridad Certificante	authorityKeyIdentifier - 2.5.29.35	keyIdentifier=<Identificador de la clave de la AC> (contiene un hash de 20 bytes del atributo clave pública de la AC Banelco)
Uso Extendido de clave	extendedKeyUsage - 2.6.29.37	Autenticación del cliente (1.3.6.1.5.5.7.3.2)
Nombres Alternativos del Suscriptor	subjectAltName - 2.5.29.17	Dirección de correo electrónico (campo optativo)
Información de Acceso de la AC	authorityInfoAccess - 1.3.6.1.5.5.7.1.1	URL=http://ac.banelco.com.ar/ocsp
Declaración del certificado calificado	QCStatement - 1.3.6.1.5.5.7.1.3	OID=2.16.32.1.10.2.3 (claves generadas por disp. FIPS 140-2 Nivel 3) OID=2.16.32.1.10.2.2 (claves generadas por disp. FIPS 140-2 Nivel 2) OID=2.16.32.1.10.1 (claves generadas por software)

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 46 de 59


Certificado de Sitio Seguro

Certificado x.509 v3 Atributos Extensiones	Nombre del Campo y OID	Contenido
Version	Version	V3 2 (correspondiente a version 3)
Numero de serie	serialNumber 2.5.4.5	<Numero de serie del certificado>
Algoritmo de firma	signatureAlgoritm	sha1RSA (1.2.840.113549.1.1.5)
Nombre distintivo del emisor (issuer)	commonName - 2.5.4.3	CN= Banelco AC
	serialNumber - 2.5.4.5	SERIAL NUMBER=CUIT 30598910045
	organizationName - 2.5.4.10	O=PRISMA MEDIOS DE PAGO S.A.
	stateOrProvinceName - 2.5.4.8	S= Ciudad Autonoma de Buenos Aires
	countryName - 2.5.4.6	C=AR
Validez (desde, hasta)	notBefore	<fecha y hora de emisión UTC> yyyy/mm/dd hh:mm:ss huso-horario
	notAfter	<fecha y hora de emisión UTC+ 1 año> yyyy/mm/dd hh:mm:ss huso-horario
Nombre distintivo del suscriptor (Subject DN)	commonName - 2.5.4.3	CN=Denominacion del sitio web de Internet
	organizationName - 2.5.4.10	O=nombre de la persona jurídica publica responsable del sitio web de internet
	organizationUnitName - 2.5.4.11	OU=Unidad Operativa de la que depende el sitio web aplicación
	serialNumber - 2.5.4.5	SN= <CUIT/CUIL> <Número de la Persona Juridica Publica responsable de la aplicación>
	countryName - 2.5.4.6	C=AR
Clave publica del suscriptor (Subject public Key Info)	publicKey Algorithm	RSA (1.2.840.1135.49.1.1.1)
	Publickey lenght	2048 bits
	Clave publica del suscriptor	<Clave publica del suscriptor>
Restricciones basicas	basicConstraint - 2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null
Usos de clave	keyUsage 2.5.29.15	digitalSignature = 1 contentCommitment = 1 keyEncipherment = 1 dataEncipherment = 0 keyAgreement = 1 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0
Identificador de clave del suscriptor	subjectKey Identifier 2.5.29.14	Contiene un hash de 20 bytes del atributo clave publica del suscriptor
Puntos de distribucion de la Lista de Certificados Revocados	CRLDistributionPoints 2.5.29.31	[1] Punto de distribución: Nombre completo: Dirección: URL= http://ac.banelco.com.ar/firma-digital/crl/Banelcoac.crl
Politica de Certificacion	certificatePolicies 2.5.29.32	Politica de certificacion: OID de la Politica Unica= Informacion de la Politica de Certificacion: Id. De la Politica de Certificacion=CPS Ubicación: http://ac.banelco.com.ar/firma-digital/docs/Politica%20de%20Certificacion%20Banelco.pdf User notice = certificado emitido por un Certificador Licenciado en el marco de la Ley 25.506.
Identificador de la Clave de la Autoridad Certificante	authorityKeyIdentifier 2.5.29.35	keyIdentifier = <Identificador de la clave de la AC>
Uso Extendido de Clave	extendedKeyUsage	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Autenticación del servidor (1.3.6.1.5.5.7.3.1)
Nombres Alternativos del Suscriptor	subjectAltName - 2.5.29.17	Dirección de correo electrónico (campo optativo)
Informacion de acceso de la AC	authority InformationAccess 1.3.6.1.5.5.7.1.1	URL= http://ac.banelco.com.ar/ocsp
Declaracion del certificado calificado	QCStatement 1.3.6.1.5.5.7.1.3	OID= 2.16.32.110.1 (claves generadas por software)

DOCUMENTOS IMPRESOS SON COPIAS NO CONTROLADAS

INFORMACIÓN PRIVADA

Prohibida su copia y distribución sin la autorización formal de PRISMA MEDIOS DE PAGO S.A.

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 47 de 59


Certificado para Autoridad de Competencia

Certificado x.509 v3 Atributos Extensiones	Nombre del Campo y OID	Contenido
Version	Version	V3 2 (correspondiente a version 3)
Numero de serie	serialNumber 2.5.4.5	<Numero de serie del certificado>
Algoritmo de firma	signatureAlgorithm	sha1RSA (1.2.840.113549.1.1.5)
Nombre distintivo del emisor (issuer)	commonName - 2.5.4.3	CN=Banelco AC
	serialNumber - 2.5.4.5	SERIAL NUMBER=CUIT 30598910045
	organizationName - 2.5.4.10	O=PRISMA MEDIOS DE PAGO S.A.
	stateOrProvinceName - 2.5.4.8	S= Ciudad Autonoma de Buenos Aires
	countryName - 2.5.4.6	C=AR
Validez (desde, hasta)	notBefore	<fecha y hora de emisión UTC> yyyy/mm/dd hh:mm:ss huso-horario
	notAfter	<fecha y hora de expiracion a establecer por AC ONTI> yyyy/mm/dd hh:mm:ss huso-horario
Nombre distintivo del suscriptor (Subject DN)	commonName - 2.5.4.3	CN=Denominacion del servicio de emision de sello de competencia
	organizationName - 2.5.4.10	O=Nombre de la persona jurídica publica o privada responsable del servicio
	organizationUnitName - 2.5.4.11	OU=Unidad Operativa relacionada con el suscriptor
	serialNumber - 2.5.4.5	SN= <CUIT/CUIL> <Número de la Persona Juridica Publica o privada responsable de la aplicación>
	countryName - 2.5.4.6	C=AR
Clave publica del suscriptor (Subject Public Key Info)	publicKey Algorithm	RSA (1.2.840.1135.49.1.1.1)
	Publickey lenght	2048 bits
	Clave publica del suscriptor	<Clave publica del suscriptor>
Restricciones basicas	basicConstraint - 2.5.29.19	Tipo de asunto = Entidad final pathLenghtConstraint = Null
Usos de Clave	keyUsage 2.5.29.15	digitalSignature = 1 contentCommitment = 1 keyEncipherment = 0 dataEncipherment = 0 keyAgreement = 0 keyCertSign = 0 cRLSign = 1 encipherOnly = 0 decipherOnly = 0
Identificador de clave del suscriptor	subjectKey Identifier 2.5.29.14	Contiene un hash de 20 bytes del atributo clave publica del suscriptor
Puntos de distribucion de la Lista de Sellos de competencia Revocados	CRLDistributionPoints 2.5.29.31	[1] Punto de distribución: Nombre completo: Dirección: URL= http://ac.banelco.com.ar/firma-digital/crl/Banelcoac.crl
Politica de Certificacion	certificatePolicies 2.5.29.32	Politica de certificacion: OID de la Politica Unica= Informacion de la Politica de Certificacion: Id. De la Politica de Certificacion=CPS Ubicación: http://ac.banelco.com.ar/firma-digital/docs/Politica%20de%20Certificacion%20Banelco.pdf User notice = certificado emitido por un Certificador Licenciado en el marco de la Ley 25.506.
Identificador de la Clave de la Autoridad Certificante	authorityKeyIdentifier 2.5.29.35	keyIdentifier = <Identificador de la clave de la AC>
Uso extendido de clave	extendedKeyUsage 2.5.29.37	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Respuesta OCSP (1.3.6.1.5.5.7.3.9)
Nombres Alternativos del Suscriptor	subjectAltName - 2.5.29.17	Dirección de correo electrónico (campo optativo)
Informacion de acceso de la AC	authority InformationAccess 1.3.6.1.5.5.7.1.1	URL= http://ac.banelco.com.ar/ocsp
Declaracion del certificado calificado	QCStatment 1.3.6.1.5.5.7.1.3	OID=2.16.32.1.10.2.2 (claves generadas por disp. FIPS 140-2 nivel 2)
		OID=2.16.32.1.10.2.3 (claves generadas por disp. FIPS 140-2 nivel 3)

DOCUMENTOS IMPRESOS SON COPIAS NO CONTROLADAS

INFORMACIÓN PRIVADA

Prohibida su copia y distribución sin la autorización formal de PRISMA MEDIOS DE PAGO S.A.

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 48 de 59


Certificado para Autoridad de Sello de Tiempo

Certificado x.509 v3 Atributos Extensiones	Nombre del Campo y OID	Contenido
Version	Version	V1 (correspondiente a version 2)
Numero de serie	serialNumber 2.5.4.5	<Numero de serie del certificado>
Algoritmo de firma	signatureAlgorithm	sha1RSA (1.2.840.113549.1.1.5)
Nombre distintivo del emisor (issuer)	commonName - 2.5.4.3	CN=Banelco AC
	serialNumber - 2.5.4.5	SERIAL NUMBER=CUIT 30598910045
	organizationName - 2.5.4.10	O=PRISMA MEDIOS DE PAGO S.A.
	stateOrProvinceName - 2.5.4.8	S= Ciudad Autonoma de Buenos Aires
	countryName - 2.5.4.6	C=AR
Validez (desde, hasta)	notBefore	<fecha y hora de emisión UTC> yyyy/mm/dd hh:mm:ss huso-horario
	notAfter	<fecha y hora de expiracion a establecer por Banelco AC> yyyy/mm/dd hh:mm:ss huso-horario
Nombre distintivo del suscriptor (Subject DN)	commonName - 2.5.4.3	CN=Denominacion del servicio de emision de sello de competencia
	organizationName - 2.5.4.10	O=Nombre de la persona juridica publica o privada responsable del servicio
	organizationUnitName - 2.5.4.11	OU=Unidad Operativa relacionada con el suscriptor
	serialNumber - 2.5.4.5	SN= <CUIT/CUIL> <Número de la Persona Jurídica Publica o privada responsable de la aplicación>
	countryName - 2.5.4.6	C=AR
Clave publica del suscriptor (Subject Public Key Info)	publicKey Algorithm	RSA (1.2.840.1135.49.1.1.1)
	PublicKey length	4096 bits
	Clave publica del suscriptor	<Clave publica del suscriptor>
Restriciones basicas	basicConstraint - 2.5.29.19	Tipo de asunto = Entidad final pathLengthConstraint = Null
Usos de clave	keyUsage 2.5.29.15	digitalSignature = 1 contentCommitment = 1 keyEncipherment = 0 dataEncipherment = 0 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0
Identificador de clave del suscriptor	subjectKey Identifier 2.5.29.14	Contiene un hash de 20 bytes del atributo clave publica del suscriptor
Puntos de distribucion de la Lista de Sellos de tiempo Revocados	CRLDistributionPoints 2.5.29.31	[1] Punto de distribución: Nombre completo: Dirección: URL=http://ac.banelco.com.ar/firma-digital/crl/Banelcoac.crl
Politica de Certificacion	certificatePolicies 2.5.29.32	Politica de certificacion: OID de la Política Unica= Informacion de la Política de Certificacion: Id. De la Política de Certificacion=CPS Ubicación: http://ac.banelco.com.ar/firma-digital/docs/Política%20de%20Certificación%20Banelco.pdf User notice = certificado emitido por un Certificador Licenciado en el marco de la Ley 25.506.
Identificador de la Clave de la Autoridad Certificante	authorityKeyIdentifier 2.5.29.35	keyIdentifier = <Identificador de la clave de la AC>
Uso extendido de clave	extendedKeyUsage 2.5.29.37	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Certificación digital de fecha y hora (1.3.6.1.5.5.7.3.8)
Nombres Alternativos del Suscriptor	subjectAltName - 2.5.29.17	Dirección de correo electrónico (campo optativo)
Declaracion del certificado calificado	QCStatement 1.3.6.1.5.5.7.1.3	OID=2.16.32.1.10.2.2 (claves generadas por disp. FIPS 140-2 nivel 2) OID=2.16.32.1.10.2.3 (claves generadas por disp. FIPS 140-2 nivel 3)

DOCUMENTOS IMPRESOS SON COPIAS NO CONTROLADAS

INFORMACIÓN PRIVADA

Prohibida su copia y distribución sin la autorización formal de PRISMA MEDIOS DE PAGO S.A.

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 49 de 59


7.2. Perfil de la lista de certificados revocados

Las listas de certificados revocados correspondientes a la presente Política de Certificación serán emitidas conforme con lo establecido en la especificación ITU X.509 versión 2 o la que en su defecto, determine el Ente Licenciante, y cumplirán con las indicaciones establecidas en la sección “3 – Perfil de CRLs” del Anexo IV – “Perfiles de los certificados y de las Listas de Certificados Revocados”.

Certificado x.509 v3 Atributos Extensiones	Nombre del Campo y OID	Contenido
Version	Version	1 (correspondiente a version 2)
Algoritmo de firma	signatureAlgorith	sha1RSA (1.2.840.113549.1.1.5)
Nombre distintivo del emisor (issuer)	commonName - 2.5.4.3	CN=Banelco AC
	serialNumber - 2.5.4.5	SERIAL NUMBER=CUIT 30598910045
	organizationName - 2.5.4.10	O=PRISMA MEDIOS DE PAGO S.A.
	stateOrProvinceName - 2.5.4.8	S= Ciudad Autonoma de Buenos Aires
	countryName - 2.5.4.6	C=AR
Fecha efectiva Proxima Actualizacion	thisUpdate	<fecha y hora UTC> yyyy/mm/dd hh:mm:ss huso-horario
	nextUpdate	<fecha y hora UTC> yyyy/mm/dd hh:mm:ss huso-horario
Identificador de la Clave de la Autoridad Certificante	authorityKeyIdentifier 2.5.29.35	keyIdentifier = <Identificador de la clave de la AC>
Numero de CRL	CRL Number	Numero de la CRL
Puntos de Distribucion del emisor	issuingDistributionPoints 2.5.29.28	[1]Punto de distribución CRL URL= http://ac.banelco.com.ar/firma-digital/crl/Banelcoac.crl Solo contiene certificados de usuario = no Solo contiene certificados de la entidad emisora = no Lista de revocacion de Certificados Indirecta = no
Certificados Revocados (Revoked certificates)	InvalidityDate	<fecha y hora UTC>
	Serial Number	Numero de serie del certificado revocado
	ReasonCode	Motivo de la revocacion
Algoritmo de Identificacion Huella Digital		sha1 (1.3.14.3.2.26)
Version de CA		V0.0
Siguiente Publicacion de lista de revocacion		<fecha y hora UTC> yyyy/mm/dd hh:mm:ss huso-horario

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

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

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 50 de 59

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:

- El artículo 33 de la Ley N° 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 19 a 21 del Decreto N° 2628/02, reglamentario de la Ley de Firma Digital, relativos al sistema de auditoría

9. ASPECTOS GENERALES LEGALES Y ADMINISTRATIVOS.

9.1. Aranceles

El servicio prestado por PRISMA MEDIOS DE PAGO S.A. será arancelado para los solicitantes y suscriptores de certificados.


Los aranceles se establecerán y modificarán a través de circulares.

9.2. Responsabilidad Financiera

Las responsabilidades financieras se originan en lo establecido por la Ley N° 25.506 y su Decreto Reglamentario N°2628/02 y en las disposiciones de la presente Política.

9.3. Confidencialidad

Todos los datos de los solicitantes y suscriptores a los cuales se aplica esta Política Única de Certificación están amparados en la Ley N° 25.326 de Protección de los Datos Personales.

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 51 de 59

9.3.1. Información confidencial

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

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

9.3.2. Información no confidencial

La siguiente información no se considera confidencial:

- a. Contenido de los certificados y de las listas de certificados revocados.
- b. Información sobre personas físicas o jurídicas que se encuentre disponible en certificados o en directorios de acceso público.
- c. Políticas de Certificación y Manual de Procedimientos de Certificación (en sus aspectos no confidenciales).
- d. Secciones públicas de la Política de Seguridad del Certificador.
- e. Política de privacidad del Certificador.

9.3.3. Responsabilidad de los roles involucrados

Administrador PKI: Responsable de la ejecución de las tareas técnicas.

Auditor: Encargado de registrar en la bitácora todas las tareas realizadas.

Coordinador: Se encarga de guiar las tareas y actividades correspondientes descritas en este procedimiento.

Custodios: Tienen a su cargo los elementos de autenticación para la inicialización (Smart Cards) del HSM y activación de la clave de la CA.


Responsable de Acceso Físico: Es responsable de facilitar el acceso a los diferentes niveles de seguridad.

Oficial de Centro de Contacto: Es responsable de recibir la documentación enviada por el solicitante y controlar la misma.

Oficial de Registro: Verifica la documentación enviada por el solicitante.

Soporte Servidor: Soporte técnico del servidor de la CA.

Soporte de PC: Soporte técnico de la PC de la Autoridad de Registro.

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 52 de 59

9.4. Privacidad

Todos los aspectos vinculados a la privacidad de los datos personales estarán sujetos a la normativa vigente en materia de Protección de Datos Personales (Ley 25.326 y normas reglamentarias, complementarias y aclaratorias). Las consideraciones particulares se incluyen en la Política de Privacidad.

9.5. Derechos de propiedad intelectual

PRISMA MEDIOS DE PAGO S.A. es propietario exclusivo de todos los derechos de propiedad intelectual de la presente Política Única de Certificación, Manuales de Procedimientos y documentos relacionados con su rol de Autoridad Licenciada reservándose todos los derechos de autor.

Todos los contenidos del sitio web “<http://ac.banelco.com.ar/>”, ya sea archivo, material, aplicación, diseño, herramientas, código fuente y/o cualquier tipo de obra y/o idea que se encuentre protegida bajo las leyes de propiedad intelectual aplicables, será de propiedad de PRISMA MEDIOS DE PAGO S.A. Asimismo, quedan incluidas dentro del mismo reconocimiento las publicaciones, o información incorporadas al SITIO.

Queda prohibida cualquier forma de reproducción, descarga, distribución, exhibición, transmisión, retransmisión, emisión en cualquier forma, almacenamiento en cualquier forma, digitalización, puesta a disposición, traducción, adaptación, arreglo, comunicación pública y/o cualquier otro tipo de acto por el cual una persona pueda servirse directa o indirectamente, en su totalidad o en parte de cualquiera de los contenidos de las obras de PRISMA MEDIOS DE PAGO S.A. protegidas por las leyes de propiedad intelectual. Obligaciones.


9.6. Responsabilidades y garantías

Sin perjuicio de las previsiones establecidas en el capítulo IX de la Ley 25.506, y de la demás legislación vigente, la relación entre PRISMA MEDIOS DE PAGO S.A. y el titular de un certificado se registrará por el acuerdo que se celebre entre ellos.

9.7. Deslinde de la responsabilidad

Los Certificadores licenciados no son responsables en los siguientes casos determinados en el artículo 39 de la Ley 25.506:

- Por los casos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados y que no estén expresamente previstas en la ley;
- Por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización;

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 53 de 59

- Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y en los manuales de procedimientos respectivos, deba ser objeto de verificación, siempre que el certificador pueda demostrar que ha tomado todas las medidas razonables.

9.8. Limitaciones a la responsabilidad frente a terceros

PRISMA MEDIOS DE PAGO S.A. será responsable por los daños y perjuicios que provoque por los incumplimientos a lo establecido en esta Política Única de Certificación, por los errores u omisiones que presenten los certificados digitales que expide, por no revocarlos, en legal tiempo y forma cuando así correspondiere, y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles. Corresponderá a PRISMA MEDIOS DE PAGO S.A. demostrar que actuó con la debida diligencia.

El Certificador que emita un certificado digital, o lo reconozca en los términos del artículo 16 de la Ley 25.506, es responsable de los daños y perjuicios que provoque por los incumplimientos a las previsiones de la ley, por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos en legal tiempo y forma, cuando así correspondiere, y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles. Corresponderá al prestador del servicio demostrar que actuó con la debida diligencia.


9.9. Compensaciones por daños y perjuicios

Las PRISMA MEDIOS DE PAGO S.A. será responsable por los daños y perjuicios que provoque por los incumplimientos a lo establecido en esta Política de Certificación, por los errores u omisiones que presenten los certificados digitales que expide, por no revocarlos, en legal tiempo y forma cuando así correspondiere, y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles. Corresponderá a PRISMA MEDIOS DE PAGO S.A. demostrar que actuó con la debida diligencia.

El Certificador que emita un certificado digital, o lo reconozca en los términos del artículo 16 de la Ley 25.506, es responsable de los daños y perjuicios que provoque por los incumplimientos a las previsiones de la ley, por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos en legal tiempo y forma, cuando así correspondiere, y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles. Corresponderá al prestador del servicio demostrar que actuó con la debida diligencia.

9.10. Condiciones de Vigencia

La Política Única de Certificación se mantendrá vigente hasta tanto no se le realice algún cambio a la misma en pos de mejorar los procesos o se modifique la normativa dispuesta por la Autoridad de Aplicación.

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 54 de 59

9.11. Avisos personales y comunicaciones con los participantes

Los avisos y comunicaciones con los participantes serán realizados por mail firmados digitalmente y/o por las vías que la ley de firma digital u otras regulaciones impongan.

9.12. Gestión del ciclo de vida del documento

9.12.1. Procedimientos de cambio

La presente Política Única de Certificación y todos los documentos relacionados que le permiten a PRISMA MEDIOS DE PAGO S.A. operar con carácter de Certificador Licenciado son revisados periódicamente con el objetivo de detectar y corregir eventuales faltas de entendimiento y/o cambios en la normativa vigente.

Las nuevas versiones contendrán fecha de revisión y la descripción de los cambios realizados en relación a la versión anterior y se pondrán en vigencia, previa aprobación de la Autoridad de Aplicación.

El procedimiento a aplicar en la generación y aprobación de la documentación será el Procedimiento de Aprobación de Políticas, documentos y Procedimientos P-AprobacionPoliticasyNormasProcedimientos.

9.12.2. Mecanismo y plazo de publicación y notificación

La publicación se realizará en <http://ac.banelco.com.ar/firma-digital/docs/PolíticaUnicaDeCertificación.pdf> y estará disponible de forma permanente. Conjuntamente con la publicación, se notificará a los tenedores de certificado vía correo electrónico previa aprobación del documento por la Autoridad de aplicación.


La presente Política Única de Certificación, sus modificaciones en los datos relativos a su licencia, serán sometidos a aprobación por parte de la Autoridad de Aplicación conforme a lo dispuesto por la Ley 25.506 en su artículo 21 inciso q).

9.12.3. Condiciones de modificación del OID

No Aplicable

9.13. Procedimientos de resolución de conflictos

De existir algún conflicto por parte de los suscriptores de certificados en referencia a la prestación de servicios de PRISMA MEDIOS DE PAGO S.A., el/los interesado/s deberán realizar el correspondiente reclamo ante PRISMA MEDIOS DE PAGO S.A. De no ser exitoso el resultado, el interesado podrá efectuar el reclamo ante la Autoridad de Aplicación. Para el caso que decidiera optar por la vía judicial, las Partes pactan la jurisdicción de los Tribunales Comerciales con asiento en la Ciudad Autónoma de Buenos Aires, renunciando a cualquier otro fuero o jurisdicción que pudiera corresponderle.

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 55 de 59

9.14. Legislación aplicable


La legislación que respalda la interpretación, aplicación y validez de la Política Única de Certificación, es la Ley N° 25.506, el Decreto N° 2628/02, y toda otra norma complementaria dictada por la autoridad competente.

9.15. Conformidad con normas aplicables


PRISMA MEDIOS DE PAGOS S.A. en su carácter de Certificador Licenciado deberá:

Conforme artículo 21 de la ley 25.506

- a. Informar a quien solicita un certificado con carácter previo a su emisión y utilizando un medio de comunicación las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de un sistema de licenciamiento y los procedimientos, forma que garantiza su posible responsabilidad patrimonial y los efectos de la revocación de su propio certificado digital y de la licencia que le otorga el ente licenciante. Esa información deberá estar libremente accesible en lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;
- b. Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a los datos de creación de firma digital de los titulares de certificados digitales por él emitidos;
- c. Mantener el control exclusivo de sus propios datos de creación de firma digital e impedir su divulgación;
- d. Operar utilizando un sistema técnicamente confiable de acuerdo con lo que determine la autoridad de aplicación;
- e. Notificar al solicitante las medidas que está obligado a adoptar para crear firmas digitales seguras y para su verificación confiable, y las obligaciones que asume por el solo hecho de ser titular de un certificado digital;
- f. Recabar únicamente aquellos datos personales del titular del certificado digital que sean necesarios para su emisión, quedando el solicitante en libertad de proveer información adicional;
- g. Mantener la confidencialidad de toda información que no figure en el certificado digital;
- h. Poner a disposición del solicitante de un certificado digital toda la información relativa a su tramitación;
- i. Mantener la documentación respaldatoria de los certificados digitales emitidos, por diez (10) años a partir de su fecha de vencimiento o revocación;

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 56 de 59

- j. Incorporar en su Política Única de Certificación los efectos de la revocación de su propio certificado digital y/o de la licencia que le otorgara la autoridad de aplicación;
- k. Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, la lista de certificados digitales revocados, las políticas de certificación, la información relevante de los informes de la última auditoría de que hubiera sido objeto, su manual de procedimientos y toda información que determine la autoridad de aplicación;
- l. Publicar en el Boletín Oficial aquellos datos que la autoridad de aplicación determine;
- m. Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas;
- n. Informar en las políticas de certificación si los certificados digitales por él emitidos requieren la verificación de la identidad del titular;
- o. Verificar, de acuerdo con lo dispuesto en su manual de procedimientos, toda otra información que deba ser objeto de verificación, la que debe figurar en las políticas de certificación y en los certificados digitales;
- p. Solicitar inmediatamente al ente licenciante la revocación de su certificado, o informarle la revocación del mismo, cuando existieren indicios de que los datos de creación de firma digital que utiliza hubiesen sido comprometidos o cuando el uso de los procedimientos de aplicación de los datos de verificación de firma digital en él contenidos hayan dejado de ser seguros;
- q. Informar inmediatamente al ente licenciante sobre cualquier cambio en los datos relativos a su licencia;
- r. Permitir el ingreso de los funcionarios autorizados de la autoridad de aplicación, del ente licenciante o de los auditores a su local operativo, poner a su disposición toda la información necesaria y proveer la asistencia del caso;
- s. Emplear personal idóneo que tenga los conocimientos específicos, la experiencia necesaria para proveer los servicios ofrecidos y en particular, competencia en materia de gestión, conocimientos técnicos en el ámbito de la firma digital y experiencia adecuada en los procedimientos de seguridad pertinentes;
- t. Someter a aprobación del ente licenciante el manual de procedimientos, el plan de seguridad y el de cese de actividades, así como el detalle de los componentes técnicos a utilizar;
- u. Constituir domicilio legal en la República Argentina;
- v. Disponer de recursos humanos y tecnológicos suficientes para operar de acuerdo a las exigencias establecidas en la presente ley y su reglamentación;

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 57 de 59

w. Cumplir con toda otra obligación emergente de su calidad de titular de la licencia adjudicada por el ente licenciante.

Conforme artículo 34 de Decreto 2628/02:

a. Comprobar por sí o por medio de una Autoridad de Registro que actúe en nombre y por cuenta suya, la identidad y cualquier otro dato de los solicitantes considerado relevante para los procedimientos de verificación de identidad previos a la emisión del certificado digital, según la Política Única de Certificación bajo la cual se solicita.

b. Mantener a disposición permanente del público las Políticas de Certificación y el Manual de Procedimientos correspondiente.

c. Cumplir cabalmente con las políticas de certificación acordadas con el titular y con su Manual de Procedimientos.

d. Garantizar la prestación establecida según los niveles definidos en el acuerdo de servicios pactados con sus usuarios, relativo a los servicios para los cuales solicitó el licenciamiento.

e. Informar al solicitante de un certificado digital, en un lenguaje claro y accesible, en idioma nacional, respecto de las características del certificado solicitado, las limitaciones a la responsabilidad, si las hubiere, los precios de los servicios de certificación, uso, administración y otros asociados, incluyendo cargos adicionales y formas de pago, los niveles de servicio al proveer, las obligaciones que el suscriptor asume como usuario del servicio de certificación, su domicilio en la República Argentina y los medios a los que el suscriptor puede acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema o presentar sus reclamos.

f. Disponer de un servicio de atención a titulares y terceros, que permita evacuar las consultas y la pronta solicitud de revocación de certificados.


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

h. Mantener actualizados los repositorios de certificados revocados por el período establecido por el Ente Administrador.

i. Abstenerse de generar, exigir, tomar conocimiento o acceder bajo ninguna circunstancia a la clave privada del suscriptor.

j. Informar al Ente Administrador de modo inmediato la ocurrencia de cualquier evento que comprometa la correcta prestación del servicio.

k. Respetar el derecho del titular del certificado digital a no recibir publicidad de ningún tipo por su intermedio, salvo consentimiento expreso de éste.

	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 58 de 59

- l. Publicar en el Boletín Oficial durante UN (1) día, el certificado de clave pública correspondiente a la política para la cual obtuvo licenciamiento;
- m. Cumplir las normas y recaudos establecidos para la protección de datos personales.
- n. En los casos de revocación de certificados contemplados en el apartado 3 del inciso e) del artículo 19 de la Ley N° 25.506, deberá sustituir en forma gratuita aquel certificado digital que ha dejado de ser seguro por otro que sí cumpla con estos requisitos.
- o. El Ente Administrador deberá establecer el proceso de reemplazo de certificados en estos casos. En los casos en los que un certificado digital haya dejado de ser seguro por razones atribuibles a su titular, el certificador licenciado no estará obligado a sustituir el certificado digital.
- p. Enviar periódicamente al Ente Administrador, informes de estado de operaciones con carácter de declaración jurada.
- q. Contar con personal idóneo y confiable, con antecedentes profesionales acordes a la función desempeñada.
- r. Responder a los pedidos de informes por parte de un tercero respecto de la validez y alcance de un certificado digital emitido por él.

Conforme artículo 36 del Decreto N° 2628/02:

Responsabilidad del certificador licenciado respecto de la Autoridad de Registro:

Una Autoridad de Registro puede constituirse como una única unidad o con varias unidades dependientes jerárquicamente entre sí, pudiendo, delegar su operatoria en otras autoridades de registro, siempre que medie la aprobación del Certificador Licenciado. El Certificador, Licenciado es responsable con los alcances establecidos en la Ley N° 25.506, aún en el caso de que delegue parte de su operatoria en Autoridades de Registro, sin perjuicio del derecho del certificador de reclamar a la Autoridad de Registro las indemnizaciones por los daños y perjuicios que aquél sufriera como consecuencia de los actos y/u omisiones de ésta.

Otras obligaciones del certificador:

- a. Notificar a sus suscriptores sobre cualquier acontecimiento que pudiera ocasionar el compromiso de su clave privada y la generación de un nuevo par de claves.
- b. Notificar a sus suscriptores y al Ente Licenciante acerca del cese de sus actividades.
- c. Emitir y distribuir los certificados a sus suscriptores, informándolos acerca de dicha emisión.

PRISMA MEDIOS DE PAGO	MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN	VERSIÓN: 1.0
		EMITIDO: Julio 2015
		MODIFICADO: Mayo 2017
		Página 59 de 59

Cumplir con las obligaciones establecidas en la Decisión Administrativa N° 927/2014 y sus respectivos Anexos.”.

9.16. Cláusulas adicionales

No Aplicable

9.17. Otras cuestiones generales

Complementariamente a las normas aplicables específicas de la Ley de Firma Digital, se aplicará el Código Civil, la Ley N° 25.326 de Protección de Datos Personales, y otras normas concordantes dictadas por la autoridad competente.